Публичная методичка V 3.0 WWH-CLUB 2019

Wwh-club стабильное зеркало.

https://wwh-club.net

https://wwh-club.us

TOR

wwhclublci77vnbi.onion

www.wwhclubl4tefzrzf.onion

Официальный Telegram канал форума.

https://t.me/WWHCLUB888

Center стабильное зеркало.

https://center-club.pw

TOR

center222xdihudu.onion

---- RUS ----

JOKER's STASH - Миллионы of CC+CVV, TR2 DUMPS, SSN+DOB.

Крупнейший даркнет маркетплейс. Ежедневные обновления!

JSTASH BLOCKCHAIN-DNS LINK: http://jstash.bazar/ (нужно установить Blockchain DNS плагин для браузера: https://blockchain-dns.info)

только этот линк! у нас нет других линков! любые другие линки - фейки!

Не знаете как открывать .BAZAR домены? ЛЕГКО!

Установите один из этих плагинов для вашего браузера (Chrome,Firefox):

Blockchain DNS: https://blockchain-dns.info/ (лучший выбор)

PeerName: https://peername.com/browser-extension/

Внимание! Не нужно ставить все плагины сразу - они будут конфликтовать друг с другом, установите только какой-то один!

Имейте ввиду, что если введете в адресную строку браузера просто "jstash.bazar" - браузер запустит операцию поиска в поисковике

Ввводите линк одним из следующих способов:

1. Со слэшем на конце, пример: "jstash.bazar/".

2. Домен с указанием протокола, пример: "http://jstash.bazar".

Если у Вас неподдерживаемый плагинами браузер или другое устройство (iOS,Android)

Вы можете использова DNS-сервера от проекта OpenNIC https://www.opennic.org/, которые поддерживают .bazar домены

Просто пропишите в настройках своего соединения один из dns серверо от OpenNIC

---- ENG ----

JOKER's STASH - Millions of CC+CVV, DUMPS, SSN+DOB.

The BIGGEST DarkNet Marketplace. Every day updates!

JSTASH LINK: http://jstash.bazar/ <= ONLY THIS LINK IS LEGIT (Blockchain DNS browser plugin required)

we don't have other links, all other links are fake/scam/clone/ripper sites !!

Don't know how to browse .BAZAR links? It's very simple!

Install one of the following browser Extension/Addon for .BAZAR blockchain-based domains surfing:

Blockchain DNS (best choice): https://blockchain-dns.info/

PeerName: https://peername.com/browser-extension/

friGate CDN: https://fri-gate.org/

Attention! Do not install them all together because they may conflict with each other, install only one of them.

If one particular plugin does not work well - try another plugin.

Keep in mind that the browser may trigger the search operation if you type "jstash.bazar" in the address bar.

There are two ways to fix that:

1. Type the domain with a trailing slash, example: "jstash.bazar/".

2. Type the domain with the protocol, example: "http://jstash.bazar".

Оглавление

Шифрование часть 1

лектор: Всех приветствую сегодняшняя лекция будет посвящена шифрованию, так что разберем все основные аспекты, а так же поговорим о шифрование в целом.

лектор: Я бы хотел обсудить и разобрать фундаментальные основы шифрования, мы изучим симметричное и асимметричное шифрование, так же слегка затронем такие понятия как: хеши, SSL, TLS, сертификаты, перехват данных при помощи утилиты SSLStrip и слабости, связанные с шифрованием. Это фундаментальные знания, необходимые для выбора подходящих средств обеспечения безопасности с целью снижения рисков.

лектор: Многие из вас если копнуть глубже вообще не имеют ни малейшего представления о своей безопасности и конфиденциальности. Они лишь только слепо могут возражать, основываясь на мнениях других людей.

лектор: Но когда речь идет о безопасности и о вашей конфиденциальности. Только Вы можете выступать гарантом своей безопасности, и никто другой.

лектор: Но наверняка уже некоторые смышленые ребята зададутся вопросом: "А как я могу выступать гарантом своей безопасности если я ничего не знаю о ней?"

лектор: Один из принципов который вы должны освоить - это принцип планирования. Все ваши действия должны быть четко спланированы.

лектор: Но для того чтобы что-то спланировать необходимо разбираться в данной области, да и ответить себе на вопросы, а что это такое и для чего это надо?!

лектор: В целом, шифрование состоит из 2-ух составляющих - зашифровывание и расшифровывание.

лектор: С помощью шифрования обеспечиваются 3-и состояния безопасности информации:

лектор: 2. Целостность – шифрование используется для предотвращения изменения информации при передаче или хранении.

лектор: 1. Конфиденциальность – шифрование используется для скрытия информации от не авторизованных пользователей при передаче или при хранении.

лектор: 2. Целостность – шифрование используется для предотвращения изменения информации при передаче или хранении.

лектор: 3. Идентифицируемость – шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

лектор: Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания).

лектор: КСТАТИ: Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не

имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию.

лектор: Давайте представим закрытою дверь на замок, для того чтобы узнать, что находится по ту сторону двери нам необходимо открыть ее ключом от этого замка.

лектор: Так и в случае шифрования данных. Только вместо замка у нас выступает алгоритм шифрования данных, а вместо ключа секретный ключ (пароль) для дешифровки данных.

лектор: Цели шифрования

лектор: Основная цель шифрования применяется для хранения важной информации в зашифрованном виде.

лектор: Вообще шифрование используется для хранение важной информации в ненадежных источниках и передачи ее по незащищенным каналам связи. Такая передача данных представляет из себя 2-а взаимно обратных процесса:

лектор: 1. Перед отправлением данных по линии связи или перед помещением на хранение они подвергаются зашифровыванию.

лектор: 2. Для восстановления исходных данных из зашифрованных к ним применяется процедура расшифровывания.

лектор: Шифрование изначально использовалось только для передачи конфиденциальной информации. Однако впоследствии шифровать информацию начали с целью ее хранения в ненадежных источниках. Шифрование информации с целью ее хранения применяется и сейчас, это

позволяет избежать необходимости в физическом защищенном хранилище (usb, ssd диски).

лектор: КСТАТИ: Примеры мы разберем в методах шифрования и уже наглядно увидим всю суть, так что не переживайте по этому поводу. (завтра)

лектор: Какие имеются методы шифрования:

лектор: 1. Симметричное шифрование – использует один и тот же ключ и для зашифровывания, и для расшифровывания.

лектор: 2. Асимметричное шифрование – использует 2-а разных ключа: один для зашифровывания (который также называется открытым), другой для расшифровывания (называется закрытым) или наоборот.

лектор: Эти методы решают определенные задачи и обладают как достоинствами, так и недостатками. Конкретный выбор применяемого метода зависит от целей, с которыми информация подвергается шифрованию.

лектор: Для того чтобы сделать правильный выбор в подходе по шифрованию, какой метод шифрования где применять, и ответить на другие сопутствующие вопросы, Вам будет необходимо понимать, что такое шифрование, как я и говорил ранее.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fpuu.sh%2FxB148%2Fa3d3261694.png&hash=abf5fe5a4fa60b849a715122c39feccb

лектор: Исходя из инфографики выше (ссылка), мы можем наглядно разобрать принцип работы шифрования

лектор: — Отправитель отправляет зашифрованное сообщение: "Привет, Marfa"

лектор: — Злоумышленники перехватывают данное сообщение, но так как у них нет ключа для дешифровки они лишь видят набор символов: "%#&$!"

лектор: — Получатель, имея ключ дешифровки, с легкостью может прочитать сообщение которое отправил отправитель в зашифрованном виде, и он уже видит текст отправителя в первозданном виде: "Привет, Marfa"

лектор: Не будет преувеличением сказать, что шифрование – это самый лучший инструмент, который только есть в нашем арсенале для защиты от хакеров и слежки.

лектор: По определениям кстати

лектор: Шифрование – это метод преобразования данных, пригодных для чтения человеком, они называются незашифрованным текстом, в форму, которую человек не сможет прочитать, и это называется зашифрованным текстом. Это позволяет хранить или передавать данные в нечитабельном виде, за счет чего они остаются конфиденциальными и приватными.

лектор: Дешифрование – это метод преобразования зашифрованного текста обратно в читабельный человеку текст. Если вы осуществите простой поиск в Google, то увидите здесь надпись HTTPS и наличие зеленой иконки замка, это означает, что все содержимое веб-страниц

недоступно для чтения людям, которые отслеживают передачу данных по сети.

лектор: Проще говоря или симметричное шифрование (метод шифрования имеется ввиду 1 из 2х та сказать)

лектор: есть два основных компонента шифрования:

лектор: 1. Алгоритм шифрования – известен публично и многие, многие люди тщательно его изучили в попытке определить, является ли алгоритм сильным.

лектор: 2. Секретный ключ – можете представить, что секретный ключ – это пароль и он должен держаться в тайне.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FABaWF56.jpg&hash=ffa46fc4208497ebfd0e9081d1ae1523

лектор: Алгоритм можно представить, как замок, а секретный ключ – это ключ к этому замку (см. На инфографике ссылка выше).

лектор: В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ.

лектор: Исходя из инфографики выше давайте рассмотрим пример, я хочу отправить Марфе какой-то файл, но я не хочу, чтоб какие-то 3-и лица могли его просмотреть. Для наглядности и простоты использования я решил зашифровать данный файл программой 7-Zip.

лектор: По этой же аналогичной структуре шифруются сектора/диски в VeraCrypt, TrueCrypt, так же возьмем для примера.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fpuu.sh%2Fxy5C8%2F4a79168b67.png&hash=ee54b45c2ccf5e9b2de6bc486895909d

лектор: Давайте разберем скриншот выше:

лектор: 1. Алгоритм шифрования – это математический процесс преобразования информации в строку данных, которые выглядят как случайный набор символов и букв.

лектор: 2. Хэш-функция – это преобразования входных данных, в нашем случае wwh-club в выходную битовую строку. Задача функции обеспечивать целостность и позволять обнаружить непреднамеренные модификации.

лектор: 3. AES-256 – указывает какой алгоритм используется (AES) и какой размер блока (256), как мы видим в 7-Zip нет возможности детальной настройки, нежели как в VeraCrypt.

лектор: 4. При помощи введенного пароля будет сгенерирован ваш ключ для выбранного алгоритма шифрования (в нашем случае AES-256), для дешифровки вам надо будет указать алгоритм дешифровки если имеется и ввести пароль в нашем случае опять wwh-club

лектор: На выходе мы получаем зашифрованный архив, который для распаковки и получении информации, что

находится внутри необходимо ввести ключ дешифровки, говоря простым языком пароль.

лектор: Вы могли заметить, что для зашифровки был использован симметричный алгоритм блочного шифрования – Advanced Encryption Standard (AES).

лектор: В данном алгоритме используется только 1-н ключ, ключ создается при помощи нашего пароля (см. 4 пункт для наглядности преобразования)

лектор: Так же Вы можете выбрать какой размер блока будет использован 128 / 256 / 512 / 1024 бит, в нашем случае были лишь варианты 256 бит и 512 бит.

лектор: КСТАТИ: Представьте себе дверь и множество замков на ней. У вас займет много времени, чтобы открыть или закрыть эту дверь. Также и с алгоритмами, чем выше битрейт, тем сильнее алгоритм, но тем медленнее он шифрует и дешифрует, можете считать это стойкостью алгоритма.

лектор: 256 / 512 бит – это также и объем ключевого пространства, то есть цифра, обозначающая суммарное количество возможных различных ключей, которые вы можете получить при помощи этого алгоритма шифрования.

лектор: КСТАТИ: Для взлома симметричного шифра требуется перебрать 2^N комбинаций, где N длина ключа.

лектор: Для взлома симметричного шифрования с длиной ключа 256 бит можно создать следующее количество комбинаций, то есть возможных ключей: 2^256 = 1.1579209e+77 или если разложить 1.1579209e * 10^77 при

расчете получается следующее число возможных вариаций (это 78-разрядное число).

лектор: 2^256 = 115792089237316195423570985008687907853269984665640564039457584007913129639936

лектор: Если что можете проверить сами это число тут http://kalkulyatoronlajn.ru/

лектор: Таким образом, для всех, кто сомневается в безопасности шансов столкновения 2 ^ 256, есть число: есть вероятность того, что столкновение будет иметь 1-н из более чем 1.1579209e*10^7= 78-разрядному числу (то число которое выше)

лектор: Все это означает, что ключ крайне сложно подобрать, даже при помощи очень мощных компьютеров, но при условии, что вы использовали длинный и рандомный пароль при генерации ключа. (про пароли подробно разберем завтра)

лектор: КСТАТИ: Про пароль поговорим отдельно, какой использовать и т.д. Вместе с програмами и почему. Чтобы не засорять вам мозг не нужной информацией на данном этапе, так что ввнезабивайте голову, сейчас обо всем поговорим..

лектор: Люди и правительства постоянно пытаются взломать алгоритмы шифрования. В этой статье я дам вам список алгоритмов, которые хороши, а которые нет, какие из них поддаются взлому, а какие на сегодняшний день невозможно взломать.

лектор: Алгоритмы симметричного шифрования

лектор: 1. Data Encryption Standard (DES) – алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 бита.

лектор: 2. Triple-DES (3DES) – симметричный блочный шифр, созданный в 1978 году на основе алгоритма DES с целью устранения главного недостатка последнего малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа.

лектор: 3. Blowfish – криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа

лектор: 4. RC4 – потоковый шифр, широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритмах обеспечения безопасности беспроводных сетей WEP и WPA).

лектор: 5. RC5 – это блочный шифр, разработанный Роном Ривестом из компании RSA Security Inc. с переменным количеством раундов, длиной блока и длиной ключа. Это расширяет сферу использования и упрощает переход на более сильный вариант алгоритма.

лектор: 6. RC6 – симметричный блочный криптографический алгоритм, производный от алгоритма RC5.

лектор: 7. Advanced Encryption Standard (AES) – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES.

лектор: Симметричные алгоритмы используются в большинстве систем шифрования, которые Вы используете ежедневно: HTTPS, Полное шифрование диска (TrueCrypt, VeraCrypt и другие), Шифрование файлов (7-Zip, WinZip и другие), Tor, VPN. Практически везде используется симметричное шифрование

лектор: КСТАТИ: Advanced Encryption Standard (AES) – это общепринятый стандарт симметричного шифрования. Для максимальной защиты используйте AES-256 где это возможно,. AES быстрый и на сегодняшний день его невозможно взломать (При условии что пароль у вас сильный, про это будет ниже).

лектор: 2-й тип или метод кому как удобнее

лектор: Асимметричное шифрование

лектор: Очень умные люди изобрели это шифрование с использованием открытого и закрытого ключей и алгоритмы, основанные на сложности определенных математических задач. Я не буду обращаться в математические детали, потому что их понимание не обязательно для вашей защиты.

лектор: Для правильного выбора средств защиты вам лишь достаточно иметь базовое понимание алгоритмов и стойкости алгоритмов, а также криптографических систем, которые вы собираетесь использовать.

лектор: Как мы знаем в симметричном методе шифрование используется 1-н секретный ключ, тогда как в асимметричных методах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания другой (секретный). Эти ключи различны и не могут быть получены один из другого.

лектор: Давайте сразу же закрепим данный материал

лектор: Симметричный метод шифрования – 1-н ключ, использует один и тот же ключ и для зашифровывания, и для расшифровывания.

лектор: Асимметричный метод шифрования – 2-а ключа открытый (публичный от англ. Public) и закрытый (приватный от англ. Private)

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fpuu.sh%2Fxy5C8%2F4a79168b67.png&hash=ee54b45c2ccf5e9b2de6bc486895909d

лектор: Итак, у нас есть файл для Марфы, который если Вы помните в разделе симметричного шифрования (см. Скриншот выше) был зашифрован с помощью программы 7-Zip с использованием алгоритма шифрования AES-256 и

сильного пароля, но как нам доставить пароль Марфе, чтобы она смогла дешифровать файл?

лектор: КСТАТИ: Самый лучший способ, что-либо передать и быть уверенным в доставке информации указанному адресату это лично в руки.

лектор: Но это не очень хорошая затея, так как мы можем попросту не знать где находится адресат, либо он может находится на столько далеко, что доставить что-либо "лично в руки" становится проблематичным, а быть может нам попросту нужна анонимность.

лектор: Асимметричные алгоритмы (с применением открытого и закрытого ключа):

лектор: 1. RSA (Rivest-Shamir-Adleman) – криптографический алгоритм с открытым ключом. Данный алгоритм очень популярен, 1-н из самых распространенных асимметричных алгоритмов из всех, что вы увидите, и я покажу вам, где вообще их искать и как использовать.

лектор: Определение: Криптостойкость этого алгоритма основана на сложности факторизации или разложения больших чисел в произведение простых множителей.

лектор: 2. ECC (Elliptic curve cryptosystem) – распространенный и приобретающий популярность алгоритм. Эта криптографическая система на основе эллиптических кривых, или ECC. Стойкость этого алгоритма опирается на задачу вычисления дискретных логарифмов на эллиптических кривых.

лектор: 3. DH (Diffie-Hellman) – Его стойкость основана на задаче дискретного логарифмирования в конечном поле. Диффи-Хеллман становится все более популярным, потому что у него есть свойство под названием "прямая секретность", мы обсудим его позже.

лектор: 4. ElGamal – схема Эль-Гамаля, и криптостойкость этого алгоритма также основана на сложности задачи дискретного логарифмирования в конечном поле.

лектор: ОПРЕДЕЛЕНИЕ: Криптостойкость (способность криптографического алгоритма противостоять криптоанализу) – этого алгоритма основана на сложности факторизации или разложения больших чисел произведения простых множителей

лектор: Скосил с определением сорян

лектор: Эти асимметричные алгоритмы помогают решать проблему обмена или согласования ключей, а также позволяют создавать так называемые электронные цифровые подписи. Так что потенциально мы можем использовать открытый и закрытый ключи, чтобы отправить Марфе наш секретный ключ защищенным образом, без возможности перехвата его содержимого.

лектор: КСТАТИ: Еще раз отмечу, в алгоритмах с применением открытых и закрытых ключей используются два ключа, а не один, как в симметричном шифровании.

лектор: Разница в том, что в асимметричном шифровании есть открытый ключ, который создается, чтобы быть известным для любого человека, то есть это публичный

ключ, и есть закрытый ключ, который должен всегда храниться в секрете и быть приватным. Эти ключи математически связаны и оба они генерируются в одно и то же время. Они должны генерироваться одновременно, потому что они математически связаны друг с другом.

лектор: Любой веб-сайт, использующий HTTPS, имеет открытый и закрытый ключи, которые используются для обмена симметричным сеансовым ключом, чтобы отправлять вам зашифрованные данные. Это немного похоже на Zip-файл, который мы видели. Они используют эти открытые/закрытые ключи и затем им нужно отправить другой ключ, типа ключа, который мы используем для Zip-файла, с целью осуществить шифрование (end-to-end разберем позже)

лектор: ЗАПОМНИТЕ КАК ОТЧЕ НАШ И ПОЙМИТЕ

лектор: Если Вы шифруете при помощи закрытого ключа, Вам нужен открытый ключ для дешифровки

лектор: Если Вы шифруете при помощи открытого ключа, Вам нужен закрытый ключ для дешифровки

лектор: В асимметричном шифровании, если сообщение зашифровано 1-им ключом, то необходим 2-ой ключ для дешифровки этого сообщения. Если вы шифруете при помощи закрытого ключа, то вам нужен открытый ключ для дешифровки.

лектор: Если вы шифруете при помощи открытого ключа, то для дешифровки вам нужен закрытый ключ. Невозможно зашифровать и дешифровать одним и тем же ключом, и это

крайне важно. Для шифрования или дешифрования вам всегда нужны взаимосвязанные ключи.

лектор: Но зачем шифровать при помощи открытого или закрытого ключа? Какая разница? Какой смысл в их использовании? Почему бы не использовать только один из них?

лектор: Специально для вас я нарисовал инфографику чтобы просто и легко объяснить всю полезность этих ключей и как их можно использовать.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FnohXXk5.jpg&hash=8833da0c52477fa5a6ba9e9d5904854a

лектор: КСТАТИ: В этой инфографике рассматриваются 2-а направления шифрования, сначала мы разберем с зелеными стрелочками, а потом с красными.

лектор: 1 способ (зеленые стрелочки)

лектор: На способе с зелеными стрелочками показано, что отправитель шифрует при помощи открытого (публичного) ключа получателя, Марфы, то это означает, что вам нужны анонимность и конфиденциальность, чтобы никто не смог прочитать сообщение, кроме получателя.

лектор: ВАЖНО: Допустим Вы зашифровываете файл при помощи открытого ключа получателя. Сообщение может быть расшифровано только человеком, обладающим подходящим закрытым ключом, то есть закрытым ключом Марфы.

лектор: Так как мы знаем, что данные ключи взаимосвязаны, одним шифруем другим дешифруем и ни как иначе.

лектор: Получатель (Марфа) не может идентифицировать отправителя этого сообщения. Так как открытый (публичный) ключ на то и открытый, что он выкладывается в обычно в общий доступ, и любой может использовать открытый (публичный) ключ Марфы для шифрования.

лектор: Когда отправитель шифрует при помощи открытого ключа получателя, сообщение конфиденциально и оно может быть прочитано лишь получателем, у которого есть закрытый ключ для дешифрования сообщения, но как я и говорил ранее возможности идентификации отправителя нет, при условии конечно если Вы сами не пришлете там каких либо данных для последующей Вас идентификации

лектор: 2 способ (красные стрелочки)

лектор: Все выше сказанное выливается во 2-ой способ использования открытый (публичных) и закрытых (приватных) ключей.

лектор: Если вы шифруете своим собственным закрытым ключом, то это означает, что вы заинтересованы в аутентификации. В этом случае вам важно, чтобы получатель знал, что именно вы отправили зашифрованное сообщение. Для этого вы шифруете при помощи своего закрытого ключа. Это наделяет уверенностью получателя, что единственным человеком, который мог зашифровать эти данные, является человек, который владеет этим закрытым ключом, Вашим закрытым ключом.

лектор: ПРИМЕР: Вы создатель какого-то программного обеспечения, но правительство негодует и всячески препятствует вашей деятельности. Смоделируем такую ситуацию:

лектор: Допустим, я хочу скачать это программное обеспечение, здесь указан хеш-сумма этого файла, однако, если веб-сайт скомпрометирован, то это означает, что злоумышленники могли подменить данный файл для загрузки и добавить к нему троян или что-то для слежки за мной, и они также могли подменить и контрольную сумму.

лектор: итак, этот хеш ничего не значит. Он не поможет обнаружить преднамеренную модификацию файла. Нам нужно что-то еще для удостоверения, что данный сайт это в действительности официальный сайт программного обеспечения.

лектор: И здесь мы подходим к сертификатам, цифровым подписям и другим средствам. Все эти документы, получаются в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость)

лектор: Об этом поговорим позже..

лектор: Думаю завтра

лектор: Шифрование данных с помощью закрытого ключа отправителя называется форматом открытого сообщения, потому что любой человек, обладающий копией соответствующего открытого (публичного) ключа, может дешифровать сообщение.

лектор: Можете считать это, как если бы вы официально поместили что-либо в Интернет для публичного доступа, и поскольку вы зашифровали его своим закрытым ключом, любой может убедиться, что именно вы, оставили это сообщение. Конфиденциальность или анонимность в данном случае не обеспечивается, но обеспечивается аутентификация отправителя, то есть вас.

лектор: Далее. Когда различные технологии шифрования используются в комбинации, типа тех, о которых мы уже говорили ранее, поскольку они все могут быть использованы в комбинации и не могут использоваться по отдельности, то они называются криптографической системой, и криптосистемы могут обеспечить вас целым рядом средств обеспечения безопасности.

лектор: Криптографическая система могут обеспечить вас целым рядом средств безопасности. В числе этих средств:

лектор: 1. Конфиденциальность – необходимость предотвращения утечки (разглашения) какой-либо информации.

лектор: 2. Аутентификация – процедура проверки подлинности, то есть мы знаем что Марфа это реально Марфа и ни кто другой.

лектор: 3. Предотвращение отказа – что означает что если вы отправили шифрованное сообщение то позже вы не сможете начать отрицать этот факт

лектор: 4. Достоверность – подлинность того что сообщение не было модифицировано каким либо образом

лектор: Примерами криптосистем являются любые вещи, которые используют технологию шифрования, это: PGP, BitLocker, TrueCrypt, VeraCrypt, TLS, даже BitTorrent, и даже 7-Zip который мы использовали для шифрования файла в симметричном способе шифрования.

лектор: НАПРИМЕР: Для того чтобы мы могли послать наш файл Марфе, мы можем использовать открытый ключ Марфы для шифрования файлов, или для передачи чего угодно в зашифрованном виде.

лектор: Но для начала, конечно, нам потребуется открытый ключ Марфы, нам достаточно получить его 1-н раз неким защищенным способом, это важно, и после этого мы сможем всегда посылать зашифрованные сообщения, доступные для чтения исключительно Марфе.

лектор: PGP – Это система которую мы можем использовать для этих целей, она использует технологию шифрования сообщений, файлов и другой информации, представленной в электронном виде

лектор: ОПРЕДЕЛЕНИЕ: PGP (Pretty Good Privacy) – компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации,

представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.

лектор: Для этих целей мы можем использовать Jabber + PGP или OTR, рекомендую ознакомиться с этой статьей https://wwh-club.net/threads/101833/, особое внимание уделить на пункты 7 и 8.

лектор: Запиши его для домашнего задания

лектор: кстати на счет ип кто использует WWH.SO

лектор: там будет в статье

лектор: или в общем другие сервера они использует сдн

лектор: то есть получается что ип адрес ресурса скрыт за СДН то естьл вы отправляете запрос

лектор: он проходит такую цепочку

лектор: ВЫ - СДН - ИП сервера

лектор: то есть сдн посредником является и сайт завязан когда с доменом работаете он будет выдавать ип сдн

лектор: и коннекта не будет с жабой

лектор: Но давайте вернемся к шифрованию. Когда речь заходит о криптографии с использованием открытых и закрытых ключей или асимметричном шифровании, есть как сильные, так и слабые стороны.

лектор: Асимметричное шифрование – открытые и закрытые ключи:

лектор: 1. Лучшее распределение ключей так как Марфа может поместить свой открытый ключ прямо себе в подпись и любой человек будет иметь возможность посылать ей зашифрованные сообщения или данные, которые сможет прочитать только она.

лектор: 2. Масштабируемость — если вы используете симметричные ключи и желаете отправить ваш файл Марфе и, скажем, еще 10-ти людям, вам придется передать свой пароль 10 раз. Это совершенно не масштабируемо. Асимметричные алгоритмы имеют более хорошую масштабируемость, нежели чем симметричные системы.

лектор: 3. Аутентификация, предотвращение отказа — это означает, если вы отправили шифрованное сообщение, то позже вы не сможете начать отрицать этот факт. Так как оно было зашифровано личным приватным ключом, вашим приватным ключом

лектор: 4. Медленные — если вы посмотрите на длину сообщения в битах (см. скриншот ниже) после работы асимметричных алгоритмов, то заметите, что она гораздо больше, чем у алгоритмов шифрования с симметричными ключами, и это свидетельство того, насколько они медленнее.

лектор: 5. Математически-интенсивные — Чем больше длинна в битах, тем больше число математических операций, а, следовательно, большая нагрузка на систему.

лектор: Симметричное шифрование – закрытый ключ:

лектор: 1. Быстрые — если вы посмотрите на длину сообщения в битах (см. скриншот ниже) после работы симметричных алгоритмов, то заметите, что она гораздо меньше, чем у алгоритмов шифрования с асимметричными ключами, и это свидетельство того, насколько они быстрее.

лектор: 2. Надежные — Посмотрите на вышеописанное по поводу AES-256 где был с расчетом числа 2^256 и убедитесь сами, а ведь есть и 384 / 512 /1024 и более..

лектор: Для наглядной демонстрации посмотрите на этот скриншот ниже

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FYTXphkH.jpg&hash=0a564677814410e84094b1eb3a6a9ea9

лектор: Для того чтобы закрепить материал, вернемся к аналогии с количеством замков на двери. С открытыми и закрытыми ключами на двери висит много-много замков, так что шифрование и дешифрование занимает гораздо больше времени. Для центрального процессора это большой объем математических операций, вот почему существуют гибридные системы, или гибридные криптографические системы.

лектор: Открытые и закрытые ключи используются для обмена ключами согласования, и мы используем симметричные алгоритмы типа AES для шифрования данных, тем самым извлекая максимальную выгоду. HTTPS, использующий протоколы TLS и SSL, является примером подобного типа гибридных систем, как и PGP.

Шифрование часть 2

лектор: Давайте теперь более детально поговорим из чего состоит шифрование в целом краткий вводный курс мы прошли давайте углубимся что же такое сам хеш и т.д.

лектор: Хеширование

лектор: Хеширование это преобразование массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины, выполняемое определенным алгоритмом. Функция, реализующая алгоритм и выполняющая преобразование, называется «хеш-функцией» или «функцией свёртки». Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения».

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2F8rkxDhV.png&hash=d7a1903626c3d3d48ad215ff33e99df0

лектор: Давайте посмотрим на изображение, видим здесь:

лектор: 1. Входные данные

лектор: 2. Алгоритм или функцию хеширования

лектор: 3. Выходные данные Результирующие выходные данные, которые всегда имеют фиксированный размер.

лектор: Хеш-функция принимает входные данные любого размера. Это может быть e-mail, файл, слово, в нашем

случае это фраза "Привет, wwh-club", и происходит конвертация данных при помощи хеш-функции в следующий вид

лектор: 732b01dfbfc088bf6e958b0d2d6f1482a3c35c7437b798fdeb6e77c78d84ccb1

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2F1pMa79c.gif&hash=9a4708baee4fc3229a9c48825b36a166

лектор: Для лучшего усвоения и разбора материала, давайте отойдем от сухого текста и сделаем наглядную демонстрацию

лектор: Как мы можем видеть из анимированной гифки выше, наши входные данные преобразуются с помощью алгоритма хеширования, а именно SHA-256, в выходные данные фиксированного размера.

лектор: Пояснение: Как мы видим, что при изменение наших входных данных путем добавления " =) " наши выходные данные имеют другой вид, так как в битовом эквиваленте множитель поменялся. Следовательно и само значение выходных данных изменилось. При возвращение к исходным входным данным значение опять имело изначальный вид.

лектор: Вы можете представить это как пример:

лектор: 1. "Привет, wwh-club" = 5

лектор: 2. "Привет, wwh-club =)" = 7

лектор: 3. "Привет, wwh-club" = 5

лектор: Сам алгоритм хеширования это второй произвольный множитель, пусть будет 2, тогда:

лектор: 1. 2*5=10

лектор: 2. 2*7=14

лектор: 3. 2*5=10

лектор: Так и с хешем, только алгоритм хеширования имеет более сложные математические операции, нежели привел я, если вам нужна конкретная формула преобразования использующаяся в алгоритме, смотрите в Wikipedia.

лектор: Важная особенность хеш-функции вы не можете конвертировать из хеша обратно в изначальные входные данные. Это односторонняя хеш-функция и для нее не нужны ключи.

лектор: Для примера опять смотрим на нашу гифку, которую я давал ранее

лектор: Привет, wwh-club > SHA-256 > 732b01dfbfc088bf6e958b0d2d6f1482a3c35c7437b798fdeb6e77c78d84ccb1

лектор: Как мы видим, мы использовали только входные данные, не какие ключи при этом мы не задействовали, и затем получили результирующие выходные данные, которые всегда имеют фиксированный размер в зависимости от вида функции, которую вы используете.

лектор: Это обеспечивает целостность и позволяет обнаружить непреднамеренные модификации. Это не

обеспечивает конфиденциальность, аутентификацию, это не позволяет определить наличие преднамеренной модификации.

лектор: КСТАТИ: Есть много примеров хеш-функций: MD2, MD4, MD5, HAVAL, SHA, SHA-1, SHA-256, SHA-384, SHA-512, Tiger и так далее.

лектор: ЧТО ИСПОЛЬЗОВАТЬ: В наше время, если вы подбираете криптографическую систему, вам стоит использовать SHA-256 и выше, я имею ввиду SHA-384 и SHA-512 и так далее.

лектор: Чтобы проще разобраться с материалом, отойдем от сухого текста и смоделируем ситуацию

лектор: Допустим Вам на обучение дали задание скачать операционную систему Windows 7 Home Premium x64bit

лектор: Мы знаем, что данная операционная система поставляется от разработчика Microsoft, далее уже идем в поиск и совершаем следующий поисковый запрос:

лектор: site:microsoft.com Windows 7 Home Premium hash

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2Fcyzpf32.gif&hash=bb4930fe4831b0ed6165264375913cf2

лектор: Оператор site: Этот оператор ограничивает поиск конкретным доменом или сайтом. То есть, если делаем запрос: site:microsoft.com Windows 7 Home Premium hash, то результаты будут получены со страниц, содержащих слова «Windows», «7», «Home», «Premium» и «hash» именно на сайте «microsoft.com», а не в других частях Интернета.

лектор: Эта информация так же является ключевой для поиска шопов с помощью операторов в поисковых системах, более подробно изучить информацию о том как искать с помощью операторов в Google используйте эту статью - https://habrahabr.ru/sandbox/46956/ .

лектор: Как мы видим из Гифки выше, я легко нашел хеш-сумму операционной системы Windows 7 Home Premium 64bit на официальном сайте Microsoft

лектор: Вот она - SHA1 Hash value: 6C9058389C1E2E5122B7C933275F963EDF1C07B9

лектор: Вообще я бы рекомендовал находить хеш-суммы и осуществляться поиск начиная от 256 и выше, но на офф сайте была только данная сумма, так что я возьму то что есть

лектор: Далее нам необходимо найти файл, который соответствует данной хеш-сумме, для этого так же используем поисковую систему Google и операторы, как искать с помощью операторов и что это такое ссылка выше.

лектор: inurl:download "6C9058389C1E2E5122B7C933275F963EDF1C07B9"

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FgTRZkuk.gif&hash=a8f431893e58fcae1c9343d9a6229e3e

лектор: После того, когда вы скачиваете этот файл, то при помощи нашей хеш-суммы можно удостовериться, что этот файл не изменялся, т.е. он обладает целостностью.

лектор: Есть инструменты, которые вы можете скачать, чтобы делать это. https://en.wikipedia.org/wiki/Comparison_of_file_verification_software

лектор: Одним из таких инструментов является Quick Hash (https://quickhash-gui.org), и я покажу на примере с ним, как сверить хеш-суммы и убедиться в целостности полученной информации.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FWQbvSAW.gif&hash=5036ece80556c5625d9da5e2dc5abd34

лектор: Как мы видим, хеш-сумма, скачанного файла, соответствует хеш-сумме данной нам с официального сайта Microsoft.

лектор: Так же я приложу ниже, информацию по другим хеш-суммам данного файла

лектор: MD5: DA319B5826162829C436306BEBEA7F0F

лектор: SHA-1: 6C9058389C1E2E5122B7C933275F963EDF1C07B9

лектор: SHA-256: C10A9DA74A34E3AB57446CDDD7A0F825D526DA78D9796D442DB5022C33E3CB7F

лектор: SHA-512: E0CB678BF9577C70F33EDDC0221BC44ACD5ABD4938567B92DC31939B814E72D01FAC882870AB0834395F1A77C2CD5856FD88D2B05FBE1D1D9CCE9713C1D8AB73

лектор: Вы можете заметить, что с увеличением этих цифр в алгоритме хеширования, длина хеша становится все больше, поскольку это длина в битах. SHA-1 - короткий, 256, 512 и MD5, который слаб и не должен использоваться вообще. Так что это является способом подтверждения того, что файл, который вы скачали, сохранил свою целостность.

лектор: Некоторые из вас наверняка зададутся вопросом: "Что, если файл, который я собираюсь скачать, уже скомпрометирован?" Допустим, вот у нас веб-сайт (https://www.veracrypt.fr) программного обеспечения VeraCrypt (https://ru.wikipedia.org/wiki/VeraCrypt).

лектор: И я хочу скачать VeraCrypt, на сайте имеются хеш-суммы файлов в кодировке SHA-256 и SHA-512

лектор: SHA-256:
6cff2cce52eb97321b1696f82e9ccefa7c80328d91c49bf10b49e38
97677896e VeraCrypt Setup 1.21.exe

лектор: SHA-512:
5c68a5a14fa22ee30eb51bc7d3fd35207f58eefb8da492f338c6dac
54f68133885c47fa2b172d87836142c75d838dac782b9faca406a
2ffb8854cc7d93f8b359 VeraCrypt Setup 1.21.exe

лектор: Однако есть одно «НО», если вебсайт был скомпрометирован, то это означает, что злоумышленники могли подменить данный файл для загрузки и добавить к нему что-либо, троян или что-то для слежки, и они также могли подменить и контрольную сумму.

лектор: Следовательно, получается, что хеш ничего не значит, то есть он не может обнаружить преднамеренную

модификацию файла. И нам нужно что-то еще чтобы удостовериться что данное программное обеспечение действительно исходит от разработчика. Что сайт VeraCrypt — это официальный сайт VeraCrypt и т.д.

лектор: И здесь мы подходим к сертификатам, цифровым подписям и другим средствам которые сейчас разберем, а пока давайте затронем не маловажную суть хеширования.

лектор: Не хочу я копировать и т.д. так как тут важно будет цветом все передать

лектор: https://i.imgur.com/d0VpoIU.png

лектор: https://i.imgur.com/I4LLHNH.png

лектор: Сейчас поговорим о Цифровых подписях

лектор: Так давайте вернемся опять к нашему VeraCrypt как узнать, что сайт действительно официальный и программное обеспечение исходит от разработчика.

лектор: Простой и довольно таки хитрый способ найти официальный сайт — это найти программное обеспечение в Wikipedia и уже там перейти по ссылке на официальный сайт программного обеспечения.

лектор: Однако мы можем так же нажать на целеный замок и там посмотреть сертификат, что именно он выдан

лектор: https://puu.sh/xQAFM/e687c816ce.png

лектор: Цифровая подпись — это значение хеша. Это результат работы хеш-функции с фиксированным размером, который зашифрован закрытым ключом отправителя с

целью создания цифровой подписи или подписанного сообщения.

лектор: С технической точки зрения цифровая подпись — это отметка, подтверждающая лицо, которое подписало сообщение. Это выдача гарантии на объект, который был подписан с ее помощью.

лектор: Для наглядности, что такое цифровая подпись открываем скриншот (https://puu.sh/xQAFM/e687c816ce.png) и смотрим на Подписывание

лектор: Подписывание: То, что вы можете видеть на инфографике выше, но исходя из нашего файла который мы разбираем

лектор: Алгоритм хеширования > Значение хеша (6cff2cce52eb97321b1696f82e9ccefa7c80328d91c49bf10b49e3897677896e) >Закрытый ключ (см. Асимметричное шифрование) = Цифровая подпись

лектор: Если объект шифрования подписан цифровой подписью, то обеспечена аутентификация, потому что объект зашифрован при помощи закрытого ключа, шифровать которым может только владелец этого закрытого ключа. Это и есть аутентификация.

лектор: Она обеспечивает невозможность отказа от авторства, поскольку, повторюсь, использован закрытый ключ отправителя. И она обеспечивает целостность, поскольку мы хешируем.

лектор: Цифровая подпись может быть использована, например, в программном обеспечении. Может

использоваться для драйверов внутри вашей операционной системы. Может использоваться для сертификатов и подтверждать, что подписанные объекты исходят именно от того лица, которое указано в сертификате, и что целостность данных этих объектов была сохранена, то есть никаких изменений они не претерпели.

лектор: А как же убедиться в том что файл действительно исходит от разработчика, в нашем случае VeraCrypt, то есть в случае обмана и т.д. вы могли со 100% уверенностью сказать, что я пользовался твоим программным обеспечением, и он был подписан именно твоей цифровой подписью.

лектор: https://puu.sh/xQB20/5166e3d0c8.gif - обычно сертификат проверяется автоматически и у вас наверно

лектор: После того когда посмотрели gif открываем скриншот (https://puu.sh/xQB5Y/c840f4670d.png)

лектор: Что мы здесь видим. Сертификат выдан: кому – IDRIX SARL, кем - GlobalSign. Итак, GlobalSign - это компания, чей закрытый ключ был использован для цифровой подписи этой программы. GlobalSign сообщает: "Данное программное обеспечение легитимно и оно не подвергалось модификации". Здесь написано: "Сертификат предназначен для удостоверения того, что программное обеспечение исходит от разработчика программного обеспечения, программное обеспечение защищено от модификации после его выпуска". Чтобы узнать, действующая ли это цифровая подпись, или нет, нам нужно повернуть изначальный процесс в обратную сторону.

лектор: То есть открываем опять наш скриншот (https://puu.sh/xQAFM/e687c816ce.png)

лектор: Проверка: То, что вы можете видеть на инфографике выше, но исходя из нашего файла, который мы разбираем

лектор: Подписанно сообщение > Открытый ключ (это файл в формате .asc имеет обычно следующий вид – https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc , закрытый ключ тоже самое так же выглядит) =Значение хеша, то есть должно получиться 6cff2cce52eb97321b1696f82e9ccefa7c80328d91c49bf10b49e3897677896e

лектор: После чего это значение хеша надо будет сверить с хешем указанным, то есть открываем там программу QuickHash прогоняем наш файл и в том алгоритме котором он нам представлен, должно все совпасть, если не совпадает то сам файл изменен, и там может быть троян, или что то для прослушки за нами, или еще что-то нехорошее

лектор: SHA-256: 6cff2cce52eb97321b1696f82e9ccefa7c80328d91c49bf10b49e3897677896e VeraCrypt Setup 1.21.exe

лектор: Я проверил полученный хеш (https://puu.sh/xQBAz/8905455dd7.png) и как мы можем видеть на скриншоте они идентичный следовательно файлы легитимное и соответствуют цифровой подписи разработчика, и этот файл точно исходит от него.

лектор: И данное программное обеспечение в случае заражение вашего компьютера WannaCry или каким либо еще другим нехорошим вирусом, будет виновен он.

лектор: Для примера, это как вы в детстве бы отнекивались что мол не сожрали конфеты, а ваша мать тычит вам в лицо докозательства, например видеозапись и говорит, у меня все записано, смотри сюда. И как бы не отвертишься, вот что делает цифровая подпись.

лектор: Прочитайте несколько раз если вы не поняли, и попробуйте вникнуть этот момент действительно важен

лектор: А то что мы видели непосредственно на этом скриншоте (https://puu.sh/xQAFM/e687c816ce.png)

лектор: Это то что Windows проверяет сертификат в подлинности, то что действительно такой сертификат зарегистрирован с таким номером все дела.

лектор: Давайте проведу аналогию чтоб понять, что же делает Windows, когда пишет эти строки (https://puu.sh/xQBLa/604166ab6c.png) в сертификате

лектор: Вы пришли в банк с фальшивыми деньгами, и они проверяют деньги через специальные растворы или приборы, и тут бац и смывается краска, или не просвечиваются водяные знаки и вам говорят, что ваши купюры не соответствуют и это фальшивка, так же и Windows.

лектор: То есть если бы кто-то другой переписал все данные сертификата и сделал копию сертификата для подписи, с такими данными то она бы не соответствовала

действительности ну — это более сложная тема, но собственно думаю понятно.

лектор: А если верификация не проходит, вы обычно видите вот такое предупреждение (https://puu.sh/xQC61/ef80678f6b.png)

лектор: Это означает, что-либо файл не имеет цифровой подписи либо Windows (вспомните работника банка) не доверяет этой цифровой подписи (а в случае с работником банка, он не доверяет в вашей купюре) вы можете ее проверить способ я описывал выше (а работник банка ну там тоже может проверить на аппарате своем или там нанесением растворов).

лектор: В линуксе с этим все просто, так как вы просто так не установите проприетарное ПО так как все ПО обычно ставиться из оффициальных репозиториев, где проходит всю проверку подробнее что такое репозиторий и прочие моменты можете как раз узнать тут

лектор: https://wwh-club.net/threads/pochemu-linux-luchshe-chem-windows.108852

лектор: можете взять как домашнее задание для изучения

лектор: и т.д.

лектор: запишите себе

лектор: Давайте пройдемся по этому материалу еще раз, потому что я уверен, некоторым все это может показаться довольно-таки трудным для восприятия.

лектор: https://puu.sh/xQAFM/e687c816ce.png - смотрим подписывание

лектор: https://puu.sh/xQAFM/e687c816ce.png - смотрим подписывание

лектор: Итак, значение хеша (самой программы то есть если бы чувак сам ее прогнал через QuciHash), которое было зашифровано с применением закрытого ключа (его личного ключа его личный отпечаток пальца так сказать в сети) отправителя или выпуска ПО. Это цифровая подпись.

лектор: Это обеспечивает аутентификацию, неотказуемость и целостность. А если вы зашифруете что-либо и вдобавок снабдите это цифровой подписью, то вы сможете добиться конфиденциальности наряду с аутентификацией, неотказуемостью и целостностью.

лектор: Цифровые подписи удостоверяют, что программа или что-либо другое получены от определенного лица или издателя, и они защищают программное обеспечение или сообщения от их модификации после того, как они были изданы или отправлены.

лектор: На этом думаю мы разобрались с цифровыми подписями.

лектор: Давайте теперь перейдем к End-to-End шифрованию (E2EE)

лектор: End-to-end шифрование заключается в том, что данные шифруются отправителем и дешифруются только получателем. Если вы хотите избежать отслеживания,

массовой слежки, хакеров и так далее, то вам нужен именно этот вид шифрования передаваемых данных.

лектор: Примерами технологии end-to-end шифрования являются такие вещи, как PGP, S/MIME, OTR, что расшифровывается как “off the record” (рус. "не для записи"), ZRTP, что расшифровывается как Z в протоколе RTP, а также SSL и TLS, реализованные правильным образом, все это может использоваться в качестве end-to-end шифрования.

лектор: Компании, которые разрабатывают программное обеспечение, использующее end-to-end шифрование и системы с нулевым разглашением, не могут раскрыть детали обмена данными вашим врагам, даже по принуждению, даже если бы они этого сами захотели. В этом и заключается преимущество end-to-end шифрования с нулевым разглашением.

лектор: End-to-end шифрование обеспечивает защиту в процессе передачи данных, но очевидно, что оно не может защитить данные после их получения. Далее вам нужен другой механизм защиты. Используйте end-to-end шифрование везде, где это только возможно.

лектор: Использование защищенного HTTPS на всех веб-сайтах становится все более необходимым, независимо от типов передаваемых данных.

лектор: Давайте я покажу что такое END-TO-END шифрование на примере с веб-сайтами

лектор: Это цифровой сертификат, тоже самое что и цифровая подпись, есть ряд отличий, там центры сертификации и т.д. вы обычно с этим не сталкиваетесь не буду расписывать, кому интересно гуглите « Центры сертификации ключей и HTTPS» и «Цифровые сертификаты»

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2Fq0aGfbn.png&hash=eafda643c4df7f9d9724f77945281151

лектор: Зеленый замочек в URL или HTTPS означает, что ваш Интернет-провайдер или, допустим, правительство, они лишь могут отследить целевой домен. Что это значит?

лектор: Допустим между нами и Google находится злоумышленник аналогично как в случае передачи сообщения в инфографике выше. Он не сможет узнать, что именно я искал, потому что это оконечное (или абонентское с английского end-to-end) шифрование между моим браузером и сервером.

лектор: Давайте разберем пример на наглядном и посмотрим, что же может узнать провайдер о нас

лектор: Для начала мы будем использовать пример не зашифрованного соединение при помощи HTTP соединения.

лектор: HTTP, HyperText Transfer Protocol — широко распространенный протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов

(то есть при клике по слову в статье перейти на другую веб-страницу).

лектор: По умолчанию протокол HTTP использует TCP-порт 80.

лектор: Для скриншотов ниже я буду использовать программу для анализа сетевого трафика WireShark.

лектор: Для эксперимента я взял сайт базирующийся на HTTP протоколе uznayvse.py после того как я кликну по ссылке запрос от сайта будет отображен в окне программы WireShark под цифрой 1-н, но давайте сразу разберем за что отвечает каждое окно программы для лучшего усвоения материала.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fpuu.sh%2Fxxprc%2Ff66caaecd9.png&hash=d7ebe6288f50a92d965fc3eebfe8484b

лектор: 1. Данная область называется Packet List – в ней вы можете посмотреть с каким сервером идет обмен данными, протокол, который используется и общую информацию о кадрах.

лектор: 2. Следующая область называется Packet Details – в ней отображаются детали пакетов который был выбран в Packet List.

лектор: 3. И последняя область называется Packet Bite – в ней отображается 16-е отображение данного пакета, также отображается смещение в виде аски, и так же если мы

кликнем правой кнопкой по данной области можем посмотреть, как все это будет выгладить в битах.

лектор: Вот что происходит, когда вы нажимаете по ссылке, все данные трафика сразу же фильтруются

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FTJvYxzB.gif&hash=cb666e07e000b63ce5d80216652413dd

лектор: Давайте разберем, полученные пакеты подробнее и узнаем наглядно о слежке, анализе и т.д.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FFVVoABb.jpg&hash=7a24d9bba16536dfa4dbaa8436e81edd

лектор: 1. Пересылаемые пакеты по нашему фильтру

лектор: 2. Целевой домен, то есть главная страница сайта без всякой ереси после слеша "/"

лектор: 3. Юзер агент, то есть параметры браузера, версия операционной системы и другие параметры..

лектор: 4. Referer – указывает с какой страницы мы перешли на эту страницу так как мы перешли с защищенной страницы, там было много пакетов с переадресацией в конечном итоге мы с этой же страницы сослались на себя же, если я к примеру, перешел с главной страницы сайта на данную то в рефере бы стояла главная страница сайта. (смотрите скриншот ниже с пояснением чтобы полностью вникнуть в смысл).

лектор: 5. Куки, либо сессия) Вот ваш и пароль приплыл) Можно зайти под вашей сессией залогиненой и шариться) от залогененного юзера то есть вас

лектор: КСТАТИ: Если вы думаете, что это потолок что может данный софт то боюсь вас расстроить это только верхушка айсберга

лектор: 6. Ну, а это уже конечная страница где мы находимся

лектор: КСТАТИ: Если вы думаете, что это потолок что может данный софт то боюсь вас расстроить это только верхушка айсберга

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2F75Zcarg.jpg&hash=8cf21012eca70ac2e91f366a4893dff9

лектор: Для того чтобы у вас после прочитанного не осталось сомнений я решил разобрать эти пункты перейдя с одной страницы веб-сайта на другую и как мы можем видеть:

лектор: 1. Refer – указывает предыдущую страницу которые мы разбирали именно с нее мы пришли на данную страницу

лектор: 2. На какой странице мы сейчас находимся

лектор: Как мы видим сам по себе протокол HTTP не предполагает использование шифрования для передачи информации. Тем не менее, для HTTP есть распространенное расширение, которое реализует упаковку передаваемых данных в криптографический протокол SSL или TLS.

лектор: Название этого расширения — HTTPS (HyperText Transfer Protocol Secure). Для HTTPS-соединений обычно используется TCP-порт 443. HTTPS широко используется для защиты информации от перехвата, а также, как правило, обеспечивает защиту от атак вида man-in-the-middle — в том случае, если сертификат проверяется на клиенте, и при этом приватный ключ сертификата не был скомпрометирован, пользователь не подтверждал использование неподписанного сертификата, и на компьютере пользователя не были внедрены сертификаты центра сертификации злоумышленника.

лектор: https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FIApps4z.jpg&hash=a981a84f81dd096b0be1d3768254d837

https://wwh-club.net/proxy.php?image=https%3A%2F%2Fi.imgur.com%2FIApps4z.jpg&hash=a981a84f81dd096b0be1d3768254d837

лектор: 1. Google – имеет использует защищенный протокол соединения HTTPS

лектор: 2. Пакет запроса данных по защищенному протоколу HTTPS

лектор: 3. Как мы видим в деталях пакета у нас только Encrypted Application Data: 000000000000016eec0818f25b5eb9bd4690883155a74b6...

лектор: никакой другой информации что содержится на веб-страницы или где находится человек у нас нет

лектор: 4. Так как у нас есть под цифрой 2-а IP-адрес с каким сервером ведется обмен пакетами, просматриваем что это за IP-адрес и исходя из полученных данных мы можем сделать вывод, что человек находится на целевой странице Google.

лектор: По сути использование HTTPS безопасно и как я говорил ранее что: Компании, которые разрабатывают программное обеспечение, использующее end-to-end шифрование и системы с нулевым разглашением, не могут раскрыть детали обмена данными вашим врагам, даже по принуждению, даже если бы они этого сами захотели. В этом и заключается преимущество end-to-end шифрования с нулевым разглашением.

лектор: SSLStrip – снятие HTTPS

лектор: Но также исходя из этого имеются атаки по снятию SSL давайте быстро разберем что это такое??

лектор: Любой атакующий, который может расположиться между источником и адресатом трафика, в нашем случае КОМПЬЮТЕРА и СЕРВЕРА, то этот атакующий может совершить атаку вида “Man in the middle” (рус. "Человек посередине"). Одна из подобных атак, которая требует весьма небольших навыков и ресурсов, называется SSL stripping (рус. "Снятие SSL"). Атакующий выступает в роли прокси здесь и подменяет зашифрованные HTTPS-соединения на HTTP-соединения.

лектор: Давайте откроем скриншот и посмотрим, что же это такое https://puu.sh/xQFWy/edbaf90d7a.png

лектор: 1. Как мы можем видеть мы отправляем запрос с http

лектор: 2. Он проходит через SSLStrip и не изменяется, так же идет дальше

лектор: 3. Сервер видит что вы пришли по небезопасному протоколу без шифрования и меняет его на безопасный с использованием шифрования то есть на HTTPS (то есть совершается 301 либо 302 редирект – это настраивается на сервере)

лектор: 4. SSLStrip видит что сервер отправил вам запрос в HTTPS (см. пункт 3) и автоматически так же изменяет его на небезопасный то есть на HTTP тем самым убирая TLS шифрование

лектор: SSLStrip здесь проксирует ответ от веб-сервера, имитируя ваш браузер, и отправляет вам обратно HTTP-версию сайта. Сервер никогда не заметит отличий.

лектор: Так как сервер думает, что вы общаетесь по защищённому протоколу HTTPS, так как он не видит, что злоумышленник (SSLStrip) изменил вам протокол на небезопасный

лектор: И что вы увидите - это будет практически неотличимо от подлинного сайта. Давайте я покажу вам, как должен выглядеть веб-сайт.

лектор: https://puu.sh/xQHeu/014bf0515b.png

лектор: 1. Мы видим защищенную версию WWH-CLUB, то есть с end-to-end шифрованием

лектор: 2. Теперь я выполнил HTTPS-stripping (снятие SSL – SSLStrip). И так выглядит версия сайта после атаки.

лектор: Как можно заметить, отличие в том, что у вас теперь нет HTTPS и большинство людей не заметят эту разницу. И как я уже сказал, сервер никогда не заметит, что что-то не так, потому что он общается с прокси, который ведет себя точно также, как вели бы себя вы.

лектор: https://i.imgur.com/i0Hr9em.png

лектор: https://i.imgur.com/SHYhxql.png

лектор: https://i.imgur.com/qLqO8qp.jpg

лектор: советую прочитать это с цветом

лектор: https://youtu.be/0wpxrPD90a4 — 1 Часть MITM. Как проводится MITM атака.

лектор: https://youtu.be/quZjKlrmCvQ — 2 Часть MITM. Атакуем сеть методам MITM

лектор: по частям запишите себе на Домашнее задание

лектор: тоже просмотрите и т.д.

лектор: более глубоко можете вникнуть по этому вопросу

лектор: Что могу сказать, как ЭПИЛОГ

лектор: Я считаю, что мы очень много разобрали по шифрованию, единственное что я не успел разобрать я написал выше, что мы не проговорили этот вариант с PGP, OTR, ZRTP, OMAXA, такие протоколы про них можно прочитать в гугле либо узнать у меня я дам информацию если она вам необходима.

лектор: Ну с пгп и отр думаю все понятно

лектор: по зртп это войс связь и омаха это новое типо шифрование из серии OTP только со своими плюшками

лектор: из офлайн меседжей шифрование чатов конференций и т.д.

лектор: Шифрование — это фантастический инструмент для приватности, безопасности и анонимности, это тот инструмент, который реально работает и злоумышленники (хакеры) будут стараться избегать его.

лектор: Говоря простыми словами.. Ни какой дурак не будет совершать прямую атаку на шифрование.

лектор: Как говориться умный в гору не пойдет, умный гору обойдет. И вам следует иметь это виду. И все что они могут сделать это найти слабые места.

лектор: Вспомните случай с Россом Ульбрихтом создателем «Шелкового пути» он попался на капче. То есть на простой мелочи, так как люди забывают о самом главном, а именно о самых простых вещах.. Азах так сказать.

лектор: То есть никто никогда не будет брутить ваши пароли прочее им гораздо проще установить вам кейлогер на вашу систему, или отправить вам ссылку на сайт с зараженным JS скриптом и произвести атаку, либо PDF файл и т.д.

лектор: Но как я и сказал шифрование, никто и никогда не захочет ломать. Атакующие будут просто пытаться обойти шифрование. Вам следует иметь это ввиду.

лектор: Безопасность – это так называемый феномен слабого звена. Она настолько сильна, насколько сильно самое слабое звено в цепочке. Надежное шифрование зачастую – это сильное звено.

лектор: Мы, человеческие создания, как правило являемся слабым звеном. Как говориться Язык мой — враг мой

Введение в безопасность на основе *unix подобных систем

лектор: Введение в безопасность

лектор: Я попытаюсь на простом языке объяснить, как вас могут теоретически взломать. Я обойдусь без сложных терминов, для обычных пользователей лекции. Так же дам вам красочное представление о взломе операционной система, а более продвинутые пользователи между строк будут читать техническую информацию.

лектор: Считаю, что пользователю любой операционной система, а тем более тем, кто связан с этим по работе, необходимо понимать, что профессиональные вирусы — это не исполняемый файл, который переименовали в документ и просят вас запустить (стиллер или ратник). И не всегда блокировка макросов не даст злоумышленнику выполнить код на вашей системе.

лектор: Сам пользуюсь различными операционками, от Windows и до Linux, и давно уже не сторонник таких холиваров, которые я разберу чуток позже на примере с Макбуками).

лектор: Я работаю на Linux, но иногда использую Windows. Далее будет возможно много негатива про Linux, но он не связан с какими-либо фанатическим убеждениями, просто я хочу объективно рассказать и убедить, что не важно, какой операционной системой вы пользуетесь — взломать вас могут везде.

лектор: Вспомните мои слова, которыми я завершил статьи по Шифрованию, а именно в Эпилоге..

лектор: Безопасность — это так называемый феномен слабого звена. Она настолько сильна, насколько сильно самое слабое звено в цепочке. Надежное шифрование зачастую — это сильное звено.

лектор: Мы, человеческие создания, как правило являемся слабым звеном. Как говориться Язык мой — враг мой.

лектор: Ваш выбор операционной системы имеет значение для вашей безопасности, приватности и анонимности. Различные операционные системы подходят для различных нужд.

лектор: Например, чтобы нарисовать для вас графику мне необходимо уходить с Linux на Windows так как мне нужен Photoshop и другие графические редакторы, об этом мы еще поговорим. Но думаю основной посыл информации понятен.

лектор: Цель данного раздела помочь вам разобраться в этой непростой ситуации. Ответить на вопросы: какая операционная система подходит под ваши требования

исходя из рисков и для чего вы хотите ее использовать, под конкретную ситуацию, под конкретные требования.

лектор: Это как в школе, научить вас ориентированию на местности, тут точно так же, так как ваша паранойя до добра вас не доведет. Ведь без знаний вы можете сделать только хуже..

лектор: Посыл и ясность

лектор: Давайте поговорим о нашем выборе операционной системы и как он влияет на вашу безопасность, потому что операционная система — это реальная основа вашей безопасности.

лектор: Есть много заблуждений, когда речь идет об операционных системах и безопасности. Вы, наверное, слышали, например, что Макбуки не могут быть заражены вирусами.

лектор: Так же множество людей постоянно обсуждает, на сколько дырявая операционная система Windows можно рассуждать годами, но интересно на сколько безопасен Linux?

лектор: И есть люди, назовем их лагерь Linux, которые считают, что Linux является самой лучшей операционной системой. Если спросить у любителей Linux, а если ли у вас антивирус, то в ответ будет только смех.

лектор: Аргумент такой — Linux создан профессионалами, и все там по дефолту (стандарту) защищено. Вот сажаем свою любимую собаку за Ubuntu и можно за ее данные не волноваться.

лектор: Вообще есть две вещи, которые бесконечны, вселенная и дураки. С вселенной все понятно, но как быть с последними? Вот как объяснить различным пользователям Windows, что нельзя работать без антивирусной защиты? А как объяснить создателям МЕГА Систем Защиты Информации (антивирусов в простонародье), что нельзя защититься от взлома матрицей доступа (это когда блокируют чтение или запись некоторых файлов, то есть разграничение доступа) и что взлом — это не всегда: «Обнаружена угроза: Процесс autorun.exe, пытается выполнить запись в системную ветку реестра».

лектор: Ваша защищенность выглядит хорошей только в теории. Допустим, вы тот самый пользователь Ubuntu, вы устанавливаете на ПК своей любимой собаки Боб эту ОС. Тогда многие утверждают следующее — если Бобу на почту придет сообщение myDocument.docx, то даже если это окажется исполняемый файл, и он его по инструкции запустит, то ничего не произойдет — ведь для большинства действий необходим пароль root (пароль администратора в смысле). Вы серьезно? Вы от нашествия представителей младших классов школы защищаетесь? Или все-таки от злоумышленников, которые являются членами преступных группировок, контролируют большие финансовые потоки и просто косят на своих собратьях бабло?

лектор: Это к отсылке тех пользователей, которые используют и слепо верят в Средства Защиты Информации (СЗС) или те курсы, которые им преподавали в учебниках по Информационной Безопасности (ИБ).

лектор: Давным-давно, когда Linux только зарождался, его пользователи в большинстве, были профессионалы. Но со временем появились удобные для простого пользователя в работе дистрибутивы и начался рост числа пользователей-домохозяек. А что делает любая домохозяйка? Правильно, совершает интернет-платежи, а там, где деньги, туда слетаются как пчелы на мед рой различного отребья, которое хочет на этом безвозмездно поправить свои финансы. 90% домохозяек пользуются Windows — и вирусы разрабатываются под эту операционную систему, и только хотя бы 20-30% домохозяек перейдут на Linux, то туда сразу будут вливаться большие финансы под разработку вредоносного ПО. И отчеты антивирусных компаний показывают о медленном, но увеличивающемся количестве таких программ.

лектор: Ок, вернемся к Бобу, единственная причина не беспокоится о своей безопасности одна — разработка троянца под его ОС нерентабельна. А вот так — экономически невыгодна, возможный доход злоумышленников будет меньше расходов. Долго ли так будет продолжаться — большой вопрос.

лектор: Но все же, технически, насколько возможно, что Боба взломают и данные уведут? Если конек безопасности Боба в том, что он никому не нужен и вирусы под его ОС пока еще не пишут — то это игра в русскую рулетку.

лектор: Алиса, подруга Боба, знает, что на счету Боба лежит кругленькая сумма монет (БЕТХОВЕНЫ)))), ключ лежит на ПК Буратино, и они вместе с Буратино решили сообразить на двоих. Что им для этого требуется:

небольшой стартовый капитал, прямые руки Буратино и немного отваги.

лектор: Алиса знает, что Боб пользуется Ubuntu 14 LTS. Как себе представляет процесс взлома Боб? Он, как и большинство пользователей, считает, что Алиса отправит ему на почту файл с вложением, которое его попросят запустить и так как он считает себя спецом в области ПК и файл он не запустит, то конечно его данные в безопасности!

лектор: Многоходовочка от Педро

лектор: Тогда Алиса идет на некоторый безымянный и теневой ресурс и покупает у Педро уязвимость к любимом браузере Боба за N-ое количество вечно зеленых. Педро не только снабжает Алису технической информации об уязвимости, но и высылает для Буратино (подельника Алисы) пример как запустить.

лектор: https://imgur.com/a/YMCfx

лектор: Уязвимость, которую получает Алиса — уязвимость нулевого дня в браузере Google Chrome. Например, открытые дыры CVE-2015-1233 или CVE-2014-3177, CVE-2014-3176, CVE-2013-6658 (см. Скриншоты выше) и сколько их еще не закрыто и о них известно только в ограниченных кругах — большой вопрос. (более подробно разберем чуть позже).

лектор: см. ссылку выше (скриншотики где)

лектор: Как видно из описания уязвимостей (см. скриншоты выше) Алиса может выполнить код в контексте процесса и работать это будет не только в ОС Windows, но

и в Linux и Mac OS. Уязвимости взяты для примера случайным образом. Еще раз повторюсь, это уязвимости БРАУЗЕРА.

лектор: Буратино составляет скрипт (JS — Java Script) и записывает туда shell-код (набор строк которые прописываются в командной строке), который должен выполнится на целевой системе — ПК Боба. Для этого ему необходимо как-то передать ссылку. Первый вариант с почтой Алиса и Буратино сразу отмели — Боб осторожный пользователь и ссылки из почты не открывает. Тогда они решили немного с импровизировать. Им известно, что Боб обычный человек и паранойей не страдает… Ладно короче не суть, для простоты Боб, просто перешел по ссылке — Алиса уговорила, там создалась прокладка, или еще какая хрень не суть важно. В общем он перешел.

лектор: После посещения Бобом ссылки в контексте процесса его браузера выполнился небольшой код, который написал Буратино — буквально несколько команд, которые в дальнейшем загрузили тело вируса и перешли в его выполнение. Но как же. Боб уверен, что Алиса просто показывает ему свои фотографии, никакие файлы на диск не загружаются, предупреждений нет, паролей от root никто не спрашивает.

лектор: Повышаем привилегии

лектор: После того как разработка Буратино начала выполнять свои первые инструкции на процессоре Боба, стал вопрос, а что делать дальше? В теории Боба даже если и произойдет заражение, то ему ничего не будет, Боб

поставил сложный пароль для root доступа, да и вводить его вдруг во что бы то ни стало он не будет.

лектор: Буратино с Алисой предусмотрели такой вопрос и заранее его решили. Тот же самый Педро подсказал им, что у него есть парочка уязвимости нулевого дня в ядре Linux, наподобие свежих уязвимостей в ядре версии 3.17 и 3.14 — CVE-2014-9322, CVE-2014-3153.

лектор: Прочитав описание уязвимостей Буратино понял, что они позволят ему выполнить код в контексте ядра ОС Боба. И все что ему необходимо это чтобы его вредоносное приложение, воспользовавшись этими свежими дырами и выполнила код в ring-0.

лектор: Пока ни о чем не подозревающий Боб рассматривает фотографии Алисы, код Буратино уже серьезно вторгся в просторы его системы и ни антивирус (его просто нет), ни чего-либо еще не могут даже отобразить сообщение об вторжении. Так как Буратино решил не останавливаться на достигнутом, то он пошел дальше. Попав на самый нижний уровень ОС Боба в котором предполагается выполнение только доверенного кода, Буратино начал поиск файла, который ответственен за запуск ОС. Как только ПО от Буратино нашло этот файл, оно модифицирует его таким образом, чтобы при перезагрузке ПК Боба продолжался выполняться код Буратино.

лектор: Rootkit (по-русски, "руткит") — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

лектор: И так Буратино и Алиса получили доступ к ПК Буратино под управление ОС Linux, но как им скрыть свое присутствие? Боб не дурак и каждые 5 минут проверят целостность системных файлов ОС. Для этого Буратино решили, что перезапишут код самой операционной системы, который загружен в память ПК Боба, но как? Ведь если те же действия провести на ОС Windows, то один небольшой системный компонент обнаружит это и принудительно перезагрузит ПК.

лектор: Боб за свою безопасность не беспокоится — ведь даже если код злоумышленника и выполнится в ядре, то ведь в последних версиях ядра Linux системные области памяти защищены от записи. Даже если Буратино и попытается перезаписать код ОС в ОЗУ, то процессор выдаст ошибку и произойдет перезагрузка ПК.

лектор: Тогда Буратино открыл документацию на процессор, который стоит на ПК Боба и стал изучать… Ему известно, что архитектура процессора Боба x86, но что это дает? Ведь на необходимые ему страницы в ядре стоит защита от записи. Тогда Буратино обратил внимание на регистр cr0 — небольшой блок памяти в котором хранятся данные с которыми работает процессор. А что будет если я 16-ый бит установлю в ноль, быстро перезапишу необходимые методы ядра и сразу же восстановлю регистр — подумал Буратино. И так и сделал, как оказалось если сбросить этот бит в ноль, то защиту от записи можно временно отключить.

лектор: Таким образом Буратино получил полный контроль над ОС Боба, да уязвимость потом нашли и исправили, но

программный код, который засел таким образом в ОС Боба уже никак не обнаружить. Ежеминутный контроль целостности показывает, что ни один файл в системе не изменен — программа Буратино просто подменяет его при чтении. Процессов новых нет — вредоносный процесс просто скрыт и если на другой ОС существуют решения, которые давно уже обнаруживают такие техники, то под ОС Боба такого нет.

лектор: В общем, заключение, Алиса и Буратино сжалились над Бобом… и удалили все его файлы. Ах ладно, если серьезно, то никогда не будьте на столько фанатично уверенным в чем-либо. Я попробовал в легкой форме и без технических терминов изложить суть проблемы.

лектор: Эпилог

лектор: Я хотел этой простой историей показать простые принципы. Как все это происходит, что необходимо четко разделять виртуализацию и использовать, ведь виртуализация это еще одна масштабная вещь в параметре вашей безопасности. Мы к этому еще вернемся.

лектор: То есть не старайтесь серфить какие-то ресурсы на своем ПК, открывать подозрительные ссылки и скачивать какое-то ненужное программное обеспечение, да и еще непонятно откуда, внимательно подходить к вопросам своей безопасности по поводу JS и включать его на доверительных ресурсах и многое другое.

лектор: Но как я обещал ранее, я не буду вас кошмарить. Обычно такие уязвимости стоят не малых денег, и факт того

что именно вас взломают уменьшается, при том что заинтересуются именно вами, вероятность крайне мала.

лектор: Оценка рисков

лектор: В этой части статьи, я хотел бы наглядно произвести некую оценку рисков и исходя из этих моментов, чтобы Вы так же могли делать это самостоятельно. без каких либо специальных навыков, чисто своей логикой. Мы не зря в предыдущей статье абстрагировались и разобрали уязвимости, моделирование проникновения и прочие моменты.

лектор: Но зачем спросите вы.. Зачем же я поведал сейчас об этом, а то что не только средства безопасности имеют значение. Мы беспокоимся о том, каков наш действительный риск в реальном мире, и чтобы определить его, нам также нужно взять в расчет историю багов и уязвимостей в безопасности. Насколько слабой, собственно говоря, была конкретная операционная система? Возможно, вас интересует вопрос, какую из операционных систем мы будем считать самой слабой? Windows, OS X или различные Linux-системы, возможно ядро Linux, что из них было наиболее уязвимым в истории?

лектор: https://www.cvedetails.com — это бесплатная база данных / источник информации об уязвимости CVE (Это общепринятый стандарт именования уязвимостей, присутствующих в коммерческих и open-source программных продуктах). Можно просмотреть сведения об уязвимостях по номеру CVE, эксплойты, ссылки на уязвимости, метасплоит модули, полный список уязвимых

продуктов и cvss отчетов об оценках и топы уязвимости с течением времени и многое другое.

лектор: Давайте попробуем поработать с данным сайтом. Для начала мы перейдем на данную страницу сайта — https://www.cvedetails.com/top-50-products.php — тут представлен список: “Топ-50 продуктов по общему количеству уязвимых уязвимостей” (с 1999 года по настоящее время).

лектор: И как мы можем видеть на первой строчке у нас находится Linux Kernel — говоря по рус. Это Линукс Ядро, как мы видим оно занимает первую строчку по количеству.. И вы наверное спросите какого хрена? Линукс ты же должен быть эталоном.

лектор: Ладно, давайте во всем разберемся! Цифры которые изображены в правом столбике, это количество уязвимостей найденных в той или иной операционной системе, или приложении.

лектор: https://i.imgur.com/yz6dmcX.png

лектор: https://i.imgur.com/LhiTLgC.png

лектор: Между данными на скришотах разница в 3-и месяца

лектор: Давайте спустимся в самый низ веб-страницы. Мы видим там следующее “ Общее число уязвимостей 50 продуктов по производителям” (см. скриншоты выше).

лектор: И как мы можем видеть Linux уже не занимает первую строчку, но вы скажите что Windows (Microsoft) постоянно обновляется, да и у нее куча продуктов на рынке

Office и другие программы, а у Apple есть различные версии операционной системы да и тоже там свои нюансы..

лектор: Да все верно. Все вы будете правы, но и у Linux есть куча всего... Давайте более детально подойдем к специфике этого использования.

лектор: Я хочу научить вас самостоятельному анализу. А лучше всего чтоб научить хотябы базе, просто чтобы вы начинали думать своей головой, а не головой какого-то школо хацкера, которых щас развелось и которые хотят продать что-то не зная саму нишу и вмногих моментов которые из нее вытекют.

лектор: Ладно не будем сильно абстрогироваться, лучше давайте все разберем на деле, а там я думаю Вы все сами поймете, о чем я хочу вам рассказать.

лектор: Переходим на страницу https://www.cvedetails.com/vendor.php?vendor_id=33 — эта страница показывает Статистику уязвимостей в Linux

лектор: https://i.imgur.com/eYcMyc6.png

лектор: https://i.imgur.com/r8bDjUF.png

лектор: Давайте ознакомимся первоночально на что стоит обратить свое внимание (см. скриншоты выше).

лектор: 1. Количество уязвимостей по годам

лектор: 2. Уязвимости по типу

лектор: Теперь необходимо разобрать, на какие параметры стоит обратить внимание:

лектор: Первое на что мы должны обратить внимание — это на количество уязвимостей по годам (цифра 1), как мы можем видеть что с каждым годом есть тренд к увеличению обнаружения уязвимостей;

лектор: Второе на что мы должны обратить свое внимание — это на степень опасности уязвимостей (цифра 2), как мы можем видеть серьезными тут являются выполнение кода (Execute Code) и переполнения буфера (Overflow).

лектор: Красный и оранжевый

лектор: • Красный столбец — это выполнение кода на стороне клиента без его ведома, думаю не надо рассказывать чем чревато.

лектор: • Оранжевый столбец — это переполнение буфера, т.е. имеется ввиду явление, возникающее, когда компьютерная программа записывает данные за пределами выделенного в памяти буфера. Чревато тем что повышение уровня привилегий и еще куча всего.. Подробнее можете ознакомиться на https://ru.wikipedia.org/wiki/Переполнение_буфера

лектор: https://i.imgur.com/ilfcwll.png

лектор: https://i.imgur.com/Ny4goay.png

лектор: И для полноты картины мы можем подняться чуть выше, и увидеть таблицу с тенденциями уязвимостей с течением времени (см. скриншоты выше) по структурированным данным мы легко можем произвести анализ, так как мы видим ранжирование данных по

временому циклу (года) а так же по степени опасности уязвиомтей (это столбцы).

лектор: Как мы видим на первом скриншоте за Октябрь 2017 года было найдено: 166 потенциально опасных уязвимостей по выполнению кода (цифра 1) и 37 потенциально опасных уязвимостей по переполнению (цифра 2);

лектор: Тогда, когда 2017 год завершился мы видим следующюю статистику: 169 уязвимостей по выполнению кода и 42 по переполнению буфера.

лектор: Маленькая ремарка, я просто обновляю обучение и по этому я могу сделать такую статистику, по сути вам не нужно ждать 3 месяца, можно сравнить по годам. Просто я подумал, что хорошо бы дать такую статистику, а старую не удалять.

лектор: https://i.imgur.com/yYYTnra.png

лектор: https://i.imgur.com/JjAUSS3.png

лектор: Подробная статистика по уязвимостям: 1я выполнение кода и 2я переполнение буфера

лектор: Так же вы можете нажать на эти цифры и посмотреть подробную статистику о уязвимостях (см. скриншоты выше).

лектор: Анализ разработчиков

лектор: Теперь у нас сложилась небольшая картина как все устроено, мы разбирали это на основе Linux, но для анализа требуются несколько кандидатов. Сейчас я расмотрю в

краткой емкой форме на примере 3-х основных разработчиков, а именно:

лектор: • Linux

лектор: • Microsoft

лектор: • Apple

лектор: https://i.imgur.com/LhiTLgC.png

лектор: мы брали этот скриншот в начале

лектор: Как мы можем видеть (см. скриншот выше) в общей статистике уязвимостей по всем продуктам:

лектор: • Microsoft — 8938 уязвимостей;

лектор: • Apple — 5408 уязвимостей;

лектор: • Linux Kernel — 2000 уязвимостей.

лектор: https://i.imgur.com/Ny4goay.png

лектор: https://i.imgur.com/oep1hkM.png

лектор: https://i.imgur.com/6GUuyXq.png

лектор: сверху вниз: Microsoft, Apple, Linux

лектор: https://i.imgur.com/ESqV1dc.png

лектор: Чтоб вам было более просто откройте и дочитайте

лектор: А то еще не поймете

лектор: https://i.imgur.com/6uNE2SP.png

лектор: https://i.imgur.com/6uNE2SP.png

лектор: https://i.imgur.com/SgrbSMH.png

лектор: Тут проще будет по скриншоту

лектор: Давайте разберем некоторые из этих убеждений, основываясь на фактах и статистике, и выясним, к чему мы в действительности мы придем, когда дело касается безопасности этих операционных систем.

лектор: Итак, 1-е мы будем разбирать Windows, на сколько дырявая операционная система Windows можно рассуждать годами. Собственно как я и говорил ранее... Достаточно взглянуть на статистику ранее описанную и у вас в сознание должна загореться та самая красная лампочка, которая бы сигнализировала вам.

лектор: Да и вообще ПЕЙН гуру виндовс все вопросы по виндовс к нему =)

лектор: Но статистика — статистикой, но давайте разберемся почему. У нее изначально была слабая система безопасности.. Стоит отдать ей должное. В более поздних версиях операционных систем Microsoft начали серьезно относиться к вопросам безопасности.

лектор: И с учетом последних продуктов, последних средств безопасности типа: BitLocker, EMET, Device Guard, Windows Hello и доверенных приложений Windows trusted apps, теперь есть вполне серьезный набор средств безопасности.

лектор: Но действительно ли это так? Вообще я соглашусь, безопасность операционных систем семейства Windows по степенно улучшается, но этого не достаточно, а тем более для нас.

лектор: В этих операционных системах все тесно взаимосвязано с серверами Microsoft, все ваши действия в системе как по ниточкам сообщают на сервера Microsoft, так же подводят Windows, особенно в актуальной версии Windows 10, проблемы, связанные со слежкой и конфиденциальностью, это не особо связано со средствами безопасности, но это отталкивает некоторых людей, что говорить уже о нас..

лектор: Я бы рекомендовал ознакомиться с данной статьей: https://wwh-club.net/threads/98628/ — чтобы вы могли со стороны посмотреть на картину в целом.

лектор: Важный момент: Если вы прочтете лицензионное соглашение от Microsoft котрое идет с каждой операционной системой семейства Windows вы увидите, что они отдадут ваш ключ шифрования от BitLocker по первому звоночку из правоохранительных органов, а это в свою очередь натыкает на мысль, какого хрена Windows?! Зачем ты хранишь мои пароли от шифрования у себя на серверах, что за херня.

лектор: Дело в том, что «ставя галочку» в лицензионном соглашении с Microsoft, пользователи дарят корпорации право распоряжаться своими данными. «Мы можем получать доступ, раскрывать и сохранять для себя ваши персональные данные, включая любой контент, любые файлы на ваших устройствах, в ваших письмах и в других видах личных коммуникаций, если у нас будут основания считать это необходимым для защиты наших клиентов или для соблюдения условий, регулирующих использование наших услуг» – гласит лицензионное соглашение.

лектор: Другими словами, все, что вы скажете в Сети, напишете, сохраните, создадите или скачаете у себя на компьютере или любом другом устройства с Win 10, все это может быть дистанционно удалено или скопировано у вас – если некто в Microsoft решит, что это им нужно. То есть, по условиям EULA Microsoft для вмешательства в личную жизнь клиентов и контроля над ней не требуется даже санкция властей!

лектор: Достаточно лишь разрешения при установке ОС от пользователей, слишком ленивых, чтобы прочитать полностью лицензионное соглашение.

лектор: Как я и сказал я не буду разбирать Windows, моя цель предоставить вам информацию, чтобы вы ее увидели и произвели какой-то сравнительный наглядный анализ.

лектор: Скорее всего я вскором времени напишу статью об этом, а далее буду ссылаться на нее... Она будет опубликована в моем разделе. Если найду на это время...

лектор: Mac OS X

лектор: Далее у нас идет, Mac OS X, на сегодня, опять же, как и Windows, содержит надежные средства безопасности. Вещи типа рандомизации распределения адресного пространства, песочница для запуска приложений, FileVault 2, настройки приватности и магазин доверенных приложений Apple (AppStore). Все сильные средства безопасности.

лектор: Но если бы не одно «НО» Mac OS X так же имеет проблемы с конфиденциальностью

лектор: Если вы обновили до Mac OS X Yosemite (10.10), и вы используете настройки по умолчанию, каждый раз, когда вы начинаете вводить Spotlight (чтобы открыть приложение или найти файл на вашем компьютере), ваши локальные условия поиска и местоположение которые направлены компании Apple и третьим лицам (в том числе Microsoft) (см. скриншот https://puu.sh/xTGkj/dbe1f88d3e.png).

лектор: там скобку и точку в адресе стерите

лектор: Washington Post так же опубликовала видео-демонстрацию отслеживания в реальном времени Yosemite.

лектор: Давайте откроем ее https://www.washingtonpost.com/posttv/business/technology/how-apples-os-x-yosemite-tracks-you/2014/10/22/66df4386-59f1-11e4-9d6c-756a229d8b18_video.html

лектор: Кстати на днях про мак тоже вышла инфа именно про взлом не очень приятная новость, я не подготовил текст под нее, но гуглиться на раз 2

лектор: Давайте разберем это видео, и у кого плохо с английским я попытаюсь разобрать все те основные моменты, которые вы сейчас просмотрели.

лектор: 1. Например, простой вывод поиска Spotlight, это средство для поиска файлов в вашей операционной системе, теперь передает ваше местоположение и названия файлов, которые вы ищете, в адрес Apple на постоянной основе. Вы можете заметить, что ваше местоположение передается в Apple даже несмотря на то, что вам не показывается соответствующая иконка с уведомлением. Они решили

утаить это уведомление под предлогом того, что пользователи будут перегружены слишком большим количеством сообщений с уведомлениями. Это означает, что если вы согласились использовать службы геолокации, то вы также согласились на передачу сведений о вашем местоположении в Apple (см. скриншот https://puu.sh/xTGyC/11d372083a.jpg)

лектор: Давайте откроем .gif анимацию (https://puu.sh/xTGZQ/58a24bfd28.gif) и разберем ее

лектор: Вы можете заметить, что данные начинают отправляться до того, как вы набираете текст, так же при нажатии клавиш, то есть по хожу набора текста, данные так же отправляются))

лектор: Как мы видим автор видео говорит: “Я ищу на своем компьютере документ под названием "секретные планы, которые слил мне Обама", а Apple получает информацию об этом вместе с моим местоположением и пользовательским ID, который является уникальной строкой из букв и цифр, используемой для моей идентификации. Apple говорят нам, что это значение меняется каждые 15 минут, но нам приходится верить в то, что новое значение не привязывается к предыдущему. Опять же, они получают информацию о нашем местоположении, и как показывает автор, что действительно он находится в офисе Washington Post, основываясь на передаваемых координатах.

лектор: Ладно давайте быстро проговорим, как же мы можем отключить эти вещи со слежкой

лектор: Чтобы отключить эти вещи, сначала нам нужно зайти в System Preferences > Spotlight (https://puu.sh/xTJ6F/e59027c2cd.png), мы видим на скриншоте все места куда заглядывает Spotlight чтобы осуществлять поиск для вас. Это может быть очень полезно. Однако, это может быть и проблемой конфиденциальности, как вы могли только что убедиться. Я бы рекомендовал отключить все, но, если вам что-то нужно можете конечно оставить.

лектор: Если вы используете Safari, то вам необходимо отключить следующее, нажмите Safari > Preferences > Search и необходимо снять галочку Include Spotlight Suggestions (см. скриншот https://puu.sh/xTJ2m/dcb32d4c13.png)

лектор: Так же есть неплохой веб-сайт (https://fix-macosx.com/), на нем представлено большое количество информации о проблемах конфиденциальность в Mac OS X. Конкретно точнее по этой проблеме, сертификат сайта истек и проект кажись помирает. Но если у кого старая ось можете разобраться с этой проблемой, так что расписывать по этому поводу я думаю нецелесообразно

лектор: Ну это старье уже так то

лектор: Далее у нас идет Linux подобные операционные системы собственно основа нашего курса. Пожалуйста ознакомьтесь с этой статьей, прежде чем читать далее — https://wwh-club.net/threads/108852/

лектор: В вашем случае я давал ее вчера

лектор: Но можете так же записать на домашку кто не ознакомился

лектор: Наверно не будем останавливаться потом кто захорчет ознакомиться

лектор: Вообще рекомендовал бы

лектор: Linux-подобные операционные системы, Unix-подобные операционные системы. Есть их большое разнообразие, я группирую их все в одну категорию. Если вы ищете самые защищенные операционные системы, то вы найдете их именно здесь, точнее даже будет сказать ТОЛЬКО здесь.

лектор: Такие вещи, как SELinux, являются хорошим примером этого, это реализация разграниченного мандатного управления доступом — MAC, которая удовлетворяет требованиям правительства и военных.

лектор: Определение: Мандатное управление доступом (англ. Mandatory access control, MAC) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как Принудительный контроль доступа. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

лектор: SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Это не столько важный момент для вас чтобы заострять на этом момент.

лектор: Мы разберем более стандартные операционные системы: Ubuntu, Debian, Fedora, Arch Linux, Tails и др — опять же, все они имеют достаточно надежные средства безопасности.

лектор: Когда мы рассматриваем Windows, Mac OS X и Linux, все они в похожих условиях.

лектор: Но когда речь заходит об их существующих средствах и функциональных возможностях безопасности. Когда мы добавляем приватность в комплект к безопасности, то нам нужно начинать приглядываться к Linux дистрибутивам.

лектор: Я бы рекомендовал для безопасности использовать Linux дистрибутивы, но вам придется пожертвовать интероперабельностью и юзабилити. Например, вы не сможете использовать Photoshop или Microsoft Office, хотя это решаемо при помощи “wine” — что это такое вы можете посмотреть на YouTube, а быть может я разберу ее в этом курсе. Я не знаю, очень много времени уходит на написание, катастрафически много..

лектор: В двух словах, если вы не знаете, существует много-много операционных систем, которые определенным образом эволюционировали с середины 1960-х годов из операционной системы под названием UNIX (она была во главе платная система для корпораций и т.д.)

лектор: Я обещал дать вам список операционных систем когда говорил, что стоит выбирать системы у которых есть деньги для быстрого устранение уязвимостей, вот можете посмотреть наглядно сколько всего дистрибутивов Linux и от кого они произошли:

лектор: Для этого откройте: https://upload.wikimedia.org/wikipedia/commons/1/1b/Linux_Distribution_Timeline.svg — плюс этой ссылки в том, что это формат *.SVG следовательно вы можете искать по данному генеологическому древу через Ctrl+F прямо в браузере;

лектор: Просто посмотрите как много операционных систем базируются на Debian, теперь вы можете вернуться к статистике которую мы делали по анализу ранее, и слегка посмотреть на нее под другим углом.

лектор: и из них все развитляется в общем посмотрите внимательно повтыкайте потом идите читайте дальше

лектор: там кстати ctrl +F работает

лектор: Я бы рекомендовал использовать дистрибутивы основанные на Debian — Debian, Kali Linux, Parrot OS, а так же Fedora, Arch Linux

лектор: В конце будет список с кучей джистриубтивов по дебиан и там же с маленькой ремарочкой

лектор: Давайте немного поговорим про эти операционные системы

лектор: Как вы уже заметили при детальном знакомстве с *.SVG инфографикой выше, 2-а основных комьюнити — это Debian и RedHat, так же есть куча других, но как я и

говорил ранее: "если у вас менее известная Linux или Unix-подобная операционная система, то вы можете обнаружить, что выпуск исправлений происходит медленнее, поскольку за ними не стоят огромные многомиллиардные корпорации, в которых выпуск всех исправлений поставлен на поток".

лектор: Так же это касается по поводу сапорта от комьюнити и так далее...

лектор: Fedora Linux — это дистрибутив Linux с одним из самых крупных сообществ пользователей, среди других дистрибутивов. Но он не такой популярный, как Debian. Среди пользователей ходит мнение, что Fedora сложна в использовании и настройке.

лектор: Весомый плюс этой системы в том что Fedora — это только свободное программное обеспечение. Операционная система Linux очень часто рассматривается как свободное программное обеспечение. Но это не на 100% верно. Хотя большинство программ, которые вы используете свободны, некоторые драйвера и прошивки оборудования имеют закрытый код. Также есть компоненты с открытым исходным кодом, но с ограниченной лицензией, например, медиакодеки.

лектор: В самом начале Linux разделя я просил Вас ознакомиться со статьей в которой описывались моменты с безопасностью и проприетарным ПО, как раз именно к этой отсылке.

лектор: Разработчики дистрибутивов определяют насколько часто их пользователи будут контактировать с проприетарным программным обеспечением. Они могут

включать в состав дистрибутива медиа кодеки, драйвера видеокарт и сетевых адаптеров, а также дополнительные модули, например, Adobe Flash. Это поможет пользователям слушать музыку, играть в игры и просматривать веб-страницы, но это несвободное программное обеспечение.

лектор: Fedora занимает принципиальную позицию в этом вопросе. Это помогает избежать судебных исков против Red Hat. Несвободное программное обеспечение просто не допускается в репозитории. Дистрибутив не будет вам мешать устанавливать такие программы, но и помогать тоже не будет. Вам придется использовать сторонние репозитории, например, RPM Fusion. Это один из моментов, почему Fedora считается сложной. Но добавить репозиторий в систему — дело нескольких минут.

лектор: Но вот такие статьи https://habrahabr.ru/post/337290 , вводят конечно слегка в заблуждение.. Так как раньше некоммерческие продукты, насколько я помню, под подобные запреты не попадали. Fedora Project хоть и спонсируется Красной Шапкой для отработки новых технологий, но является некоммерческой структурой и прибыли не извлекает из своей деятельности, насколько я понимаю. Странно это все.

лектор: Arch Linux — это независимо разрабатываемый дистрибутив Linux, оптимизированный для архитектур i686 и x86/64, ориентированный на опытных пользователей Linux.

лектор: В целом, вам нужно быть компетентным пользователем, чтобы использовать эту систему, вам нужно быть в курсе об этом заранее. Она использует Pacman, менеджер пакетов собственной разработки от создателя Arch Linux. Pacman обеспечивает установку актуальных обновлений с полным контролем зависимостей пакетов, работая по системе плавающих релизов или роллинг-релизов. Arch может быть установлен с образа диска или с FTP-сервера.

лектор: Поясню менеджер пакетов / репозиторий — это как App Store или Google Play откуда вы в 2-а клика можете скачать и установить нужное Вам приложение или программу.

лектор: Установочный процесс по умолчанию предоставляет надежную основу, позволяющую пользователям создавать настраиваемую установку. Вдобавок, утилита Arch Build System (ABS) предоставляла возможность легко собирать новые пакеты, модифицировать конфигурацию стоковых пакетов и делиться этими пакетами с другими пользователями посредством Arch User Repository (Репозиторий пользователей Arch). Это легковесный дистрибутив Linux. На него ставится преимущественно свободно-распространяемое и опенсорсное программное обеспечение и ПО из поддерживаемого сообществом репозитория AUR.

лектор: Ubuntu — Чтобы отмести этот вопрос сразу скажу что Ubuntu отправляет ваши данные 3-им лицам без вашего согласия.

лектор: Если вы пользователь Ubuntu, и вы используете настройки по умолчанию, каждый раз, когда вы начинаете вводить Dash (чтобы открыть приложение или найти файл на вашем компьютере), ваши условия поиска отправляются различным трем лицам, некоторые из которых рекламируют вас.

лектор: Кстати можете вспомнить ситуацию про Windows которая решила раздавать WIndows 10 бесплатно, но в итоге соберает все данные якобы для рекламы, то есть всю вашу личную информацию и т.д. В общем не хочу повторяться по этой причине, так как уклон точнее не в сторону нее, я уже достаточно поговорил думаю про нее. Если вы хотите больше информаци по этой системе, ознакомьтесь хотябы с Лицензионным соглашением WIndows. И у вас начнет дергаться глаз)

лектор: На счет Ubuntu чтобы предотвратить отправку данных 3-им лицам, вам нужно выполнить ряд инструкций на этом сайте https://fixubuntu.com/ следуем указанным здесь инструкциям, здесь показано, как изменить нужные настройки. Ранее мы разбирали похожую ситуацию на примере Mac OS X.

лектор: Однако я в любом случае не рекомендую Ubuntu, я лишь привожу это для вашего интереса в том случае, если так получилось, что вы используете эту систему. Ubuntu лучше в целях приватности и анонимности, чем Windows или Mac OS X. Я рекомендую Ubuntu людям, не имеющим опыта работы с Linux и считающим что приведенные выше дистрибутивы слишком сложные для усвоения для них.

лектор: Есть форки Ubuntu Mate там вроде как это пофикшено

лектор: Debian — это операционная система, основанная на Linux, это дистрибутив Linux. Она целиком состоит из свободного программного обеспечения с открытым исходным кодом, большая часть которого находится под универсальной общественной лицензией GNU.

лектор: Дистрибутив Debian содержит более 51 000 пакетов скомпилированных программ, которые упакованы в отличном формате для легкой установки на вашу машину. Все они бесплатны. Это похоже на башню. В основании находится ядро, над ним — основные инструменты, далее идут все программы, которые вы запускаете на компьютере. На вершине этой башни находится Debian, тщательно организующая и складывающая все это воедино, чтобы все компоненты могли работать вместе.

лектор: С таким подходом ваша система не будет стучаться на домашние сервера Microsoft.

лектор: Tails — дистрибутив Linux на основе Debian, созданный для обеспечения приватности и анонимности. Является продолжением развития ОС Incognito. Все исходящие соединения заворачиваются в анонимную сеть Tor, а все не анонимные блокируются. Система предназначена для загрузки с LiveCD или LiveUSB и не оставляет следов на машине, где использовалась. Проект Tor является главным спонсором TAILS. Операционная система рекомендована к использованию «Фондом

свободной прессы», а также использовалась Эдвардом Сноуденом для разоблачения PRISM.

лектор: Его используйте только для серфа к примеру

лектор: Так как наебетесь с ним шо мамма не горюй жопа ваша будет гореть как адово пекло

лектор: К примеру пришли куда-то сунули флешку со своей ОС посерфили вытащили все

лектор: Kali Linux — GNU/Linux-LiveCD, возникший как результат слияния WHAX и Auditor Security Collection. Проект создали Мати Ахарони (Mati Aharoni) и Макс Мозер (Max Moser). Предназначен прежде всего для проведения тестов на безопасность.

лектор: Предшественником Kali был BackTrack, созданный на базе нескольких linux-дистрибутивов. Первоначально предназначался для использования на ОС Slackware, а затем плавно перешёл на Ubuntu. После основой стал Debian.

лектор: Parrot OS — Набирающий популярность сесурити-дистрибутив, основанный на Debian-linux. Довольно простой в освоении, подходит и для новичков и для профессионалов. Этот дистрибутив нацелен как на проведение тестирования на проникновение, так и на анонимную работу в сети Интернет.

лектор: Довольно легкий и эффективный инструмент, многие security специалисты нашли в нем замену все более «прожорливому» Kali, тем более что Parrot использует репозитории Kali для обновления. Использует графическое оркужение MATE и дисплей-менеджер LightDM.

лектор: По фукнционалу он похож на Kali Linux, здесь тоже вместе с системой поставляется огромное количество специального программного обеспечения для тестирования безопасности.

лектор: Как вы можете видеть все системы которые я упомянул выше в основном так или иначе базируются на Debian. (начиная с убунты и ниже

лектор: То, как вы будете разруливать с обновлениями безопасности в Linux, будет зависеть от дистрибутива, который вы используете. Я собираюсь рассказать об обновлениях безопасности на примере Debian и систем, созданных на основе Debian.

лектор: Смотрите, здесь https://wiki.debian.org/Derivatives/Census указаны все производные от Debian дистрибутивы. Многие из них — это операционные системы, важные для области безопасности, такие как Kali, Tails и так далее. Проект Debian выполняет отличную работу по обеспечению обновлений безопасности для Debian.

лектор: Вот тут можете почитать про дистрибутивы прочее

лектор: Безопасность — это приоритет для этого проекта и этой операционной системы.

лектор: Если вы хотите найти детали проблем безопасности, для исправления которых выпускаются патчи, то взгляните на страницу с информацией по безопасности, представленную Debian.

лектор: https://www.debian.org/security

лектор: Если вы спуститесь ниже, то увидите все обновления. Можете нажать на любое обновление и получить больше информации об этом конкретном обновлении. Можете перейти в каталог Mitre CVE и узнать больше по данной уязвимости которую вы выберите. Здесь подробная информация об этой уязвимости. Еще больше деталей видим здесь. И отсюда мы можем попасть в различные источники для большего количества сведений, и в принципе, можем даже найти код эксплойта для данной уязвимости. Мы это разбирали ранее на примере сайта https://www.cvedetails.com .

лектор: По заявлениям Проекта Debian, они обрабатывают все проблемы безопасности, доведенные до их внимания, и исправляют их в течение определенных разумных сроков. Они также говорят, что множество предупреждений безопасности координируются другими поставщиками свободного ПО и публикуются в тот же день, что и найденная уязвимость, а также, что у них есть внутренняя команда Аудита Безопасности, которая ищет в архивах новые или неисправленные ошибки безопасности. Они также верят в то, то безопасность путем сокрытия не работает, и что общедоступность информации позволяет находить уязвимости в безопасности, и это круто.

лектор: Все это хорошо, вот почему я рекомендую дистрибутивы основанные на Debian в качестве основной надежной операционной системы для повседневного использования, когда речь идет о безопасности, приватности и анонимности.

лектор: Мною было принято решение не давать разбор примера установки и т.д единтсвенное что вы должны понять что надо записывать установочную флешку в ddimage режиме через rufus к примеру, а линуксоиды могут использовать команду dd для этого.

лектор: https://i.imgur.com/tD3lDok.png

лектор: Вот что такое дд имейдж

лектор: Для того чтобы попросту не засорять и не делать кашу у вас в голове, если есть те люди/группа людей которые плотно решили освоить линукс среду. Поставить систему, можете напрямую обращаться ко мне или как я и говорил ранее обращаться через переписку ВОПРОС / ОТВЕТ.

лектор: Где уже всс будут консультировать и помогать с теми или иными вопросами, по сути сегмент ваших действий аналогичен как при работе с Windows и то что раскажет вам Пейн, так что отличается пожалуй чуток установка, а так все аналогично.

лектор: Очень много видео находиться на YouTube где показан пример установки операционной системы, разбиения диска и другие моменты.

лектор: Линукс это удивительная система, с которой нужно учиться работать и она станет вашим верным другом. Это как с домашним животным, как его на тренируете как его освоите, таким покладистым и полсшуным он будет для вас.

Безопасность и анонимность в сети. Настройка виртуальной машины

лектор: Доброго времени суток, дамы и господа! Сегодня я проведу лекцию на тему "Безопасность и анонимность в сети. Настройка виртуальной машины"

лектор: Лекция будет поделена на несколько частей:

- Безопасность

- Виртуальная машина и смежные параметры(разбор виртуальной машины для сёрфинга для общения, разбор виртуальной машины для вбивов),

- Хранение и оборот средств

лектор: В ходе лекции я объясню базисные методы и параметры, а также дам полезные ссылки и рекомендации.

Начинаем с превой и основной-базисной части.

лектор: Безопасность.

Начнем с того, что должно быть и так всем предельно ясно, что каждый должен принять как определенное "ТАБУ" и никогда так не делать:

лектор: Не трепитесь языком, не в интернете, не в жизни. Мы с вами не фрилансом занимаемся, следовательно никому никогда не нужно знать, откуда вы, как вас зовут, сколько детей и любую другую личную информацию, НЕ важно, кто спрашивает - друг или знакомый, любой может оказаться не тем, кем себя позиционирует, и даже я.

лектор: Как говорится: "Личное должно оставаться личным, рабочее - рабочим"

лектор: Никнеймы. Не используйте никнеймы, которые вы взяли из своего id вконтакте, стима, эмейла или любого другого сервиса или сайта. Использованные в белой сфере никнеймы - могут вывести людей из серой сферы на вас, бывало такое, что хватало просто погуглить никнейм человека, чтобы узнать всё о нём и его близких.

лектор: Не регистриуйте эмейлы и аккаунты на свой номер телефона, сервисы предоставляющие услуги почтовых ящиков запросто выдадут информацию по требованию. Для приема смс можно использовать онлайн сервисы, например: <http://sms-area.org/>

лектор: Таких сервисов много, можно их просто погуглить по запросу "принять смс для регистрации"

лектор: Почтовики, такие как gmail.com & hotmail.com могут регистрировать почту без приёма смс, если айпи ранее не был заюзан в их системе. Для mail.com смс не требуется.

Не используйте личные почты при регистрации на серых сайтах и шопах, заводите отдельные для этих целей.

лектор: Никогда не стоит думать, что вот, "я не настолько крупная рыба, чтобы меня искали" - нередко такие люди потом ищут деньги на адвокатов, не стоит самозаблуждаться, никогда не пренебрегайте безопасностью, ведь лучше спать спокойно.

лектор: Следущее ТАБУ: никогда не работать по РУ/СНГ/Украине и всему постсоветскому пространству. Не бить в такие шопы, не использовать такие карты и сервисы -

ничего, иначе на вас быстро выйдут спецслужбы. В новостях чаще показывают тех, кто работал по своей стране, - забавное наблюдение.

лектор: Приём посылок осуществляйте только через посредников, пересыл сервисы или дропов. Не светите свои имена нигде.

лектор: Jabber и все остальные средства коммуникации лучше хранить в виртуальной машине, если храните на основной - лучше отключить сохранение истории и паролей.

Если вам дорога собственная задница, её уют, комфорт и неприкосновенность - лучше соблюдайте эти табу.

лектор: Jabber используйте на безопасных серверах, к которым есть доверие, например:

wwh.so и остальные серверы wwh

exploit.im

zloy.im

лектор: Никогда не принебрегайте Гарант-Сервисом, даже на неочень большие суммы, лучше сберечь нервы и деньги, и потерять немного времени, чем наоборот! Не важно, клубень, модератор или друг - он такой же человек, как и Вы, НЕзависимо от количества и цвета лент под никнеймом, НЕзависимо от репутации, каждый может пуститься во все тяжкие и начать кидать своих/чужих. Прецедентов куча, в первую очередь учитесь на чужом опыте.

лектор: Приступим к разбору виртуальной машины и смежных параметров

Рекомендую использовать virtualbox или vmware. Не забываем включать виртуализацию в биосе вашего ПК - иначе виртуальная машина не сможет работать.

лектор: Лучше будет, если вы поместите образ виртуальной машины в закриптованную флешку(или ssd) или контейнер. Для флешки лучшие параметры это USB 3.0, 32-128gb.

SSD чем больше тем лучше, но смотрите по Вашим нуждам. Криптовать мы будем следующим софтом:

а) truecrypt 7.1a

б) veracrypt

Оба варианта взаимозаменяемы. Используйте или а, или б.

лектор: Вариант а - трукрипт версии только 7.1a, остальные небезопасны, и веракрипт - продолжение рода трукрипта, поскольку трукрипт был заброшен разработчиками. Я использую вариант б - veracrypt.
<https://veracrypt.codeplex.com/>

лектор: Криптуем флешку/ssd, или создаем контейнер на пк, и внутрь контейнера помещаем образ виртуальной машины. Теперь перед запуском виртуалки, Вам будет необходимо сначала вскрыть зашифрованный контейнер с помощью пароля. Как криптовать - можно посмотреть в справке самой программы или загуглить, это не сложно и требует нажатия буквально нескольких кнопок.

лектор: Есть два альтернативных контейнерам варианта, а именно:

- криптование всего жесткого диска на вашем компьютере

- создание скрытой ОС

лектор: При обычных контейнерах ключ шифрования можно вытащить из файла гибернации и снять с ОЗУ, поэтому отключаем гибернацию на своих компьютерах. Но при использовании скрытой ОС, можно поместить всю информацию и файлы внуть нее, и даже если вас будут пытать, вы сможете выдать пароль шифрования от обычной белой ОС, в то время как скрытая будет мирно хранить ваши файлы.

лектор: Шифрование всего жесткого диска - долгое (у меня на 1тб диска уходит примерно 6 часов шифрования), но надежное средство, так как с гибернации даже если она включена ключи уже не вытащить, а чтобы успеть снять с ОЗУ, надо очень постараться, остается только брут, и тут мы переходим к следующему пункту безопасности, а именно - пароли.

При скрытой ОС или шифровании диска, для запуска системы нужно будет ввести пароль в boot-loader'e, то есть даже до пароля учетки виндовс, до включения самой системы

лектор: На любом форуме, странице в социальной сети, почте или скрытом контейнере необходимо соблюдать ОБЯЗАТЕЛЬНЫЕ пункты при выборе пароля:

1. Длинна не мене 15 символов, лучше все 30

2. Верхний+нижний регистр, цифры и спец символы. Пример хорошего пароля: sHO&D=633qwvBB!aC{6} - на брут этого пароля уйдут десятилетия, а то и столетия.

лектор: 3. На один форум/шоп/сайт - один, уникальный пароль.

4. Двухфакторная аутентификация - используйте везде, где есть возможность.

5. Хранить пароле можно, например, в keepass или голове :)

лектор: Если использовать одинаковые пароли, велика вероятность взлома всего, что можно.

Никто не застрахован от слива или продажи базы данных на каком-то шопе дедиков, например.

лектор: Злоумышленники просто получают ваш пароль, а потом по-кругу пускают по всем сервисам/форумам, и забирают все что можно.

лектор: Но надежный пароль это не панацея, ведь могут перехватить прямо из вашей системы, подцепив на неё стиллер, малварь или другой вирус. Выход банален и прост - создайте отдельную виртуальную машину (вообще любую) специально для софта и грязных, непроверенных файлов.

лектор: И запускайте все ТОЛЬКО на этой виртуальной машине, пусть лучше страдает она, чем ваш компьютер. Соблюдать элементарные правила гигиены намного проще, чем потом терять аккаунты или выплачивать пострадавшим, поэтому не поленитесь и сделайте, зато будете спать спокойно.

лектор: Предназначение виртуальной машины для Вас будет делиться на два пункта, а именно:

- Сёрфинг, общение, повседневное использование

- Работа, вбивы

лектор: В зависимости от предназначения настройка будет делиться на два типа, начнем с первого, здесь нам важнее анонимность и безопасность, чем состояние системы готовности к вбивам, однако первый подпункт совпадает в обоих случаях.

лектор: Список минимальной необходимой базы программ для серфинга и общения:

- VPN. - Как минимум один, в идеале doubleVPN(двойной). Используем VPN стран третьего мира или хотя бы другого континента. VPN сервис НЕ должен вести логирование. При подключении VPN'a ваш ip должен измениться на ту страну, которую вы включили. Проверить это можно здесь: whoer.net

Впн ставим на основную машину

лектор: - TOR Browser

<https://www.torproject.org/>

Если у сайта есть зеркала в onion зоне(в торе), используйте эти возможности для сохранения бОльшей анонимности!

лектор: - Jabber / ICQ

Судя по тому, что в данный момент Вы все читаете это в джаббере, описывать эту програму смысла нет, но пару рекомендаций возьмите во внимание:

лектор: 1. Не светить жабой! Начнут брутить, начнут спамить и это прибавит головняков, а это никому не надо. Если очень хочется - для публичного выставления заведите отдельный джаббер-аккаунт.

лектор: 2. OTR шифрование. В кленте джаббера PSI+ он включается в плагинах, для Pidgin скачивается и устанавливается, проблем возникнуть не должно. Отр - шифрование, более обезопасивающее пространство общения. Для ICQ он также есть. Не рекомендую использовать скайп, он небезопасен.

лектор: Также заменяйте в системе свои DNS, например, на гугловские <http://support.li.ru/google-dns/win7/>

Их можно еще прописать в роутер. Для пущего эффекта можно использовать софт DNSCrypt, - возьмите на заметку и самостоятельно ознакомтесь с функциями в интернете.

лектор: - Браузер для серфинга (рекомендую firefox) - отключаем webrtc. WebRTC позволяет сторонним пользователям на раз определять IP-адрес пользователя сети, минуя программные заслоны VPN, TOR, SOCKS и других сетевых защитников <https://whoer.net/blog/article/kak-otklyuchit-webrtc-v-raznyx-brauzerax/>

лектор: - Если используете соксы или туннели, то proxifer+plinker. Разбирать не будем, на форуме очень много информации по этим двум прогам.

лектор: - Можно также замкнуть интернет через фаерволл так, чтобы при падении VPN'а на виртуальной машине не было выхода в сеть, и не утек Ваш реальный ip. В некоторых VPN клиентах есть такая функция, или можно повозиться с фаерволлом.

лектор: Параметры виртуальной машины для вбивов:

Для вбивов можно использовать любую виртуальную машину, все зависит от ваших нужд и шопов.

лектор: Но, необходимый софт для работы и параметры я все же назову, приступим.

лектор: 0. VPN, об этом мы говорили ранее.

лектор: IP мы подбираем с помощью SSH-туннеля и SOCKS5.

SSH туннель - это туннель, создаваемый посредством SSH соединения и используемый для шифрования туннелированных данных. Используется для того, чтобы обезопасить передачу данных в интернете

Socks5 позволяет создать цепь из нескольких серверов, тем самым достигается анонимность в сети.

лектор: 1. Бразуры. Firefox с подменой вебртс, хром с отключенным вебртс и несколько портабл браузеров хром/фаерфокс.

Подменить webrtc можно с помощью этого расширения: <https://wwh-club.net/threads/webrtc-podmena-ip-rasshirenie-dlja-brauzera.42828/#post-550221>

Если хотите использовать хром, устанавливайте расришение WebRTC leak prevent или подменяйте вебртс другими способами (есть на форуме)

лектор: 2. Софт для использования туннелей и соксов: proxifer и plinker/bitvise

3. Teamviewer (на виртуалке и на вашей основной машине) (необязательно)

4. NotePad++ для временных записей

5. Если есть и если нужен - антидетект

лектор: Параметры:

Начнем с параметров ip адреса (дедика/туннеля/сокса)

лектор: Отрицательные параметры:

- Двусторонний пинг и принадлежность к хостинг провайдеру

Принадлежность к хостеру = ip находится в облаке, такие айпи в работе лучше не использовать.

лектор: Двусторонний пинг детектит туннели, соксы, впны по пингу, я пробивал крупные мерчи и с ним, но это все же отрицательный параметр, решение - перебор страны впн или поставить TOR перед туннелем, если не помогло - замена айпи.

лектор: - DNS - не страны ip скорее негативно сказывается(но не критично), а так информации много на форуме по этому поводу.

лектор: - Flash, uptime, OS.

По желанию можно поставить флеш, но сейчас он есть далеко не у всех реальных пользователей.

лектор: Uptime - время бесперебойной работы вашего айпи, странно, если ваш айпи работает без перебоя уже несколько месяцев, не так ли?

лектор: Время(timezone) системы должно совпадать с временем ip-адреса.

лектор: OS - распростанненость, повседневность и доверие. Например, большинство рядовых пользователей используют виндовс. Тот же xp будет прибавлять больше фрода по той причине, что система устаревшая, соответственно win10 - наборот, больше доверия. Золотая середина - вин7.

лектор: Винда и браузеры должна быть именно англйисими, это все палится. Но если при этом какая-то программа в системе будет на русском - в этом ничего страшного, антифрод это не сможет обнаружить через браузер.(Flash должен быть eng)

лектор: ProxyScore + Riskscore ip - на это обращают внимание антифрод-системы, поэтому старайтесь брать с нулевыми или минимальными показателями. Некоторые сервисы по продаже доступов(socks/туннель/дедик) предоставляют эту услугу непосредственно внутри сервиса.

лектор: Открытые порты (8080, 8081, 3128, 80, 81 и так далее): это далеко не всегда негативный параметр, так как это действительно распространенное заблуждение, отнесем это к нейстральному параметру.

лектор: Некоторые сайты проверки анонимности сканируют айпи и считают, что если какой-то порт открыт, то айпи является прокси и понижают его анонимность. Но на самом деле это не так, большинство таких айпи это всего-лишь веб-админка роутера. Если бы через такие админки можно было так легко сделать прокси, их бы делали миллионами, это можно проверить самому.

лектор: Так как массовое сканирование портов во многих странах запрещено, крупные мерчи вместо скана портов обращаются за услугами к таким сервисам, как maxmind, который в свою очередь предоставляет такие услуги, как maxmind fraud check & maxmind geo check api, так что если какой-то сервис показывает отрытые порты у ip адреса(например whoer или 2ip.ru), это в большинстве случаев не является негативным показателем. И даже если такие сервисы покажут хороший результат, не факт, что потом с этого ip адреса у вас что-то выйдет вбить.

лектор: На моей практике крупные мерчи неоднократно успешно пропускали ордера с айпи адресов, где сайты проверки анонимности находили открытые порты и определяли тем самым айпи как прокси, исходя из этого смею предположить, что открытые порты это совсем не всегда плохо, и не стоит зацикливаться на этом, тем более, что фактически не владея ip адресом, вы ничего с этим не сделаете. Но по желанию можно подбирать ip-адреса и без

портов, или с открытым 80 - он допустим при любом раскладе, так как является естественным.

лектор: Геолокацию айпи адреса лучше подбирать максимально близко к зип-коду холдера карты. Например, если у холдера карты зип-код 85012, нужен айпи с зип-кодом 85012 или 8501* - то есть так близко, насколько это возможно.

лектор: Перед вбивами можно посерфить по полуряным сайтам типа youtube/amazon/facebook и прочим, некоторые серьезные антифроды могут палить вашу историю бразура. Странно, когда человек с пустой историей бразуера срываясь летит покупать гифты на тысячу долларов, не так ли?

лектор: АнтиФрод также может видеть tabname - открытые вкладки в браузере в данный момент, и определять с какого сайта пришел человек.(И по какому запросу)

лектор: - Audiofingerprint - отпечаток аудио, относительно серьезная система защиты. Смотрим различные статьи по этой теме, не все используют.

лектор: Серъезные мерчи также могут проверять сайты по списку, на которых вы залогинены (<https://browserleaks.com/social> - можете проверить здесь, например). На практике при залогиненом, например, фейсбуке - это плюсик, но не критично.

лектор: Для рандомизации фингерпринтов(отпечатков системы) при вбиве в один мерч/шоп можно делать следующие действия:

- Менять браузеры, менять версии браузеров

- Менять шрифты в системе, разрешение экрана

лектор: - Набивать или импортировать куки(cookies)

- Плагины и расширения в браузере.

- Менять систему

лектор: Кстати о расширениях, напрмямую мерчи не могут видеть установленные в браузере расширения, однако они могут отправлять запрос браузеру типа "Установлено ли расширение с таким-то id". Таким образом мерчи могут детектить определенные расширения, такие как, например, CanvasDefender.

Вариант обхода этого - замена id расширения(гуглите) или просто НЕустановка оного в браузер.

лектор: Ну и конечно не используем одни и теже переменные при нескольких вбивах, например эмейлы.

лектор: При проверке местоположения ip(геолокации) старайтесь не ориентироваться на whoer.net - там стоит устаревшая maxmind geo база, используйте сайты ip-score и maxmind.

лектор: Несколько сайтов от себя для проверки системы и ip:

whatleaks.com - чек всего, включая timezone

2ip.ru/privacy - чек портов, двустороннего пинга, хостинг провайдера и прочего

whoer.net - поменьше посещяйте этот сайт, очень задрочен, абсолютно все мерчи среднего и выше уровней крайне негативно относятся к кукам этого сайта + в отдельных случаях посещение этого сайта вгонит ip сокса / ssh в maxmind fraud chek базу.

<https://www.maxmind.com/en/home?rId=iplocation> - геолокация айпи непосредственно от максмайнд. Конечно точность платной и бесплатной базы разнится, но на моей практике в 75% случаев стоит доверять именно этому сайту.

browserleaks.com

ip-score.com

noc.to

Скопируйте себе этот список сайтов

лектор: Где хранить, как выводить заработанные деньги?

Конечно bitcoin!

лектор: Рекомендуемые кошельки:

<https://blockchain.info/ru/wallet/>

bitcoin core

лектор: Лично я использую первый. На форуме в разделе "Криптовалюта" можно найти списки кошельков и самостоятельно изучить, выбрать, что Вам больше подходит. Не стоит хранить деньги в биткоин постоянно, так как курс может как возрасти, так и упасть. Поэтому оценивайте свои риски и желания самостоятельно.

лектор: Qiwi - принимают к оплате не все, но как один из вариантов, возможно.

Плюсы киви: Возможность прямого вывода на карту, если не светить номер телефона, угнать практически невозможно

лектор: Минусы: могут заблокировать кошелёк, русская платежная система, а значит выдаст любые данные по первому требованию, следовательно убедительно рекомендую если и использовать киви, то только в следующем формате:

лектор: - Левая сим карта, возможно виртуальная

- Левый эмейл

- Переводить деньги по-возможности киви-ваучерами(яйцами)

лектор: - Не использовать свой телефон, купите левый или используйте виртуальную сим.

- Вывод только на карту дропа.

- Не использовать свой ip и компьютер (можно виртуалку)

лектор: Варианты вывода денег из онлайна в реальную жизнь, если с киви все понятно, то с биткоином посложнее, а именно:

- Обменники. Через обменник можно обменять деньги с биткоин на карту или киви, или банк.

лектор: - Вывод сразу в НАЛ. Есть обменники, которые предоставляют такую услугу.

- <https://localbitcoins.net> - своего рода обменник, ищете менял с хорошими отзывами.

лектор: То, что биткоин анонимен - миф и заблуждение, все транзакции в блокчейне как на ладоне, их несложно отследить, просто для регистрации не нужны никакие личные данные. Поэтому для сохранения анонимности средств рекомендую пользоваться биткоин-миксерами. (смотрим форум, раздел Криптовалюта)

лектор: Кроме онлайн безопасности есть еще и офлайн, смею порекомендовать свою статью на эту тему:

https://wwh-club.net/threads/ctatja-obratnaja-storona-luny.54525/

Карты

лектор: Всем привет сегодня лекция по CC -погнали

лектор: Каждый из вас так или иначе сталкивался в своей жизни с CC,но это было немного в другом "ключе"

лектор: Первое, что начинающий в этом деле должен изучить, так это конечно же информацию о кредитных картах, проще говоря картон / CC

лектор: Credit card (CC) - это кредитная карта,картон, картошка,и т.д

лектор: Первым делом нам нужно найти картон. Самый простой вариант это купить его у продавца

лектор: При покупки вы получите картон примерно в таком формате:4306651004564350 | 10/10 | 826 | Richard Lang | 56 Groveview Cir | Rochester | 14612| NY | USA | 661-298-0881

(Формат у каждого продавца бывает разным)

лектор: 4306651004564350 - Номер кредитной карты.

10/10 (10 месяц / 10 год,) - Дата окончания действия карты.

826 - Защитный код карты CVV/CVV2

Richard Lang – First и Last Name (Имя, Фамилия)

56 Groveview Cir – Адрес

Rochester – Город

14612 – Zip code (зип)

NY (New York) – Штат

USA – Страна

661-298-0881 - Телефон

лектор: BIN - bank Identification Number - первые 6 цифр в номере кредитной карты, индификатор банка который выдал карту

лектор: каждая банковская организация имеет собственный уникальный номер. Информацию по каждой карте вы можете найти в сервисах через поиск. Делаем запрос в гугле, bin check и далее переходим по ссылкам и вводим наши первые 6 цифр

лектор: Например карта 4306651004564350, где 430665 - номер банка который выдал карту

лектор: 10/10 - exp (срок действия карты) 09 месяц 10 год

лектор: 826 - cvv (секретный код)

лектор: Richard Lang - имя хранителя карты (cardholder name)

лектор: 56 Groveview Cir - улица (street)

лектор: Rochester - город (city)

лектор: NY - штат (state)

лектор: 14612 - зип код (zip code)

лектор: US - страна (coutry)

лектор: 661-298-0881- PHONE NUMBER (Телефон)

лектор: К USA CC еще можно добавить SSN, DL, MMN, DOB(эту информацию вы будете изучать на других лекциях)

лектор: За дополнительные $ вы можете пробить дополнительную информацию:DOB - дата рождения SSN - номер социального страхования MMN - Mothers Middle Name (отчество матери, так сказать)

лектор: поговорим о видах CC

лектор: чаще всего используються Visa,MasterCard,American Express,Discover

лектор: Номера кредиток Visa начинаются с цифры 4

у них имеется защита под названием Verified by Visa (VBV)

3х значный CVV код

лектор: Verified by Visa(VBV) - используются для защиты номеров карт Visa от несанкционированного использования. Проще говоря у холдера есть код который он должен будет ввести при покупки чего либо

лектор: Номера кредиток MasterCard начинаются с цифры 5

у них защита под названием MasterCard SecureCode (MCSC)

3х значный CVV код

MasterCard SecureCode - принцип работы тот же, что и у VBV

лектор: American Express начинаются с цифры 3

имеют уже 4х значный CVV код

лектор: Discover начинаются с цифры 6

3х значный CVV код

лектор: далее речь пойдет о типах и уровнях CC

имеються 3 типа карт ,кредитная,дебетовая,предоплаченная

лектор: кредитная (credit) -карта, на которую можно покупать в кредит, т.е. не имея на счете достаточно денег. Размер кредита определяет банк-эмитент

лектор: дебетовая(debet) карта, пользоваться которой можно только в пределе имеющейся на счету суммы

лектор: предоплаченная(prepaid) карта с предварительно оплаченной суммой - смарт-карта, в которой хранятся электронные деньги, заранее оплаченные владельцем карты

лектор: предоплаченная карта не персонализирована, то есть на ней не будет указано имени и фамилии владельца,это главный конек предоплаченных банковских карт

ею можно расплачиваться как в реальных, так и в интернет-магазинах. Лимит карты ограничен только лишь суммой которая на ней находиться

лектор: По уровням карт пройдемся , от классики до black. Чем выше категория карты, тем больше у нее стоимость обслуживания, и тем более богаче ее владельцы, тем более на ней может находится денег

лектор: Существуют карты классической категории, золотой, платиновой и более высокие карты, как например, MasterCard Black Edition или Visa Black. С повышением категории карты растут кредитные лимиты на ней. К примеру кредитный лимит по карте классик может составлять 1к$, так на кредитке уровня платинум кредитный лимит может составлять 10к$+

лектор: Для работы я советую брать кредитные и дебетовые карты от уровня голд и выше, а именно распрастраненные голд, платинум, сигнатуре, ворлд, блек. Последнюю встретить вероятность мала. В сша их не выдают как у нас тиньковы и тд

лектор: Каждая кредитная компания (American Express, MasterCard и Visa) называет свои кредитные карты более высокого уровня немного по-другому

лектор: У Американ Экспресс это BLACK| Карта позиционируется как символ принадлежности держателя к верхушке общества и может быть выпущена только человеку, имеющему соответствующий общественный статус

у MasterCard это World Signia| Кредитная карта высшей категории в линейке продуктов от MasterCard с личной подписью владельца «золотом» на лицевой стороне

у Visa это Black Card -такой уровень имеет повышенный уровень безопасности, предотвращающий возможность несанкционированного доступа к денежным средствам

лектор: самыми премиальными CC,что перечислены выше владеет особая каста людей на планете они же "массоны"шутка,этот уровень имеет более высокие кредитные лимиты и отсутствуют какие либо лимиты на расходы,такие карты очень сложно найти и стоить они будут очень дорого,они скорей для профи только

лектор: далее поговорим о о том как проходит оплата с CC

лектор: Процесс оплаты кредитной картой в интернете не такой простой как кажется на первый взгляд

лектор: в то время как вы нажимаете кнопку конфирм(confirm) и ней происходит куча процессов. Отвечает за эти процессы, процессинговый центр банка

лектор: Процессинговый центр — это высокотехнологичная система обработки платежей по банковским картам в сфере электронной коммерции

лектор: основная задача процессингового центра — предоставить шопам возможность принимать платежи по кредитным картам

лектор: Кроме того процессинговый центр координирует расчеты между банком-эмитентом карты, банком-эквайером (осуществляющим авторизацию транзакций), шопом и кард холдером

лектор: Банк-эквайер – банк, предоставляющий магазину услуги по обработке карточных платежей

лектор: Банк-эмитент — банк выпустивший карту, которой покупатель пытается оплатить товар

лектор: Процесс оплаты товара/услуги по кредитной карте выглядит так: вы оформляете заказ на сайте шопа и выбирает оплату с помощью кредитной карты

лектор: шоп переадресует покупателя на защищенную форму оплаты процессингового центра,на защищенной форме оплаты вы указываете информацию о кредитной карте

процессинговый центр подтверждает статус и параметры шопа в системе

а также осуществляет проверку сформированного запроса на соответствие установленным требованиям и системным ограничениям и передает сформированный запрос на авторизацию в банк эквайер

осуществляющий проведение авторизации по платежу, получив запрос на авторизацию транзакции, банк эквайер

направляет его в соответствующую платежную систему (Visa, MasterCard и т. д.)

лектор: платежная система определяет банк-эмитент, которым была выпущена кредитная карта, после чего направляет запрос на авторизацию в процессинговый центр банка

лектор: После того, как банк-эмитент подтвердил авторизацию платежа, процессинговый центр передает магазину положительный результат авторизации

лектор: а тот в свою очередь уведомляет вас об успешной оплате заказа. Вот такой вот сложный процесс происходит после того как вы нажали на кнопку оплатить

лектор: Что в свою очередь делает шоп, когда принимает оплату?

лектор: когда все пункты описаные выше прошли успешно и вы видите что оплата принята, шоп берет ордер в обработку

Обработка состоит из ручной проверки ордера, уточнение деталей ордера адреса шипа(не всегда), при уточнении деталей шоп делает звонок на указаный номер в ордере для подтверждения ордера

лектор: Именно по этому желательно писать номер на который вы сможете принять звонок

лектор: После уточнения всех деталей шоп начинает готовить товар для доставки

лектор: Если вы вбиваете егифт то доставка осуществляется сразу после проверки, если вы вбиваете стафф то могут отправить его как в тот же день, так и на следующий

лектор: Вбивать стафф не стоит в пятницу, так как передача стаффа в доставку будет осуществлена только в понедельник

лектор: После передачи стаффа в доставку, вам по почте или в личном кабинете магазина приходит трекинг намбер(tracking number)

лектор: Как правило это набор букв и цифр по которому вы можете отследить где находится ваш товар

лектор: Далее вы просто следите за вашим товаром по трекинг номеру и радуетесь когда он доставлен, но может быть такое когда кард холдер видит что деньги сняты с карты, в таком случае он звонит в банк

лектор: Тот в свою очередь делает звонок в магазин и сообщает что покупка была совершена мошейническим путем

лектор: В трекинг номере в таком случае будет написано что отправитель запросил возврат товара. В таком случае не стоит огорчаться и попробовать вбить новый ордер с новой CC и вам непременно повезет!

лектор: далее речь пойдет о том какие меры предпринимает шоп, когда идет оплата с CC

лектор: В магазине так же идет проверка ордера системой антифрода,чтобы исключить всемозможные мошейнические манипуляции с банковскими картами

лектор: Антифрод представляет из себя систему которая анализирует ваши действия в интернете на предмет мошейничества

лектор: за многие годы в у него сформировался портрет мошейнических действий и действий настоящих владельцев карт

лектор: система начинает вас анализировать с самого первого момента,как только вы зашли на сайт

лектор: она смотрит зашли ли вы с браузера или же с мобильного приложения,смотрит что вы покупали,когда покупали ,как часто покупали

лектор: смотрит на ваш ip адрес,cookie, включающие идентификатор http-сессии, и т.д.

лектор: объединяет всю эту информацию и анализирует ее с действиями холдера

Ваша задача максимально подстраиваться под кард холдеров, для этого нужно прогреть шоп, об этом я расскажу на следующей лекции,которя будет в четверг 15 февраля

лектор: после прогрева шопа трепетно набирать все данные, вы тратите свою месячную зарплату на покупку дорогущего ноутбука

лектор: Врятли шоп поверит что вы так просто зашли и потратили месячную зп рядового американца

лектор: Как правило если вас спалили то вам сразу не дадут оплатить товар. Отчаиваться и выкидывать CC в этом

случае не стоит так как информация может не дошла до банка и вас заблокировали на уровне шопа

лектор: В таком случае пишем/звоним в шоп и говорим что я пытался купить у вас ноут но что то не получилось

лектор: Не забывайте, вы американец который давно хотел купить ноут но вам этого не дали

лектор: В шопе вам скажут почему вы не можете сделать ордер. Будь то вы не прошли антифрод систему шопа, или же банк заблокировал вашу транзакцию

лектор: В первом случае можно узнать как же вам все таки сделать ордер, вам предложат варианты решения, выбирать вам

лектор: Если же заблокировал банк то легче выкинуть сс чем осуществлять звонок в банк, так как там очень жесткая идентификация которую не пройти.

Посреды

лектор: Всем привет

лектор: Сегодняшняя лекция будет состоять из 2х частей: посреды и дропы

лектор: 1 часть Посреды

лектор: Посред это – логистическая компания, занимающаяся доставкой товаров из одной страны в другую. Посред используется в 2х случаях: когда у шопа нет международной доставки, и когда просто хотите сделать консолидацию паков.

лектор: Посреды созданы не для нас кардеров, а для обычных людей, которые хотят заказать какой то товар с США

лектор: К примеру вещи из гепа и других магазинов, у которых нет доставки в другие страны кроме как США.

лектор: Посреды так же есть в европпе, но используются не так часто.

лектор: Консолидация паков – это процесс объединения нескольких посылок в одну, для снижения стоимости доставки. Условия консолидации нужно уточнять у посредов, прочитав соответствующие разделы сайта.

лектор: На сегодняшний момент, очень много посредов задрочены, поэтому надо искать своего посреда

лектор: Как же найти «своего посреда»

лектор: Своего посреда можно найти только экспериментальным путем, присылая туда паки, и смотря на реакцию посреда. Приведу основные моменты, на которые нужно обращаться внимание.

лектор: 1. Вбивать поэтапно. Сделали 1-2 вбива, дождались доставки, посмотрели, как отреагировал посред. Выслали себе.

лектор: 2. Использовать разные виды вбивов для разных акков. То есть, на 1 акк посреда вбиваем с CC, на второй с e-гифта, на 3й акк посреда вбиваем с палки и тд. Делается для того, чтобы понять что нравится посреду, а что нет. Потому что одни посреды спокойно принимают паки, вбитые с CC, другие могут локнуть акк за такое. Кто-то из посредов с

удовольствием принимает паки, вбитые с е-гифтов, а кто-то нет. Поэтому очень важно завести на первом этапе несколько акков, и когда какой-то из-за аккаунтов локнут, будете знать за что.

лектор: 3. Избегать посредов, требующих к оплате кредитные карты или денежные переводы. Лично я отдаю предпочтение посредам, принимающим оплату с БТС или пейпала. Зачастую бывает так, что при оплате посреда "своей картой", с этой же карты должен быть сделан и стаф - что невозможно. За денежные переводы тут понятно. Это палево. Таких посредов лучше сразу обойти стороной.

лектор: 4. Обращать особое внимание на тарифы посреда (принятие, хранение, пересыл). Бывает такое, что принятие пака бесплатное, а стоимость за хранение пака, начинает начисляться на следующий день. Либо же наоборот - Принятие платное и дорогое, и хранение бесплатное. Нам лучше всего подходит посред, где принятие пака бесплатно и бесплатный срок хранения составляет от 30 до 60 дней.

лектор: 5. Внимательно изучить правила посреда по принятию паков. Обычно пишут с чего принимают, а с чего нет, и какие документы требуются во время получения и во время отправки паков.

лектор: Нашли подходящего по условиям посреда, переходим к регистрации и получения адреса.

лектор: Посреды бывают с личным кабинетом, и без.

лектор: На посредах с личным кабинетом, идентификация пака происходит по личному номеру, обычно он написан в адресе и при доставке вам нужно писать этот номер.

лектор: Соответственно продавец видит что это большие цифры, и то что это посредник

лектор: Оптимальным в таком случае будет написать это как номер офиса к примеру.

лектор: Второй тип посредов, которые не требуют регистрации.

лектор: Там просто написан адрес склада без всяких личных номеров.

лектор: В таком случае идентификация пака происходит по Имени и Фамилии на паке.

лектор: Итак, как же нам зарегестрировать посредника?

лектор: Первое что нужно, но не обязательно купить комплект документов.

лектор: Я обычно этого не делаю, потому что мой посредник никогда не требует этого

лектор: Но лучше это сделать.

лектор: Что входит в комплект документов.

лектор: Паспорт, основная страница и страница с регистрацией, снилс, документы подтверждающие адрес вашего проживания, обычно счета за услуги ЖКХ.

лектор: Найти того кто отрисовывает это довольно таки сложно, но когда у вас зависнет на посреде пак, то пукан начинает подгорать

лектор: Дальше, опять же в качестве рекомендации завести ВПС той страны куда будет шип, и выполнять все манипуляции с посредом с этого дедика.

лектор: Опять же, я этого не делаю, захожу на посреда прямо с ВПНА юсы, с разных айпишников и все хорошо.

лектор: Итак, регнулись мы на посреде, что мы видим в первую очередь?

лектор: Как правило у посредов несколько адресов на территории США

лектор: Склады в Нью Джерси, склады в Делавере, иногда в Калифорнии

лектор: Лучше слать в Делавер.

лектор: Этот штат является безналоговым и доплачивать за товар не придется.

лектор: Получили адрес. Адрес будет вида:

лектор: Имя Фамилия

600 Markley St. Suite 107451

Port Reading, NJ 07064

лектор: Итак, первая строка понятно, при оформлении заказа в интернет магазине Имя пишем в First Name

лектор: Фамилию в Last Name

лектор: В Adress line 1 пишем

лектор: 600 Markley St.

лектор: В адрес лайн 2 пишем

лектор: Suite 107451

лектор: Собственно это мой редактированный адрес, суите это офис, цифры после него это личный идентификатор на посреде.

лектор: Port Reading это город

лектор: NJ - Нью джерси штат

лектор: последние 5 цифр это зип

лектор: Во многих посредниках есть кнопка добавить заказ

лектор: Это значит что если вы получили трек от продавца, то можно добавить пак в личный кабинет. Это ускорит обработку пака посредом.

лектор: Дальше советы по работе с посредами.

лектор: 1. Не слать сразу после регистрации аккаунта миллион паков. Отлежите недельку, лучше 2. Вышлите 1-2 пака за недельку. И постепенно увеличивайте количество. Здесь работает правило раскачки, как и во многих других темах. Ни один нормальный человек не будет за неделю слать на аккаунт 10 айфонов, 25 штук плейстейшнов, и еще столько же часов. Обратите на это особое внимание.

лектор: 2. Четко изучить правила работы посредов, это позволит избежать потери паков. Прочитайте страницы FAQ или правила приема и пересыла посылок - у вас сразу

отпадет большая часть вопросов, и сэкономите кучу времени.

лектор: 3. Не перегружать посреда дорогими паками. Лучше завести несколько акков, и слать на каждый по немногу. Ни один нормальный человек не будет покупать себе 10 айфонов за 10 дней. Помните об этом. Посред эта таже контора, которую мы нагибаем, поэтому вести себя должны соответствующе.

лектор: 4. Не использовать посреда, для вбива дорогой техники, лучше использовать дропа. Так вы не убьете аккаунт, в случае чарджа. По статистике посреды убиваются либо тонной копеечного стафа, либо дорогим. Акки, которые принимают товары средней ценовой категории, на опыте живут дольше всего.

лектор: 5. При вбиве указывать скайп номер телефона или ГВ. Не стоить писать номер телефона посреда или холдера. То есть в графе шиппинг адрес - пишем либо номер ГВ (гугл войс), либо скайп. Так мы снижаем палевность наших действий, и всегда можем принять звонок, либо просто узнать о том что он был.

лектор: Рекомендации к пересылу товаров себе: 1. Не превышать таможенного лимита (для России) 1000 EUR или 1200 USD в месяц - на один пак. То есть если вы указали что стафа в паке на 1200 баксов, то в этом месяце на тоже имя вы уже не сможете выслать пак. Он встрянет на таможне, и в итоге придет с таможенным уведомлением, все что свыше лимита, придется платить 35% от стоимости. В связи с поледними событиями, в 80% случаев для отправки

паков в РУ - посреды просят ИНН / СНИЛС получателя, поэтому я и говорил о покупке полного комплекта документов. Но так как Мы не знаем в скольких руках они могут быть - то самое лучшее это договориться с соседом алкашем что он будет принимать ваши паки, и взять с него все доки. Поверьте за бутылку хорошего вискаря - он все сделает)

лектор: Продолжаем

лектор: 2. Всегда занижать стоимость товаров на шмотки. Например если вы шлете кроссовки найк за 300 баксов, пишите что кроссовки НАЙФАЙ и указываете стоимость 30-40 баксов. Я всегда так делаю. То же касается и сумок, штанов, вообщем всей вещевухи. Всегда прокатывает. Потому что возиться и устанавливать четкую стоимость вещевухи никто не будет. Только не нужно писать что шмотки фейк или реплика, такие категории товаров очень жестко регламентированы к ввозу в таможенный союз + 90% посредов такое тоже не любят. Поэтому лучше написать несуществующий бренд, или найти в интернете кросовки на эту сумму и написать что это они.

лектор: 3. Что касается часов – просим раздербанить коробку, и выслать часы отдельно, коробку отдельно. Но лучше всего часы слать вкупе с остальным стафом. Когда в паке 10-15-20 позиций, по моему опыту такие паки намного легче проходят таможню, чем когда в паке 1-2 позиции.

лектор: 4. Что касается ювелирки – пишем что это бижутерия. И по многу класть в пак не следует. Лучше выслать цепочку отдельно, кольцо отдельно. Рекомендую

слать ювелирку с кучей шмоток, меньше шансов что спалит таможня. Хотя все равно драг металлы хорошо палятся рентгенами. поэтому лучше не наглеть, не шлите 15 киллограмовый пак, с содержанием золота на 1кг - 100% не пройдет таможню)

лектор: 5. Технику высылать по 2-3 позиции в паке. Например 1 айфон + 1 PSP + 1 видеокарта. Не нужно в 1 пак напихивать по 10 позиций всех товаров. Помните, что если одинаковых позиций в паке от 5 и больше, то попадете под коммерческую партию, и тогда потеряете пак. Так как запросят накладные, выписки со счетов и тд. Поэтому я всегда технику закидываю свитерочками, курточками, штанишками. Чем больше всякой фигни - тем лучше. Это мой опыт, Вам такое может не подойти, но все таки попробуйте.

лектор: 6. Не копить паки на посреде, особенно ценные. Пришел айфон / айпад / ролекс на посреда – сразу высылайте. Лучше заплатить лишние 60 баксов за доставку, чем потерять все. То есть вбивая на посреда, смотрите на дату доставки, и прикидывайте примерные сроки. Вбиваете например айфон, шиппинг 3-5 дней, значит в следующую среду будет на посреде, соответственно, сегодня вбили еще пару вещей, с таким же шиппингом. В следующую среду - четверг стаф пришел, например 5 позиций чего-то - все, нажали кнопочку отправить пак, оплатили - ждем. Не надо паки собираться месяцами... к хорошему не приведет.

лектор: 7. Оплачивать посреда только своими деньгами. НИКАКОГО КАРЖА. Не пилите ветку, на которой сидите. Сделали акк палки или же ВСС киви, закинули денег на СС

- оплатили. От 50-100 баксов, наш кошелек худее не станет, и акк будет служить Вам очень долгое время. Лично мой акк на посреде живет уже год и 2 месяца, и все хорошо, все прекрасно.

лектор: Полезные ссылки:

лектор: Список посредов для ознакомелния: http://wwh-club.net/threads/5-2-dostavka-pakov-i-spisok-286-posrednikov-v-19-stranax-mira.2140/

Сканы документов: http://wwh-club.net/threads/prodam-skany-pasportov-i-foto-s-pasportom-v-rukax.308/

лектор: Так же советую использовать для приема паков в ру дропов.

лектор: На форуме есть человек paydrop, принимает паки в ростове на дону, и стоимость приема как правило 800-1к руб

лектор: Гораздо надежнне, но и дороже соседа алкаша.

лектор: Итак, по посредам закончили.

лектор: Дальше идут дропы

лектор: Дропы – это обычные люди, которые принимают Ваши паки. Дропы бывают 2х видов: разводные и неразводные.

лектор: Разводные дропы – это дропы, которые не знают, что принимают карж посылки. Всегда существует возможность пропажи дропа с посылками. Такие дропы ищутся например на джоб сайтах или подобных конторах. Обычно на таких дропов не высылают дорогие паки. Срок

жизни таких дропов составляет 10-15 дней. Стоимость принятия посылок такими дропами обычно 50-70 баксов.

лектор: Неразводные дропы – вид дропов, которые четко осознают на какие риски идут. Риск потери паков сведен к минимуму. Такие дропы получают хорошую зарплату и срок жизни дропов в среднем 2-3 месяца. Однако, у них чаще всего несколько другие правила работы. Подробнее о правилах можно узнать у дроп сервисов, предоставляющих услуги дропов. Стоимость приема обычно 70-100 долларов либо % от стоимости пака.

лектор: Последнее время дроп-сервисы стали работать на скуп, то есть принимают пак – выплачивают Вам ваш %. У разных дроп сервисов – разные виды товара под прием и соответственно разный %. За ликвид технику эпл – могут дать до 55%. Вбив стафа на скуп – избавит вас от проблемы с доставкой товара в РУ и его продажей, и поможет намного быстрее заработать. Однако сумма заработка будет намного ниже, чем если бы вы привезли стаф себе и продали в РУ.

лектор: Если выслали товар на скуп, с момента отправки пака на дропа, до получения выплаты в среднем проходит неделя. А если высылаете товар на посреда и хотите продать в РУ – в среднем потребуется 4-5 недель. Тут уже Вам решать, быстро и мало, или долго и побольше.

лектор: Как только дропы получают пак, для отправки на посреда, дроп сервису требуется лейбл.

лектор: Лейбл – это подобие почтового бланка. То есть бумажка, в которой написано от кого выслано, с какого

адреса идет, кому адресовано и на какой адрес. Такие лейблы можно заказать на форуме у соответствующих продавцов. Обынчо карж лейбл стоит около 5-10 баксов, если лейбл белый, цена может достигать и 500 долларов. Чаще всего белые лейблы используются для отправки паков сразу в РУ, дабы обеспечить безопастное прохождение паков по всем инстанциям.

лектор: Пример лейбла можно посмотреть тут: http://prntscr.com/iekzf5

лектор: 1 – ФИО отправителя

2 –Улица отправителя

3 – Город / Штат / Индекс отправителя

4 – ФИО получателя

5 – Улица получателя

6 - Город / Штат / Индекс получателя

7 – Дата отправки

8 – Вес посылки

9 – Дата доставки

10 – Трек номер посылки.

Прогрев шопов.

лектор: всем привет

лектор: Я хотел бы свою лекцию подразделить на 3 основные части:

1. Я расскажу вам о прогреве шопов.

2. Расскажу вам о прозвонах шопов для верификации заказов.

3. Расскажу вам немного про реруты.

лектор: Начнём с того, что дадим определение, что такое прогрев шопов. Прогрев, это звонок в шоп перед заказом, целью которого является расположить к себе сапов и соответственно повысить шансы на отправку пака.

лектор: прогревы осуществляются в основном двумя путями :1. Через прозвон. 2. Общение в лайв чате. ну либо самый деревянный способ на мой взгляд-через имейл

лектор: начнём с лайфа

лектор: вообще я считаю что это не самый эффективный способ, но всё же имеет место быть

лектор: во-первых, по причине того, что сапы не общаются с вами вживую, они не слышат вас и не могут понять кто сидит на другом конце, поэтому вы не вызываете у них повышенного доверия

лектор: во-вторых, лайв чаты обычно есть только в более менее крупных шопах, где ваш разговор просто затеряется среди сотен других и никакого внимания к себе вы не привлечёте

лектор: лайв чат хорош, когда вам нужно что-то проверить в заказе, но вы не может прозвонить или не хотите отдавать деньги за прозвон, ну либо если вы действительно хотите узнать что-то конкретное о товаре, но для прогрева не очень

эффективен(по крайней мере ,по моей практике сложно судить об этом мне)

лектор: кроме того, если у вас не очень высокий уровень англ языка, это с вами может сыграть злую шутку, так как некоторые сапы могут обращать внимание на ваше написание текста, на вашу грамотность и соблюдение правил грамматики,условно говоря ,если вы делаете заказ от какого-нибудь John Jones, а пишите фразами типа I am don't know , то вы как минимум смутите агента

лектор: так что не рекомендую по гугл переводчику составлять письма или общаться с сапами, если не уверены в своих силах

лектор: далее расскажу про более эффективный метод прогрева

лектор: прогрев по телефону

лектор: здесь тоже есть свои нюансы

допустим прогрев крупных магазинов, где сидят десятки/сотни сапов, на мой взгляд не очень эффективный. в таком случае лучше запрашивать звонок после самого вбива, так как сап сможет сделать пометки о том, что звонил покупатель и интересовался статусом заказа

лектор: если вы сделаете это до заказа, то сапу просто некуда будет делать заметки

лектор: и это может вам помочь ускорить обработку вашего заказа, однако возможновас попросят позвонить ещё раз, для верификации

лектор: то есть такой звонок для разогрева не заменяет звонок для верификации, если такой потребуется

лектор: далее расскажу про прогрев маленьких шопов

лектор: прогревы таких шопов, я обычно делю на 2 вида

лектор: 1. Прикидываюсь шлангом и задаю кучу вопросов сапу.

лектор: это подходит, например, для прозвонов небольших шопов с электроникой/шмотками, можно расспрашивать характеристики того или иного товара

лектор: спрашивать наличие характеристики и т.д

лектор: задать вопросы про скорость доставки и тд

лектор: грубо говоря, мы просто прикидываемся типичным американским потребителем

лектор: особенно хорошо это сработает в шопах, где сап с которым вы беседуете и будет отвечать за отправку товара и обработку заказа

лектор: 2. Второй случай несколько сложнее

лектор: Этот случай имеет отношение к магазинам, продающим что-то специализированное, например музыкальные инструменты, профессиональное оборудование, автозапчасти.

лектор: здесь важно понимать специфику товара, его предназначение, иначе прогрев смысла иметь не будет, а то вы посыпетесь

лектор: Если вы покупаете запчасти, важно понимать для чего она и для какой марки.

лектор: Я часто прозваниваю шоп с музыкальными инструментами, особенно гитары,

так как я в этом неплохо понимаю, это играет хорошую роль, ибо сап при общении со мной начинает доверять и соответственно быстрее и охотнее процессит заказ.

лектор: Так же хочу затронуть тему прогрева шопов для отправки на разный бил/шип

лектор: американцы очень отзывчивые люди и на этой отзывчивости можно сыграть, чтобы придумать легенду для отправки на разный бил-шип

лектор: не пытайтесь пропихнуть легенду, о том , что вы шлёте посылку к маме/папе/брату пока вы у них в гостях, это всё ерунда, которая вам не поможет

лектор: в штатах очень часто случаются катаклизмы, в основном на юге

лектор: на этом и стоит играть

лектор: поэтому, иногда для составления легенды, я использую эти события, для вызова доверия к себе

например происходят очередные ураганы в луизиане, или флориде или алабаме, да в любом месте

лектор: и допустим у нас как раз есть сс с тех мест

лектор: а шипнуть надо например в орегон или вашингтон

лектор: если объяснить сапу, что вы спасаясь от ураганов и ливней уехали в родственникам на другой конец страны и не взяли что-то жизненно необходимое и теперь пытаетесь это купить, то ваши шансы на отправку товара возрастают в разы

лектор: если допустим ничего подобного не происходит в сша на данный момент, можно рассказать легенду о том, как термиты поели ваш дом, или как у вас завелись здоровые тараканы, которых вы только только отравили и теперь не можете вернутсья домой, так как там ещё не выветрилась вся эта дрянь

лектор: амеры очень сильно сопереживают в таких случаях

лектор: Забудьте о легендах про : уехал к родственникам, к маме и тд. это уже малоэффективно, чем сложнее и безнадёжнее ваша ситуация, тем больше шанс

лектор: подведу итоги по прогреву

лектор: Прогрев это всё равно не панацея, даже для маленьких шопов, поверьте в США не осталось ни 1 шопа наверное ,который бы не страдал от фрода, поэтому ко всем заказам шопы относятся очень и очень серьёзно, потому не удивляйтесь если даже после прогрева, вам будут отказывать в отправке, это номральный процесс, не все шопы ведутся на это, однако если грамотно подойти к разогреву, вы останетесь в + ,главное вам нащупать идеальную схему, по которой вы будете работать

лектор: Далее хотел бы вам рассказать о верификации ордеров

лектор: Очень часто, после вбива к вам будут приходить сообщения-позвоните нам для подтверждения покупки или что-то подобное

лектор: некоторые шопы, не хотя слать заказ, но боясь нарваться на реального холдера, говорят что они не смогли верифицировать детали сс с банком

лектор: я уверен в том, что некоторые шопы тупо опасаются слать ваш заказ, по каким-то причинам (фрод пометил ,айпи далеко от биллинга, айпи в блеке), но боятся случайно нарваться на реального кх, поэтому и пишут такую ахинею

лектор: несколько раз у меня поулчалось доставать такие паки

лектор: но 98% таких случаев заканчиваются не в вашу пользу

лектор: А в некоторых случаях действительно биллинг не совпадает

лектор: тут можно пытаться прозвонить в банк (предварительно, как минимум пробив доб и ссн, без этого даже не пытайтесь) и пытаться разрулить ситуацию с биллингом

лектор: но опять же, очень маловероятно что вы с банком что-то сможете решить, если вы не знаете какой там реальный биллинг(можно тыкнуть пальцем в небо пробив бг и посмотреть последний адерс кх, но это очень дорого и неоправданный риск)

лектор: но по факту-проще вбить в другое место и посмотреть что будет там

лектор: Теперь рассмотрим вопросы, которые спрашивают сапы для верифа

лектор: в основном сапы сверяют одно и тоже , мейл, 4 цифры cc, биллинг/шиппинг адрес

лектор: но могут задать вопросы с подковыркой

лектор: во многих шопах могут спросить вопрос с подковыркой, например, название и номер телефона поддержки вашего банка который написан сзади

лектор: или ближайшую улицу к вашему адресу (кстати рекомендую перед каждым звонком открыват адрес кх в гугл мэпс чтобы иметь возможность ответить). вообще вопросов с подковыркой может быть великое множество, всего не предусмотришь, однако, как минимум поиск адреса кх в гугл мэпс позволит вам ответить на многие вопросы, которые вас могут спросить

лектор: 1. Ф.И.О. Холдера:

2. Em@il Холдера:

3. Данные cc:

4. Биллинг (адрес холдера): -

5. Шиппинг (адрес доставки): -

6. SSN\DOB\Количество лет (если есть информация)

7. Сайт куда вбивали или куда нужно сделать ордер: -

8. Номер ордера:

9. Дата и время ордера:

10. Название товара (ссылка на товар)

10.(Для EGIFT) Имя получателя, мыло получателя (recipient): -

11. Сумма ордера:

12. Номер куда звонить:

13. Номер с которого звонить(если нужна подмена):

14. Название банка, выпустившего карту:

15. Телефон службы поддержки банка (если нужно прозвонить банк, индивидуально)

16. Письмо с конторы, куда и по какому поводу звоним (ссылка на фото): -

17. Причина и цель звонка, описание Вашей ситуации: -

лектор: вот форма для прозвона, сохраните её себе и заполняйте инфу по ней, не ленитесь, вам же лучше от этого

лектор: так же часто спрашивают вопрос как лучше звонить, с подменой или разницы неТ?

лектор: считаю что лучше звонить с подменой, это вызывает больше доверия к вам

лектор: для некоторых шопов это обязательное требование-звонок с биллинг номеа кх

лектор: Ну и в заключении хотел бы немного рассказать вам о реруте

лектор: рерут/редирект-это смена адреса на посылке, на адрес дропа/посреда

лектор: как его делать рассказывать не буду, но расскажу немного технической составляющей

лектор: начну с рерута юпс. при реруте юпс, запрос на измнение ареса виден сразу, в течении 5-10 минут трек перекрашивается в жёлтый цвет и вы видите фразу : Запрос на изменение адреса доставки, но радоваться этому пока рано, шоп может вполне быстро развернуть посылку назад и вы уже с ней ничего сделать не сможете(запрос на возврат всегда стоит выше других и отменить его нельзя)

лектор: с рерутом федекса несколько сложнее

лектор: в феде запрос на рерут отображается только в городе кх

лектор: и бывает разных типов-1. надпись: запрос изменения доставки

лектор: тут в целом всё ясно, пак после этого повернётся и поедет куда надо

лектор: иногда трек горит красным и выдаёт вам-требуется действие, по большей мере это особенности феди и эта надпись исчезнет через несколько часов

лектор: вам выдадут новый трек

новый трек может отображаться как трек на возврат товара и висеть прямо на сайте, если увидели его, тыкните на него и посомтрите место назначения, если оно совпадает с местоположением дропа(иногда может быть другой город, но тот же штат, тогда чекните в гугл картах расположение городов, это скорее всего будет тот же город прсото другая его часть)

лектор: либо новый трек придётся втаскивать звонком , если пак не движется уже некоторое время, обратитесь к прозвону или позвоните сами в почту, вам выдадут новый трек

Антидетекты

Браузер-антидетект нового поколения

Мы рады представить Вашему вниманию самый удобный и безопасный

инструмент для профессиональной работы в сети Интернет

Пожизненная скидка 5%-10 % на все лицензии

https://ls.tenebris.cc/registration?promocode=WWH2019

лектор: Приветствую всех, кто решил посетить лекцию по Антидетектам. Сегодня мы поговорим про различные антидетекты, которые хорошо зарекомендовали себя в нашей сфере работы, виды антидетектов, разберемся в некоторых тонкостях и особенностях работы с антидетектом при вбиве и не только.

лектор: Для начала разберемся с вами, что вообще такое в целом «Антидетект»? Антидетект – это решение (программа, браузер, плагин для браузера и.т.п.), которое позволяет обходить различные Антифрод системы в интернете, будь это онлайн банкинг, или же интернет-магазин или же клиент, установленный на компьютере для игры в покер. Антидетект позволяет использовать одну и ту же машину для работы, не меняя ее, путем обхода

различных детектов. Благодаря этому, Антифрод система каждый раз думает, что перед ней новый пользователь, или же, наоборот, тот же пользователь, в том случае если нам необходимо под кого то «закосить». Задача современных антидетектов это не просто уникализировать пользователя, а дать ему возможность слиться с толпой.

лектор: Объясню очень просто и доступно: в первом случае, если представить что Touch ID на Iphone –это антифрод система, и чтобы его разблокировать нужно каждый раз прикладывать НОВЫЙ палец, то благодаря антидетекту, мы можем сделать очень и очень много отпечатков пальцев, и каждый раз спокойно и успешно проходить эту защиту. Можно сказать, что антидетект - это как перчатка, которая позволяет одному пальцу оставлять огромное множество отпечатков. Во-втором случае ,если представить что Touch ID на Iphone –это антифрод система, и чтобы его разблокировать нужно каждый раз прикладывать один и тот же палец, что впринципе и соответвует действительности на Iphone, то мы можем «скопировать» палец владельца и успешно обойти защиту(естественно зная примерно как должен выглядеть этот отпечаток).

лектор: Следует понимать, что современные антифрод системы не стоят на месте и совершенствуются с каждым днем - если ранее для идентификации использовались самые простые методы, то на сегодняшний день оценивается целый ряд факторов.

лектор: В данном контексте антидетект выполняет очень важную роль, и при правильном использовании несомненно позволит вам получить результат, но успех не обеспечен

лишь одним фактом его использования - нужно правильно и осознанно подходить к работе в конкретном направлении, что придет только путем познания и приобретения опыта.

лектор: Вы можете посмотреть на то, какое огромное количество факторов учитывает современный антифрод на примере весьма распространенной системы Threatmetrix. Как видите, браузер играешь лишь одну из ролей, хотя и на фронте событий: (Посморите видео после лекции)

https://www.youtube.com/watch?v=2PQxoQQOPpY

лектор: Еще отличным примером для анализа АФ систем можно указать:

https://developers.seon.io/?shell#request

Советую посмотреть данный пример на досуге, особенное какое огромное количество параметров относится к E-mail, использованию e-mail адреса в других сервисах (Скриншот: http://prntscr.com/isj1yg) , номеру телефона и.т.д.

лектор: Антидетекты бывают двух видов: Железные Антидетекты и Браузерные. Разберем каждый из них поподробнее.

Железный антидетект позволяет подменить параметры железа компьютера или виртуальной машины. Как пример, можно привести: подмену информации о процессоре, видеокарте, биосе, сетевой плате и различных других устройств.

Железный антидетект может быть необходим при работе в сфере покера, казино и др. сферах, которые связаны с установкой клиентских программ под Windows.

лектор: Примером железных антидетектов могут служить:

1) CCTools 7(Многие слышали об этом софте, использовали, он уже давно неактуален, но в свое время сыграл немалую роль)

2) VirtualBox Hardened Loader- патч для железного антидетекта Virtual Box. Подробнее об этом рассказывает Vector T13 в своих вебинарах «Антидетект виртуальной машины» (Данные вебинары можно найти на YouTube) . Было хорошо актуально в конце 2016 года, хотя данное решение и сейчас имеет место быть.

лектор: 3) Также от Vector T13 вебинар по антидекту WmWare. К соожалению, вебинар только один, продолжения не последовало. Поэтому тема раскрыта далеко не полностью.

4) Antidetect 2018 Pro OpenSource by Vektor T13 – Новое бесплатное решение в области железного антидетекта от Вектора для Virtual Box. Данное решение актуально и поддерживается автором. К особенностям я бы выделил полноценную поддержку видеокарты на VirtualBox. Минус данного решения заключается одновременно и в его плюсе: решение бесплатное, следовательно, полноценной поддержки (бесплатно) по данному решению вы не получите.

лектор: 5) Aff combine – по сути первый железный антидетект VmWare, полностью актуальное и готовое решение в 2018 году. Включает также браузерный антидетект на основе браузера Mozilla Firefox. Продается у нас на форуме. Цена 1000$. Скидка клубням 20%.

Единственный ЖЕЛЕЗНЫЙ актуальный антидетект на форуме.

лектор: Браузерный антидетект - это программа, позволяющая эмулировать браузер на основе заданных параметров. Проще говоря, с помощью эмуляции различных параметров, мы можем имитировать любую систему (Windows, Linux, Android, IOS, MAC OS, Blackberry) и браузер (FireFox, Safari, Chrome, IE, Opera и Др.),а также даже игровые консоли (Playstation, Xbox).

Браузерные антидетекты бывают двух типов:

1 тип: Антидетект на основе обычного браузера с «вшитым» в него расширением (Chrome) или Addon'ом (Mozilla Firefox). В основном все антидетекты этого типа (Antidetect 7.1, Антидетект от Серта(Cert), Антидетект от Good Job, Fraudfox, Антидетект от Vector T_13)

лектор: Здесь Антидетекты можно поделить на еще две категории:

А) Антидетекты, использующие физический браузер Firefox. К этой категории относятся: Antidetect 7.1, Антидетект от Good Job, FraudFox, Антидетект от Vector T_13)

Б) Антидетекты, использующие физический браузер Chromuim. К этой категории относятся: Антидетект от Серта(Cert), Байтовский антидетект 8.

Антидетект на основе физического браузера Chromium намного сложнее, затратнее по вложениям и знаний

требуется больше, поэтому обычно цена на такие браузеры выше.

лектор: 2 тип: Антидетект, написанный на исходниках движка. Из тех примеров, что я знаю, сюда можно отнести Linken Sphere.

Антидетекты, написанные непосредственно с использованием исходников движка позволяют более глубоко подходить к вопросам реализации подмен.

Подробнее о существующих браузерных антидетектах, которые стоят нашего внимания:

лектор: Антидетект от Серта(Cert) – антидетект на основе Chromuim. Привязывается к железу, т.е. использовать можно только на 1 системе. Хорошо зарекомендовал себя, автор, Cert – один из самых первых разработчиков антидетекта в целом, а тем более на основе браузера Chromuim. Обновления не сильно часто, но стабильные. Продается на Верифе, стоит 5000$. Было время, когда пользовался этим антидетектом. Сейчас не имею и не использую. Как по мне цена продукта необоснованно высокая. Даже если бы имел свободных 5000$ - не взял бы его. Как по мне его цена в разы ниже. Каждое обновление также платное и стоит от 50 до 300$. Даже если пропустили какое-то обновление и не взяли, то придется оплатить все предыдущие обновления, чтобы получить последнюю версию. По моему мнению, с учетом имеющихся остальных антидетектов на рынке, брать новичку не стоит.

лектор: Байтовский антидетект 8 - антидетект на основе Chromuim. Автор продукта Байт, автор Antidecet 5,6,7,

которые хорошо зарекомендовали себя в свое время. Антидетект 8 – неизвестный продукт, всего 4 клиента. В его теме отзывов нет. Продается на Верифе, цена: 3000$ + 100$ в месяц абонентская плата. По моему мнению, с учетом имеющихся остальных антидетектов на рынке, брать новичку не стоит. Вроде как ничего сверхъестественного по сравнению с другими антидетектами на Chromuim там нет, а развивается продукт как то медленно.

FraudFox, Антидетект от Vector T_13 – выделил их в одну категорию так, как по сути FraudFox неактуальный антидетект, а антидетект Vector T_13 не особо годится для работы, слишком «сырой» и автор на него забил. Продукт Vector T_13 позиционируется как средство повышенной анонимности и не годится для работы (сам Vector T_13 так позиционирует его). Продукт бесплатный, каждый может скачать и ознакомиться с ним на сайте автора.

лектор: Антидетект от Good Job – антидетект на основе Firefox. Привязывается к железу, т.е. использовать можно только на 1 системе.Не частые обновы, судя по отзывам, автор ложит «мужской прибор» на клиентов и достучатся до него не так просто, а тем более получить поддержку по программе. Продается на верифе, полная лицензия стоит 2250$ + абонентская плата 200$ в месяц. Не использовал даже. Брать не стоит.

лектор: Теперь мы подошли к антидетектам, которые отличные по соотношению цена-качество, подходят новичкам, и которые стоит иметь в своем «арсенале»:

Linken Sphere (Сфера)- антидетект, написанный на исходниках движка Chromuim. Продается у нас на форуме. К плюсам можно отнести: Отличный саппорт, частые обновления, нет привязки к системе, подмена всех основных отпечатков, встроенный функционал для работы с ssh, socks и tor, собственный уникальный socks сервис, интегрированный в Антидетект, возможность вбивать сразу с нескольких вкладок, т.к. 1 вкладка как виртуальная машина, а таких вкладок можно открыть очень много и др. плюсы.

лектор: Минусы, как для новичка, будут: ежемесячная абонентская плата в 95$ (5% пожизненная скидка пользователем BBX), недоступен шоп с конфигурациями, т.е. конфиги; если нет PRO подписки (цена 475$), нет возможности полной настройки параметров windows.navigator . совокупность параметром позволяет рекомендовать его, сам также использую.

Поясню сразу, что такое конфиг. Конфиг – это код на javascript, который содержит информацию о браузере и системе(параметры javascript браузера, параметры WebGL, набор шрифтов и др.) По сути конфиг является слепком системы и браузера. Использование конфигов еще больше сокращает время, т.к. не нужно самому прописывать и придумывать все параметры, а просто загрузил конфиг, проредактировал, если нужно, и работаешь.

лектор: Конфиги бывают реальные и генерированные. Реальные – это те конфиги, которые «скопированы» с настоящих компьютеров, путем сбора параметров, а генерированные конфиги – это сделанные с помощью

программы (генератора). Минус генерированных конфигов заключается в том, что не всегда параметры могут быть верные и соответствовать ОС или браузеру или же вообще иметь значения, которые не свойственны реальной системе.

лектор: Antidetect 7.1 – антидетект на основе Firefox. Продает у нас на форуме Billy Bones. Цена по акции для обучающихся 50$. Иногда использую антидетект и по сегодняшний день. Продукт полностью стоит своих денег. Хороший вариант для новичка. Антидетект берется навсегда; нет абонентской платы и привязки к браузера к системе, т.е. вбивать можно и с основной машины, и с виртуалки, и с системы друга, соседа и.т.п.

Конфиги также можно приобрести сразу, без необходимости выполнения каких-либо условий. Antidetect 7.1 – позволяет более тонко настроить некоторые параметры, например в windows.navigator. К минусам можно отнести, что автор (Байт) забил на софт и обновлений не будет, антидетект не подменяет некоторые отпечатки, например audiofingerprint, webGL, некоторые конфиги требует ручной донастройки.

лектор: Любой антидетект сокращает затраты времени на вбив, т.к. не нужно париться насчет чистки куков в системе, настройки WebRTC в системе, установки, плагинов в браузер, шрифтов в системе и.т.п.

Также благодаря антидетектам, есть возможно подойти к шопу «с разных сторон», т.е. вбить в него с ОС Windows, Mac, с мобильного устройства и различных браузеров.

Иногда в определённые шопы или мерчи проходимость какой-либо ОС или браузера бывает выше.

Если смотреть со стороны денежных затрат на вбив, то по сравнению с VNC, дедиками, антидетект экономит еще и деньги. Конфиг стоит 1-3$+ носок (0.2-1$) или туннель (1-2$). Хороший же дедик обойдется от 10$(и то не факт, что в него НЕ вбивали в ваш шоп, особенно если он популярный, а также дедики часто «умирают», если они добыты с помощью брута); цена VNC же начинается от 20$.

лектор: НО!Вплане вбивов, антидетект не панацея и не кнопка бабло. Не стоит использовать только антидетекты. Бывают ситуации, когда вбив идет лучше с реальный устройств (мобильный телефон для вбива, ноутук/компьютер для вбива без виртуалок) . Поэтому советую «иметь в своем арсенале», настроенные виртуалки для вбивов, эмулятор мобильного устройства (Genymotion, Nox), реальное мобильное устройство для вбива, несколько антидетектов и.т.д.

Антидетект, помимо вбивов можно и нужно использовать для своей безопасности и анонимности в сети. Использование антидетекта в вашей цепочке безопасности осложняет вашу деаномизацию любыми спец. службами.

лектор: Советы по обеспечению вашей безопасности с помощью антидетектов:

Во-первых, использовать на разных форумах, сайтах, разные конфиги (разные ОС и разные браузеры)

Во-вторых, периодически (например раз в 3 недели) менять ОС или Браузер на каждом форуме и сайте.

В-третьих, хранить сам софт и браузеры, в которых встроены дополнения, расширения, на закриптованной флешке или жестком диске или контейнере.

лектор: Для антидетекта Linken Sphere (Сфера) можно добавить:

А) Не ставить галочку для запоминания пароля, а хранить его у себя в голове. Это нужно для того чтобы избежать попадания доступа к вашим кукам, сессиям, конфигам третьим лицам.

В) Использовать в цепочке подключения TOR или TOR+SSH TUNNEL. НЕ убирать галочку с параметра «Save and encrypt cookies before exit»

Для Antidetect 7.1 можно добавить, что после того как сам сгенерированный браузер станет не нужен для работы или вбива, его стоит незамедлительно удалять, а не скапливать огромное количество, т.к. каждый браузер занимается около 100 мг, и при большом количестве браузеров это все занимает немалое количество ГБ, плюс каждый браузер содержит историю, куки, что не будет плюсом при получении доступа к браузерам третьими лицами.

лектор: Теперь рассмотрим на практике работу с 2-мя антидетектами: Antidetect 7.1 и Linken Sphere (Сфера).

лектор: Antidetect 7.1

После покупки Antidetect 7.1 и конфигов для него (в идеале для новичка брать около 20 конфигов; для начала хватит с

головой, а если понадобится больше – всегда можно докупить), после установки и запуска антидетекта (насчет покупки, установки, запуска и настройки обращаться к @Billy Bones) перед вами откроется такое окно: Скриншот с пояснениями - https://prnt.sc/h2wovg

лектор: Пробежимся по каждому из пункту и по настройке:

Пункт «1» - Данная кнопка создает браузер, а точнее его Portable версию, в которую вшит Addon антидетекта. Браузер не имеет привязки к железу и с него можно работать на любой машине и передавать кому угодно, хоть партнеру, хоть соседу. Для того чтобы галочка загорелась и была активна, нужно выбрать любой ФИЗИЧЕСКИЙ браузер из контейнера (Цифра 5 на скриншоте)

Пункт «X» - Данная галочка определяет, будет ли вшит addon антидетекта в Portable браузер или нет. Если не будет галочки, то будет создан обычный portable Firefox той версии, которую вы выберете из контейнера (цифра 5)

лектор: Пункт «2» - Данная галочка отвечает за наличие Flash в браузере. По личному опыту скажу, лучше создавать браузере без Flash, использовать Flash, когда это реально необходимо и может повлиять на вбив.

Пункт «3»- Отвечает за физическую версию Flash в браузере. Из списка можно выбрать разные версии. Физическая версия – это та, которая будет использоваться для подмены, мерчи и шопы не видят ни физическую версию браузера или Flash, они же видят ту версию или тот браузер, что задан в конфиге.

лектор: Пункт «4» - Копирует путь к папке созданного браузера.

Пункт «5» - Выбор физической версии браузера. Можно выбрать версию Firefox от 41 до 49. Определяет версию Firefox в которую будет «вшит» Addon Антидетекта. Если же не поставить галочку в пункт «X», то будет обычный Firefox Portable браузер.

лектор: Пункт «6» - Выбор конфига из выпадающего списка. Конфиги нужно загружать в папку «configs», предварительно распаковав из архивов.

Пункт «7» - Показывает краткую информацию о выбранном конфиге.

Пункт «8» - Отвечает за WebRTC. При включенном пункте, сюда нужно вписать IP носка, туннеля, с которого вы собираетесь совершить вбив.

лектор: Пункт «9» - Позволяет изменить язык конфига на нужный из списка.

Пункт «10»- Позволяет добавить дополнительно англ. язык. Когда это нужно? Например, если пытаетесь «закосить» под холдера из Германии, у которого основной язык системы немецкий, можно добавить еще и английский, т.к. у многих на компьютере несколько языков, например английский и русский у жителей РФ.

лектор: Пункт «11» - Позволяет открыть папку последнего созданного браузера.

Пункт «12» - Позволяет выбрать часовой пояс и установить его в системе 1 кликом.

лектор: Насчет использования конфигов и генерации. Генерации конфигов в версии 7.1 нет, можно использовать ее, если иметь версию 6.5, но смысла в этом особого нет. Конфиги лучше использовать все, кроме Internet Explorer, т.к. они бывают глюченные и нерабочие. Лучше всего использовать конфиги с браузером Firefox, т.е. Win XP, 7,8,10, MAC, Android + Firefox Browser.

Теперь по настройке в самом окне, перед созданием браузера: обязательные пункты, где должны стоят галочки: «X» и «8».

«9», «10», «2» - необязательны, при необходимости только.

лектор: Допустим, вы выбрали конфиг, создали браузер, открыли папку с браузером. Поговорим про некоторые настройки вручную, которые вы можете сделать в созданном браузере.

Открыли папку с браузером, далее, открываем:\ ff_Ваша.Версия браузера\App\Firefox\browser

Пример: ff_46.0.1\App\Firefox\browser

Там будет два необходимых нам файла, открываем Notepad++ , потом первый файл:«jsoverrider.json». Что же там можно поменять?

лектор: Во-первых, языки можно проредактировать вручную как нужно, для этого нужно изменять значение параметра «Language» и «Languages» (если он есть)

Во-вторых, можно включить или отключать JAVA (НЕ ПУТАТЬ с JAVASCRIPT!!)

Для этого нужно найти параметр «javaEnabled» и изменить его значение с True на False (или наоборот). Пример: «function javaEnabled() {return true;}» на «function javaEnabled() {return false;}»

В-третьих, можно подредактировать параметр «Useragent» и «appVersion», я бы даже сказал, что это необходимо, т.к. конфиги, которые у вас будут, будь то Firefox, Chrome, Opera, Safari и др., будут уже старые по версии браузера.

лектор: Возьмем, например, конфиг Firefox. Там будет, к примеру, Useragent: «Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1» и appVersion: «5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1»

Версия Firefox по этим параметрам сейчас 40.1, она уже устарела, нам нужно поменять ее на более современную, поменяем к примеру на стабильную версию 48.0. Для этого меняем кусочек в указанных двух параметрах «Firefox/40.1» на «Firefox/48.0». Сохраняем изменения, открываем whoer, либо другой чекер и радуемся изменениям.

Так можно поменять любой параметр, зная примерно, что он делает и означает. Этому спокойно можно научиться самому, уделив этому немного времени. Относится к любым АД, не только к 7.1.

лектор: Переходим ко второму файлу: «jsoverrider.js». Там можно подправить WebRTC и отпечаток Canvas. Открываем этот файл.

Canvas в файле: можно изменить, можно отключить подмену Canvas, тем самым сделать стоковый (стандартный) канвас браузера Firefox.

Для того чтобы изменить отпечаток Canvas нужно изменить значение переменной «var CanvasWebglRandomParameter», т.е. поставить, например в нем другие цифры. (Скриншот: https://prnt.sc/h2y65s)

Для того чтобы вернуть стоковый (стандартный) канвас вашего браузера, то нужно удалить строчку «return context.b_fillText(CanvasWebglRandomParameter, 2, 17);»

Вбивы могут идти лучше со стокового канваса, могут лучше с подменой канваса, может вообще не быть никакой разницы, особенно если шоп маленький или просто-напросто не запрашивает параметр канваса вашего браузера.

лектор: Далее WebRTC. В этом файле можно отредактировать все 3 WebRTC(1 внешний, 2 внутренних)

Переменная «ipAddressRemote» содержит внешний WebRTC.

Переменная «ipAddressLocal» содержит внутренний WebRTC.

Еще одно значение внутреннего WebRTC я отметил на скриншоте под цифрой «2» Скрин: https://prnt.sc/dny2q9

лектор: Также на этом скриншоте я показал: Синие области, границы кода каждого из 3 WebRTC. Это может понадобиться, например, чтобы удалить один ненужный

внутренний WebRTC. Красная область показывает то, что нужно удалить, чтобы WebRTC был полностью отключен.

Также внешний и 1 внутренний WebRTC можно изменить налету в самом браузере. (Скриншот: https://prnt.sc/h2yyko)

Хочу дополнить, что на скриншоте я указал, что для чего нужны другие колонки.

лектор: На этом по настройке антидетекта 7.1 все. Некоторые фишки, советы, ответы на вопросы я опубликовал в своей теме – FAQ По Антидетект/

https://wwh-club.net/threads/faq-po-antidetect-otvety-na-voprosy-ot-xerl.67155/

https://wwh-club.ws/threads/faq-po-antidetect-otvety-na-voprosy-ot-xerl.67155/

Будет полезно почитать после лекции тем, кто собирается брать Антидетект 7.1

лектор: А мы переходим к следующему Антидетекту, под названием «Linken Sphere» (Сфера).

лектор: После покупки, установки, и запуска браузера (по вопросам, которые связанны с покупкой, установкой и запуском программы, обращаться к @nevertheless или к саппорту) в первую очередь нужно настроить общие настройки браузера. Находятся они во вкладке «Edit», далее из выпадающего списка находим «Preferences». Скриншот: http://prntscr.com/itjman

На скриншоте я выделил самые необходимые настройки для новичка. Обо всех остальных можно посмотреть и прочитать в документации на сайте.

лектор: Итак, 1 пункт - поисковая система по умолчанию, т.е. этот параметр устанавливает какая поисковая система будет открываться, если вы будете вбивать запрос в адресной строке браузера. Для вбивов удобнее поставить ПС Google, для анонимности и безопасности DuckDuckGo.

2 пункт – данный параметр позволяет указать сайт, который будет открываться после создания сессии. Для вбива удобно указывать какой-либо чекер, whoer, detect.cc, browserleaks и др., кому какой удобнее.

лектор: 3 пункт – позволяет установить физический размер экрана, очень важный параметр, советую ставить его каждый раз под сессию (конфиг). Проверить данные параметры (device-width, device-height) можно здесь: https://browserleaks.com/css

4 пункт – определяет то, каким образом будет производиться подмена системного времени. Важный параметр. Есть два варианта: 1) Посредством Javascript. 2) Будет изменяться системное время. Лучше всего выбирать второй вариант, system override, как по мне он 100% не палевный, т.к. по сути мы не подменяем время через Javascript, а как будто изменяем его вручную в системе.

лектор: 5,6 пункт – данные параметры я бы отнес к безопасности. В идеале, если вы очень переживаете насчет своей безопасности: на 5 пункте ставить галочку, на 6 –нет.

Собственно, 5 пункт – позволяет использовать TOR при авторизации в антидетекте.

6 пункт – позволяет выбрать, сохранять или не сохранять пароль от вашего аккаунта при входе.

лектор: 7 пункт – данный пункт позволяет закрыть порты в Web Sockets. Web sockets – это протокол, предназначенный для обмена сообщениями между браузером и веб-сервером. Говоря простым язык, посредством Javascript сайт может чекнуть ваши открытые/закрытые порты Web Sockets.

Чекер: http://www.andlabs.org/tools/jsrecon.html

По настройкам чекера: IP Adress – «127.0.0.1», Start Port, End Port – тут указываем диапазон портов (минимум 2), например Start Port: 5939; End Port: 5940. Protocol : WebSockets. После сканирования вам покажет открыты или закрыты данные порты. В примере я использовал порт «5939» - он относится к TeamViewer. Вот эти порты относятся к технологии VNC (5900,5901,5902,5903) 3389 – технология RDP и.т.д.

По настройке этого пункта: Без нужды лучше ничего не менять.

лектор: порты 80;8080 закрыть таким образом не получится сразу говорю)

лектор: Остальные параметры направлены больше на юзабиллити(дизайн шрифта, размер, бекапы, прокси для обновлений и.т.д.)

Далее переходим к настройке сессий браузера. Каждая сессия по сути – это отдельная система, как виртуалка, которая имеет свой конфиг.

Подробнее про бесплатные и платные конфиги и отличия в настройке при работе, мы поговорим чуть позже; для начала нужно разобраться с важными настройками сессий браузера для новичков.

лектор: Начнем с разбора первого раздела. (Скриншот: http://prntscr.com/itjucp)

лектор: 1 пункт – Выбор сессии (конфига) из списка.

2 пункт – Данный пункт нужен для создания новой сессии. Для этого нужно ввести имя сессии в данное поле.

3 пункт – окно заметок сессии. Очень полезная функция. Для того чтобы не запутаться в сессиях и упростить себе жизнь по анализу вбивов, советую указывать всю полезную информацию в данное поле(Proxy Score, Risk Score, В какие шопы вбивали, каким методом, использованную карту, результат вбива и.т.п.)

лектор: 4 пункт – позволяет установить цвет сессии, цвет сессии будет отображаться во владках браузера (скрин: http://prntscr.com/h3njn3)

5 пункт – позволяет скопировать полностью сессиию, включая отпечатки canvas, audio, fonts, rects (при необходимости).

6 пункт – позволяет изменить имя сессии(переименовать сессию).

лектор: 7 пункт – данный пункт позволяет сменить алгоритм подмены канваса, проще говоря, это второй вариант его подмены (про первый будет ниже). Какой из вариантов лучше использовать? Ответ: Оба, в разных шопах может быть различный результат, поэтому пробовать лучше 2 варианта и эмпирическим путем анализировать какой лучше в вашем случае.

8,9,10 пункт – позволяет включить/отключить HTML 5 Хранилище, пункт 9 – позволяет сохранять данные и использовать их даже после перезагрузки браузера, пункт 10 – позволяется сохранять и использовать данные посредством стандарта хранения больших структурированных данных «IndexedDB» . Если коротко – не вникая в теорию. Для вбивов должны быть включены оба этих пункта (исключение: вбив с телефона blackberry, для всего остального, вплане безопасности, пункты 8,9,10 лучше отключить.

лектор: Перейдем к очень интересному разделу для многих «Отпечатки и другие настройки» (Скриншот: http://prntscr.com/itkiz7)

лектор: 1 пункт – включает/выключает подмену Canvas. Каждый уже слышал про этот параметр. Собственно, что делает эта подмена в сфере – она уникализирует канвас, не изменяя при этом сильно «его картинку», благодаря чему он выглядит более менее естественно. Чекнуть канвас можно здесь: https://browserleaks.com/canvas

Если сильно изменять картинку канваса, а именно пользоваться популярными дополнениями для браузеров

firefox и chrome по изменению канваса, это все 100% можно спокойно увидеть шоп. Вот чекер в browserleaks, который определяет это: https://browserleaks.com/proxy (Параметр: HTML5 Canvas Protection). Также и со шрифтами, параметр «CSS Fonts Protection»). На данный момент минус технологии уникализации Canvas заключается в том, что на выходе получается 100% уникальность, и это касается всех антидетектов. Но, тем не менее, некоторые АФ системы очень неприязненно реагируют на слишком высокую уникальность, поэтому пробуйте периодически отключать данную функцию, если возникли подозрения, что шоп не дает из за данного параметра.

лектор: 2 пункт - включает/выключает подмену Аудио отпечатка. Аудио отпечаток, конечно, не настолько популярный как в канвас, но со временем все больше и больше банков, шопов внедряют его в свои антифрод системы. Чекер: https://audiofingerprint.openwpm.com/

Антидетект успешно подменяет для каждой сессии 4 параметра: Fingerprint using DynamicsCompressor (sum of buffer values), Fingerprint using DynamicsCompressor (hash of full buffer), Fingerprint using OscillatorNode,Fingerprint using hybrid of OscillatorNode/DynamicsCompressor method

лектор: 3 пункт - включает/выключает подмену шрифтов. Очень популярный детект, подменить легко и без антидетекта, но помимо подмены отпечатка, сфера позволяет настроить список шрифтов, что является несомненным плюсом. Чекер: https://browserleaks.com/fonts (два параметра «Fingerprint»)

4 пункт – включает/выключает подмену rects . Если коротко, это подмена координатной системы браузера. Элемент «getClientRects» позволяет получить точное положение и размер пикселя нужного элемента, а в зависимости от системы, а точнее разрешения экрана системы, шрифтов и еще множества других параметров, результаты будут различны. Сфера же позволяет подменить это, не слишком сильно изменяя их, что на практике не палится Антифрод системами. Чекер: https://browserleaks.com/rects (Параметр: «Full Hash»)

лектор: 5 пункт – Включает/ отключает использование случайных плагинов. Данный параметр позволяет добавить в вашу сессию случайный набор плагинов, что позволяет избежать детекта по плагинам. Функция нужна для тех, у кого бесплатные конфиги, и кому лень вручную прописывать плагины. Естественно в платных конфигах набор плагинов включен.

6 пункт – включает/выключает сохранение и шифрование cookies после выхода из сессии. Должен быть обязательно включен. Дополнительным плюсом для безопасности является шифрование.

лектор: 7 пункт – включает/выключает Flash. Тут также как и с антидетектом 7.1 – без сильно необходимости не включать, flash – дополнительная возможность задетектить вас. Технология на данный момент является устаревшей, все ее возможности давно имеет html5, поэтому из за его отсутствия мало кто на вас косо уже не посмотрит.

8 пункт – при включении данного пункта, каждый раз после открытия сессия будет иметь новые отпечатки, что я описал вам выше. Для вбивов в этом нет никакой необходимости, для безопасности – можно использовать.

лектор: 9 пункт – позволяет выбрать какие отпечатки делать новые, случайные (Canvas, Audio, Plugins, Rects, WebGL, Fonts, Media Devices) . Относится к пункту 8.

10 пункт – данный параметр блокирует вывод хеша канвас. Нужно использовать в том случае, если вы уверены, что ваш шоп или мерч плохо реагирует на 100% уникальность канваса. (Скриншот: http://prntscr.com/h3pk3m)

лектор: Переходим к разделу «Настройка и выбор типа подключения» (Скриншот: http://prntscr.com/itkxrv)

лектор: 1 пункт – позволяет выбрать из выпадающего списка тип подключения. Сейчас я разберу самые необходимые для работы новичку.

лектор: No proxy- данный режим позволяет использовать прямое подключение, т.е. интернет берется с вашей системы. Он необходим если вам уж очень сильно хочется работать с Proxyfier, Bitvise SSH и прочий софт для использования туннелей и носков. Как по мне данный режим не нужен, т.к. не позволяет использовать преимущество сферы в использовании одновременно разных сессий, в каждой из которых настроено отдельное подключение носка или туннеля, в зависимости от того, что нравится использовать вам. Исключение из данной ситуации: это использование роутера, в котором имеет возможность подключить носок или туннель в самом

роутере, а не на вашей системе. (На форуме продается такой настроенный роутер)

лектор: Tor – данный режим подключения советую использовать для вашей цепочки безопасности, при серфинге теневых форумов и для того чтобы зайти на форумы через тор, например форум Verified.

Socks, SSH Tunnel – обьединил данные режимы. Первый относится к использованию Носков (Socks 5) а второй к использованию Туннелей (SSH). Данные режимы можно и нужно использовать для вбивов. Для каждой сессии можно настраивать разные подключения и использовать одновременно, т.е. по сути все равно что вбивать сразу с нескольких систем (виртуалок). Вбивать с носков или туннелей – это лишь на ваше усмотрение, кому с чем больше нравится работать. Я лично использую носки для вбивов, LuxSocks. Но проблема в том, что с недавнего времени у них проблемы с носками, количество носков резко упало вниз. Поэтому сейчас я дополнительно использую сокс -сервис «Faceless».

лектор: Sphere socks – Соксы, поднятые на мобильных устройствах. Данные мобильные носки исключительно для клиентов сферы, они интегрированы прямо в антидетект. Данное решение позволяет еще больше сэкономить время и повышает юзабиллити и уникальность антидетекта, т.к. IP данных носков - из общего пула мобильных операторов, следовательно, Антифрод системы могут относится к вам более лояльно. Для лучшей результативности советую с данными носками использовать конфиги Android устройств

(Мобильные телефоны + Планшеты). На сегодняшний день носки находятся на стадии внедрения)

лектор: 2 пункт – Поле для ввода ip носка/туннеля и порта.

Пример ввода SOCKS 5: 173.244.217.119:1081

3 пункт – данная галочка позволяет отключить внутренний IP. Т.е. при использовании данного пункта, отображаться будет лишь внешний IP webRTC.

4 пункт – авторизация носка/туннеля. Собственно все туннели с авторизацией, поэтому вводить сюда логин и пароль обязательно, а вот носки (Socks) не так часто бывают с авторизацией, поэтому если у вас нет логина или пароля, поля оставлять пустыми.

лектор: 5 пункт – включает/выключает подмену WebRTC. Если выключить подмену, то WebRTC будет соответствовать WebRTC вашей системы, где установлен антидетект.

6 пункт – Данная галочка отвечает за Внешний IP WebRTC. Нужно отключать галочку, когда IP для подключения отличается от того IP, который получается на выходе (проверить на любом чекере можно, например на whoer.net). Приведу пример с Luxsocks, после покупки носка я получаю вот такой вот ip:порт для подключения «212.83.165.56:29007», я проверяю на whoer.net, а там IP «97.113.91.76», следовательно, эту галочку я должен отключить, и в поле «ВНЕШНИЙ IP WEBRTC» для грамотной подмены, я должен написать вот этот IP «97.113.91.76»

лектор: 7 пункт – данный пункт позволяет включить подмену IPv6. Использовать нужно лишь в том случае, если на вашей системе идет «утечка» данной информации. Проверить утечку можно здесь: https://browserleaks.com/ip

«IPv6 Leak Test».

8 пункт – отключает подмену WebRTC, т.е. при включении данной функции WebRTC будет показывать что выключен (disabled). Чекер: whoer.net

лектор: 9 пункт – позволяет установить свой DNS. Необходимо использовать в том случае если у вашего носка или туннеля нет DNS или же он другой страны., либо же вам нужно подменить DNS не для вбива, а для вашей безопасности . Кнопка «check DNS» -проверяет работоспособность указанного вами DNS сервера. Обратите внимание, что работа с этим параметром очень важна - DNS имеет такое же значение, как и сам IP. Кроме того, часто бывает, что при покупке соксов без собственного DNS вами показывается DNS системы (именно это происходит по умолчанию, если данное поле не заполнено, а сокс не обладает собственным параметром), и вы ловите деклайны по причине подозрительной активности.

10 пункт – данная кнопка «Check Proxy/ Geo» позволяет автоматически при ее нажатии проверить Носок для подключения на работоспособность, а также автоматически установить на основе его геоданных (по базе MaxMind) и Ip: Часовой Пояс, Внешний WebRTC, GPS)

лектор: Переходим к 3 разделу программы: https://prnt.sc/itkq52

лектор: 1 область – отвечает за UserAgent. Нажав на кнопку «manage»,можно редактировать, добавлять, удалять Useragent’ы. После из выпающего списка можно быстро выбрать нужный Useragent в 2 клика. Кнопки сверху («Chrome», «Safari», «MSIE»,«Other») позволяют производить очень быстро выборку по типу браузера.

Хочу уточнить, что на сайте, в личном кабинете есть раздел «Юзерагенты» - там бесплатно можно выбрать готовые юзерагенты по ОС, Браузеру и типу устройства.

2 область – отвечает за язык (language) сессии. Можно выбрать из выпадающего списка страну, и язык пропишется автоматически, можно прописать самому вручную в поле для ввода, которое находится правее.

лектор: 3 пункт – Блокировка всплывающих окон. Данная функция запрещает создание всплывающих окон. Использовать только при необходимости, иногда у шопа или мерча бывают «необходимые» всплывающие окна.

4 пункт – Все что нужно о нем знать новичку, это если сайт прогружается с ошибками, или что-то не работает на сайте, что не позволяет до конца совершить вбив, стоит включить эту функцию. Без необходимости не включать.

лектор: Следующий раздел- https://prnt.sc/itklmh

лектор: 1)Config manager – проще говоря, бесплатные конфиги. Тыкнули по кнопке, выбрали тип браузера, выбрали ОС, нажали сгенерировать и бесплатный конфиг загрузился.

2)Настройка WebGL. Данный раздел позволяет настроить все возможные параметры WebGL 1, WebGL 2, отключить WebGL, если это необходимо, а также сгенирировать его, если лень настраивать.

3)Расширенные настройки. (Скриншот: https://prnt.sc/h3q2d0) Данный раздел позволяет прописать вручную плагины, добавить вручную http заголовки, отредактировать вручную более 27 Javascript параметров.

лектор: 4)Шрифты. Данный раздел позволяет отредактировать набор шрифтов, т.е. можно создать полностью свой список шрифтов, которые будут видеть антифрод системы помимо подмены самого отпечатка шрифтов.

5)Эмуляция разрешения окна. Эта фича позволяет скрыть свое реальное разрешение экрана, и оно будет совпадать с данными юзерагента. Полезно при работе с мобильных конфигураций.

6)Эмуляция тач скрина - просто MUST HAVE при работе с мобильных конфигов. Полноценная эмуляция тачскрина как на мобильных устройствах. Ни в одном из существующих антидетектов кроме этого, нет такой функции.

лектор: 7,8) Данные два значения задают разрешение экрана. 7- ширину экрана, 8 – высоту экрана. Пример 1920x1080

лектор: Идем далее, следующий небольшой раздел. Скриншот: http://prntscr.com/itkmis

лектор: 1 область - отвечает за подмену геопозиции. Latitude – географическая широта, longitude- географическая долгота.

Ставить геопозицию необязательно прямо под ZIP вашего туннеля, вполне нормально и естественно будет смотреться если поставить геопозицию до 10 км от вашего носка. Пример на скриншоте: http://prntscr.com/h3pyv1

Меткой в Google maps отмечены координаты носка, вокруг него круг – так вот область круга это и есть достаточно естественная геопозиция для данного носка/туннеля.

лектор: 2 область – отвечает за подмену таймзоны, а попросту говоря- установка часового пояса и времени. Время можно поставить либо выбрав штат из выпадающего списка, либо выбрав тайм-зону из выпадающего списка.

Опять же хочу уточнить, что при нажатии кнопки «check proxy/geo» геопозиция и время устанавливается автоматически, что экономит нам драгоценное время.

Разобрались со всевозможными настройками сферы, которые могут понадобиться, теперь перейдем уже наконец к работе с данного продукта.

лектор: 1 вариант – у вас имеется аккаунт PRO и доступ к конфигшопу. Схема работы – покупаете нужный конфиг в конфигшопе, добавляете его в сферу, настраиваете тип подключения, WebRTC, DNS при необходимости, нажимаете кнопку Check proxy/geo (автоматом настраивается часовой пояс и геопозиция,) далее выбираете галочками те отпечатки, которые хотите подменить и

вперед вбивать. На деле то, что я описал, занимает около минуты.

лектор: 2 вариант – у вас нет доступа к конфигшопу, тогда вы можете выполнять настройку двумя путями. Первый - установка нужного Юзерагента (выбор из готовых или загрузка своего, что предпочтительнее), после чего происходит генерация параметром при помощи встроенного генератора .

После генерации вам потребуется посмотреть, подправить, подкорректировать параметры WebGL, Расширенные настройки, Шрифты, и т.д. Второй вариант - использование встроенных бесплатных конфигов (их порядка 50 000) - создаете сессию, нажимаете Config manager, выбираете нужный браузер и ОС, получаете конфиг реального устройства из встроенной базы. С ним ничего дополнительно делать не нужно - далее ничем не отличается от первого варианта: настраиваете тип подключения, WebRTC, DNS при необходимости, нажимаете кнопку Check proxy/geo (автоматом настраивается часовой пояс и геопозиция,) далее выбираете галочками те отпечатки которые хотите подменить и вперед вбивать.

лектор: Однако, встроенные конфиги имеют свойство задрачиваться, потому что ими пользуется достаточно большое количество людей, да и качество их объективно похуже тех, что в шопе, и это может негативно влиять на результат, хоть для пробы сил новичка они вполне подходят.

Также возможно не загружать бесплатный конфиг, а самому собственно его написать в сфере с нуля, но что для первого варианта, что для второго, нужно иметь опыт, знания всех параметров. Обо всех параметров подробно можно прочесть в документации продукта + Google в помощь.

Еще по полезным фишкам в данном Антидетекте:

лектор: 1) В Антидетект встроен собственный Web Emulator – данный инструмент позволяет имитировать поведение реального пользователя, посещая сайты в автоматическом режиме. На практике это нужно для того чтобы сократить рутинную работу по набору Cookie’s файлов сайта, истории посещений сайтов, проще говоря «прогреть» систему перед вбивом в шоп. Можно также задать настройки эмулятору, чтобы он имитировал поведение пользователя в шопе перед вбивом.

лектор: 2) Ввод данных при вбиве упрощен – в антидетект встроен собственный Vbivotron (пример софта для системы на нашем форуме: https://wwh-club.net/threads/vbivotron-2014.15997/). Функция удобная, но обратите внимание на то, что некоторые сайты очень неприязненно относятся к копированию, и даже специально настроенные интервалы человекопобного ввода могут попадать под антифрод. Пользуйтесь функцией, если на собственном опыте уверены, что шоп никак не реагирует на такой ввод.

Поиск шопов, мерчи

лектор: Лекцию разделим на 2 части, с небольшим перерывом, так как объем материала будет большим.

лектор: Часть 1 – Поиск шопов.

Часть 2 – Разбор мерчей.

лектор: И так, поехали. Часть 1. Поиск шопов.

лектор: Начну пожалуй сразу с предупреждения: искать шопы, запросами типа: buy apple iphone X, или buy macbook pro, или buy Gucci jeans – смысла нет. Так как на первых страницах поисковых систем – будут всегда шопы гиганты, наподобие BestBuy, Amazon, Seers и тд. Работать с ними можно, но там нужен совершенно другой подход и опыт. Взять первую попавшуюся CC и вбить на 10к долларов не получится, не старайтесь.

лектор: Так как же найти нужные шопы? Вот лишь несколько вариантов:

лектор: 1. Искать шопы можно, используя сео-оптимизационные ресурсы, одного из сайтов нужной тематики. Сео-оптимизация – это комплекс мер по внутренней и внешней оптимизации сайта, для продвижения его в поисковых системах. Соответственно чем выше позиция сайта в поисковике – тем больше посещаемость, и соответственно для его продвижения использованы более высокочастотные запросы.

лектор: Например: по запросу Gucci jeans гугл выдает следующую картину. http://prntscr.com/gpqxsz, за пример возьмем 5й сайт : http://prntscr.com/gpqxig. Переходим на сайт, находим любую необходимую категорию (в данном случае заужинные джинсы) и нажимаем правой кнопкой мыши на свободной поле в поле браузера.

лектор: Нам нужна строка View Page Source http://prntscr.com/gpqy48 - нажимаем на нее, получаем это: http://prntscr.com/gpqyez - видим, в строке meta name – прописаны запросы, по которым продвигается данная страница. Нам остается только скомпилировать запросы со своими и идти искать уже более точечно, например: если сделать такой запрос «clothes shop+inurl:super slim jeans» то гугл выдаст http://prntscr.com/gpqzqh и http://prntscr.com/gpqzu9.

лектор: 2. Шопы так же можно искать через «операторы запросов», о которых более подробно можно почитать тут https://sites.google.com/site/tilromen/poleznoe/kak-pravilno-sostavit-poiskovoj-zapros-google, а еще лучше поизучать их на сео форумах, много чего интересного там найти. Как пример приведу следующий оператор запроса: clothes shop+ inurl:e-gift - даст нам список шопов, у которых есть фраза e-gift в ссылке, или «clothes totes egift» - Двойные кавычки позволяют найти только то выражение, которое в них содержится.

лектор: 3. Шопы можно так же искать через ибей, однако не у всех есть свои сайты, нужно искать. Достаточно просто перейти на интересующий нас товар, и посмотреть информацию о продавце, если это шоп – мы увидим, обычно страница красочно оформлена, и имя продавца наподобие: freeshippngshoes, bestshoes, goodwatches и др. Изучайте внимательно. Дальше нам останется вбить в гугл эти данные и перейти на сайт шопа, если такой существует. Однако не всегда удается сразу обойти антифрод систему

шопа, иногда проще вбить в ибей (но об этом на лекциях по бруту).

лектор: 4. Шопы так же можно искать через Амазон. Заходим на amazon.com, вводим в строке поиска запрос, например SSD. Нас интересует левый столбец http://prntscr.com/dusrr7 , спускаемся ниже, нам нужна строка «Seller» и нажимаем «See More» http://prntscr.com/dussij , нас перебросит на следующую страницу http://prntscr.com/dust0d. На этой странице представлены продавцы товаров данной категории. Нам остается скопировать их названия и вставить в гугл, а дальше по аналогии с предыдущим.

лектор: 5. Шопы так же можно искать парсерами, например Баттерфляй. Минус парсеров в том, что находят много всякого мусора, поэтому придется сайты перебирать вручную. Хотя безусловно они иногда очень сильно помогают.

лектор: 6. Шопы так же можно искать через SQL Dumper, при правильном составлении дорок – можно найти очень сладкие шопы, однако дампер кушает много проксей, поэтому придется постоянно в него подгружать новые. Вообще он нужен для поиска уязвивостей на сайтах, но и под поиск шопов достаточно просто адаптируется

лектор: 7. Так же шопы можно искать на тематических форумах, например: форум молодых мам, или рыболовный форум. При правильном подходе и СИ - вам сольют кучу шопов, которые очень долго будете искать в интернете. Спасибо молодой маме Мишель – подсказала отличный

шоп с дорогущими детским колясками и беспонтовой антифрод системой. Шоп к сожалению закрылся, а коляски приехали в РУ)

лектор: 8. Шопы можно поискать на сайте http://www.resellerratings.com

лектор: Сверху выпадающее меню store ratings. Там выбираем browse all stores by category и с лева будет менюшка с категориями. Выбираем например apparel and jewelry. Видим "sort by" и кликаем

лектор: Так у нас отобразится на первой странице сайты с самым низким рейтингом. Но этих сайтов в разделе одежды и бижи 468 страниц. Примерно 70% из них с нулевым рейтингом и примерно три четверти из тех 70% шопов - мелких, хорошо дающих. Бывает попадаются шопы, вроде на этом сайте рейтинга вообще нет, но по факту шоп крупный и хрен просто так что вышлет.

лектор: На самом деле существует множество способов найти нужные нам шопы, с нужным товаром, однако я чаще всего использую именно эти методы работы. Я рекомендую Вам экспериментировать именно с операторами запросов, так как это наиболее быстрый и удобный вариант поиска шопов.

лектор: По моему опыту иногда крупные магазины шлют намного лучше, чем мелкие, но это скорее исключение и прямые руки, чем просто везение). Пытаться пробить нужно все понравившиеся шопы.

лектор: Иногда бывает и скамерский шоп попадется, например встречал один где Канаду Гуз стоили 200 баксов, поэтому в такие шопы лучше мат не бить, они созданы нашими коллегами для сбора мата. Внимательно изучайте шоп перед вбивом.

лектор: Часть 2. Разбор мерчей и их особенности.

лектор: Мерч - это электронный агрегатор обработки поступающих платежей, иными словами – это та программа, которая непосредственно принимает платежи через сайт. Мерчей огромное множество, как крупных, так и самописных.

лектор: Для определения мерча я чаще всего использую сайт http://builtwith.com/, - у кого есть возможность можете купить там подписку за свои кровные, стоит 500 баксов в месяц, не вздумайте скардить – не получится. Вбиваем адрес шопа в строку, и нам выдаст всю информацию по шопу, в разделе E-commerce, будет нужным нам мерч. Иногда мерч не показывается, тогда приходится высматривать по переадресациям в браузере либо бить наугад, такое тоже бывает.

лектор: Что касается евро мерчей, то чаще всего их можно увидеть во время чекаута, то есть когда уже вбиваете карту, так как большинство евро шопов - не размещают инфу о мерче на страницах.

лектор: Ниже приведен список мерчей, часто встречающихся по юсе:

лектор: 1.Shopify – считается что с каждым месяцем его все сложнее и сложнее вбивать, но нет. Все намного проще, нужно подстраивать систему под этот мерч. Мерч любит реальное железо, и ему практически пофиг на носки и туннели, главное железо и уникальный фингерпринт системы. Очень важная тонкая и грамотная настройка системы. А вообще мерч палит и деды, и подмену айпи. Не утруждает себя даже письмами об отмене заказа и письмами о возможном мошенничество с вашей стороны. Выход - идеально настраивать свою систему для вбива.

лектор: Под каждый мерч у меня отдельно настроенная вирта, и соответственно я просто меняю носки и бью.

Чтобы найти шопы на этом движке используем следующий поисковой запрос: Ecommerce+Software+by+Shopify+dildo

2. WooCommerce – достаточно интересный мерч. Встречался мне не так часто, по проходимости все зависит от шопа. То есть на какой уровень безопасности настроен мерч. Некоторые шопы отгружают тоннами, из некоторых и бакс не вытащить.

лектор: BigCommerce – в принципе все тоже самое что и выше.

Шопы ищуться так: dildo+ giftcertificates.php –найдет все шопы с гифтами дилдо))

4.Magento и его производные. Самый любимый мой мерч. Прост в работе и не особо капризный.

Шопы ищуться dildo+ .com/checkout/cart/ - собственно корзина, dildo+ .com/customer/account/ - аккаунт.

лектор: 5.Shoprunner – он же мерч/движок многих монобрендовых шопов. Достаточно легок для работы. Так же можно пробивать его с брута.

6.Zen Cart – тоже достаточно часто встречается. Бьется чуть посложнее, чем предыдущие, но особых хлопот не доставляет.

7.PrestaShop –в принципе все тоже самое. Чистый носок + хорошо настроенная система и будем Вам счатсье.

лектор: 8. OpenCart – самый мой нелюбимый мерч. Даже при идеальном вбиве – может послать. А вбивы на «от*бись» проходят. До сих пор его понять не могу.

9. X-Cart – найти не так легко, но если шоп начал давать – то готовьте фуры

лектор: С учетом особенностей настройки ABC-системы в шопах, часто бывает такое, что шопы не видят фул адрес холдера, а видят только ЗИП. Поэтому иногда целесообразно брать карту под зип посреда/дропа, и вбивать на их адрес бил=шип. Такие шопы можно найти только тестами.

лектор: Так же рекомендую взять ролку (тот же кредит ван), и пробивать понравившиеся шопы на мелкие суммы на адрес холдера, дабы увидеть движения по карте. Некоторые шопы списывают бабки сразу, некоторые холдят, некоторые списывают в момент отправки пака, поэтому владея этой информацией, можно с легкостью подобрать мат и метод работы с конкретным шопом

лектор: Так же приведу примеры евро мерчей:

1. SagePay (Сага)- вбв всегда, каждый шоп любит разные типы карт. По амексу нет сейфкея. ЮК и ЮСУ по сброс кушает, но не все бины . Если карта вошла, практически всегда высылают. Что касается авиа, то тот же самый принцип.

лектор: Stub Hub + virtual pos terminal – очень часто встречается на сайтах, которые продают билеты на всевозможные мероприятия. Вбивать этот мерч достаточно сложно, ВБВ – всегда, юсу не удавалось впихнуть ни разу, только ЕУ. Палит все, вплоть до цвета носков на вас, но он стоит того).

https://prnt.sc/gpr913 - вот собственно как выглядит вбив.

лектор: 2. BancaSella - один из замечательных мерчей вбв. На ура юса и юк под сброс. Бывает чудо и вбв нет. 100% попадание если транза прошла.

3. Adyen - тоже красавчик, лезут все страны, сейфкея нет, дискавер в большинстве шопов, а это верный обход вбв. Однако даже с вошедшей картой, шоп может докопаться. Что касается авиа/отелей – если карта вошла, 100% попадание. Бронь и билеты, считайте у вас в кармане.

лектор: 4. Bucharoo- сложный голландский мерч. ВБВ/Сейфки, Можно вбить и юсой – но крайне редко – скорее исключение. Однако есть шопы, с которыми проявив СИ, можно вбить по посу юсу или другой еу мат.

5. Wirecard - сейф кея нет, как и амекса практически, замечательно кушает ЮСУ, по крайней мере последние 2 месяца. Бывает и без вбв.

6. Erstes - тот же вайркайрд.

7. SaferPay - сейф кей, только еу. Иногда без вбв.

лектор: 8. Euro payment service – отлично заходит юса мат под сброс. Юк мат кушает хоть на 10к, без каких либо претензий

лектор: PayPal и все его братья - тут ясно, не рассматриваю, будут отдельные лекции

лектор: Zerogrey - как и прежде кушает все, только бины посвежее подавай. 99% вероятность что на первый заказ будет нужна отрисовка. Если сделано хорошо (фото а не скан) то успех гарантирован. Советую всегда заводить акк в шопе, если карта выживет после первой отправки - выжимать с нее максимум

Европа и Азия

лектор: сегодня мы говорим о еу и азии, я бы сказал в целом о работе по миру. Стоп Флуд)

лектор: Работа с картами других регионов(отличные от us) несет в себя ряд особенностей, оно и логично, т.к. от региона к региону разные банковские системы.

лектор: Я бы советовал смотреть на это направление, когда есть либо уже багаж знаний(и я говорю в общем про механику работы и настройку машины) , либо у вас есть деньги на тесты, но конечно лучший вариант когда вы имеете и то и то.

лектор: Направление интересное, но требует вливаний, начните работать по нему, вести статистику, и увидете закономерности.

лектор: Лекция будет нести больше обзорный характер, важные параметры вам скажу ниже

лектор: И так начнем, но прежде выделю одно из главных преимущест мата еу и азии - не подключена система AVS ,кто забыл ссылка ниже

лектор: https://wwh-club.net//threads/3-2-2-avs-sverka-imeni-adresa-zapros-dopolnitelnyx-dannyx.2135/

лектор: А и давайте разберемся сразу что такое 3ds(он же vbv/mcsc)

лектор: https://wwh-club.net/threads/3-3-2-vbv-mcsc.2108/

лектор: Бин это первые 6 цифр карты, ну я надеюсь вы это уже знаете.

лектор: Помним что система AVS есть в Англии(uk), и странах которые рядом(ирландия,шотландия) т.к. они бывают обслуживаются банками англии.также на корпах англии нет авс системы.Так-же существует Автовбв, то есть когда вы нравитесь фроду, код 3дс не запрашивается, может быть настроено на стороне шопа или банка.

лектор: К примеру шоп может просто не запрашивать вбв до определенной суммы, скажем он просто имеет несколько мерчей, или у мерча подрублен динамический 3дс.

лектор: Помним, что вбив карты в стране кардхолдера может иметь последствия ввиде быстрого чарджа.

лектор: Прогреваем шоп, обязательно общаемся. СИ наш главный инструмент. Общение с шопами, получение обратной связи, все это важно. Как минимум экономит ваши деньги, когда вы перед вбивом узнаете важную инфу,такую например как - каких стран материал проходит.

лектор: Только представьте, вы можете общаться с шопами(рассказывать им свои истории, быть как холдер), вы можете прозванивать банки и узнавать причину деклайнов и т.д.

лектор: Если с англ. трудно, то используйте гугл транслит, или плагин для браузера grammarly.com

лектор: Как правило по миру(то есть за пределами us) общение с шопами/конторами идет по почте,реже по телефону

лектор: При интернациональных вбивах, готовьтесь к тому что могу запросить доки, это нормально, удобнее будет если вы сразу будете отрисовывать доки,чтобы при запросе шопа не делать их слишком долго. Разве что по юсе могут спецом запрашивать доки,чтобы тянуть время и пришел чардж.

лектор: CC с 3дс кодом и CC без 3дс , все просто.

лектор: То есть где-то 3дс код ты знаешь, где-то нет, где-то он просто не установлен на карту или вообще не нужен для работы, или его можно поменять как пароль на почте(либо легче, либо нереально).

лектор: Что касается сброса 3дс кода(типо сброса пароля) - его можно изменить зная доп.инфо по карте, типо доба или

ссн, либо другие данные в зависимости от страны и бина. https://prnt.sc/fyheyl

лектор: Далее материал и способы работы разделяются в зависимости от стран, и способов приема вбв(статичный,в смс коде,2фа в банк приложение)

лектор: К примеру с чем можно работать:

лектор: Usa/Uk карты со сбросом 3дс кода - он относительно безболезненно сбрасывается на юсе, по юк сбрасывается по добу,зипу, но все чаще и чаще прием по телефону в смс.

лектор: Вбивают - лезет по всему миру, в азию, европу и другие регионы

лектор: Да, по ey/ca/uk/au/usa можно сбросить 3дс код и поставить свой зная только доб, но надо искать бины которые подойдут вам, ибо все реже и реже так легко код можно поменять, и все чаще умирают карты после смены кода. Но если есть средства то можно попробывать собрать базу бинов.

лектор: Usa и Остальные страны non-3ds - тут уже надо самим выводить статистику что куда лезет, допустим юса нонвбв почти не лезет в европу, а вот в азию уже залезет, так же найти ey бины без вбв достаточно трудно, но в целом реально

лектор: Что стоит отметить - по азии почти везде 3дс код идет в смс, по ey все еще встречается статичный код,но все реже и реже.Так же по usa крупные банки ставят прием 3дс

кода по телефону или он приходит на почту(но в целом еще много банков с легким сбросом 3дс по добу или ссн).

лектор: Тенденция на рынке такая что купить мат с известным кодом очень тяжко или почти не реально, более реальный вариант брать его за % от прибыли(суммы транзы), но это уже совсем другая история)

лектор: В подборе карт не всегда стоит отдавать предпочтение только жирным бинам типа gold/platina/signature , это лишь один из пунктов при выборе карты, не забывайте смотреть на банк эмитент, страну. Как минимум страну это точно, в Индии на голде может ничего не быть, а в Сингапуре на классике может лежать оочень много денег, здесь в общем включаем логику, можете гуглить страны и смотреть какая у них там обстановка.

лектор: Чтобы было понятнее расскажу о методах вбива, используя различный мат. (в обще это все довольно логично, и все способы базируются на том что - куда бить и что бить)

лектор: То есть смотрим сс которые мы можем купить, и смотрим шоп и куда он доставляет(не забываем про СИ, и изучить шоп)

лектор: Допустим - юса/юк мат со сбросом можно бить в еу шопы с вбв, и делать доставку на любой адрес,точнее они не увидят если вы укажете биллинг не с карты, нету системы avs.

лектор: Так же как - бить еу карты в юсу,с доставкой в европу, да запросят доки,да будет вериф, но если шоп средний и больше, и есть доставка,то отправят.

лектор: Если есть материал с известным кодом вбв то пусть сама фантазия подскажет куда его вбить - а это либо самый ликвидный товар, гифты, и так далее, думаю когда он окажется у вас в руках вы сможете понять что с ним делать,с неба он не падает.

лектор: Сортировка/опредление 3дс защиты у шопа(наличие у мерча). Это актуально, так как многие шопы могут просто не указывать у себя наличия 3дс защиты, имеет место так-же и тот факт что (в основном в азии) значок 3дс может быть на сайте шопы, но по факту его там нет,так отпугивают кардеров.

лектор: Хоть какую-то инфу по мерчам глянуть/дополнить можете здесь -

https://wwh-club.net/threads/obzor-merchej-eu.57552/

лектор: Чтобы определить наличие 3дс шопа, я как правило беру карту на которой есть 3дс и я точно это знаю, и вбиваю ее в шопы, если окно 3дс открывается(я скидывал скрин выше) то 3дс есть) если нет,то нет.

лектор: Обращаем внимание на регион лок, работая с разными странами вы можете столкнуться с ним, не дает сделать транзу в стране/шопе отлично от страны кардхолдера.

лектор: Так-же помним о таможенных лимитах, естественно вся инфа есть в гугле.

лектор: Страница вбв имеет свой антифрод который нужно пройти, как правило это не трудно за исключением уже подуставшей Германии.(к вопросу о регион локе,это один из способов как банк определяет - ip не совпадает со странной биллинга карты)

лектор: Да у карт с 3ds как правило долгий чардж (кроме юк и юсы), и если оплата произошла то вина лежит на холдере, собственно шоп за нее ответственность не несет, поэтому даже если шоп видит запрос из банка,то может отправить.

лектор: у амекса существует аналог вбв,это сэфкей (но шопы с поддержкой этой защиты мало распространенны)

лектор: В заключение хочу сказать что тенденция такая, что везде стараются чтобы 3дс код был по смс,либо 2фа через приложение, вбивы со сброшенным кодом либо быстро умирают, либо код просто не сбросить. Учитывая что мат с известным кодом достать трудно, то стоит либо вбивать в шопы где нету 3дс защиты,либо ее нету на карте(либо автовбв).

Вбив от А до Я

лектор: Всем еще раз привет.

лектор: Что есть вбив и из чего он состоит?

лектор: В общем и целом вбив выглядит следующим образом:

1. Нашел шоп

2. Подобрал материалы под вбив (карта, сокс/туннель/дедик, адрес/посредник)

3. Вбил

4. PROFIT

лектор: Но... когда вместо Order Success вы начинаете получать order cancelled / decline, приходит понимание, что на самом-то деле, деталей/подводных комней/чертей в тихом омуте - называйте как хотите - намного больше, чем 3.

лектор: Возможно вы об этом никогда еще не задумывались, но именно это и могло/может быть причиной ваших канцелов. Прямо сейчас я предлагаю разобрать из чего состоит вбив и с чем его едят.

лектор: Возьмем за основу называние каждой детали "переменной". Назовем группу переменных, подходящие под одну категорию - блоком; каждый блок состоит из нескольких подпунктов и переменных внутри него, приступим к подробному рассмотру блоков и переменных внутри них:

лектор: Блок CREDIT CARD:

- bin (первые 6 цифр карты, определяет банк-эмитент, страну выпуска, уровень карты, наличие/отсутствие vbv)

лектор: На том или ином бине может стоять ограничение на платежи, лимиты расхода средств / лимиты на оплату в интернете, или он просто может быть "безденежным", различиные типы VBV/MCSC и его сброса(сброс вариативен в зависимости от бина);

лектор: autovbv bins - когда вбв на карте есть, но НЕ требует ввода пароля и процессится автоматически.

лектор: Про VBV читаем здесь: <https://wwh-club.net/wiki/vbv-mcsc/>

Зацикливаться на этом подпункте не стоит, но как минимум взять на заметку надо. По этому записывайте каждый бин, встречающийся вам в работе, а также результат работы с ним.

лектор: - Уровень карты, тип карты

Уровень карты, Classic / Platinum / Premier / Gold и т.д, а также Debit / Credit. Исходя из уровня карты, может делать предположения о наличии баланса на оной. Логично, что на платиновых кредитках будет больше, чем на дебетовых классиках - чисто статистически. <https://wwh-club.net/wiki/visa-tipy-kart/> | <https://wwh-club.net/wiki/mastercard-tipy-kart/> | <https://wwh-club.net/wiki/amex-tipy-kart/> |

лектор: - валидность карты

Ничто не имеет значения: ни качество айпи, ни настройка системы, если - карта мёртвая. Стопроцентно убедиться в этом можно только прозвоном в банк (или при наличии энролла к карте). Чекеры нередко убивают карты, поэтому слепо верить им нельзя, а США карты до вбива лучше не чекать вообще.

лектор: - billing info/address - адрес кредитной карты(billing address, биллинг - адрес проживания кардхолдера), к сожалению, переодически на картах проскакивают кривые

биллинги, и в случае вбива кривой карты в мерч, который проверяет AVS (например почти все шопы USA) такая карта не войдет.

лектор: Причины способствующие этому - это метод добычи карт, почти всегда информация о карте к нам попадает та, которую холдер ввёл где-то CAM. Он может заказать что-то на работу, в дом тещи и так далее.

лектор: Методы борьбы с этим есть различные, расскажу о нескольких, которые использовал лично:

A) Пробив биллинга холдера до вбива карты

лектор: B) Поиск информации о холдере в общедоступных источниках, например, путём поиска в гугле Имя+зип (John Woods 18462) и проверки соответствия адреса и имени на различных сайтах и соц. сетях.

лектор: C) Вбив определенных бинов и типов карт. К типам карт можно отнести Business Cards (карты для бизнеса). Это рабочие карты, которые часто зарегистрированы на компанию/организацию (по этому не удивляйтесь, если вдруг вместо имени на такой карте увидите что-то типа "Mike Stewart Washington Water Restoration")

лектор: Плюс вбива таких карт в том, что в биллинг у них ровный в 99% случаев, чем не могут похвастаться иные типы карт, по причине того, что компания заказывает товары или оплачивает услуги приминительно к своему рабочему адресу, то есть, биллингу. Минус - далеко не все бины будут давать.

лектор: - чек карт. Есть несколько типов чеков карт:

A) Авторизация и списание. На карте авторизируется рандомная сумма денег (от $0.01 до бесконечности, но обычно не более $1), по такому же приципу происходит чек вбивом куда-либо при списании суммы.

лектор: B) Пре-авторизация и/или отмена авторизации. При пре-авторизации сумма не списывается из-за быстрой отмены оной; при отмене авторизации, зануление(отмена) происходит уже после непосредственной авторизации суммы

C) Прозвон в банк

лектор: Каждый банк и бин по-разному относится к разным рода чекам карт, но в основном влияние это негативное(особенно при работе по США) и бывает убивает карты (даже пре-авторизация)

лектор: Следующий блок - Блок маскировки:

Первый пункт будет называться "человеческий фактор". В данный момент многие банки автоматически анализируют сумму месячных трат и тип транзакций кардхолдера, и из-за абсурдного поведения (это когда 65-летняя дама покупает себе сноуборд) возможны(подчеркиваю, возможны) отказы транзакций со стороны банка.

лектор: Этот пункт не критичен, но не упомянуть его нельзя. Шоп передает информацию о транзакции банку, поэтому вам надо набирать минимальный фрауд-скор для обхода антифрод систем - ориентируйтесь на это.

лектор: К этому пункту есть подпункт "Образ поведения". Под этим я подразумеваю мотивацию и цель человека,

покупаещего что-либо в данный конкретный момент в конкретном шопе.

лектор: Создайте себе образ, станьте холдером, вы вбиваете свою карту, а не чужую, поверьте в это! Вы 65-ти летняя старушка и решили подарить сыну ноутбук? Поговорите об этом с саппортом шопа и спросите совета, почитайте описание товара, ошибитесь при вводе текста, ваши глаза уже не такие, как в молодости!)

лектор: Сокс и туннель в целом можно сгруппировать и назвать блоком ip-адрес, тогда переменные в данном блоке следующие:

лектор: - чистота ip по блэк-листам

- открытые порты

Я рассказывал об этом на своей лекции по безопасности, короче говоря это не является не негативным, не позитивным параметером в большинстве случаев.

лектор: - геолокация ip адреса по базе maxmind(или иной важной)

У whoer.net и ряда иных сайтов подключена устаревшая max-mind geo база, поэтому расход информации о геолокации от вбиваемого сайта в сравнении с whoer и некоторыми подобными сайтами может быть очень координальный и критический, вплоть до другого штата.

лектор: У определенных сайтов стоят собственные гео-базы, часто на этих сайтах вам предлагают автоматическое заполение зип-кода, города и штата, поэтому при вбиве в

такие шопы лучше ориентироваться на информацию предостовляемую ими и исходя из неё подбирать материал.

лектор: - proxy & risk score

- провайдер, хост-нейм, DNS, принадлежность ip хостинг-провайдеру

Интернет провайдер ip, хост-нейм может рассказать о принадлежности айпи к облачному хостеру (см. лекцию Безопасность и настройка вирт машины)

лектор: - дальность zip code ip от zip code cc

На примере: владеем картой с зип-кодом в биллинге 97401, значит зип ip должен быть максимально близким к зипу, то есть 97401 / 9740* / 974** и т.д. - однако это напрямую зависит от вашей темы и места куда вы вбиваете, для е-гифтов надо подбирать максимально близко, для вещевухи в зависимости от ситуации: под дропа/посреда или холдера.

лектор: Дедик, виртуальная и физическая машины входят во вторую группу маскировки, соответственно являются одтельным блоком и имеют свои группы переменных, а именно:

лектор: - ОС

Версия виндовс / линукс и т.д.

- браузер (Браузер, версия, WebRTC настройки, coockies)

лектор: Серъезные мерчи также могут запрашивать у браузера информацию об установленных плагинах(могут проверять только путём запроса id конкретного(ых) плагина(ов)), проверять сайты по списку, на которых вы

залогинены (<https://browserleaks.com/social> - можете проверить здесь, например). На практике при залогиненом, например, фейсбуке - это плюсик, но не критично.

лектор: Что есть набивка coockie?

- Набивака куки, серфинг по различным сайтам - иммитация реального пользователя ДО вбива.

лектор: Странно выглядит, когда человек с "голым и пустым" браузером идёт покупать гифтов на тыщу баксов, не так ли? Поэтому создаем образ рядового юзера-хомяка, посерфив предварительно по сайтам всяких локальных поликлиник/ресторанов, амазонов, ебеев, фейсбуков и тд, в общем об этом я рассказывал на своей лекции по настройке системы и безопасности, сейчас напоминаю так как имеет место.

лектор: - всевозможные отпечатки (шрифты, fingerprint, audiofingerprint и многие прочие)

Совокупность отпечатков генерирует ваш уникальный слепок пользователя, остающийся в системе, решается путем смены системы (смены дедика и тд), подмены ряда точечных отпечатков(таких, как шрифты, разрешение экрана, частота видеокарты, etc.) и/или использованием антидетекта.

лектор: Блок-процесс вбива. По моему мнению сам процесс вбива состоит из нескольких вещей, которые, как и все переменные, могут варьироваться и/или видоизменять себя:

- способ попадания в шоп (например, с гугла, или же с фейсбука/твиттера, иных мест)

лектор: Да, это тоже важно. Да, шопы это тоже видят! В той или иной степени это тоже имеет значение. Есть несколько типов перехода, расскажу о них начиная от менее трастовых переходя к более трастовым соответственно:

лектор: А) прямо по ссылке с домашней страницы браузера, например, browser > amazon.com

В) с поисковиков, например, google.com > amazon

лектор: С) Социальные сети, партнерки, различные купонные/кэшбековые сервисы.

Шоп отслеживает откуда вы пришли, наимение задроченные методы = наиболие трастовые!

лектор: - ручной ввод текста или копировать-вставить - антифрод это палит, вы при покупках со своей карты копируете своё имя из буфера обмена? Не думаю.

лектор: - прогрев шопа

Серфинг по шопу, ОСОЗНАННЫЙ выбор товара, чтение отзывов, методов доставки. Удаление/добавление товаров в корзину[из], регистрация аккаунта в шопе(и возможная временная отлежка оного), предварительный прозвон или общение с саппортом.

лектор: - вбив прозвоном / нет

Часть шопов располагает возможностью order by phone - ордер по телфону. Случается, что у холдера не грузит/глючит сайт и тогда на помощь приходит оператор поддержки, который собственноручно вводит данные вашей карты и тд. Плюс в том, что фактически антифрод не видит

вашу систему/ip адресс, соответственно не оценивает риски на основании этих факторов.

лектор: - биллинг = / ≠ шиппинг

Соответствие вводимного биллинг адрес шиппинг адресу, случается, что ордера отменяют из-за различия. Бороться можно следующими способами: проходить антифрод по всем остальным показателям / прогрев шопа (например, в лайв чате пообщаться и сказать, что хотите купить подарок другу etc.) / поиск позволяющих такое делать шопов / вбив биллинг = шиппинг = дроп/посред (при проверке AVS системой не прокатит в большинстве случаев), вбив неликвида, на который не "затянут антифрод".

лектор: - шиппинг

Ряд адресов широкоизвестных посредников может быть в черном списке у многих точечных шопов и мерчей, так же мониторятся дубли (покупали ли на этот адрес ранее в одном и том же шопе)

лектор: - емейл под холдера и под получателя(в случае с гифтами)

Почта тоже имеет определенный риск-скор. Наиболее трастовые - корпоративные почты по типу name@mysite.com. Наиболее фродовые - все, у которых упрощен процесс регистрации (например, mail.com, иначе говоря те, где при регистрации не надо принимать смс)

лектор: Кроме всего прочего, некоторые мерчи обращают внимание на имя в адресе почты (name@mysite.com) - могут

проверять наличие имени / фамилии холдера - также не критично, но также и важный плюсик.

лектор: Как вы сами можете наблюдать, переменных немалое количество. Поэтому, когда будут канцелы, дважды подумайте о количестве иных переменных, напрямую влияющих на результат работы. Аналогию создания этого списка можно провести в любой работе, будь это работа с палкой, покером, банками или партнерками.

лектор: Блок последствий вбива. Существует много различных вариантов последствий вашего вбива, рассмотрим основные:

лектор: - Decline. Деклайн. Шоп даже не позволил вам повесить ордер, часто это означает, что у вас проблемы с картой, поэтому в первую очередь стоит обратить внимание именно на неё и см. Блок CC. В остальных случаях у сайта или технические проблемы и закручены гайки(редко), или вы не проходите антифрод(или шопа или банка) от слова совсем и где-то палитесь, в таком случаем см. Блоки "Маскировки", "ip-адрес" и "Процесс вбива"

лектор: - Cancel. Канцел. Ордер повесился, но через время(или сразу) на эмейл пришла отмена ордера, причины: не прошли антифрод / шоп прозвонил холдера / что-то не так с картой и шоп не смог списать деньги.

лектор: Не прошли антифрод и ему что-то не понравилось - 2 варианта развития дальнейших событий:

1 - отмена непосредственно от антифрод системы шопа (или банк не позволили провести транзу)

лектор: 2 - по сумме набранных очков фрод индикаторов ордер попал в ручную обработу (это когда менеджер вручную одобряет/отменяет ордеры) и его отменил менеджер, или прозвонил холдера.

лектор: В остальном если с первым случаем всё ясно, то остальные стоит разобрать несколько более подробно.

лектор: Шоп прозвонил холдера - да, есть такие шопы, которые звонят всегда, также есть шопы которые могут звонить только на определнные ордера (например, на егифты) и/или от конкретной указанной суммы заказа (например все ордера $500+)

лектор: Методы борьбы с этим следующие: указание своего/своего прозвона телефонного номера с целью в случае необходимости принять на него звонок / указание левого номера (например, какой-то соседней кафешки с холдером) или несуществующего номера.

лектор: Однако из-за AVS системы в ряде стран такие ордера также могут страдать, лично я никогда не шаманю с номером холдера так как в моей работе совпадение AVS должно быть 99.99%, так что смотрите по своим нуждам и желаниям/темам.

лектор: Третий и последний вариант - это канцел из-за проблем с картой. Означает, что холдер либо успел спалить, либо ваш шоп процессит ордера не сразу, а уже после того как ордер оставил покупатель, и тогда он может схавать

даже мертвую карту и дать вам ордер, но денег с неё, понятное дело, не спишет.

лектор: - запрос шопом дополнительной верификации в виде фотографии идентифицируещего документа(паспорта/водительских прав) или фото карты. Означает, что вы где-то недотянули антифрод или ваш ордер показался подозрительным. Возникает также в случаях, когда шоп уже порядком задрочен и запрашивает верификации при малейшем подозрении.

лектор: - запрос дополнительной верификации путём прозвона, просят вас позвонить чтобы "уточнить" некоторые детали. Обычно гоняют по бэкгранду(см. лекцию по пробиву), в зависимости от шопа также можно означать, что у карты кривой биллинг.

Как бороться? Пробивать, звонить, отрисовывать. Если ордер или тесты стоят того. Заносим результаты в записи и делаем выводы.

лектор: Последний пункт лекции - Checklist. Чеклисты, мой метод работы по точечным шопам путём разрабатывания и отработки подхода применительно к ним.

лектор: Из себя представляет список пунктов (обычно 10-20), рассказывающих как можно пробить конкретный шоп на основании тестов вбива этого шопа, различные полезные заметки, выведенные на основании опять же опыта(например, как быстро приходят ордера/канцел) - мне это помогает в работе, своего рода создание шаблона, на который надо ориентироваться для успеха.

лектор: Пример моего чек-листа по одному крупному шопу:

"ШОП *****.COM

- Должны быть ровные биллинги

- Вбив должен происходить с одной попытки на 1 айпи. Исключение: 2 попытки

- Только ручной ввод и неповторяющиеся ранее переменные (а-ля почта)

- Рассматривать вариант вбивов с дедиков

- Если не прошел анти-фрод, но карта ровная, канцел придет на почту в течении 25 минут

- Когда ордер не пропускает антифрод система, мерч дает деклайн с текстом: Unable to process credit card at this time, processor reported (Authorization Failed)

- Если у карты недостатончо баланса или кривой биллинг, мерч дает деклайн с текстом: Please double-check your billing address and credit card information.

- Заходили следующие бины: 517805 464018 на такие-то суммы...*

И так далее.

лектор: Как вы могли заметить, блоки делятся в пунктовом и групповом порядке, по-порядку склассифицировать группы можно следующим образом:

Блоки Credit Card, Маскировка(система) - консолидированно - подготовка к вбиву.

лектор: Блоки Процесс вбива, последствия и чеклисты - результат подготовки к вбиву и, собственно, последствия. Важно прослеживать причинно-следственную связь между подготовкой и результатом, чтобы научиться понимать, где и когда виноваты вы, а где шоп или поставщик материала.

лектор: «Те, которые отдаются практике без знания, похожи на моряка, отправляющегося в дорогу без руля и компаса… практика всегда должна быть основана на хорошем знании теории».

Самореги Paypal

лектор: Ладно товарищи, всем привет еще раз

лектор: сегодя расматриваем самореги пп

лектор: сначала разберем теоретическую часть, потом регнем саморег и дальше ответы на вопросы

лектор: итак PayPal - палка/ пп. аккаунт пейпал регнутый вами - соответственно саморег пп

лектор: думаю это понятно

лектор: самый главный плюс саморега это долгий (как правило) чардж

лектор: и если прошла транза, то скорее всего товар отправят

лектор: и доедет он без проблем.

лектор: тоесть проблем как с сс, отмена транзы, разворот пака с саморегами нет

лектор: но естественно есть и минусы у саморегов

лектор: а именно раскачка аков

лектор: слепить саморег и сразу вбить с него стаф за 1к не получится

лектор: это возможно, но это скорее исключения из правила

лектор: поэтому саморег нужно разкачивать мелкими покупками/транзами

лектор: для того чтобы создать саморег необходимо:

1- фулка

2- телефон

3- ба

4- cc/вcc

лектор: ФУЛКА- это данные на реального амера

лектор: вот пример фулки

лектор: Dale S Murray

7955 Colee Cove Road

Saint Augustine,

FL us 32092

SSN - 593-12-7088

MOB - 904-237-3757

DOB - 09/16/1966

лектор: Dale S Murray - фио

лектор: 7955 Colee Cove Road - адресс

лектор: Saint Augustine,

FL us 32092 - город/штат/зип

лектор: SSN - 593-12-7088 - номер социального страхования

лектор: MOB - 904-237-3757 - телефон

лектор: DOB - 09/16/1966 - дата рождения

лектор: фулки проще всего покупать. обычная фулка стоит 0.5$

лектор: фулка с высоким КС(кредит скор) 2-3$

лектор: намного лучше по качеству фулки когда покупаешь сс на хта и пробиваешь к ней фулку

лектор: а идеальный вариант это заролить эту карту и подвязать к пп

лектор: такой вариант о хорош и на новореге можно сразу оплачивать / сендить 200-300$

лектор: 2- ТЕЛЕФОН

лектор: нам нужно будет принимать смс от пп

лектор: поэтому номер телефона в палке мы указываем тот к которому у нас есть доступ

лектор: а именно гв(google voice) или textnow

лектор: 3- БА

лектор: ба можно привязать к палке двумя способами

лектор: 1- инстой через лог-пас

2- миниками

лектор: 1- привязка инстой значит что в палке мы выбираем нужный нам банк, вводим логин пароль от него, дальше выбираем нужный счет и линкуем к палке.

лектор: 2- миниками. а каждого банковского счета есть аккаунт и роутинг номер. так вот для привязки этого счета к пп, мы водим эти номера и отправляем на них минидепозиты

лектор: минидепозиты это два начисления от пп на этот счет до 1$ которые списываются потом одной суммой

лектор: в стейте это выглядит примерно так

лектор: verifing PP john smith +0.10

verifing PP john smit +0.20

-0.30

лектор: аккаунт и роутинг номера ибо продаются сразу вместе с ба либо можно пробить через соответствующие сервисы на форуме

лектор: лучше всего брать ба сразу с номерами

лектор: это может пригодится в будущем при отрисовке стейтов или в случае необходимости конфирмнуть ба еще раз

лектор: стоимость ба 1-30$ в зависимости от банка и баланса ба

лектор: при покупке обязательно обращайте внимание на условия замены ба

лектор: рекомендую на начальных этапах брать ба 5+ к

лектор: 4- CC/VCC

лектор: по cc сказал выше, что касается всс используйте visa vanilla card

лектор: вводим даные карты, конфирмим ее миниками и карта привязана

лектор: по теории мы закончили

Методы работы с саморегами Paypal

лектор: тема на самом деле весьма обширна и тут всегда есть место проявить свою креативность

лектор: мы рассмотрим самые расспространенные варианты

лектор: итак- первое правило, ведем себя как реальный амер

лектор: так вот

лектор: если саморег не дал покупку, сенд, донат- помогает отлежка, уменьшение суммы транзакции, смена товара/селлера/почты/шопа

лектор: повторюсь, перед тем как работать с саморегами, настоятельно рекоменду почитать архивы по палке

лектор: разберем сленг

лектор: инстант-мгновенно

сенд- отправка денежных средств с одого ака пп на другой

миники- минидепозиты

стейт - statement - выписка из банка

лектор: по организации работы, как я говорил палку берет числом, и когда саморегов у вас накапливается приличное число то особенно остро становится вопрос ведения статистики и отчетности

лектор: поэтому советую вам сразу завести стату в экселе или подобной проге, кому как удобно

лектор: в стату я обычно вписываю:

дату реги ака

дату привязки ба

дату последнего действия

какой ба привязан (миники если есть)

почту

и место для заметок

лектор: туда записываю транзы, когда клирнется и подобную инфу

лектор: помимо этого, как говорил выше, советую поставить thunderbird, сборщик почт для удобства мониторинга своих саморегов

лектор: некотрые варианты нестанартной регистрации аккаунта пп:

лектор: 1) через оплату с CC

лектор: ищем донат принимающий оплату пп, пробуем оплатить с cc на 1-2$. вводим данные, ставим галочку

лектор: "Зарегистрировать аккаунт пейпал"

лектор: оплачивае и получаем саморег с одной транзой

лектор: потом заходим в ак, через эд мани добавляем dob и ssn

лектор: если все орм то цепляем гв, дальше ба и в отлегу на 3-7 дней

лектор: сразу обьясню, отлега, это когда мы вообе не заходим в ак пп после удачной транзы

лектор: 2) выставляем инвойс на пустое мыло

лектор: "пустое мыло" это почта на которую еще не зарегистрирован аккаунт пейпал

лектор: с саморега пп выставляем инвойс на пустое мыло, на эту почту приходит письмо с инвойсом, переходим по линку с него и оплачиваем инвойс ванилкой (до 100$ заходит норм)

лектор: одновременно качаем два своих ака

лектор: 3) сенд на пустое мыло с трастового ака пп

лектор: трастовым аком может быть как наш саморег хорошо раскачанный, так и аккаунт пп реального амера с множеством успешных транз

лектор: во втором случае придется проявить креативность ну например купить игровые ключи и продать амерам на форуме с оплатой через пп на пустое мыло

лектор: соль этого метода в том, что к такому саморегу у палки изначально будет выше оверие и его гораздо проще будет сливать

лектор: дальше

лектор: виды оплаты в самореге пп:

1- с сс/всс

2- с ба (е-чек и инста)

3- с баланса пп

4- бмл

лектор: поясню про оплату с ба

лектор: она бывает двух видов:

1) е-чеком

2) инстой

лектор: оплата ечеком занимает 3-5 банковских дня/дней

лектор: простыми словами это банковская операция списания средств с прилинкованого к пп ба и перевод их на другой аккаунт пп

лектор: оплата истантом это тот же ечек но с одним отличием

лектор: в случае инсты палка доверяет нашему аку пп и отправляет деньги сразу, как бы кредитуя нас, а сама потом ждет пока очистится ечек

лектор: день когда перевод средтв с ба на пп завершен и называется днем очистки (клира ечека)

лектор: рассморим рефы (refunds)

лектор: реф это отмена покупки и возврат средств

лектор: как правило палочники применяют рефы с целью залить деньги на балик пп

лектор: какие тут есть особенноси и подводные камни

лектор: если оплата происходила с сс- то при рефе средства возвращаются на сс

лектор: если с БА ечеком который очистился - падает на баланс пп

лектор: если с ба ечеком, средства списались с ба но сама транза в пендинге- через 3-5 бизнес дней упадет на баланс

лектор: если с ба инстантом- через 3-5 бизнес дней упает на баланс

лектор: с бмл реф упадет назад на бмл

лектор: варианты слива баланса пп

лектор: 1- обнал

2- слив в стаф

лектор: варианты обнала:

лектор: 1) сенд с балика на выводной ак пп и вывод с него на visa (около 3 бизнес дней)

лектор: 2)вывод а ба на этом же самореге

лектор: самый простой и эффективный на мой взгляд метод

лектор: оплатил, рефнул, сналил

лектор: слив в стаф

лектор: иногда в стаф слить проще чем сналить

лектор: но там меньше процент если вбивать на скупов и долбше ждать профит если слать себе стаф

лектор: для этого регаем ак ибея, пп к ибею не линуем

лектор: качаем его мелкими транзами с балика

лектор: да, регаем ак ибея на данные посреда

лектор: набиваем 5 фидбеков мелочухой

лектор: и можно начинать бить на посреда айфоны, макбуки с баданса наших саморегов

лектор: дальше

лектор: бывает что ак с баликом ушел в лимит на 180 дней

лектор: ничего страшного, такой ак откладываем, через 180 дней вяжем свой выводной счет и сливаем балик

лектор: да, добавлю по ибейке, наш ак ибея лучше перевести в бизнес ак

лектор: так будет чуток легче литься

лектор: если саморег не дает:

лектор: помогает отлега

лектор: 3-7 дней

лектор: или снижение суммы вбива, смена селлера, шопа

лектор: не делайте много попыток однотипных действий

лектор: как минимум получите анюжиал активити

лектор: в худшем случае лимит

лектор: это называется удрочить ак

лектор: делайте 3 попытки, больше не желательно

лектор: связки для работы с саморегами пп

лектор: 1) 1вирта=1 саморег + туны/соксы

лектор: 2) основа+ антик + туны /соксы

лектор: 3) деды домашки со скрытой учеткой

лектор: 4) вирт машина+ портабл под каждый сам + туны/соксы

лектор: 5) основа+ сфера+ соксы

лектор: 6) рега ака основа+ сфера+ соксы. вбив ака с hvnc

лектор: лимиты :

лектор: 1) легкий- принять смс, смена пароля, секреток, привязка/конфирм ба

лектор: 2) средний- нужна отрисовка паспорта, iD, стейт CC/ба, пруф адреса. рассмотрение два бизнес дня

лектор: если за это время не сняли то нужно звонить в палку

лектор: 3) тяжелый- все вышеперечисленное плюс разъяснение по транзам

лектор: процент того что снимут такой лимит крайне мал

лектор: проще загнать на 180

лектор: на этом пожалуй все.

Брут Paypal

лектор: Добрый вечер всем! Сегодня я ваш лектор и тема нашей беседы - вбив

брученных аккаунтов платежной системы Paypal или коротко - брут пп.

лектор: Я дам вам основную информацию по работе с данным направлением кардинга и отвечу на вопросы, которые могут у вас возникнуть в ходе лекции. Поехали!

лектор: Начнем с небольшого вступления

лектор: Работаю с палкой с момента регистрации на форуме и прохождения обучения.

лектор: Завлекло это направление в первую очередь своей простотой и доступностью для меня тогдашнего.

лектор: Т.к. для работы нужен просто дедик, сами аккаунты и адрес куда слать.Все остальное это уже дело техники.

лектор: За это время палка много раз подкручивала свой антифрод и работать становилось все сложнее и дороже. Но и мы не стояли на месте и каждый раз узнавали что-то новое.

лектор: Чтобы вы понимали, как изменился антифрод за эти 2 года в работе с брут пп, приведу пример.

лектор: Раньше, когда я только начинал, можно было делать так.

лектор: Заходишь в любой шоп с ликвидом (айфоны и прочее). Пробуешь вбить туда палку, и когда мы ввели лог пас я просто добавлял адрес посредника, палка этот адрес жрала и какой нибуть телефон ехал ко мне на склад. Возможно вам еще не понятно что тут такого. Но если вы начнете работать в этом направлении и после будете перечитывать эту лекцию, вы поймете что сейчас это сделать почти нереально, или было бы большим везеньем.

лектор: теперь непосредственно о работе с брут пп

лектор: Начнем с покупки аккаунтов для работы.

лектор: В силу того, что у селлеров бывают разные чекеры, вид самого аккаунта, который вы купите, может время от времени меняться, но в целом информация там написана одна и та же.

лектор: Для примера:

лектор: ==========

sklotovich@aol.com:Sklo5151

Holder name - shellie klotovich

Address - shellie klotovich|Po box 160||CROCKETT|CA|94525

Primary e-mail: sklotovich@aol.com

Limited: - False

Country - US

Phone - 19253815811

Balance - USD|0

Card - CC 5805|11/17

Bank 8134|J.P. MORGAN CHASE BANK, N.A.

Transactions:

85,05 USD-Bank account 30.06.2017

85,05 USD-Jennifer Nicolini 10.06.2017

233,00 USD-Bank account 29.05.2017

210,00 USD-Jennifer Nicolini 29.05.2017

==========

лектор: Тут в целом должно быть все понятно и без знания английского языка

лектор: но кратенько объясню

лектор: В начале идет логин и пароль от самой палки. Далее ФИО (Holder name), адрес (Address), почта, телефон, лимит\нелимит, страна аккаунта, телефон, баланс, кредитная карта, банк (БА) и транзации, которые были совершены владельцем с этого аккаунта.

лектор: Перед покупкой желательно определиться с тем, какую страну Вы будете бить.

лектор: Это в основном такие направления - юса, еу (европа) и экзотика (по сути все остальные страны).

лектор: Сказать, какую страну бить лучше я не могу. Лично я начинал свой путь с юсы аккаунтов, но Вам бы посоветовал начать с еу аккаунтов, т.к. по моим наблюдениям там ордера заходят лучше.

лектор: Ребят, все понятно из выше написанного? вопросов нет или есть?

лектор: идем дальше, только начали

лектор: На данный момент все продаваемые аккаунты можно разделить на 2 категории - с транзакциями (1) и без транзакций (2).

лектор: Второй тип аккаунтов еще называют нулевками

лектор: Чем хороши аккаунты 1 типа, так это тем, что КХ там активен, есть покупки в различные шопы или сервисы, и процент того, что ваш вбив пройдет конечно намного выше

лектор: Нулевки чаще всего использую для угона аккаунта, и последующего прикрепления БА со сливом его в шопы\сервисы.

лектор: Найти продавцов брут палки вы можете в соотвествующем разделе на

форуме - https://wwh-club.net/forums/ss-full-info-ba-paypal-pr-material.429/

лектор: https://wwh-club.net/forums/ss-full-info-ba-paypal-pr-material.429/

лектор: Теперь перейдем к теме "С чего вбивать".

лектор: 1. Dedicated servers (дедики) Чаще всего у продавцов встречаються таких видов : Домашки (Home) \ Серверки (Servers) \ Амазон (Amazon)

лектор: 2.SSH (тунели) \ socks (носки) \ proxy (прокси)

лектор: Не могу сказать с чего нужно вбить чтобы дало 100%, я думаю сами понимаете

лектор: Но, ориентируясь на то, что вы только начинаете свой путь, и вам как никому другому важен хоть какой-то положительный результат, я бы посоветовал начать с дедиков.

лектор: Только не берите домашки сразу по 10 баксов

лектор: хоть селлеры и говорят что они самые лучше и чистые, нам пока такое не нужно

лектор: вы так больше на материал потратитесь и разоритесь

лектор: Берите домашки - серверки до 300-400 рублей

лектор: Любил и люблю вбивать с амазон дедиков, они в среднем 64 рубля стоят

лектор: Тем, кто чуть попрошаренней, советую использовать схему "вирту+тоннели".

лектор: Продавцов всех этих богатств вы так же сможете найти в соответствующих разделах на форуме.

лектор: Для работы с дедиками используйте программу - mRemoteNG.

лектор: Теперь представим, что вы купили аккаунты брут палки и определились с устройством, с которого будете бить.

лектор: Теперь осталось понять: а куда вбивать и с какой целью? По старой схеме я разделю то, куда мы можем вбить на 2 категории

лектор: 1.Физический товар

2.Электронный товар

лектор: Первую категорию товара вы можете вбить либо на посредника, с последующей транспортировкой к себе, либо на дропа, со сдачей товара за процент.

лектор: Про вторую категорию наверное догадались, в нее входят различные гифты

магазинов, которые можно так же сдать скупам\продать\самим вбить себе

на посреда.

лектор: Очень внимательно отнеситесь к выбору посредника, т.к. бывают попадаються очень неприятные компании, которые рассматривают посылки под микроскопом, и любое несоотвествие влечет к бану аккаунта.

лектор: Еще немного важных моментов. После НГ 2018 палка заметно подкрутила

антифрод и сейчас даже просто зайти в аккаунт бывает проблемотично.

лектор: Как нам это сделать? Берет любой шоп с каким нибуть неликвидом и через мгновенный чекаут пробуем купить на КХ какую нибуть мелоч (максимально дешевую).

лектор: Далее пишем в адресной строке paypal.com и смотрим результат. Если вы в аккаунте, отлично. Если нет, берите другой ак и повторяйте опирацию.

лектор: даже если СЧ, это не значит что вы не сможете попасть в личный кабинет. Если выскочило сч, попробуйте написать paypal.com, много времени не потеряете, но где то сможете и вас перепинет в ЛК

лектор: там уже можно шопы смотреть и в них попробовать вбить, уже хорошо

лектор: Секьюрити чек

лектор: ЛЧ - личный кабинет

лектор: Большую часть шопов можно разделить по способу вбива на 2 категории. Первый, это так скажем "классический". Когда вы нашли шоп - положили товар в корзину - нажали кнопку чекаут - ввели билинг\шипинг адрес - выбрали способ оплаты PayPal - вас перебросило на сайт палки где вы ввели лог пас - шоп вписал адрес в палку - вы оплатили ордер.

лектор: Вторая категория пробивается через быстрый чекаут, через который мы как раз и пробуем в начале попасть в ЛК пайпала. Как он выглядит? Вы найшли шоп, положили любой товар в корзину, и там сразу увидете кнопку - Check out with PayPal. Это и есть кнопка быстрого чекаута. При нажатии на нее и вводе лог пала, вы увидете при ревью адрес КХ. Вот пример шопа, чтобы вы понимали, с таким чекаутом - shop.lego.com.

лектор: Шопы только с таким чекаутом пробиваються так.

лектор: В начале бы берете шоп 1 категории, дошли до ревью, когда шоп вписал нужный вам адрес вы НЕ

оплачиваете покупку, а оставляете аккаунт отлежаться сутки-двое.

лектор: Обязательно созраняете куки в sendspace.com если это дедик и он может сдохнуть

лектор: Потом идете в шоп с быстрым чекаутом (2 категория), и уже там при нажатии

кнопки Check out with PayPal вы увидите свой адрес, на который с легкостью сможете сделать ордер.

лектор: обязательно научитесь сохранять куки

лектор: Это очень важно в работе с палкой. Дедик может помереть, и все ваши старания с отлегой будут

напрасны. Смогли попасть в аккаунт - это уже повод сохранить куки.

лектор: Если это дедик, то скачайте сразу на него портабл мазилы (до 55 версии) и установите расширение для работы с куками, лично я пользуюсь advanced cookie manager, но вы можете поискать что-то свое.

лектор: Хотел бы еще указать на большую ошибку новичков. Когда будете пробовать бить палку, берите не большие суммы, примерно 50-100$

лектор: т.к. вам сейчас главное получить хоть какой то результат. Не бейте ebay.

Хотя прям если очень хочеться, можете попробовать, но главное не на большие суммы!

лектор: Любой материал, будто бы это дедик или сокс, вы всегда его подбираете

под штат если это юса, и под страну если это еу (европа).

лектор: Сохраняйте любые результаты. Я всегда работал с екселем. Если вбив прошел -записывайте все, что может пригодиться - шоп, почту куда вбили, лог пас самой палки, откуда вбили (дедик, соксы), если ордер есть то его номер запишите и т.д.

лектор: Так же хотел бы заметить такой очень важный момент. Палка работает с плавающим антифродом и если вы сегодня работаете, и по вашей методике делаете за час пару ордеров, то это совсем не значит, что завтра у вас получиться тоже самое.

лектор: Вот чтобы знать, когда палка немного "подкрутила" антифрод и прочие нюансы, советую всегда мониторить раздел с обсуждением работы брут пп на форуме -

https://wwh-club.net/threads/rabota-s-brut-pp.69279/unread

Работа с Брут аккаунтами

лектор: Ну что же, начнем наверное. Если кто опоздал, по логам нагонит

лектор: Сегодня мы поговорим по брут. Это самое выгодное по финансовым затратам направление в кардинге, из минусов в нем только противоположно затратам - затраты времени. Вспомним, что такое брут

лектор: Брут - процесс перебора строк логин:пароль из базы, с помощью софта на предмет валидности к нужному вам сервису

лектор: Что нам для этого надо:

лектор: 1. Базы

лектор: 2. Прокси

лектор: 3. Сервер

лектор: 4. Софт

лектор: Теперь обо всё по порядку

лектор: 1. Базы. Что это такое и где это берут? База - слитый дамп взломанного сайта, где хранятся учетные данные пользователей в виде логин:пароль. В виде логин:пароль не всегда, могут быть и хэши, но в основном продают в чистом виде

лектор: У баз есть несколько характеристик.

лектор: Это приватность - отношение количества уникальных комбинаций логин:пароль к отношению тех комбинаций, что уже давно пылятся в паблике

лектор: Это валид - соотношение количества строк логин:пароль, с которыми мы можем попасть на почту к холдеру

лектор: Ну и тематика с географией

лектор: 2. Прокси. Прокси вы выбираете индивидуально, а если вы нашли свой идеал, никому о нём не рассказывайте. Это такой же "хлеб", как посреды и дающие темы. Если вам

нужно сбрутить аккаунты какого то слабо защищненного сервиса, вроде небольшого шопа с шмотом, можете брать первые попавшиеся. Если нужно брутить Амазон, Ебей, ПП, то тут придется искать

лектор: 3. Сервер. Нужен он лишь для того, что обеспечить софту нормальные условия для работы, увеличить вашу безопасность и для того, что бы ваш брут работал без перебоев. К выбору сервиса стоит подходить исходя от своего финансового состояния, предложений под подобные запросы хватет на эксплоите, ценник колеблется от 10 баксов и выше, в десятки раз выше

лектор: Сразу отвечу на возможный вопрос, можно ли брутить на своем компе/виртуалке. Можно, только в случае с виртой эффективность будет низкой(системные требования), а на своей основе НИЧЕГО купленного на форумах нашей тематики запускать не рекомендую. Сегодня софт нормальный, а завтра с апдейтом ваши битки уедут к разработчику софтины

лектор: 4. Софт. Самое главное, без чего и брутить то не получится. Приобретается под нужный вам сайт на ВВХ, Эксплоите и на БХФ(ох зря). Смотрите внимательно на отзывы и на то, как давно этот кодер выплыл в паблик. Довольно часто, кодеры пилят годноту, а потом забивают хрен на обновы. Обновы будут делать только люди, которые крепко замотивированны наработанной репой и финансами

лектор: Софт так же пишется под заказ, на тех же форумах.

лектор: Есть ещё такая штука как "комбайны", это софтины, где собран брут сразу под много разных сайтов. Брать я вам их не рекомендую, потому что в начале продаж он работает нормально, но потом всё начинает отваливатся и кодеры часто сливаются. В начале пути 2 раза так споткнулся

лектор: Сайт для работы с друт аккаунтами вы можете найти и самостоятельно, хоть нишу уже и поимели во все щели, незанятые дырки есть и сейчас. Для начала, вам нужно оценить, как часто люди используют этот сайт, понятное дело, что на Ебей и Амазон количество "гудов" будет в разы выше, чем на непопулярном сайте с шмотом, только вот работа по этим сервисам будет очень разной. Девственный магазин, который ещё не выгребали, будет давать легко и непринужденно, а для работы с гигантами придется выложить нехилую сумму на тесты

лектор: Так же, вы должны проверить, сохраняет ли сайт кредитку. Для этого берём 2 деда (2 вирты + прокси, либо слепки антика), берем одну CC, почту на mail.com и идём вбивать с первого дедушки. Сохраняем при оплате платежные данные. Потом имея на руках лишь логин с паролем, идём в этот же шоп со второго деда, пробуем зайти в аккаунт и сделать второй ордер

лектор: Если прокатило, у вас не просит ни CVV, ни других каких то данных, которых у вас нет, значит по шопу можно с брута поработать

лектор: Оценивайте, будет ли ликвидно его брутить, заказывайте софт и в бой. Чистый шоп это всегда удовольствие

лектор: Еще фишка есть, о которой я раньше часто упоминал. Не стесняйтесь пользоваться Гуглом, он знает все. Если вы думаете, что шоп девственный, это ещё не значит что это так. Пробуйте вбивать в запросе www.nameshop.com кардинг, carding, вполне возможно, что он всплывет где то у нашиз собратьев в черном спске

лектор: Теперь пройдемся по тому, как именно мы можем вбивать

лектор: Вариантов у нас несколько. Мы либо тарим это всё на посреда, варварским способом, либо тарим на дропа так же по варварски, можем бить на адрес КХ, если шоп шлет почтой, которую можно редиректить, пикапить и т.д.

лектор: Немного побробнее

лектор: 1. Прямой на посреда или дропа. Мы просто заходим в аккаунт, меняем шиппинг адрес на свой, не затрагивая биллинг(актуально для Юсы) и бьём. Прокатило - трясёмся и ждём конфирма, не прокатило - лопатим аккаунты дальше

лектор: Тут лучше на дропа бить всё таки. Во всех шопах сидят люди, менеджеры, они прекрасно знают адреса посредов, умеют юзать Гугл

лектор: Кстати, о Гугле. Пробивайте своих дропов из админок

лектор: Они могут быть "запаленными", на такой адрес приход товара как праздник, обычно если в черном списке есть, шоп сразу аккаунт заблокирует

лектор: Так же, старайтесь не трогать имя холдера. Если Джон Вик сменил адрес, это приемлемо, но если он внезапно ещё и имя сменил, особенно на Васю Пупкина, то шансы у вас падают в нули. Если юзаете посредов, то регайте их на данные неславянские, каких нибудь Джамшутов и у нас и там хватает

лектор: По поводу пикапа могу сказать только то, что шансы вбить у вас примерно такие же, потмоу что суммы должны быть большими, а вот получение запикапленного товара тот ещё головняк. Тут и дропа могут принять и он сам скрысить может, да и ДС кушать хочет, может потерять ваш пак

лектор: Так же, могу вам посоветовать внимательно изучать шоп, по которому вы работать собираетесь, читайте досконально. У них часто есть какие либо акции, фишки, котрые при фантазии и должном уровне скила дают раздолье для действий

лектор: Как пример, в одном шопе можно было бить с брута, делать рефаунт на баланс до момента отправки стафа, а на балик уже тарить там ликвид гифты. Другой пример - так же возвращался баланс, но его можно было перекидывать по партнерам магазина, скарженный с такого балика товар был для всех антифродов "чистым" и работа шла отменно. Примеров на саом деле много, так что не ленитесь почитать 15 минут. Кардинг и в частности брут это не тупой перебор аккаунтов, но и работа головой

лектор: Теперь по самим брут аккаунтам, они не только с картами бывают. Есть и с привязанными аккаунтами

Пейпала, да и с другими платёжками хватет. Самый простой в освоении и работе - аккаунт+CC, всё по старинке, вам мешает только антифрод шопа, а антифрод банка обычно не так влияет на вбив. А вот с ПП вы и весь головняк палки с её ПМС получаете. Кроме того, что сам шоп забрить может, ещё и палка будет сыпать СЧ, СМ и т.д.

лектор: ПП хорошо для "посмотреть" как оно работает, стоят аккаунты копейки

лектор: Но для работы не советую, если вы с палкой не дружите плотно

лектор: Вбили вы всё таки ваш товар, ордер в пендинге. Что нам мы можем сделать для того, что бы увеличить вероятность того, что вам этот стаф вышлют?

лектор: Мы можем только повлиять на то, как доступна холдеру аккаунта будет информация о этой покупке

лектор: Для начала, мы разбираемся с аккаунтом. Меняем там почту, пароль и телефон на свои

лектор: Почту регайте уже после удачног овбива под имя холдера, регать можете на mail.com, делается это быстро, СМС принимать не надо там

лектор: Если ордер небольшой, ставьте номер из головы, если большой, то свой скайп поставьте или номер прозвона

лектор: Это поможет только в том случае, если холдер уже и забыл про этот шоп и ему не пришла СМС от банка

лектор: К сожалению, в сфере интернерт платежей разитие ушло далеко и часто у холдеров есть и пуш уведомления на телефон и смс-ки и сами шопы звонят

лектор: Но если КХ раздолбай, то первые несколько дней он может и не заметить, а дальше уже ничего сделать не сможет

лектор: Для профилактики, если ордер большой, мы может нагрузить ему спама на почту. Но это такой себе вариант и нужен лишь для подстраховки, если ордер сильно важный. Скорее холдер узнает о трате по СМС или уведолению на телефоне

лектор: Так же, смотрите контактные данные КХ не только в инфе о шиппинге, но и в биллинге, там часто дублирован номер телефона и вполне возможно что и данные о ПП аккаунте, где почта может быть другой

Брут Ебей + Paypal

лектор: Всем привет. Сегодня мы поговорим о брут ебей+пп (PayPal), разберем что это такое и с чем его едят.

лектор: Я лично работаю в этом направление примерно год, застал как и хорошие времена, так и не особо, например как сейчас.

лектор: Сразу отмечу, что я не заработал миллионы, но, если учитывать, что уходило минимум затрат и времени, то я считаю это хорошим и доступным способом заработка.

лектор: Сегодня мы научимся вбивать брут аккаунты от ебей и на протяжение всей лекции постараемся более подробно познакомиться с этим гигантом - Ebay.

лектор: Начнем в первую очередь с плюсов, которые нас ждут:

лектор: Это легкодоступный материал, думаю, если вы немного листали шопы, то почти в каждом видели ebay+pp, ebay+cc, абсолютно разных стран

лектор: На самом деле сейчас с ebay аккаунтами не очень хорошо, потому что они умирают в течении несколько часов, так как сломался способ авторазации с помощью которого чекали акки.

лектор: Основная страны eBay аккаунтов USA и UK, которые выделяются, но есть еще и IT,DE, CA тоже насколько знаю, но сейчас большинство селлеров продают это как микс либо под другим названием разные страны. Все эти аккаунты имеют вариацию либо с пп, либо с cc соответственно с привязанным аккаунтом пейпал, либо картой.

лектор: Собственно вот так выглядит лог аккаунта:

лектор: hneil@live.co.uk:neil1976 / Access Email: NoCheck / UserID: neil132011 / FeedbackScore: 17 / Orders in the last 60 days: No / CC: No / PP: Yes / Country - GB / State - Scotland / City - Aberdeen / Street - 1 lossie place / Zip - ab166tj / Phone - 07927 938797 / Seller: No

лектор: Разберемся по порядку мыло ходлера/доступ к мылу(такое не во всех шопах есть и стоит в пару раз дороже)

/айди юзера на ебее, он же логин(чаще всего заходите именно через Юсерайди, нежели емейл)/Кол-во отзывов(нам чем больше, тем лучше, но по факту, если отзывов очень много, то владелец аккаунта быстрее заметит нашу покупку с его аккаунта)/покупки за последние 60 дней(чаще всего говорит нам об активности аккаунта, чаще всего с таких не покупается кстати говоря, но зато холдер может вообще и забыть про свой аккаунт)/привязанная карта/привязанный пейпал/страна/штат/город/адрес/зип/телефон/продавец или нет, но думаю, что тут вы и сами разберетесь это я так.

лектор: Собственно цена на эти же аккаунты. Ебей аккаунты - это дешево, если мне не изменяет память, то за 1 аккаунт мы платим от 20 до 30 рублей это за ЮСА, ЮК аккаунты, микс страны же будут дешевле, наверное сами понимаете почему

лектор: Среда работы, например ваш дедик, сокс, внс, тунель и все, все, что можно придумать для работы. Лично я раньше работал на дедике и обрабатывал больше 100 аккаунтов с одного дедика это как минимум, думаю, что с теми же внс должно также работать, но лично не тестил, так как ранее было довольно дорого брать внс и порой внс живет намного меньше, чем дедик, но в последнее время я сменил направление, но об этом позже.

лектор: Насколько знаю, что лучше всего идет с реального телефона, но я лично не пользуюсь, так как просто не умею настраивать телефон и желательно нам пригодится пропатченный роутер приобретать, если же мы решим хорошо работать с телефона.

лектор: Праздничные дни. Как и во всех шопах фрод ослабляется, можем с энтузиазмом пробовать суммы, которые мы не могли пробовать до этого.

На этом же плюсы заканчиваются, теперь пройдем к минусам, их примерно столько же.

лектор: Собственно минусы:

лектор: Легкодоступный не значит хороший, а именно я часто слышу вопросы что-то типо “подскажи селлера аккаунт, магазин, тему, форум и все, все, все” идеального шопа нет, все только тестировать, если вам нужно я дам список шопов с аккаунтами, которые знаю, некоторые использую, но время идет и я не могу сказать или точнее назвать какой-то из шопов хорошими.

лектор: Сейчас эта проблема особо актуальна, потому что аккаунты быстро дохнут.

лектор: Вот так например выглядит плохой аккаунт https://imgur.com/PEXanW6 , то есть он уже залочен и вы на него зайти не сможете.

лектор: У каждого селлера свои правила, то есть у одного замена в течении 3 часов, а у другого 6, а один вообще 12, но если селлер порядочный, то он должен сделать замену. Сразу же совет, если вы купили аккаунты, то сразу идите их

отрабатывать. Я честно не знаю, как ебей палит, что аккаунт сбручен, но через время его могут заблокировать. Быстро отработали, вбили что хотели или не вбили, но аккаунт отработали и у вас, и у селлера нет никаких проблем. Не откладывайте аккаунты никогда!!!

лектор: Сейчас кажется вообще нет гарантии на аккаунты у многих(по выше сказанной причине)

лектор: Нам будет трудно найти незадроченные сокс дедики, тунели(их особенно), разве что внс обычно чисты. Это брут, он общедоступен, поэтому привыкайте, что сокс задрочен, дедик убит. Найти кристально чистые материалы очень сложно сейчас, но это возможно. Лично по дедикам могу сказать, что на форуме нет хороших дедиков. Есть нормальные, но никак не хорошие, поэтому привыкните, что на них нужно будет еще надевать носки, но я пробовал не все сервисы, которые есть у нас, поэтому может я не прав в грязности. Приватные шопы с дедиками неплохи. Рискскор и проксискор мы не можем прочекать, когда же селлер продает нам, меня лично уверяют, что самый лучший, которых у них есть, а в приватных скорее всего будет встроен, но само собой за денюжку нужно брать чем меньше показатели, тем лучше.

лектор: Например вот скриншот одного из приватных сервисов с дедиками https://imgur.com/a/u4eTx96

лектор: Сразу предупрежу, что для тех кто планирует работать с дедиками. Покупаем только домашки, серверные пропускаем. У нас же с вами не стоит дома сервер с которого мы делаем покупки, верно?

лектор: Сама задроченность ебея. С этим мы вообще ничего не можем делать. У ебея бывают своеобразные месячные, как и у палки. Чаще всего это приходится на конец месяца. В основном с 25 числа и до конца месяца +- пару дней лучше не лезть в это время.

лектор: Перейдем непосредственно к самому вбиву. Я разделю направления на 3 части.

лектор: Вбив на кх с последующим реройтом. Тут дает на неплохие суммы и в основном это ЮСА, потому что там дропы, реройты, скупы, вообщем все добро там, но я лично не работаю по этому направлению, так как с юсой все хуже и хуже, но никто вам не запрещает работать по UK, но насколько я знаю, что там с реройтом туго. Тут могут быть трудности с почтами.

лектор: В юсе 3 основные почты - это fedex, usps, ups

лектор: fedex с запретом - реройтят, usps с запретом тоже реройтят, ups с запретом - считай пропало

лектор: Но если вы покупаете у какого-то частника на ебее, то вероятность того, что у него стоит запрет на реройт небольшая

лектор: хотя есть некоторые продаваны, которые следят прям за треком и развернут его обратно, если вы его реройтните. Таких встречал пару штук всего, но никак от этого не спастись, но если вы все же попали на такого, то просто запишите его логин, чтобы не попасться потом на эти же грабли.

лектор: Вбив со сменой адреса. Суммы тут не большие. В среднем до 150 фунтов(200 баксов), но это мелочь, а приятно. Страна работы ЮК(разные страны тоже пойдут), потому что по моему опыту адрес тут меняется намного лучше, но как плюс, что шипать мы можем прямиком в СНГ, либо любую другую страну на нашего дропа, посреда, дядю Васю. Шипать на себя я крайне не советую!!! Многие говорят, что сумма маленькая, да что тебе будет не бойся, но палить свое имя не надо. Услуги дропа для нас довольно дорогие, если же мы будем работать по вещевухе, как я писал выше до 150 фунтов, поэтому дядя Петя с соседнего подъезда думаю не откажется сходить за посылочкой за магарыч, опять же шанс того, что за вами придут минимальный, но какой-то % риска есть всегда в любом деле.

лектор: Диджитал направление, они же цифровые товары, если в нашем деле, то гифт карты. Все эти гифт карты, ваучеры, игры, игровая валюта. Список просто огромен, но лучше просмотрите темы скупов, там вы найдете %, а также полный список того, что они покупают, но если вы не нашли ваш гифт в скуп листе, то не расстраивайтесь, возможно его тоже заберут, но лучше уточнять перед покупкой самого гифта нужен ли он скупу или нет, чтобы не понести потери в случае нерентабельности.

лектор: Ебей это наверное самый легкий способ добыть гифт карты, который есть, а и да страна этого направления USA. Есть также немного и в UK, но в основном все гифты USA. У амеров с гифтами просто болезнь.

лектор: Максимум, что я покупал тут это гифт виктория сикрет на 500 долларов, большей стоимости я и не видел. Тут товары разделятся на два типа. Есть егифты, а есть бумажные, если их так можно назвать, но мы смотрим не на это.

лектор: Нам нужно, чтобы селлер отправлял номер карты и пинкод выглядит он чаще всего вот так

лектор: card number: 0064933006058171 95

Pin: 4234

лектор: Либо же гифт карта игровая/ключ, определенное кол-во символов например AAAA-AAAA-AAAA-AAAA, у всех разное кол-во

лектор: С помощью этих данных можем прочекать баланс карты, их же мы потом и передадим скупу. Так вот нас устраивает только отправление ебей меседжем, либо же на мыло привязанное к нашему пейпал аккаунту, но для последнего нам нужно покупать аккаунт ебея с доступом к почте. Это довольно редкость, но найти можно, правда цена будет отличаться. Я видел около 150 рублей за аккаунт в одном шопе. Но запомните, что гифт карты и игры это не единственное, что вы можете найти в диджитал направлении. Все зависит от вашей фантазии, потому что поиск ебея не особо умно работает, поэтому некоторые вещи вообще лучше искать через гугл, например “buy dildo on ebay”.

лектор: И так вбив, решать с чего вбивать вы будете решать сами, некоторые используют мобильные устройства, но их

довольно трудно настраивать и как правило работа с ними медленнее, чем с чего угодно, но и профитнее.

лектор: Дедик довольно дорого для старта, поэтому начнем или советую начать с виртуалки+соксы. Ресурсов где купить соксы очень много, но я лично беру на випах, но если хотите делать серьезные суммы, а именно выше озвученных ранее, то рекомендую отказаться от них, да и если хотите работать по Америке, то про випы лучше забыть, а Европа еще пойдет. После того, как мы натянули носок заходим на вхоер и шкала анонимности должна доходить до 90 как минимум, но лучше 100.

Самая частая проблема с которой я постоянно сталкиваюсь, что у сокса днс другой страны. Тут мы бессильны, но раз мы его взяли, то будем пробовать. Я лично всегда пробую все же это брут как никак о на то и брут, что берется количеством, а не качеством. Браузер юзаем либо мозилу, либо хром. Также нам нужно будет скачать расширение, чтобы после каждого аккаунта чистить наш браузер. Тут погуглите, их очень много на любой вкус и цвет, но я лично юзаю портабл мозилу, что после перезапуска все удаляется.

лектор: Вип72 соксы это скорее для того, чтобы просто попробовать. Стоят они дешево, но и качество такое себе. Есть много ресурсов хороших с соксами, такие как люкссоксы, фейслесс, сокскlаб(тут кажется даже мобильные соксы есть). Но все, кроме последнего ушло в приват и за аккаунт тех же люксов нужно закинуть зелени, фейслесс в этом плане дешевле. Не знаю, открыта ли там сейчас рега, но месяц назад регистрация была 50$, которые же упадут вам на баланс.

лектор: Переходим на ebay.com лучше это делать из гугла, если же мы делаем ЮСУ под реоут, либо диджитал товары используем домен .com, маленькие товары со сменой адреса мы используем ebay.co.uk.

лектор: Нажав на Sign in переходим на такую страницу

https://imgur.com/h0y80OH , сюда мы входим под нашим userid и паролем, рекомендую сразу с userid пробовать входить, потому что с почты часто не хочет.

лектор: Первый вбив всегда совершаем разминочный или как его называют прогрев, а именно это недорогой товар, я обычно покупаю какой-то мяч до 10 баксов или еще какой-то мусор. Например один из этих трех товаров https://imgur.com/a/rycIL тут выбираем, что душе угодно, ведь это просто разогрев, но если мы работает по ЮК и нам нужно сменить адрес, то стоит обратить внимание на доставку, то есть есть ли в нашу страну доставка и сколько она стоит.

лектор: В последний месяц я часто натыкался на то, что я хотел купить кросы, которые стоили 50 фунтов, но и доставка в мою страну стоила столько же, поэтому не поленитесь, поищите селлера, который отправляет дешевой почтой, какой бы почтой вы не отправляли с Англии, то придет оно вам на укрпошту, если в юа и на почту России, если же в ру, поэтому же бьющиеся товары я не рекомендую, чтобы не испортить себе настроение) сами знаете какие у нас почты

лектор: Эту прелесть мы видим где-то в середине страницы - https://imgur.com/vwh8Qvm , а за ней находим нужную нам

страну - https://imgur.com/vwh8Qvm 16 фунтов это норм доставка. Опять же, если мы по ЮСА под редирект, то эти все пункты мы пропускаем, только смотрим какой же почтой отправляет продавец, потому что некоторые нельзя редиректить, а на некоторый товар вообще может стоять запрет на редирект, но это чаще всего на дорогой, нам до такого еще рано

лектор: Диджитал так же ничего не трогаем, просто покупаем наш разогревочный товар.

лектор: В ЮК же перед покупкой мы меняем адрес, как пример тут мы видим один адрес доставки https://imgur.com/Yoijj6E , но часто попадаются и много, если же адрес один, то мы меняем на нужный прямо в нем, если же их много, например от 3 и больше, то пытаемся добавить свой, только не забудьте поставить галочку make this adresse primary.

лектор: Вот так выглядит фулл поменянный адрес, телефон указываем ненастоящий, просто нужной вам страны - https://imgur.com/a/HVV57 .

Если дало сменить, то синяя кнопка оплаты вновь горит https://imgur.com/a/o320F , если нет, то вы увидите ошибку, можете забить на этот аккаунт после того, как нам не дало сменить адрес, но перед этим зайдите и удалите адрес, который вы писали до этого в настройках аккаунута.

лектор: Дальше самое сладкое это опять же поиск товара. Переходим к поискам, советую покупать что-то неликвидное, то есть там не ломитесь попробовать купить аирподсы, видяшки и всякое такое, а шмот, неликвид

электронику, потому что со сменой в другую страну не особо крупные суммы дает.

лектор: Listings я всегда выставляю buy it now, чтобы отсеять ненужные аукционы, которые только мозолят глаза.

лектор: Sort я всегда меняю с Best Match на Newly listed, чтобы показывало товары, которые недавно выложили.

лектор: Обратить внимание также стоит и на селлера, который продает. Не выбирайте селлера с репутацией 0-50 самый оптимальный 100-200, но а также гиганты, часто они быстро шипают, у них легко купить.

лектор: Первую страницу поиска лучше пропустить вообще и начать с 2-3, кстати говоря некоторых селлеров нужно бомбить, поэтому лучше их записывать, как вообщем и все действия лучше записывать, но честно у ебея я какую-то закономерность дал - не дал перестал наблюдать в последнее время, но список селлеров на ебее действительно вам поможет, не нужно много расписывать просто логин или ссылку на него и пару слов например:

PR0$3LL3R228 - прислал кирпич вместо айфона.

PussyEater99 - быстро шипнул, быстро добавил трек.

Это конечно в шуточной форме, но я надеюсь, что вы меня поняли.

Переносимся на стадию, что ордер уже сделан, теперь нам нужно замести следы и выжидать наш трек/gift card, если вы не рероутите, а шипаете куда-то в определенное место, как например в моем случае в СНГ, то просто раз в 2 недели

отправляете вашего человека на почту чекнуть, если же трек все таки не пришел

лектор: Но в случае с рероутом трек нам обязателен, как и имя кх, так и адрес, куда нам идет пак.

лектор: Мы можем сменить абсолютно все данные в ебей аккаунте без каких-либо подтверждений, поэтому можете этим заняться, но как я заметил, что это не особо помогает, так как через все очень быстро восстанавливают.

лектор: Как вариант всегда существует флуд почты, но и он часто не спасает, когда у КХ просто стоит приложение пейпал и ему показывает, что деньги ушли, но не стоит огорчаться, если аккаунт восстановили, то товар все еще могут выслать, так как мы предприимчиво в ордерах нажимаем кнопку More actions>Hide order, теперь может существовать шанс, что КХ просто не заметит наш ордер, а как вытащить трек с мертвого аккаунта расскажу далее.

лектор: Есть много сервисов, которые предлагают эту функцию бесплатно, как ни странно, то есть всегда есть шанс, что большая рука большего брата доберется и до вашего пака, но ни я, ни мои знакомые с таким не сталкивались пока что.

лектор: https://imgur.com/a/exkmJ нажимаем как на скриншоте и нам в адресной строке будет отображена ссылка. Далее, мы видим в ссылке пару параметров - это itemid и transid. Именно в моей ссылке itemid - это 173009293376, а transid - это 1801961736007, вот их же нам и нужно сохранить.

лектор: В случае с диджитал товарами просто мониторим либо личные сообщения на аккаунте пока он нам доступен, либо почту, если же решили раскошелится. На этом собственно все.

Пикап, Перехват

лектор: Всем привет еще раз

лектор: Сегодня тема лекции Пикап/Перехват

лектор: Попрошу сразу, если у кого то в процессе лекции возникнут вопросы, задавать их когда я сообщу что можно задавать вопросы. Если по информации которую в данный момент прошли возник вопрос, записываем его в блокнот и потом быстро копируем я отвечаю и продолжаем.

лектор: Разберем что это такое и как по этому направлению работать.

лектор: По пикапу я советую работать упорным людям, которым не жалко бабла на тесты.

лектор: К примеру люди бьют ебей, палку и тд

лектор: Они имеют с одной успешной операции дай бог 300-400$, и плюсом ко всему это может занимать куда больше времени.

лектор: В пикапе все по другому. если вы нашли дающий магазин, то с одного ордера профит будет 1к+

лектор: Для работы желательно знать английский язык, или иметь на зарплате прозвона, тк звонить придется очень много, на счет отрисовок не так часто встречаются запросы.

лектор: Как я уже говорил, на тесты нужно приличную сумму денег. Сейчас не как раньше, взял сс, вбил в первый попавшийся магазин и ждешь товар, это не только в пикапе но и во всех других темах. Щас все очень сложно и найти что то дающее сложно. Нужно много работать.

лектор: Думаю на тесты хватит 1-1.5к$

лектор: В эти деньги входят затраты на СС, а желательно это должна быть роллка. Только суть ролки не изменить адрес телефон и тд, то есть мы не дрочим банк, не набираем очки фрода, а ролка просто что бы знать баланс, принять миники в редких шопах.

Второй пункт затрат это дедики. Цена на хорошие дедики достигает 25$ И один дедик можно использовать в один шоп. Вот и считайте. 1к баксов на грубо говоря 30 проб.

лектор: Но есть и светлая сторона

лектор: Вложили, и окупили за пару ордеров. Помоему неплохо.

лектор: Теперь к конкретике.

лектор: Берем дедик домашку чистую(с носков и тунелей что бы дало надо попотеть), можно антик(браузер линкен сфере тоже подойдет), идем покупаем сс под зону пикапа, заходим в магазин выбираем стафф и бьем.

лектор: В принципе все просто

лектор: Но как и в других направлениях много подводных камней.

лектор: О всех подводных камнях расскажу в процессе лекции.

лектор: Существует 2 вида пикапа.

лектор: Это пикап на поддельные документы владельца карты(кх)

лектор: И пикап на имя дропа.

лектор: Не думаю что нужно связываться с пикапом на имя дропа, ибо это давно не практикуется.

лектор: В 95% случаев преобладает пикап на поддельные документы.

лектор: Термин Fake ID - поддельные документы.

лектор: Сервисы для пикапа не стабильны. В данный момент на форуме их пара штук рабочих, бывает что вообще нет сервисов, бывает не можешь выбрать от их изобилия.

лектор: https://wwh-club.net/threads/usa-pick-up-service-druzhba-prinimaem-paki-po-fejk-id-na-otdelenijax-pocht.75565/

https://wwh-club.net/threads/skup-servis-po-fake-id-moon.92791/

лектор: Вот пара сервисов для примера.

лектор: Там вы увидите условия, карту покрытия, скупаемый товар.

лектор: Можно написать сапорту и пообщаться, они как правило общительные.

лектор: Теперь поговорим о видах работы.

лектор: Раньше в сервисах было 3 вида работы.

лектор: Работа 50 на 50, работа под скуп, работа под пересыл

лектор: В данный момент в сервисах в большинстве своем осталась только работа под скуп

лектор: Но можно попробовать договориться, и думаю получится наладить отношения и работать по остальным видам.

лектор: Теперь о каждом виде по порядку.

лектор: Работа 50 на 50

лектор: Это значит

лектор: К примеру, вы вбили макбук с тачбаром

лектор: и вдруг захотели себе такой, пишете сервису, хочу этот ноутбук, он говорит давай 50 на 50

лектор: в этом случае вы делаете еще один такой макбук(пикап сервис может предложить что то другое схожее по сумме)

лектор: И в итоге один макбук отправляют вам, другой сервис забирает себе тем самым покрывая расходы

лектор: Работа под скуп

лектор: тут все просто, вы вбили макбук с тачбаром за 2к

лектор: он дошел, и сервис вам выплачивает процент. у всех сервисов разные проценты. пусть это будет 35% за Apple

лектор: Товар забран дропом, скуп выплачивает вам 700$

лектор: Все довольны.

лектор: Последний вид работы, работа под пересыл.

лектор: Этот вид очень редко встречается, да и не очень то он хорош.

лектор: Вы сделали макбук с тачбаром, говорите перешли но от 50 на 50 отказываетесь

лектор: в этом случае сервис вам говорит, покрой расходы и вышлем. Как правило покрытие расходов это 35%

лектор: Вы платите сервису 700$ + доставка баксов 30-40 и он пересылает макбук вам на посреда, в РУ никто не отправляет.

лектор: + с посредника в ру доставка баксов 50-100 в зависимости от посредника

лектор: По видам работы все

лектор: После вбива у вас 2 варианта

лектор: 1 вы видите красные буквы что вы мошейник и идите работайте на завод

лектор: 2 спасибо за ваш ордер, номер ордера, информацию пришлем на почту.

лектор: Разберем первый вариант

лектор: не нужно опускать руки, реальные американцы так же страдают от всего этого.

лектор: Что мы делаем? Мы берем и звоним менеджеру шопа

лектор: ругаться

лектор: Говорим что мы тут потратили 40 минут на выбор и оформление

лектор: и нас послали

лектор: просим разобраться

лектор: Вам менеджер может сказать что давайте попробую проведу операцию по телефону

лектор: или же вас отправляют в фрод отдел

лектор: Если вам говорят что давайте по телефону, сообщаете все данные. и есть возможность что ордер еще пройдет(это значит что накосячили в настройке системы и антифрод шопа не пустил транзу)

лектор: Если же не проходит это уже ошибка банка

лектор: и вас так же отправляют во фрод отдел, там вам злобный дядя говорит давайте конференцию с банком и дальше у вас просят всю возможную информацию которую вы не знаете, это может быть что угодно, вопросы по кредитам, машинам, домам и так далее.

лектор: В общем тут просто кладем трубку и выкидываем сс, она умерла

лектор: Сделать ничего не получится, можно попробовать в инстантчекмейт ее заюзать на будущее)

лектор: Теперь второй вариант после оформления ордера.

лектор: Есть такие магазины которые не сразу списывают деньги с карты, а спустя какое то время

лектор: они то вам и пишут что спасибо за ордер и тд

лектор: И спустя 2-3 часа вы на почте замечаете что ордер канцеллед или же заморожен.

лектор: Если заморожен то обычно просят позвонить для уточнения инфорации, тут все по старому сценарию. вы звоните, и менеджер может либо просто уточнить адрес, либо же перенаправляет вас на фрод отдел, которому вы сказать ничего не в силах.

лектор: Если же у вас все получилось, и после уточнения адреса вам приходит информация с трек номером и все хорошо.

лектор: Но и сейчас не стоит радоваться)

лектор: Все это подвоные камни

лектор: Теперь нам нужно что бы пак не уехал домой к владельцу карты

лектор: а остался на почте

лектор: В народе называется холд

лектор: тк когда все хорошо в статусе трека пишется Hold for pickup

лектор: что мы делаем, берем трек и звоним в транспортную компанию(ЮПС, Федекс)

лектор: И там говорим что бы не доставляли на адрес владельца посылку, а что бы оставили и мы сами все заберем

лектор: тут так же 2 исхода событий

лектор: Первый говорит что все хорошо и спустя 5 минут проверяя трек вы видите надпись Запрошено оставление пака на почте

лектор: Тут ждем и на след день как правило запрос одобрен и посылка лежит ждет пока ее заберут

лектор: Посылка лежит 5 дней, если в течении 5 дней ее не забирают, то она возвращается обратно в магазин, деньги на карту.

лектор: Теперь второй исход событий

лектор: Вам говорят что холд сделать невозможно.

лектор: Идем на хитрость

лектор: Там где покупали товар ищем имя фамилию менеджера

лектор: и уже в транспортную компанию звоним от имени менеджера магазина

лектор: Говорим что обратился клиент и просит оставить пак на почте

лектор: Обычно не отказывают

лектор: Но примерно год назад ввели такую штуку как програмный холд на действия

лектор: Это значит

лектор: что вы позвонили от имени менеджера, сотрудник компании хочет сделать холд но программа в которой он это делает выдает ошибку что холд невозможен

лектор: в этом случае забываем магазин потому что холд не сделать вообще никак.

лектор: идем ищем новый.

лектор: После успешного холда, когда вы все сделали

лектор: передаете информацию сервису и сидите ждете пока они заберут посылку

лектор: чекаем трек, бывает что его разворачивают, и посылка едет обратно

лектор: Когда видим слово Деливеред начинаем радоваться, это значит что сервис забрал пак

лектор: но не всегда))

лектор: Иногда холд почему то не ставится

лектор: и доставщик забирает и везет пак на адрес доставки

лектор: может это ошибка доставщика

лектор: скорее всего так и есть

лектор: дак вот если вы чекнули трек и там написано Out for delivery

лектор: стоит бить тревогу и звонить в транспортную компанию ругаться

лектор: чтобы доставщик привез пак обратно на почту

лектор: не всегда успеваешь и тогда пак просран

лектор: такие случаи бывают но редко

лектор: Если ваш пак доставлен и дроп сервис говорит что забрали

лектор: просто ждем выплаты

лектор: Теперь о отчетности

лектор: Советую завести табличку куда будем вносить информацию

лектор: для удобства и что бы не бить в один не дающий магазин по 10 раз

лектор: вид таблицы щас скину

лектор: Дата / Шоп сс / Шоп товара / Страна сс / тип карты / бин сс / банк сс / прогрев шопа / устройство / алекса / тел кх или скайп / сумма ордера / метод доставки / первичный результат / трек / полное пояснение

лектор: Так же не советую работать одному, слишком много затрат и временных и денежных

лектор: Собрались в команду из 2-3 человек

лектор: и тестим разные магазины скидывая статистику в общаг

лектор: гораздо легче.

лектор: Очень важно брать трубку когда перезванивает магазин.

лектор: Был случай что вбил ноут за 3к

лектор: шоп перезванивает просто уточнить адрес

лектор: и радости менеджера небыло передела когда я взял трубку

лектор: он на радостях ускорил мою доставку.

лектор: очень часто люди вбивают и забивают болт на звонки и тд

лектор: это их важная ошибка.

Работа на Андроиде

лектор: Так ребят, начинаем лекцию по Андроиду(ведру)

лектор: настроить андроид под вбивы под силу каждому. напоминает настройку вирту только со своими особенностями)

лектор: я бы выделил 2 вида работы с андроидом

лектор: 1) простой вариант , без глубокой настройки - это вбив с браузера

лектор: 2)глубокая настройка, вбив с приложения

лектор: Но в любом случае надо получить роот права на устройстве (не путать с админ правами, это совсем другое, нужно для выолнения ряда других функций,это так для общего развития некоторые думают что root=админ права)

лектор: я всегда делаю это через kingo root(гуглим) , скачиваю апк файл на телефон и устанавливаю . самый простой способ получить рут права

лектор: сейчас скину список программ и пробегусь по ним

лектор: kingo rooT

xposed installer(framework)

device id changer Pro

Proxy droid

xprivacy

ccleaner

root cloak

location cheater

лектор: и так, для чего они нужны

лектор: Основа основ для вбива с приложений на ведре это xposed framework. Это системная программа для изменения настроек прошивок(версий OS). Ее мы еще затронем в разборе вбива с приложения

лектор: device id changer pro меняет данные о железе вашего телефона (imei) и другие параметры это модуль xposed framework

лектор: Proxy droid - через него ставим соксы. я не работаю с туннелями и вам не советую

лектор: DNS Forwarder - в прокси дроиде иногда не работает корректно подключение днс с сокса(просто инет не работает на телефоне) для подмены используем это приложения

лектор: ccleaner думаю все знает,удобно чистить на телефоне мусор

лектор: location cheater служит для подмены данных о местоположение

лектор: root cloak (модуль framework) служит для того чтобы скрывать от других приложений,что телефон имеет рут права

лектор: xprivacy Это прога которая подменяет симкарту и не только,она либо разрешает либо запрещает видеть определенные сведения всем приложеним. В дополнение к ней я советовую приложене sim card, на нем можно отточить то что запрещать , а что разрешать приложениям видеть,чтобы в них отображалась корректная информация об устройствах

лектор: Все приложения выше (кроме клинера) не работают без рут прав

лектор: Начнем разбор настройки для работы с приложениями

лектор: ставим xposed installer после того как получили рут права,и через него устанавливаем framework. Скажу сразу,здесь мы столкнемся с трудность поставить фреймворк , нам нужен андроид на версии 4.4.4 (на него проще всего поставить эту прогу)на версиях выше сделать это крайне проблематично , но если вы умеете ставить кастомныЙ рекавери и прошивать архивы то можете попробывать . В остальном советую у кого прошивка выше откатить самим ведро на 4.4.4 или отнести в сервисный центр и вам там прошьют ,стоит это не дорого .Плюс на 4.4.4 гораздо удобнее работать чем на версиях выше.

лектор: А вот ссылка на 4pda там найдете инсталлер на 4.4.4.(и версии выше)

лектор: https://4pda.ru/forum/index.php?showtopic=425052

лектор: После того как поставил xposed framework ставим следующие программы

лектор: device id changer Pro имеенно Pro

Proxy Droid

DNS Forwarder

ccleaner

Location cheater

лектор: эти все программы скачиваются в плей маркете

лектор: xprivacy

root cloak

лектор: эти программы скачиваются xposed installer. заходим в раздел загрузка и там в поиске их ищем и устанавливаем

лектор: Ну и важное примечание. apkpure.com сразу сайт в закладки , и скачать приложения sim card (зеленая симка на ярлыке)

лектор: Когда вы поставили все выше перечисленные программы нужно зайти в xposed installer ,раздел модули и поставить галочки на всех модулях (device id ch/root cloak/xprivacy)

лектор: Потом зайти в раздел фреймворк и прожать быстрая перезагрузка чтобы модули установились, если этого не сделать модули не будут корректно работать

лектор: На данном этапе у нас устройство почти готово к вбивам

лектор: Сейчас немного расскажу про модуль xprivacy , очень полезная штука когда работаешь с серьзными шопами,банками и тд , лично я его юзаю для подмены сим карты,по факту возможностей у него больше заходим в него и переходим в раздел параметры, трогаем только те значения что связаны с симкой

лектор: а это

лектор: номер телефона

лектор: MCC

лектор: MNC

лектор: код страны

лектор: оператор

лектор: ICC ID

лектор: ID подписки

лектор: Возьмем за основу номер 4356681778, если кто подстраивается под холдера и ему нужно пробить оператора ,идем сюда http://www.whitepages.com

лектор: Что такое MCC с этим можете ознакомится здесь https://m.wikipedia.org/wiki/Mobile_Country_Code , из этой же страницы можете взять значение для нашего параметра в проге

лектор: MNC это код оператора, посмотреть код нужного оператора(нужной страны) вы можете так же здесь https://en.wikipedia.org/wiki/Mobile_country_code

лектор: страна и оператор тут все ясно

лектор: Теперь что же такое icc id и id подписки, и как его прописать

лектор: icc id это серийный номер симки,который всегда состоит из 19 цифр

лектор: https://i.imgur.com/HzmKDk7.png

лектор: первые 2 цифры 89 всегда ставятся по дефауту, это относится к отрасли,ее индификатор

лектор: Дальше то что выделено , это идет код страны ,длинной от 1 до 3 цифр

https://i.imgur.com/5uIizLl.png

лектор: по юсе это 01. по другим странам значение отличаются (точнее наиболее распространен по юсе 01)

лектор: Так поскольку мы подстраиваемся под юсу ,в значение ICC ID первые 4 цифры будут всегда 8901 , а остальные 15 цифр можно писать рандомно

лектор: https://i.imgur.com/1xoxBvF.png посередине кстати это просто номер рандом симки , а самая последняя цифра вычисляется методом лун

лектор: https://en.wikipedia.org/wiki/Luhn_algorithm

лектор: его примменяют к примеру для рассчета номера банк карты и тд, если будете работать в карже думаю когда то еще услышите это

лектор: ID подписки (в xprivacy) А вообще это называется sim imsi .как его прописать. Смотрим картинку https://i.imgur.com/uAfNjDl.png , он всегда состоит из 15 цифр , Прописываем сначала значение MCC , затем MNC, затем остальные цифры пишем рандомно,чтобы в итоге было 15 символов в этом поле

лектор: Как сделать чтобы данные подменялись , когда устанавливаете новое приложение , xprivacy кидает уведомление,и те данные что нужно подменить, нажимаете на кнопку запретить(deny)

лектор: И вот тут пригодится приложение simcard , которое поможет набить руку какие значения подменять

лектор: Теперь опишу как происходит вбив

лектор: ставим сокс в прокси дроиде, там прописывае ip,port , не забудте указать тип прокси, так же попробуйте поставить галочку чтобы днс был с сокса но если не будет работать инет вырубите эту опцию и все заработает (если сокс не мертвый) и включаем

лектор: Идем на whoer.net смотрим какой часовой пояс , идем в настройки ставим часовой пояс и язык под холдера

лектор: если не работает dns через прокси дроид то заходим в dns forwarder , выбираем ip и врубаем его

лектор: потом в location cheater задаем координаты, я обычно ставлю в паре метров от нужного адреса (под айпи или шип адрес)

лектор: идем опять на whoer и смотрим все ли норм поставилось

лектор: Если слетел сокс,выключаем прокси дроид,днс форвардер , и читер , и заново включаем их , это происходит не на всех устройствах , но лично я чтобы все нормально работала ,пару раз включаю и выключаю эти проги,раздражает,ну а что поделаешь)

лектор: Чтобы проверить работает location cheater или нет,скачиваем гугл мапс,и там смотрим(прожать кнопку мое местоположение)

лектор: Если все работает, то скачиваем нужное приложение и открываем root cloak

лектор: заходим в рут клоак заходим в первый раздел (добавить/удалить приложение) нажимаем на плюсик ,и ищем наше приложение,после этого чтобы сохранить настройки заходим xposed installer ,раздел фреймворк,и нажимаем быстрая перезагрузка .После этого

лектор: даже если вы удалите это приложение,его запомнит рут клоак и делать это каждый раз не нужно

лектор: После вбива ,чтобы начать следущий нужно зайти в device id changer ,в первом разделе device id нажать random all и apply, затем зайти в xposed installer раздел фрейворк , и нажать быстрая перезагрузка,чтобы железо поменялось

лектор: и так, собственно мы научились подменять данные о железе и тд

лектор: Теперь заново ставим приложение и вбиваем , не забываем менять данные в xprivacy

лектор: Если надо условно бить палку перебором и чтобы каждый раз не качать приложение,не регать гугл акк что очень утомляет , юзаем сайт apkpure.com там можно скачать приложение и добавить на телефон

лектор: то есть как отработали акк,удалили приложение,поменяли данные,перезагрузили устройство,просто устанавливаете приложение заново

лектор: Теперь перейдем к вбиву с браузера

лектор: Здесь все намного проще, в целом любая версия андроида подходит для работы

лектор: для работы с браузером нам надо

лектор: 1) сам браузер (chrome. ff , родной браузер телефона)

2) ccleaner (или менеджер приложений,есть в настройках на каждом телефоне)

3)прокси дроид

4)dns forwarder

5)location cheater

лектор: в случае работы с браузером,железо менять не обязательно, но переустанавливать браузер желательно,и чистить его

лектор: Вбив почти такой же как и с приложения, просто пропускаем пункты , с device id changer/root cloak/xprivacy

лектор: в основном бьют с мозиллы (так как там webrtc отключается так же как и на компе), либо с родного бразуера(на новых версиях ведра -редкость). чистим кэш (и историю) через ccleaner или менеджер приложений после каждого вбива обязательно

лектор: на apkpure можно скачивать предыдущие версии приложение (если там к примеру надо разные версии браузера)

лектор: А и да забыл добавить,я как правило работаю из под левых сим, но тем кто работает с wi-f1 к- примеру необходим впн, в целом удобен Tunnel Bear (качаем на гугл плей) ,там все интуитивно понятно, включаем его перед прокси!

Покер

лектор: Всем привет. Сегодня лекция на покерную тему.

лектор: Сразу скажу что данная тематика излишне сложная для людей малознакомых с онлайн покером. Следовательно новичкам в теневой сфере никогда не игравшим в онлайн покер (посиделки с друзьями под пиво со ставками по 50рублей не считаются) я настоятельно рекомендую пропустить эту информацию и отправиться практиковаться с чем-то более понятным.

лектор: Немного теории и терминологии. Аккаунты делятся на 2 типа:

лектор: Сливной (так же называют Карж) - аккаунт с "левыми" бабками, бывает:

Самореги - с депозитом через СС или БА

Брут / с логов - уведенный у пользователя аккаунт с его же бабками (брут - перебором паролей, с логов - путем заражения ПК пользователя)

лектор: Выводной (выводник) - аккаунт с чистыми деньгами предназначенный для дальнейшего выигрыша у сливных и вывода на платежные системы.

лектор: Идея заработать в покере сводится к тому чтобы деньги находящиеся на сливном ак-те (черные) сделать своими (белыми / серыми). Варианта два: выводить со сливного ак-та на платежную систему к которой у нас есть доступ, либо намеренно проигрывать за покерным столом выводному ак-ту и уже с него выводить на платежную систему.

лектор: Ключевые действия на старте работы:

Первое - заводим профиль еще на 3+ тематических площадках, это очень-очень важно, так вы сможете гораздо быстрее находить нужные контакты и материал.

лектор: Второе - читаем мои статьи по работе с дедиками https://wwh-club.net/threads/vbej-svoju-mechtu-metod-pod-xajdom.76414/#post-935703

дедики - основной материал при работе с покером, научившись работать правильно на старте вы сэкономите уйму времени.

лектор: Виртуалка критически не подходит под покер румы где для депозита/игры необходимо устанавливать клиент, т.к. установленный клиент выпаливает виртуализацию

лектор: ВНЦ вероятно являются неплохой альтернативой РДП, но есть момент, холдер в параллельной сессии увидит установленный клиент покер рума

лектор: На дедике(РДП) можно создать отдельную учтеную запись и установить клиент только для этой учетной записи, это важно помнить при установке приложения

лектор: Методы создания сливного ак-та:

лектор: 1) Выбор страны

По странам подходящим нам для создания аккаунтов, определяем очень просытм действием - открываем клиент нужного нам покер рума, находим турнир с макимальным количеством регистрация и просматриваем список участников, смотрим откуда они. Далее идем в шоп / к селлеру материала (дедики / тунели, СС) и смотрим какой старны материал есть в наличии. Игроков из какой страны много и под которую есть материал начинаем тестировать.

лектор: - 2) Выбор метода заведения баланса

Есть 3 варианта заполучить сливной аккаунт с балансом:

- а) Саморег и сделать на него депозит

Регистрируем аккаунт через покерный клиент(предварительно загрузив его), для этого нам потребуется валидная почта (клиент проверяет возможность

доставки писем и ругается если почты не существует), придумать логин и пароль.

Купить почты можно тут - https://buyaccs.com/

После регистрации не рекомендую с ходу жать кнопку депозит и вбивать номер CC, некотрое время покликайте по вкладкам покер рума, откройте столы на условные фишки, поиграйте минут 5-10, только после заходите в депозит и начинайте с небольшой суммы (30-150$). По возможности вводите какой-либо код предоставляющий бонус при депозите, найти можно несколько минут поюзав гугл или на оф. сайте.

лектор: б) С брута / логов нулевка и сделать депозит или с готовым балансом

Заходим в аккаунт, так же можно немножечко поиграть на условки, дальше если есть почта от ака, то заходим в нее и выставляем фильтр на письма от нашего рума, чтобы они сразу удалялись и холдер нас не спалил.

Теперь берем CC и забиваем ее в ак, первый депозит так же рекомендую делать до 400$.

лектор: На этом этапе у нас появляется аккаунт с балансом, осталось его монетизировать.

лектор: Варианты:

1) Продать за %, так себе вариант, высокий процент не получить.

2) Проиграть деньги за столом другому аккаунту к которому уже подвязана нужная платежка.

3) Привязать свою платежку к этому аккаунту и вывести деньги.

2ой вариант наиболее предпочтителен, но главное не жадничать, сливать аккуратно, понемногу, предпочтительно на столах 6макс Омахи.

лектор: ВАЖНО !!! Не жадничайте, бывают ситуации когда вам ну очень нужно выиграть раздачу на аккаунте куда делается залив, но карты легли таким образом что у сливного аккаунта сверх сильная комбинация. Проиграйте ему, даже если вам придется потратить несколько часов чтобы восстановить баланс - это значительно лучше чем отправить оба аккаунта в блок.

лектор: Зависит от покерной комнаты, в некоторых очень жестко и работать с ними не стоит, в некоторых ВББ нет

лектор: Так же и с картами, на некоторых стоит принудительное ВББ на каждую транзакцию, на некоторых от какой-то суммы

лектор: Поэтому я в лекции рекомендую начинать с небольших сумм 30-150$

лектор: Сам работал всегда только со старзами и 888 покер, на ПС ВББ принудительного не было, на 888 было от 150$, но так же пропускало любые транзакции с определнных бинов Австралии и Новой Зеландии без ВББ

лектор: Да, важный момент, практически все покер румы не работают с США, поэтому материал нам потребудется Европы, Азии или других стран

лектор: Теперь поговорим про "выводник"

лектор: Где создавать ?

1) Физический ПК - вариант надежный, но при объемах не очень удобный.

Начать можно со своего ПК и попросить у друзей доступ по тимвиверу.

Использованные ПК можно юзать повторно сменив HDD/SSD и сетевой адаптер, IP - проще всего новый модем.

лектор: На начальном этапе я рекомендую этот вариант, т.к. ваши средства будут максимально защищены и у рума не может быть претензий к железу.

лектор: 2) Моб. устройство - вариант столь же надежный, но менее удобный на этапе заливов / прокачке, зато легче менять.

Все как в первом пункте, только теперь у вас маленький девайс.

Чистить я не рекомендую, так же хороший вариант менять б/у трубки + новая симка.

лектор: 3) Дедики - не очень надежный, но удобный и легкозаменяемый.

Сразу скажу забудьте про серверные ОС - они нам не подходят.

Основной плюс дедиков это масштабируемость, сколько времени вам понадобится чтобы найти 15 разных телефонов или ПК. С дедиками же 150$ и вот у вас 15 уникальных конфигов на хоум винде.

Плюсом так же является то, что они находятся в разных регионах.

На этом плюсы закончились и пошли минусы. а они довольно существенные.

Первое и самое стремное это отсутсвие гарнтий того что дедик до вас не был использован под этот же покер рум, это приводит к автоблокировке аккаунта с кучей неприятных верификаций, в конечном итоге свои деньги вы вернете в 90% случаях имея необходимый комплект док-ов, но ни о каком заливе и речи быть не может + эта процедура не быстрая, в это время деньга лежит мертвым грузом.

Второе и не менее неприятное - дедик может сдохнуть в любой момент, смена ИП это плохо и может так же повлечь за собой вериф. Ну и самый маловероятный, но все же возможный пункт, т.к. доступ к дедику есть не только у вас, ваш ак-т может быть попросту уведен.

лектор: Важным дополнение к информации по выводнику является страна, РУ/СНГ вполне хороший вариант, так проще работать, при этом никаких законов глобально мы не нарушаем, даже если доказать факт умышленного слива денег это лишь нарушение правил покерной комнаты.

лектор: Как создать аккаунт и сделать депозит ?

Регать покерный аккаунт стоит на уже купленные доки в комплекте пас + селфи с пасом в руках, страна документов должна соответсвовать ИПу с которого вы заходите, я всегда выбирал РУ.

Это архиважная часть, все остальные документы легко рисуются, но пас + селфи лучше иметь заготовленное.

Далее нам нужно сделать депозит используя любой из предложенных системой методов.

лектор: После выводник нужно прокачать и сделать красивый залив, основные условия:

1) играем энное количество раздач за теми же столами где планируем сливать баланс с карж (до заливов)

2) прокачиваем аккаунт успешными вводами / выводами средств (до заливов)

3) аккуратная игра во время слива, не жадничаем и не собираем 100% баланса себе (не более 70%, за исключением супер удачных ситуаций, например вам дают АА, а карж аккаунту КК)

лектор: На этом основная теория заканчивается, с каждым отдельно взятым покер-румом появляются свои моменты, проверить которые можно только на практике, удачной работы.

Enroll

лектор: Начнем пожалуй.

лектор: Мой ник Fox. Сегодня я буду вашим лектором на тему Enroll.

лектор: Я вам расскажу, что это такое, где это взять, и как это использовать. На мой взгляд – это самый простой способ работать по вещевухе.

лектор: Что такое Enroll?

Это самая обычная CC(кредитная карта), либо же дебетовая(но за всё время работы по Enroll’у нашел лишь один банк который дает возможность заролить дебетку) и личный кабинет к этой карте.

лектор: Смена Billing address

Большинство банков позволяют онлайн способом в личном кабинете сменить billing адрес на тот, который нам нужен (дроп/клиент/посред).

лектор: Для чего нам это нужно? В USA есть система сверки billing адреса и shipping адреса, называется AVS. Об этом вы должны уже были узнать из первых лекций. И в юсе большинство шопов очень принципиальны в этом плане.

лектор: Если billing не совпадает с shipping’ом, то шоп либо откажется оформлять заказ, либо же закидают вас кучей разных проверок и верификаций.

лектор: Так вот, чтобы это обойти, нам и помогут роллки. В них есть возможность сменить billing адрес КХ, на свой. Это делается всё очень просто в личном кабинете. Просто заполняете форму адреса, на нужный вам. После этого идём в шоп, и бьем billing=shipping.

лектор: Как правило смена проводится 2-5 рабочих дней (зависит от банка, чаще всего – 3). Выходные в счёт не идут.

лектор: Также отмечу, не во всех банках есть такая возможность. Есть банки где смена биллинга происходит

прозвоном, либо же вообще отсутствует данная возможность.

лектор: Мини-депозиты/Миники

Так же доступ в личный кабинет на позволяет посмотреть мини-депозиты(Мини-депозиты/мини-депы/миники).

лектор: Это микро-транзакция, которую с вас списывает шоп. Как правило сумма миника будет в районе 1-2 долларов. Эта транзакция служит как верификация вашей карты в шопе

лектор: Шоп с вас снимает небольшую сумму денег и просит вас сказать какую именно сумму они сняли с вашей карты, или же код транзакции, который шел с данным миником

лектор: Если вы назвали его, то все Ok. Уровень доверия шопа к вам намного увеличивается и со стороны шопа проблем с данным ордером 99% не возникнет, но это относится только к тем шопам, для которых миники – всё.

лектор: Есть шопы которым плевать на билл=шип, им главное верифнуть миники. Если у них миники верифнул, то с ордером 99%, что проблем не возникнет.

лектор: Приведу вам пару примеров чтобы вы поняли о чем речь.

лектор: У меня есть роллка какого-то банка, который позволяет увидеть инстантом(без ожидания) миники. [19:19:03] лектор: Я иду в Steam, и вбиваю её на соточку баксов. Steam сразу блокирует на неделю мой аккаунт для

ручной проверки данной операции, либо же предлагает принять миники для верификации.

лектор: Я отправляю эти миники, Steam шлет 2 мини-транзакции. Захожу в роллку, смотрю какие две транзакции пришли от Steam, и подтверждаю их в Steam’е. Все, холд снимается, Steam к карте привык, и дальше раздеваю эту карту в том-же Steam уже без каких-либо задержек и холдов.

лектор: Второй пример

лектор: Skrill без миника разрешает депнуть в акк 140 баксов, но если я подтвердил миник, то уже могу туда депать до 5к.

Но, хочу отметить заранее. Большинство контор а-ля Steam, Skrill итд. Уже задрочены роллками, и пропускают определенные бины/банки/карты. Как узнать какую пустит? Проверить методом «Проб и ошибок», либо же узнать у тех кто уже знает(но такую информацию вам вряд ли расскажут за «Спасибо»)

лектор: VBV/MCSC

Это можно сказать интернет пин код. Если он в снг приходит в смс, то в ЮСЕ он статический, то есть один и не меняется. КХ его устанавливает сам.

лектор: VBV(Verified by Visa) - если карта VISA.

MCSC(MasterCard Secure Code) - если карта MasterCard.

У Amex и Discover данного вида защиты нет вообще.

лектор: Обычно вы можете его установить при вбиве. В момент оплаты у вас выскочит окно и запросит данный код, там можно либо сразу поставить свой, либо просто сбросить старый и так же поставить свой, либо же установить его заранее.

лектор: Вот сайт для Visa: https://verified.visa.com/aam/activation/landingPage.aam

Аналогичный есть и для MasterCard. Я его не сохранил, но у нас на форуме его можно найти, не раз его упоминали

лектор: По итогу, если в шопе установлен запрос VBV кода и вы его ввели, то это еще один хороший плюс в доверии шопа к вашей покупке

лектор: Есть такие шопы и сервисы, которые без вбв вообще не пропустят ордер.

лектор: Смена телефона

Последний момент, который мы рассмотрим из плюсов энролла, это смена телефона холдера в карте.

лектор: Ни для кого не секрет что мы можем позвонить с подменой номера, который был указан при покупке карты/или мы нашли в кабинете, но, шоп всегда может перезвонить на номер, с которого мы звонили.

лектор: Если шоп это сделает, то попадут они на холдера, нам это не надо. Нас не спасет даже звонок со своего, номера который мы могли купить в скайпе, потому что из шопа сейчас очень часто звонят в банк чтобы сверить адрес, имя холдера, а так же его телефон.

лектор: И если в банке говорят что информация не сходится, то сразу шоп отменяет транзу, и банк блочит карту. Конец, нет у нас ордера, и карта мертва.

лектор: В этом случае нас и спасет энролл. Вместе с биллинг адресом мы можем поменять и телефон. В итоге при звонке шопа в банк, вся предоставленная информация совпадает и пак благополучно поедет на вашего дропа.

лектор: Но тут есть и другая сторона монеты. В последнее время многие банки, при любой подозрительной активности на роллке, могут прозвонить КХ. То бишь, если их фроду(про это позже), что-то не понравилось, то, к примеру, при смене биллинга, они могут позвонить КХ и уточнить: «Это вы меняете биллинг?», кх конечно-же ответит что не он, и роллка умрет, карта перевыпустится.

лектор: Где взять?

Мы с вами теперь знаем что такое Enroll, возникает следующий вопрос: «Где взять?».

лектор: Тут есть два варианта: Купить у нас на форуме, либо-же заролить самим.

лектор: Первый способ:

Идем на форуме в раздел "кардинг предложения" и покупаем энролл у понравившегося селлера, например у меня :D

https://wwh-club.net/threads/prodam-primary-enroll-ne-pablik.81568/

лектор: Второй способ, уже сложнее, пытаемся роллить собственными силами

лектор: Заранее вас могу предупредить, может фортануть и с первого раза, а может и с пятого не получится зароллить карту.

лектор: Моя первая роллка получилась с первого раза, а потом я не смог сделать карт 6 подряд.

лектор: В данном случае мы должны знать банки которые роллятся с минимум информации, должны купить CC, и пробить к ней ту самую информацию

лектор: Разные банки требуют разную инфу для энролла

лектор: Могут попросить просто SSN/DOB, а могут по харду просить и девичью фамилию матери, и пин код, и биллинг телефон, ответы на бекгрунд холдера, код который предоставляется банком, комер аккаунта и так далее.

лектор: Нам нужны те, которые просят SSN/DOB

SSN - номер социально страхования холдера

DOB - дата рождения холдера

лектор: У нас на борде много сервисов которые занимаются данным видом пробива, рекомендую обращаться к Синдикату.

лектор: Далее получив ssn/dob мы идем на сайт банка и пробуем делать энролл заполнив соответствующие поля с требующейся для этого информацией.

лектор: Если все ровно - то мы получаем тот самый энролл

лектор: Что может быть "не ровно":

Вы вводите свои данные, но вам не дает зароллить карту, тут несколько ответов:

- Карта мертвая
- Информация пробита не верно
- Карта не принадлежит человеку, который был указан при покупке, а настоящий холдер мама/папа/жена/муж/сын
- Карта не является основной, а служит лишь как дополнительная карта которая привязана к основному счету мужа/жены/ мамы/папы или кого-то еще

лектор: Иногда, когда мне писало, что данные которые я ввожу не подходят, но карта при этом 100% валид, я мог пробить еще данные мужа/жены, и очень часто подходило и карта роллилась, такое часто случалось с банками boa и synovus

лектор: Но таким рекомендую заниматься, когда будет опыт и свободные деньги

лектор: И последний вариант:

- Карта была зароллена до вас, то есть холдер уже зарегистрировал личный кабинет

Это мы рассмотрим поподробнее.

лектор: Primary Enroll и ReRoll

Есть два вида Enroll

1. Primary - холдер до вас еще не делал личный кабинет, и вы спокойно сами его делаете

2. ReRoll - до вас был уже сделан личный кабинет, НО банк дает возможность восстановить логин и пароль. Чаще всего для этого надо иметь ту же самую информацию что и при энролле primary, иногда мы можем попасть на бэкграунд холдера в виде секретных вопросов.

лектор: Так-же многие банки для ReRoll’а требуют указать установленный Username либо E-mail. В таком случае, чаще всего, смысла биться дальше нету, ибо информация для восстановления придёт на почту КХ.

лектор: Чтобы попасть на примари энролл, я вам могу посоветовать брать карты максимальным сроком годности карты, то есть свеже-выпущенные карты, с эксп датой **/21или **/22

лектор: Чем больше эксп дата, тем лучше

На много больше вероятность что у холдера не дошли руки до создания личного кабинета

лектор: Как правило баланс который мы можем использовать подписан – available credit.

Баланс который КХ потратил – Current Balance.

лектор: Расскажу для тех кто не знает как работают кредитные карты. Грубо говоря, КХ берёт кредит в банке, и средства эти держаться на карте, а не наличкой. Соответственно Current balance – это та часть кредитных средств которая израсходована, а Available credit – то, сколько ещё доступно. Не путайте эти понятия!

лектор: 444796 - вот бин банка Credit One. Роллится и реролится он очень легко, но балансы там бичевые. На

этом банке можно потренироваться, так как он позвляет делать реролл и роллится 9 карт из 10, но даже 1к там увидите очень редко. Чисто руку набить можно.

лектор: Последний банк который я использовал был боа, там обычно хорошие балансы, но много карт уже зароллено, реролл сделать нельзя, а примари редко попадаются.

лектор: Расскажу вам как у меня все происходит

лектор: Я беру бины которые знаю что роллятся и иду на ХТА смотрю что есть по наличию

лектор: Выбираю несколько карт, пробиваю к ним ссн доб, и пробую роллить

лектор: При энролле я беру дед/ssh/сокс под холдера карты

лектор: Иду на сайт, и пробую роллить

лектор: Все карты которые получилось зароллить я откладываю до понедельника

лектор: В понедельник беру сокс/ssh/дед уже под штат дропа и меняю адрес

лектор: Дальше адрес меняется от 2-5 дней будних дней, выходные не учитываются

лектор: Обычно жду опять же понедельника, и иду вбивать. Не стоит бомбить сразу роллку в кучу мест, вбили в один шоп, ждем пока пак не будет доставлен и идем вбивать ее еще раз, если карта все еще жива.

Gift и E-Gift

лектор: В ходе лекции я раскрою эту тему и дам вам понимание данной ниши настолько глубоко и всесторонне, насколько я могу это сделать исходя из своего опыта работы в данном направлении.

лектор: Физические гифты и егифты

Для тех, кто не знает: гифт - в переводе с английского - "Подарок". Это подарочный сертификат, предоплаченная карта, на сумму номинала которой можно купить товар в шопе этого гифта.

лектор: Гифты бывают физические и электорнные, Gift и E-Gift. Физические приходят получателю (или покупателю) на почту или в почтовый ящик в реальной жизни, в то время как электронный гифт приходит получателю(покупателю) на эмейл(электронную почту).

лектор: Основная разница между вбивом физических и электронных гифтов(далее - егифт) проявляется в следующих тонкостях работы:

Под физический гифт нужны адреса для приёма, большая часть официальных посредников их не принимают, в большинстве шопов их нельзя отозвать, разница во времени между вбивом и получением готового к использованию гифта на руки, да и AVS-система не везде пропустит ордер.

лектор: Физический гифт можно отоварить напрямую в офлайн-магазине, прийти и просто рассчитаться им на кассе. С егифтом так тоже можно, но далеко не во всех шопах.

лектор: Хотя на егифты антифрод зятанут сильнее, но при этом с ними нет необходимости обходить AVS, не нужны дропы, посредники и ожидание нескольких дней между вбивом и получением, следовательно оборачивать средства внутри работы можно в разы быстрее. Гифты продаются в основном номиналами от $1 до $1000. В некоторых шопах при оплате можно складывать несколько гифтов.

лектор: Шопы делятся на нексолько основных типов:

- Точечные. Шоп продаёт свои собственные гифт-карты, своего магазина. У таких шопов антифрод слабее относительно следующих двух типов шопов.

- Мультигифтовые, реселлеры. В шопе продаются десятки или сотни гифтов различных шопов, например: ebay.com. У таких шопов средний антифрод.

лектор: - Агрегаты. Непосредственные производители и одновременно продавцы гифт карт, антифроды у них одни и сильнейших.

Стоит сразу осознать, что, если у точечных шопов антифрод слабее, чем у агрегатов, это не значит, что пробить их будет легко.

лектор: Прямой вбив в гифтах - вбив непосредственно в шоп, чей гифт вы планируете заполучить. (Купить гифт ebay на ebay). Вбив в посредника - очевидно, вбив в реселлера. Реселлеры обычно пробиваются легче(особенно не паблик), ориентируйтесь на это. Искать шопы также, как и все остальные, пара дополнительных лайфаков будет в этой лекции.

лектор: На результат работы напрямую будут влиять следующие параметры:

1. Устройство + система

2. Айпи

3. Карты

лектор: Поскольку я раскрываю эти пункты в лекции "Вбив от А до Я", здесь я расскажу в двух словах то, что напрямую влияет на работу конкретно с гифтами, подробнее раскрытие темы системы и айпи смотрите в лекции "Вбив от А до Я".

лектор: 1 - Устройство. Топовые шопы сложно пробивать с обычной виртуальной машины, посколько антифрод их детектит. Для топовых шопов надо использовать либо реальные устройства (например, мобильный телефон), либо удалённые доступы(дедики, VNC-машины), или же антидетекты.

лектор: 2 - Многое зависит не только от чистоты айпи адреса, но и от провайдера. Есть провайдеры, находящиеся в зоне риска для антифрода, есть также и хостинг-провайдеры. Использования таких провайдеров негативно сказывается на вбиве. Обращайте на это внимание и записывайте провайдера.

лектор: Пара примеров неплохо проявиших себя интернет-компаний по личному опыту: qwest, charter, cox, att, verizon, comcast. Их можно смотреть в шопе при покупке сокса или туннеля. Пара примеров плохо проявивших себя провайдеров: rr.com, myfairpoint.net. Но это не значит, что

можно забить на чистоту. Напротив, чистота айпи по блэкам и риск-прокси скору не менее важна.

лектор: 3. Карты. Рекомендую использовать наименее популярные банки. НЕ такие, как Chase, BofA, CapOne, WellsFargo и прочие. Естественно, с этих и остальных популярных банков можно вбить, тем не менее, с менее известных проходимость выше. Уровень и тип карты некритичен. Чаще всего для вбивов используются MasterCard и Visa. Amex тоже возможно, но с амексом ключевую роль играют бины, да и чарджи быстрее в разы.

лектор: Чек карт до вбива

Карты не стоит чекать перед вбивом гифтов, если вы не уверены в бине и чекере. Во-первых, потому что сама операция покупки гифта входит в число операций повышенного риска у банков.

лектор: Во-вторых, потому что чекер нередко убивает карты и является еще более фродовой операцией, чем покупка гифтов, в сумме эти два параметра повышают риск смерти карты, а следовательно траты времени и неуспешного вбива.

лектор: Брут аккаунты + смена биллинга

Под шопы также можно писать бруты, загружать базы mail-pass и собирать аккаунты этих шопов.

лектор: Зачастую в шопе холдер оставляет привязанной свою карту, и с неё также можно купить гифт. Но, здесь существует проблема - CVV. Даже если сохраняется карта, в большинстве шопов(и во всех крупных) CVV придется

вводить каждый раз при покупке, и поскольку им мы не владеем, у нас есть 3 варианта использования брут аккаунтов, а именно:

лектор: А) Поиск шопов, где CVV сохраняется. Такие есть, но они в основном мелкие, поэтому искать их не просто.

В) Изменение биллинга(добавление нового) помимо биллинга холдера. Берём брученный акканту и просто подвязываем к нему новую карту и биллинг.

лектор: В чем смысл, спросите Вы? - Смысл в том, что данный аккаунт был создан реальным человеком, он совершал успешные покупки без чарджей, следовательно антифрод настроен к нему более лояльно чем к новорегу.

лектор: Но не стоит забывать, что добавление новой карты и биллинг-адреса в уже существующий аккаунт является относительно фродовым действием, поэтому данный способ вбива не панацея, но имеет место быть. Иногда можно побрутить аккаунты, добавить карты/биллинги и отлежать неделю-две, это имеет смысл.

лектор: Я рассказываю об этом виде вбива не потому, что он приоритетный, а потому, что существует. По факту для большинства крупных шопов(например, mircosoft, walmart и прочие) брутов невероятно мало, или же они работают крайне нестабильно, из чего возникает сложность такого вида работы - найти кодера, заплатить, найти хорошие прокси под брут, абузоустойчевый сервер и так далее. Если надумаете попробовать себя в этой нише - на первых порах никогда не начинайте с крупных всемирноизвестных шопов.

лектор: С) Покупка за бонусы. В некоторых шопах такое есть, накопительные баллы и скидки, но я такого почти не встречал.

лектор: Вбив с палки.

Вбив с брут paypal возможен также, как и с карт, но здесь ключевую роль играют шопы. Потому что гифты, в основном, приходят на почту аккаунта пейпал, к которой у нас почти никогда нет доступа(если не брутить мыло+палку) или не покупать пп с доступом к мылу. При вбиве с палки шопы нужно подбирать тщательно, а тестировать интенсивно.

лектор: Вбив с саморегов палки реален и функционирует, но есть другие способы более выгодно и проще налить самореги, поэтому этим мало кто занимается.

лектор: Вбивать прозвоном гифты можно также, как и другой товар. Но не все шопы относятся к этому хорошо, а некоторые, наоборот, только прозвоном и вбиваются. Начинать с этого не рекомендую, но взять на заметку этот вариант необходимо.

лектор: Эмейлы и сообщения

При покупке егифта в большей части шопов вам предложат ввести эмейл получателя, затем, при регистрации или вбиве, свой эмейл. Важны не только доменные зоны почт (gmail.com/yahoo.com/etc.), но и текст в ней до @, поскольку антифрод обращает на это внимание и бывает, когда отмена ордера приходит только потому, что антифроду не понравился ваш емейл.

лектор: Я рекомендую при регистрации вписывать туда имя и фамилию кардхолдера с карты, а доменную зону выбирать максимально естественную (не mail.ru) и наименее фродовую(не mail.com). Лучшие варианты: корпоративная почта(mysite.com), gmail.com, hotmail.com(outlook.com), yahoo.com.

лектор: Хорошая почта под холдера будет иметь вид "имя-фамилия@домен.ком" после регистрации, например, jonathanblake@gmail.com. Цифры в почте это нормально, поскольку часто имя при регистрации уже занято - jonathanblake16@gmail.com.

лектор: С покупателем разобрались, теперь про получателя - здесь всё также, как и с холдером, за исключением доменной зоны. Для разнообразия рекомендуется использовать отличный домен почты от покупалетя (то есть если @gmail.com покупатель, то @yahoo.com получатель), по факту же это не критично, в остальном все также. Если слабая фантазия, имя получателя можно генерировать, например, здесь: <http://www.fakenamegenerator.com/>

лектор: Безусловно есть шопы, где можно отправлять прямо на свою почту, однако если шоп предлагает вам ввести эмейл получателя - вписывать туда почту холдера будет подозрительно и неестественно в большинстве случаев.

лектор: На странице оформления заказа и выбора номила егифта, будет возможность ввести персональное сообщение получателю.

Это действительно влиятельный пунктик, и влияет он напрямую на результат вбива. Даже если все идеально

(система, карта, почты и так далее), но в сообщении написано что-то невообразимо глупое или подозрительное, то при обработке заказа (особенно вручную) отмена ордера может последовать даже из-за этого.

лектор: Бывали случаи, когда отмены гифтов были из-за неграмотно написанных текстов где менеджеру магазина было очевидно, что покупатель американцем не является, бывало из-за полного отсутствия сообщения.

лектор: Дайте волю своей фантазии и пишите, хотя бы, естественно, необязательно круто и много. Напишите приветствие, пожелание, поздравление или тезис/цитату из книги. Представьте, что дарите этот гифт своей девушке или сестре и не думайте о том, что вы его покупаете с чужой карты.

лектор: Иногда может прокатить текст со специальных сайтов, найти которые можно загуглив "поздравление с днем рождения на английском" или "поздравление с помолвкой" и т.д. Минус в том, что эти сайты уже задрочены, поэтому для создания "скелета" и развития фантазии/пополнения словарного запаса использовать их можно и нужно, но как полноценный инструмент для повседневного использования они не годятся. Не стоит принебригать этим параметром вбива егифтов.

лектор: Продолжая тему параметров при вбиве гифтов, рассмотрим телефонный номер.

При егифтах, особенно в магазинах США, очень важную роль играет прохождение антифрода по параметру AVS. Очень важную, но, однако, не критичную. Новичкам при

вбиве в шопы средней и выше руки советую писать именно номер холдера. Причина простая - 90% шопов не звонят, или звонят только в особых случаях - когда вы не прошли антифрод и им нужна верификация именно таким способом.

лектор: Однако этих случаев меньше, чем отмен из-за несовпадения AVS. Безусловно, есть и топовые ликвидные шопы, которые переодически звонят холдеру для подтверждения заказа, но их можно вычеслить только эмпирическим путём, то есть, тестами и вбивами. Шопы помельче могут звонить, поэтому можно пробовать писать другой номер телефона или свой google voice/skype. Лично я всегда пишу только номер холдера.

лектор: Скупы и списки шопов.

На нашем и других форумах полно скупов егифтов, каждый со своим процентом, отзывами, условиями и методами работы, разными списками скупа ликвид/нелеквид егифтов и шопами. Скупов можно найти здесь: <https://wwh-club.net/forums/vcc-prepaid-cheki-gift-karty-kupony-vauchery.81/>

лектор: Перед началом работы рекомендую сравнивать условия, проценты и отзывы у различных скупов, выбрать своего скупа дело тонкое :)

Но я завёл разговор о них не для этого, а для того, чтобы показать Вам самое простое - шопы прямо перед глазами, в темах скупов можно найти как ликвидные шопы, так и неликвидные, гифты которых добыть проще. Есть также и скупы сугубо неликвидных гифтов, под меньший процент, но и работать так проще.

лектор: Скупами на форуме варианты куда деть гифт не заканчиваются. В интернете полно площадок, где перепродать гифт можно даже американцам, думающим, что покупают белый подарочный сертификат. Самый простой пример: <https://localbitcoins.net/> - здесь гифты могут скупать даже по бОльшему проценту, но иногда нужны верификации, поэтому подбирать скупа нужно не менее тчательно, чем на форумах.

лектор: Таких площадок десятки, каждую нужно тестировать и анализировать, на каждой можно найти какой-то интересный шоп, которого нет в списке у форумных скупов. Поставив дело на поток, продажу гифтов можно запустить не только на специализированных площадках, а даже на ebay.com, но к новичкам понимание этого придет только с большим опытом, а с большим опытом сложность работы увеличиватеся в сотню раз, имейте ввиду.

лектор: Ликвид и неликвид гифты можно определить по предлагаемому проценту. Классическая ставка процента для неликвида: 25-45%, для ликвида - 45-90%.

Выставляя или предлагая скупу гифт не из списка и предлагая процент, ориентируйтесь на ассортимент магазина. Если в нём техника - просите от 40 до 70%, если вещи - 25-50% в зависимости от брендов.

лектор: Отоваривание

Отоваривание гифтов на адрес посредников или дропов производится с айпи под штат или город, с дедика, сокса или туннеля. Имя при этом необязательно использовать то

же самое, которое значилось в получателе гифта при покупке. В основном только совсем мелкие шопы могут "спросить" за это, и в случае чего можно решить это прозвоном.

лектор: При отоваривании ликвид-гифтов топовых шопов старайтесь не использовать задроченные адреса публичных посредников, иначе аккаунт может уйти в бан и вы лишитесь гифта.

лектор: Проверку баланса гифта(проверку валидности) на сайте шопа лучше осуществлять с айпи страны шопа, не проверяйте с VPN Германии или свего домашнего айпи-адреса, иначе система может заблокировать гифт. День-в-день отоваривать гифты не рекомендуется, подождите сутки, и здесь уже важно время работы, так как по выходным физический стаф в основном не отправляют.

лектор: Шип мелкого стафа на кх и добавление товара в корзину.

Многие вбивалы гифтов рано или поздно задаются вопросом: "А что, если добавить носки за доллар в корзину покупки в добавок гифту и купить их на адрес холдера? Прибавит ли это лояльности антифрода?". Ответ - НЕТ.

лектор: В вашей козрине всё ровно остается егифт, и анализ ордера антифродом будет проходить всё еще как ордер с егифтом. Это имеет смысл делать только в разное время - сегодня купили носки и прогрели этим шоп, завтра с этого же аккаунта купили гифт

лектор: Добавить и удалить товар в корзину в качестве прогрева шопа, - можно, но небязательно. Посёрфить по шопу, почитать описание товаров, посмотреть каталог перед непосредственной покупкой егифта - да.

лектор: Перевбив ранее использованных карт и аккаунтов шопов

Перевбив как явление можно разделить на два варианта действий с картой:

А) перевбив карты после деклайна или канцела

В) перевбив карты после успешного ордера и потраченного егифта

лектор: Рассмотрим каждый из вариантов подробнее.

А - делается это в тех случаях, когда вы не уверены, что отмена или деклайн были по причине мертвой карты. Грубо говоря, не прошли антифрод - пошли попытать удачу в другой шоп. Имеет смысл, так как иногда это работает, да и затраты на материал никакие не нужны, единственное, что при вбиве в 2 разных шопа обслуживающихся одним мерчем - перевбив почти всегда будет бесполезен, так как ваши данные уже есть в системе, потому что мерч у двух разных шопов общий, поэтому обращайте внимание на мерчи.

лектор: При варианте В у нас есть несколько решений, которые необходимо принять до вбива. Первое и главное - бить в тот же шоп, или другой? С одной стороны, шоп нас уже знает, мы провели успешный ордер и вроде как это должно добавить лояльности, с другой же стороны это

может и вызвать подозрения у шопа из-за однообразности товара и действий покупателя.

лектор: Из рекомендаций по принятию этого решения могу только сказать, - принимайте решение самостоятельно в зависимости от того, жив ли еще ваш доступ(Сокс, туннель, дедик) или нет. Если жив, то можно попробовать вбить в тот же шоп с этого же айпи, если нет - заменяем айпи и идём в другой шоп.

лектор: Второй вопрос - на какую сумму перевбивать карту? Больше, или на такую же, или же меньше? Я обычно ориентируюсь на уровень и тип карты. Если это дебетка низкого уровня (classic) то бью на такую же сумму, как и раньше. Соответственно если уровень карты выше (platinum и так далее) или тип credit, то можно попробовать увеличить сумму.

лектор: Минус перебива в том, что мы не знаем, жива ли эта карта до сих пор, а плюс, что нам не надо её покупать; перевбив приносит интуитивное понимание работы антифрода конкретных шопов и их отношение к повторной покупке, также это даёт рабочие бины. При перевбиве рекомендуется менять получателя.

лектор: Важнейший плюс перевбива заключается в простой истине: это значительно сократит время на выяление причины деклайнов и канцелов, направит на путь истинный и укажет где искать ошибки, а, следовательно, рано или поздно приведет к решению.

лектор: Деклайн или канцел? Но в другой шоп прошло? - Вывод прост, не прошли антифрод шопа или банка!

Деклайн или канцел в нескольких шопах? - Вывод: бин говно/карта мертвая или плохой сокс/система. Можно попробовать найти безотказный шоп с диким неликвидом и проверять на нём карты :)

лектор: На основании этого создайте собственную методику выявления проблемы, ведь Обучение - это Учеба. Учитесь учиться, как говорится :)

лектор: Время суток для вбива и время ответа от шопа (конечного результата)

Часто новички задаются вопросом - В какое же время суток всё таки бить? Ответ: зависит от шопа, его расписания и рабочих дней.

лектор: Некоторые крупные шопы могут выдавать гифты инстантом даже ночью в выходные, в то время как в мелких шопах придется ждать рабочего времени в будни.
Начинайте бить в будниии дни, по мере приобретения опыта можете бить в любое время суток и таким образом выяснять как реагирует шоп (тестировать его).

лектор: Несколько типов реакции шопов для понимания:

1 - Гифт пришел инстант (мгновенно, до 5-ти минут)

2 - Гифт пришел в течеии 1-12 часов. - это среднее время процессинга при условии рабочего времени магазина. Это нормально. Но, если этот же шоп ранее уже выдавал вам гифт инстантом, значит в этот раз вы где-то не дотянули при прохождении антифрода и процесс проверки затянулся или перешел в ручную проверку.

лектор: 3 - Шоп запросил верификацию. Про верификции я рассказываю на своей леции "Вбив от А до Я".

4 - Инстант канцел (многовенная отмена ордера) - что-то шопу настолько не понравилось, что он присылает отказ мгновенно. Иногда может означать отмену со стороны банка или мёртвую карту. Можно попробовать перевбить в другой шоп.

(19:59:20) лектор: 5 - Процессинг затянулся на сутки и более - ручная проверка в крупных шопах, иногда означает попытки прозвонить холдера или вбив в нерабочее время. В двух словах: или недотянули, или не тогда вбили.

Записывайте время и результаты(реакции) каждого шопа и мерча для приобретения методов работы с ними.

лектор: Арифметика профита

Предположим, карты мы покупаем за $10/шт, сокс или туннель $1.5/шт - минимальный набор необходимых инструментов для вбива. Если вы будете бить с дедиков, прибавляйте вместо сокса за $1.5 цену дедика, то есть от $4 до $10-12/шт. Цены средние, они могут меняться в зависимости от шопов.

лектор: За данное возьмем ликвидный гифт номиналом $100, скупающийся по 60%. Складываем затраты на материалы, от номинала гифта высчитываем свой процент, убираем разницу между затратами и выручкой - получаем чистую прибыль. (10+1.5) - (100*60) = $48.5 чистого профита с одного успешного ликвид гифта, сделанного с первой попытки.

лектор: Но не всегда всё так гладко, ведь с первой попытки гифт может не прийти, и тогда затраты будут расти, и чтобы окупиться Вам придётся пытаться вбивать гифты на всё большие суммы, 150, 200, 300$ - а в топовых шопов такие суммы надо уметь вбивать, ведь антифрод у них сильный, новички просто потеряют деньги и пойдут ныть, что карж мёртв.

лектор: Именно поэтому я советую всем начинать вбивать неликвид гифты, скупаемые по 25-40% в зависимости от шопа. При таких же затратах на материал, номиналы гифтов можно успешно тащить в несколько раз больше относительно ликвид шопов, так как магазины средней руки пробиваются на порядок легче.

лектор: Затраты: 11.5$, номинал гифта: 300$, процент скупа 25%, тогда чистый профит = $63.5 - даже больше, чем с ликвидного гифта, но при этом обойти антифрод чуть ли не в разы проще.

лектор: В гифтах важно всё.

Время суток, карта, ip, операционная система, девайс, эмейлы, адреса, банки, шопы, мерчи и всё, что я перечислил в лекции. Все настраиваемые параметры нужно довести до машинального воспроизведения, все теоретические знания до отскакивания от зубов, все неизвестные X и Y научиться вычислять методом исключения и путём тестирования.

лектор: Только тогда вы сможете адекватно работать в плюс на гифтах, поэтому будьте готовы к сливу денег на первых порах если вы начинаете свой путь с гифтов, и напротив, не начинайте с гифтов, если ваш бюджет ограничен или мал.

лектор: Единая формула успешного вбива гифтов сводится к:

Параметры подготовки(ip, система, карта и т.д.) + шоп(мерч, задроченность, ликвидность, верификации и т.д.) = Here is your eGift Card!

A + B = C.

лектор: Начиная работать по гифтам, мой статистический exel-файл насчитывал около 60-ти вбивов, успешных из которых было 4 или 5. Это 8% успеха. В пересчете на доллары - сумма трат на материалы в тот момент уже привышала $700 до момента, когда я начал выходить в профит. Почему так получилось? - Потому, что на тот момент я еще не знал всего того, о чём рассказал вам в этой лекции.

Вбива Ликвид стаффа с помощью Enroll

лектор: Приветствую всех! Сегодняшняя лекция будет посвящена теме вбива Ликвид стаффа с помощью Enroll

лектор: На данной лекции мы узнаем:

1. Как нужно грамотно использовать enroll при смене биллинга.

2. Основные ошибки которые не нужно допускать при вбиве.

3. Как выстраивать логические цепочек при вбиве

4. Ну и самое главное - это результат. Как сделать так, чтобы любимая кофта gucci была у Вас на руках!

лектор: Возможно у некоторых уже возникает вопрос, а что такое Enroll ?

Именно поэтому для начала я бы хотел заострить Ваше внимание на разборе этих непонятных слов, которые будут частенько использоваться в лекции.

лектор: Чтобы у Вас как у слушателей / обучающихся не возникало проблем в усвоении и понимании материала.

Для удобства Вы можете скопировать эти слова-определения к себе в блокнот, чтобы на протяжение лекции могли невольно подглядывать если вдруг возникли трудности в понимании.

лектор: Слова-определения:

лектор: Enroll (на рус. “Энролл” или “Енролл”) - это cc (Кредитная карта) с доступом в банк, где в дальнейшем можно сменить биллинг адрес холдера.. .

лектор: Дроп - определение обширное, но в нашем случае это человек который принимает товар и в дальнейшем его пересылает.

лектор: Посред - компания которая занимается отправкой Вашего купленного товара из сша/еу к Вам в снг

лектор: Холдер - Хозяин карты, банка, аккаунта и тд

лектор: Билл (Он же биллинг) - Личный адрес холдера

лектор: Шип - Адрес на который заказываем товар

лектор: Идем дальше

лектор: Подготовка материала

лектор: У многих новичков да и не только, думаю сразу складывается вопрос в голове: " А где же брать эти самые enroll ? " или " У кого покупать ? "

Ответ на это дело простой - купить у селлеров!

лектор: На площадке есть множество селлеров с продажей енролла со сменной биллинга.

лектор: Нам нужно брать енролл со сменной биллинга онлайн (Как правило биллинг меняется 3-ое суток). Выделите или запишите себе этот момент

лектор: Также нам нужен будет дроп, именно дроп, а не посред, потому что биллинг на посреда просто на просто не сменится и Ваш материал улетит в блокировку

лектор: Что по поводу системы?

лектор: По этому поводу мнения спорные, кто-то любит бить с дедиков (Исключительно брут), кто-то с ВНЦ (Удаленное управление компьютером, ВНЦ также можно приобрести у селлеров на форуме) , вариантов много, их можно перечислять и перечислять...

лектор: Лично мой первый вбив с помощью енролл был с дедика под город дропа.

В любом случае IP-address обязательно должен быть не под билл енролла, а под дропа.

лектор: Ход работы

лектор: Заходим на наш купленный материал, заходить исключительно с ип под дропа. У многих думаю сразу появляется вопрос: " Почему менять билл не с ип холдера ?"

лектор: Опять же, можно использовать и ип под холдера, а какой от этого смысл? Включаем логику, сразу ставим себя на место холдера, представьте, Вы переезжаете жить в другой город, допустим из New Yourk в Dallas при самом переезде, мысли у Вас точно не будут о том, что нужно Вам прям сейчас сменить биллинг в банковском аккаунте. Соответственно Вы по факту переезда будете менять биллинг адрес

лектор: С этим моментом думаю всем понятно.

Идем дальше.

лектор: Сразу же после смены биллинга, именно с момента подачи заявки, то есть сразу, идем и выбираем шоп в который будем бить. Запомните раз и навсегда такой момент, пробить можно абсолютно любой шоп! Какая бы защита у него не была, если шоп создан для обычного человека, то и мы можем с него сделать товар.

лектор: Расскажу про поиск шопа на своем примере:

Когда я начал работать по этой теме, с поиском шопа я особо не парился (Как же, некоторые скажут, шоп который дает - это залог успеха) Отнюдь нет! Залог успеха только в грамотной построенной логической цепи для пробития шопа!

лектор: И так, на тот момент, зашел я в гугл и написал " buy gucci " , перешел сразу на 2-ую страницу и тыкнул рандомно на шоп, все! Больше ничего не нужно! Где-то покупать шопы и заниматься прочим бредом, крайне не советую.

лектор: Только своя наработка и личный поиск приведет к успеху. Запомните одну вещь, деньги за деньги никто Вам никогда не продаст. (Возможно Вам на пути встретятся “ селлеры “ , которые будут продавать “ Волшебные шопы “ , которые дают “ яблоко в ру “ . Смысл думаю понятен.) У таких людей ничего не покупать!

лектор: Заходим в шоп, регистрируемся на данные холдера роллки (Full name вписываем холдера, биллинг и шипинг адрес - дропа)

лектор: Много у кого думаю возникнет вопрос: " почему нужно сразу регистрироваться в шопе? А если билл не сменится, да и смысл пока не готов главный инструмент для вбива ", всегда я убеждаюсь в одной вещи, 40 % успеха - прогрев аккаунта! Это самая основная часть (по моему мнению) для достижения результата.

лектор: Как происходит прогрев? Да и что за зверь такой?

лектор: А зверь этот, что-то между тяжелым и простым, я бы его назвал безгранным.

Работу по прогреву можно выполнить по разному, но к этому вопросу я настоятельно рекомендую подойти серьезно.

лектор: Для прогрева аккаунта я рекомендую использовать максимально большое количество Вами известных способов, я Вам расскажу их всего несколько.

лектор: 1. Серфинг - думаю самый популярный способ поддать жару Вашему аккаунту!) Без серфинга Вы ничего не сможете вбить, только если в самый дырявый шоп. Нам

нужно постоянно лазить по сайту, смотреть товар, почитать правила сайта, посмотреть параметры товара, материал и тд

лектор: Всегда себя ставим на место настоящего холдера, я не думаю, что холдер бы зашел и за 5 минут сделал заказ, нет! Американцы да и многие европейцы очень трепетно относятся к выбору какого либо товара, пусть это будут даже обычные носки

лектор: Настоящий пендос, перед покупкой какого либо товара, все про него прочитает, почитает кучу отзывов, подумает 100 раз нужно это ему или нет, потом посмотрим качество материала, сверит с другими аналогами товара, только потом уже будет покупать, это мне известно по личному опыту с пендосами

лектор: Прогревать наш аккаунт, нужно каждый день до того момента как сменится биллинг.

Проще говоря, зашли на аккаунт час-два посмотрели товар (Близкий к тому который будем заказывать

лектор: К примеру если мы будем заказывать кофту гучи, серфим только кофты или просто бренд гучи, иногда заходим на что нибудь другое), на следующий день проделываем ту же операцию и так до смены билла.

лектор: 2. Прозвон, чат

Как показывает практика, прогрев данным типом очень сильно подталкивает к успеху. Сразу ставим себя на место холдера. Допустим, Вы зарегистрировались в шопе,посмотрели товар и у Вас сразу же возникло

несколько вопросов, куда наш любопытный холдер побежит их спрашивать? Конечно же в онлайн чат.

лектор: Вопросы могут быть разные, суть совсем не в них, а в том, что при общении в чате, фрод нам начинает все больше и больше улыбаться, потому что мы начинаем подходить под описание настоящего холдера!)

лектор: Для тех людей кто дружит с английским:

Задавайте разные вопросы: " Сколько по времени занимает доставка " , " А если вещь не подойдет смогу ли я её поменять?" , " Я хочу сделать подарок брату, сможете ли Вы сделать подарочную упаковку ? " и так далее... вопросов может быть много, включайте свой мозг и думайте!

лектор: Для тех людей кто не владеет знанием английского языка:

На форуме есть много различных прозвон-сервисов у которых есть услуга " прогрев чата" , за определенную сумму (как правило не большую 5-8 $) они заходят на Ваш аккаунт и общаются с магазином.

лектор: Способов значительно больше, но в основе я использую эти два способа

лектор: При следующем ходе работы 2 разворота события:

лектор: 1. Банк меняет биллинг и все счастливы.

2. Банк блокирует аккаунт. Что делать в этом случае? Обращаемся к прозвонщикам, шанс разблокировки аккаунта примерно 30-40 процентов. Тут все зависит от банка и на сколько у Вас много информации на холдера.

лектор: На какую сумму покупать товар?

лектор: Вопрос очень деликатный, тут опять же, все зависит от банка и лимита по карте холдера. Как узнать лимит? Опять обращаемся к прозвонщикам.

лектор: Смысл разговора с банком должен быть таким, что холдер хочет сделать покупку в интернете (Допустим Вы будете вбивать на сумму 1500 долларов) и узнает, нормально ли пройдет оплата? то бишь не будет ли каких проблем?

лектор: Тут 2 варианта:

лектор: 1. Ваша будущая покупка соответствует лимитам и банк говорит " Все хорошо, можете осуществлять покупку "

2. Либо же " У Вас лимит по карте на онлайн транзакции 1000 долларов, мы можем увеличить Ваш лимит

лектор: 2-ой вариант самый распространенный. Мы это делаем не только для того, чтобы узнать лимит в банке, но и для прогрева транзы, что это может значит? А то , что мы сейчас прямым текстом уведомили банк, что будем делать заказ на 1500 долларов! И банк уже об этом знает! Что может быть лучше?

лектор: Всегда помните. Появились какие-то проблемы с заказом, сразу обращайтесь к звонилам, хороший прозвонщик может вытащить очень многое.

лектор: Если от шопа не решаемые диклайны, проблема у Вас, а не у шопа! Всегда тщательно проверяйте систему, все ли у Вас правильно настроено. При вбиве нужно учитывать

очень много факторов, не все так просто как кажется, с каждым вбивом Вы будете более и более опытнее.

лектор: Давайте немного поговорим о построение логических цепей и какие факторы нужно учитывать при вбиве.

лектор: Бывалым данная информация может конечно показаться очевидная, но многие новички соответственно про это не знает. Расскажу Вам кратко про основные факторы.

лектор: - Настроенная машина для вбива

Еще раз повторюсь, чтобы все прошло гладко, обязательно используйте замену ип под дропа! Почему? я описывал выше.

лектор: Вообще для удобной работы и более качественных вбивов, я советую купить сферу, ознакомится более подробно и приобрести можете в данном топике:

https://wwh-club.net/threads/brauzer-linken-sphere-opisanie-i-otzyvy-polzovatelej.87703/

(Обучающимся 1 месяц БЕСПЛАТНО! Писать по контактам в топике)

лектор: Лично я ею пользуюсь на протяжении 3-ех месяцев, вбивы и прочая работа идет значительно лучше чем с тех же дедиков. Да и по деньгам она Вам будет намного выгоднее, цена на домашний дедик 8-10 долларов, цена на сферу 100 долларов месяц, вот и считайте! Соксы стоят копейки

лектор: Так же работа с VNC намного лучше чем с дедиков. По выбору машины для вбива, тут индивидуальный подход

лектор: -Почта

Тут лучше использовать домен gmail . Так же, если холдера звать к примеру " Leen Helson ", то почту я советую делать примерно такой : " leenhelson001@gmail.com " , кто занимается базами емайл:пасс поймет, что в основном амеры используют имя фамилию или просто фамилию для логина почты, самый распространенный вид.

лектор: -CTR+C CTR+V

Ошибка многих новичков! Любые данные пишите руками! И только руками! Никогда не надо ничего копировать и вставлять, будь это логин, пароль, биллинг и так далее... 90 процентов системы антифрода смотрят на это, потому что настоящий холдер, свой адрес или данные от карты точно не будет копировать и вставлять!

лектор: -Заходы с разных ип

Очень часто случается такое, что в процессе 3-ех дневного вбива, умирает носок либо же дедик, кто давно в работе, думаю эту неприятную ситуацию знают хорошо. Если у Вас такое случилось, не вздумайте брать первый попавшийся дедик или сокс и лезть в аккаунт, будь это банк либо же аккаунт в шопе!

лектор: При такой ситуации, подберите максимально похожее ип с тем что было, пробуйте найти такой же зип, если нету зипа город. Если этого не сделать, со стороны шопы - это будет выглядеть так. Проходите регистрацию

Вы с Техаса, день сидите смотрите товар, через 3 часа вы заходите с лас-вегаса, не странно ли?

лектор: Сразу вспоминаем про очки фрода, которые нам не очень нужны, да и улыбка фрода сразу начинает спадать. Если такое происходит пусть даже с одного города, но с разных адресов, тут ничего страшного, допустим Вы приехали к другу у него посидели. прошли регистрацию, полазили вместе с ним, посмотрели товар, следом приехали домой и опять зашли на сайт. Ситуация простая.

лектор: С этим думаю понятно.

лектор: Факторов очень и очень много, каждая мелочь может и будет влиять на прогресс! Всегда представляйте себя на месте холдера! Ведь вы обычный американец который хочет сделать заказ.

лектор: -Время вбива

Не в коем случае, не рекомендую вбивать в пятницу, субботу и воскресенье! Делаете вбив исключительно с понедельника по четверг! Потому что высылают товар именно по этим дням, если вы сделаете вбив в выходной день, Ваш товар вышлют в понедельник и шанс, что к этому времени транзакцию отменят очень велик!

лектор: Переходим к самому вбиву!

лектор: Тут все просто, ничего выдумывать не нужно. Выбрали товар, прочитали отзывы (если они есть) , посмотрели качество материала, добавили в корзину!

лектор: Если товаров несколько, идем дальше смотреть различные товары, минимум 15 минут, нашли?! Молодцы! Добавляем товар в корзину!

лектор: Ни в коем случае не переходите на товар по ссылкам. Допустим, у Вас под заказ взяли 3 кофты гучи, Вы соответственно скидываете клиенту сайт, где искать эти кофты, клиент Вам скинул 3 ссылки, открывать их строго на другой машине, можно на основной, а искать этот товар в шопе руками, иначе опять придут злые очки фрода!

лектор: Переходим к самой оплате товара!

лектор: В Биллинг адрес вписываем холдера банка, имя фамилию + адрес дропа (когда он сменился в банке)

лектор: В шипинг имя фамилия дропа, адрес соответственно тоже, различия в биллинг и шипинг только в фулл найме

лектор: У многих сразу вылезет вопрос: " А как отреагирует шоп, если имена разные, это же сразу вызывает подозрение " Вызывает ли подозрение?! Я бы не сказал.

лектор: За бугром это очень частое явление, когда холдеры заказывают товар на брата, маму, папу ,сестру и так далее, как правило они живут вместе! Зачем да почему? Многие сильно заняты, чтобы забирать посылку, например работой, Учебой, а мама которая всегда сидит дома, запросто с этим справится, либо же когда делают подарок кому либо

лектор: Обычное явление, тут шоп особо не будет заморачиваться, потому что по сути, в этом ничего такого нету.

лектор: Нажимаем конфирм! Если Вы сделали все правильно, то увидите столько приятную зеленую табличку.

лектор: Что делать если появился канcл?

лектор: В первую очередь - успокоится! Да зрелище не совсем приятное, ведь вы так старались, а тут моментальная отмена! Но пугаться не стоит, в первую очередь, перепроверьте правильно вы ввели все данные, номер сс, експ, билл! Если нет, то поправьте и пробуйте снова!

лектор: Если же да, все равно еще раз нажимайте конфирм, потому что обычный холдер так бы и сделал. Если опять та же песня, звоните сразу же в шоп и тревожно узнавайте, что случилось и почему так произошло, ведь у вашего брата через 2 дня день рождение и Вам очень нужны эти вещи! Обычно они помогают и вбивают карту либо по телефону, либо повторно делаете Вы и все проходит.

лектор: Далее, рекомендую прозвонить шоп либо написать в лайф чат! Сказать примерно такую вещь : " Я сделал заказ, все ли нормально и когда примерно доставят? " И опять же, вам так срочно нужны эти вещи!)

лектор: В обычной практике, все проходит на ура, высылают товар! Но и тут есть подводные камни, канcл тоже очень любит прилетать на почту, если же Вы увидели эту табличку, сразу звоним в шоп и узнаем, что за дела. В таких случаях, если мы все делаем правильно, зачастую просто напросто банк отменяет транзакцию, причина того в 90 процентов случаев, является звонок холдера и отмена платежа.

лектор: Сразу же пишем прозвонщику и пробуем вытянуть транзакцию, если нет, то увы! В каждом деле, есть неприятные вещи. Тут мы не отчаиваемся и идем дальше.

лектор: Давайте подведем итоги.

лектор: Сегодня мы научились:

лектор: - Грамотно выставлять логические цепи при вбиве

лектор: - Изучили основные факторы работы с енроллом

лектор: - Поняли как важно использовать прозвон сервис, что без него далеко мы не уедем

лектор: - Делать правильный прогрев аккаунта! Поняли , что это обязательная часть вбива!

лектор: Ну и надеюсь в дальнейшем, Вы сделаете и будете делать товар с помощью енролла!

лектор: Домашнее задание:

лектор: Задание#1 Выпишите в блокнот, журнал, тетрадь , куда Вам удобнее, те вещи, которые Вы не знали до этой лекции и постоянно старайтесь повторять это, чтобы у Вас засело в голове, ведь допустив одну малейшую ошибку, можно просто напросто потерять товар, деньги за материал и самое главное - это время, ведь оно бесценно. Деньги можно заработать, а время вот Вы не вернете, используйте его с умом

лектор: Задание#2 Каждому сделать минимум 2 попытки такого вбива! Выписывать себе весь алгоритм работы!

Пример алгоритма:

1. шоп - www dwdwd . com (ПРИМЕР!)

2 Банк ролки + бин (Первые 6 цифр карты)

3. Описание полного метода работы:

Какие были звонки и сколько + Результаты звонков

Методы прогрева

Поведение шопа (Письма от него и тд)

Старайтесь записывать все все факторы которые были в процессе!

4. РЕЗУЛЬТАТ!) (Надеюсь он у Вас будет положительный)

лектор: Неудачные алгоритмы или проблеменные (в процессе) , можете скидывать мне в пм, я буду помогать и поправлять их. Проблемные будем пытаться вытащить

Отели

лектор: приветствую всех, сегодня мы поговорим о таком направлении работы как бронирование и аренда

лектор: а конкретнее отели, автомобили, экскурсии

лектор: завтра обсудим авиабилеты, а также завтра поработаем в форме вопрос-ответ

лектор: просто сегодня нет смысла по вопросам так как завтра еще будет инфа которая возможно даст на все ответы

лектор: существует несколько способов сделать бронь в отели за чужой счет:

лектор: оплата по форме авторизации – Оплата СС через агента – Оплата через БУКИНГ - Оплата ревардами

лектор: сейчас поговорим подробно по каждой из этих тем

лектор: 1) Вариант по форме авторизации

лектор: И так что это вообще такое:

лектор: Скачиваем http://rghost.ru/6BsVFb7Jn и внимательно смотрим!!!

лектор: Форма авторизации — это анкета в которой указываются все данные плательщика, срок проживания и данные карты, данной формой КХ подтверждает свое согласие на списание средств

лектор: далее работник отеля, вводит данные карты в ПОС-терминал и совершает оплату

лектор: Теперь все по порядку:

лектор: Идем на http://www.booking.com/

лектор: выбираем отель, делаем бронь на того, кого будем заселять, можно обойтись и без booking.com а сразу звонить в отель

лектор: звоним в отель и представляясь агентом запрашиваем форму авторизации для оплаты бронирования

лектор: Примерный диалог выглядит так:

лектор: - Привет, я из турагенства «XXXXX» мы хотим забронировать номер для нашего клиента. Возможно ли оплатить через форму авторизации?

лектор: - Да, конечно

лектор: - Очень хорошо, отправьте форму на travel@xxxxx.com

лектор: Заполняем форму авторизации:

лектор: Credit Card Holder's Name вписываем КХ или вымышленное имя

лектор: Hotel Guest Name вписываем того, кого будем заселять

лектор: Телефоны указываем скайп с автоответчиком

лектор: Делаем отрисовку, тут важный нюанс, лучше делать отрисовку не в виде сканов, а в виде фотографий в руке

лектор: Отправляем все это на мыло, указанное в форме, часто просят отправить по факсу, тут нужно звонить и просить дать адрес емаил

лектор: Получаем слип-чек (чек подтверждения проведенной транзы)

лектор: Без этого чека никогда никого не селите!!!!

лектор: Необходимо соблюдать максимальные лимиты на одну транзакцию

лектор: Не делать более 2-3к$, так как очень часто на большие суммы стоит ограничение на совершение платежей

лектор: Что делать если стоимость брони 4к на 10дней?

лектор: Разбиваем на две брони: первая на 2к 5 дней и вторая на 2к 5 дней

лектор: Схема выглядит так:

лектор: Заходим на http://www.booking.com/ делаем брони на того кто будет проживать (можно делать хоть за месяц до заселения)

лектор: За 2-3 дня до заселения звоним в отель, получаем форму авторизации – оплачиваем

лектор: Заселились

лектор: За 1-2 дня до начала второй брони звоним с того же номера в отель, получаем форму авторизации – оплачиваем

лектор: Самые лучшие карты для внесения оплаты это: Малазия, Сингапур, ЮАР, Германия,нам важем максимальный срок на чарж

лектор: К прозвону и отрисовкам надо подойти максимально серьезно!!!

лектор: Качество должно быть высокое, сомнений у работников отеля быть не должно!!!

лектор: 2) Вариант вбива в агента

лектор: Существует огромное множество агентов посредников между отелем и человеком кому этот отель нужен

лектор: Главное отличие тут в том, что агент имеет свой мерч для приема оплаты за отель

лектор: Разберем на примере Expedia.com

лектор: Бьём с деда или туннеля, подбор туннелей и дедов штука очень серьёзная!!!

лектор: у агентов очень жесткий антифрод, поэтому всё делаем максимально четко!!!

лектор: мат подбираем тоже внимательно, зип тунеля/деда должен совпадать с зипом СС если бьете юсой

лектор: нету мата под зип, значит не берем этот тунель/дед, так как даже если оплата и пройдет, то бронь не даст, а если и даст, то потом будет отмена, проверено многократно!!!

лектор: еще есть один нюанс который повышает шансы

лектор: Можно вписать в проживающих КХ, далее он может просто не приехать, а еще лучше прозвонить отель от имени агента, через которого делали бронь и попросить поменять Имя и Фамилию КХ на нужное нам

лектор: надо понимать, что Expedia.com очень популярный, и дает он очень неохотно, но агентов очень много и надо просто искать

лектор: скажу сразу поиск агента дело дорогое и долгое, тут нужно подойти системно – пробовать разный мат, разные схемы и тд..

лектор: обязательно записывайте все свои действия во время тестов, что бы потом точно понимать как вбивать и тд..

лектор: соответственно на эти эксперименты нужно иметь свободные средства

лектор: основной минус такого вбива это жуткий антифрод, часто нужен прозвон и отрисовки и так далее

лектор: но все это окупается плюсом: редко бывают отмены брони во время проживания. Это связано с тем что затраты на фрод мерч берет на себя)

лектор: На что стоит обращать внимание:

лектор: Очень часто мерчи сверяют телефон из данных СС, ну и частенько звонят — при малейшем подозрении, тут мы можем сами изначально проверить, активный ли номер у КХ, и если он включен и КХ берет трубку то надо зафлудить его насмерть что бы телефон он выключил, ну или купить СС где номер не активен

лектор: И соответственно когда из мерча они дозвониться не смогут то они напишут на мыло, и надо будет прозвонить самим

лектор: Еще обращайте внимание на сам отель который вибираете, если он новый или не популярный могут зафродить по подозрению на залив

лектор: 3) Вбив в booking.com

лектор: Booking.com — одна из крупнейших компаний на рынке онлайн-тревела

лектор: У них всё очень просто — отели выставляют свои обьекты, пользователи выбирают подходящие и платят отелям, которые раз в месяц выплачивают Букингу комиссию

лектор: ТО есть букинг не чаржит вообще и своего мерча не имеет!!!

лектор: Когда вы вводите на сайте данные CC booking по защищенному каналу пересылает ваши данные отелю

лектор: А отель списывает с вас деньги в какой-то момент времени по своему усмотрению

лектор: Может списать сразу, может через месяц, а может вообще не списывать и попросить вас об оплате на месте

лектор: Списание оплаты абсолютно непредсказуемая вещь, и определяется оно исключительно владельцем отеля, но никак не Booking.com

лектор: И тут надо быть готовым ко многим вопросам типа: покажите карту, оплатите налом и так далее

лектор: Надо понимать что когда вы или ваши клиенты заселяетесь то все эти вопросы могут возникнуть, и говорить с вами будут не по русски, а еще может возникнуть ситуация когда нет стафа который вообще может помочь по вопросам оплаты

лектор: вбили, дальше очень желательно проконтролировать списание средств, прозвоном в банк на робота или если били с ролки то необходимо посмотреть транзы онлайн

лектор: Если бьете евро то по обстоятельствам, чаще всего там ничего не узнаешь…

лектор: Но при ситуации когда отель не смог списать средства с карты они могут написать на мыло и тогда можно сунуть другую CC

лектор: НО ЧАСТЕНЬКО ОНИ ЭТОГО НЕ ДЕЛАЮТ!!!

лектор: Дальше ждём некоторое время и звоним в отель и говорим

лектор: «Привет я Вася Пупкин, только что оплатил номер через букинг. Проверьте пожалуйста все ли оплачено и не нужно ли дополнительных затрат от меня» ну желательно ещё просто поговорить немного: поспрашивать про погоду, про цены в баре, спросить сколько такси стоит в городе и так далее

лектор: Вы должны быть похожи на настоящего туриста!!!

лектор: Если все в порядке то можно селиться

лектор: У букинга и сервисов типа него, Агода например, очень серьезный минус в том, что частенько прилетает чарж во время проживания. В такой ситуации приходиться платить самому наличкой. А в том случае если КХ поднимает кипишь то можно пообщаться с местной полицией)))

лектор: Соответственно НИКОГДА нельзя бить матом той страны куда едет турист!!!

лектор: Важный аспект: А КАК ВООБЩЕ ОТЛИЧИТЬ АГЕНТА ОТ ПСЕВДО АГЕНТА

лектор: то есть при поиске мерча мы должны понимать принципы его работы и уже исходя их этого решать для себя подходит он Вам или нет

лектор: Первоначально читаем гугл, отзывы о сервисе, так называемый how it work соответственно бьем мы в сервисы иностранные и читаем тоже не на ру сайтах))))

лектор: Далее вбиваем тест с ролки и смотрим в транзах кто списывает деньги, если списывает сам отель то это не агент а сервис типа букинга, если списывает сам мерч сайта куда били значит это агент

лектор: Прошу обратить внимание на то что даже вбив в агента нет гарантий что бронь не слетит во время проживания!!!

лектор: 4) Брут аккаунты ревардов

лектор: Получить заветную бронь можно используя различные программы лояльности

лектор: Они есть двух типов:

лектор: Программы лояльности банков эмитентов CC, я думаю все об этом знают

лектор: КХ при том, когда расплачивается картой за каждый потраченный доллар получает: мили / поинты / реварды на виртуальный счет

лектор: И их можно потратить отели/авиа/авто или еще на что-то

лектор: И второй тип – это программы лояльности сетей отелей / крупных тур агенств / больших магазинов и тд

лектор: Работать с ними конечно не так просто, и на эксперименты нужно довольно много денег, к этому нужно быть готовым

лектор: Первоначально собирается информация о существующих программах лояльности, потом надо

написать софт для брута, найти аккаунты ну и попробовать сделать бронь

лектор: Там нюансов много и у каждой такой программы свои фишки… разобраться в них можно только попробовав

лектор: Основная заморочка: а даст ли делать бронь не на холдера ака а на левого Васю?

лектор: Нетрудно догадаться, что чаще всего не даст)))

лектор: Тут можно поступить так:

лектор: Пробовать прозвоном менять данные гостей в самом мерче, но тут нужно быть готовым к тому что будут пробовать набрать холдеру и встает вопрос активности номера

лектор: Можно позвонить в отель и сказать «Привет вместо меня приедет Вася с женой»

лектор: Еще вариант по скану (отрисовке): при заселении показывается бронь, а в случае если возникает вопрос: "Где человек на которого забронирован номер"

лектор: отвечаем: "Его пока нет, будет позже"

лектор: и показываем ксерокопию его паспорта которую предварительно отрисовали и распечатали

лектор: Сами аки мы брутим сами, так же можно покупать у логоводов, ну и иногда селлеры продают что-то но чаще всего ничего стоящего не продадут))))

лектор: Еще есть варианты совмещать, например, взять аккаунт и прилинковать к нему новую карту, и ей оплатить

лектор: Аренда АВТО

лектор: есть два варианта бронирования автомобилей

лектор: оплата полностью через агента (наш вариант)

лектор: оплата части с карты обычно 30-50%, и остальное через кассу непосредственно (нам это не подходит)

лектор: вбив стандартный описывать все не имеет смысла

лектор: и так вбив прошел удачно, и вы идете получать тачку, дальше вам придется внести депозит за авто со своей карты на которой есть ваше имя!!!

лектор: http://prntscr.com/gwsw9a

лектор: карту используют для блокировки некоторой суммы в качестве страховки и после сдачи авто сумма размораживается через 3-5 дней

лектор: на что нужно обратить внимание:

лектор: обязательно читайте правила пользования сервисом

лектор: убедитесь, что вы оплачиваете 100% за аренду, и никаких доплат не потребуется!!!

лектор: Обязательно смотрите на минимальный возраст водителя, часто на это не обращают внимание и просто не выдают автомобиль!

лектор: всегда имеем с собой деньги на оплату при слете!

лектор: Карта которую вы оставляете должна быть вам не важна, то есть если вы пользуетесь такой услугой по нее надо сделать карту что бы после аренды залочить ее, так как деньги могут снять и через несколько месяцев!!!

лектор: Экскурсии

лектор: один из них viator.com вбивы тут стандартные, расписывать смысла нет, остановлюсь на некоторых нюансах

лектор: антифрод чаще всего тоже очень серьезный

лектор: также как с букингом попадаются сервисы которые не чарджат сами, редко но такие встречаются, так что при тестах необходимо обратить внимание

лектор: при заполнении данных мы указываем данные для трансфера, то есть отель откуда забрать и телефон

лектор: Отель можно указать соседний, и просто подойти туда, но не нужно опаздывать что бы водитель не стал названивать в отель вам в номер

лектор: Если вы оставляйте номер телефона то тоже смотрите на кого он оформлен

лектор: Так же не стоит бить матом той страны где идет экскурсия)

лектор: Дальше хочу рассказать вам обязательные правила при пользовании карж-отелями:

лектор: До заселения всегда прозванивать в отель и подтверждать, что с бронью все в порядке!!

лектор: ВСЕГДА иметь деньги наличными, что бы при слете вы могли бы все оплатить!!!

лектор: Не тратить денег больше чем есть!!!!

лектор: При оплате формой всегда дожидайтесь получения «слип-чека» так как даже при прозвоне вам могут сказать, что все в порядке, а после заселения окажется что нет, и придется платить свои

лектор: НИКОГДА не давать свою карту, её могу просить для депозита или еще для чего, если просят – оставляйте наличные!!!

лектор: СРОК ПРОЖВАНИЯ не должен быть больше 14 дней, вы должны сами понимать – чем меньше тем лучше!!!

лектор: НИКОГДА и НИКОМУ не говорить откуда бронь и тд, никто не должен знать про карж!!!

лектор: Не рекомендую селится в РУ отели по каржу!!! В России при заселении у вас попросят паспорт, там есть все данные, найти вас труда не составит!!!

Авиа

лектор: Добрый вечер, сегодня поговорим, пожалуй, об одной из самых профитных тем в карже – авиа билеты

лектор: Сначала я Вам расскажу о разных вариантах добычи билетов,

лектор: потом поговорим о безопасности всего этого мероприятия,

лектор: а уже потом я отвечу на ваши вопросы

лектор: Итак, какие есть варианты:

лектор: АГЕНТЫ – ФОРМА – РЕВАРДЫ – ВБИВ В АК

лектор: агент – это посредник, например, bravofly.com, между огромным количеством авиакомпаний и пассажиром, оплата при этом поступает агенту

лектор: этот вариант безопасен для того, кто летит, так как при слёте все вопросы к тому посреднику кто билет выписал

лектор: чаще всего агенты — это сайты с мерчами с оплатой с ВБВ

лектор: то есть у нас тут три варианта:

лектор: CC+ВБВ = бронь держится лучше всего, но мат очень дорогой и найти его весьма затруднительно

лектор: В евро мерчи мат юса+вбв раньше лез нормально – сейчас лезет тоже не особо)))

лектор: CC ноувбв бины тут слет возможет в любой момент, очень зависит от страны CC от самого мерча и от много чего еще

лектор: CC амекс – сами cc амекс не имеют ВБВ как такового, сейчас что то сделали вроде, и какое-то время назад были мерчи которые амекс хавали, и если бить амексом Австралии или Новой Зеландии то давали

лектор: сейчас этот способ менее эфективен, так как все прочухали и затянули фрод

лектор: так же до сих пор находяться мерчи без вбв, но их очень мало и они очень жёсткие)))

лектор: Я довольно долго занимаюсь билетами, и дам несколько советов:

лектор: если вы решили попробовать себя на этом поприще – убедитесь в том что вы вообще умеете вбивать, без опыта со стафом, гифтами и тд не нужно вообще начинать, так как здесь понадобиться опыт и в понимании того как работает антифрод, и в настройке машины под вбив и в отрисовках и в прозвонах

лектор: не начинайте поиск мерчей авиа без хорошего капитала – который вы можете спокойно слить

лектор: научитесь работать системно

лектор: то есть когда вы нашли некий мерч который по вашему мнению должен давать, вы должны разработать систему для его тестирования

лектор: нужно попробовать разный мат

лектор: Нужно тестировать разные направления, если не дало РФ это не значит что не даст еще что то

лектор: Разные сроки бронирования и тд, многие не дают если мало время до вылета

лектор: Разные суммы купленных билетов, дешевые дает а дорогие нет

лектор: Прежде чем лететь самому или отправлять клиентов вы должны быть убеждены на 100% что ваш метод надежен!!!

лектор: На сегодняшний день тема авиа сильно побита, и даже мат с вбв не дает никаких гарантий успеха

лектор: В зависимости от авиакомпании и направления от пассажиров могут на стойке запросить отрисовку сс, например, все нюансы вы должны знать заранее

лектор: Очень часто оплата проходит нормально, тикеты дают но происходит слет, чаще всего это доп проверка платежа или еще что то. Тут надо прозванивать и разбираться в причинах слета, что бы далее продуктивнее работать

лектор: При работе с матом ВБВ стоит рассмотреть сам вбив поподробнее:

лектор: Настраиваем виртуалку, все должно быть идеально, после вбива производим чистку, если пользуемся Антиком то чистим и его

лектор: Покупаем носок или тунель, важно что бы он был быстрый и чистый, подбираем максимально близко под айпи КХ

лектор: Данные по АйПи КХ и юзерагенту КХ получаем от селлера СС+ВБВ

лектор: Заходим на сайт агента, если мы бьём ВБВ то надо на 100% знать что там он есть), выбираем билет оплачиваем

лектор: На примере СС+ВБВ Немцев опишу как там что

лектор: CC DE FULL INFO CLASSIC (это бины классик), цена на такие сс до 50 евро (лимит-гарантия в среднем 500евро)

лектор: CC DE FULL INFO HIGH (это бины от премиума до корпоративных), цена таких cc до 75 евро. CC HIGH бывают с лимит-гарантией до 750 евро

лектор: CC DE FULL INFO BUISNESS (бины карт бизнес и корпорейт и т д), цена на такие cc до 90 евро. Лимит-гарантия до 1300-1500 евро

лектор: понятно что цифры вестьма средние, и лимит-гарантия и цена могут отличаться в разы

лектор: так же на сегодняшний момент есть селлеры которые вообще не дают лимит гарантии

лектор: они пользуються тем что такой мат редок и пользуется огромным спросом

лектор: не покупаем никогда фуллки – SPARKASSEN (название банка), во первых мелочные, во вторых мощная антифрод система, в третьих, по ним нет замен

лектор: Естественно, если карта не валидная, тоже делается замена

лектор: Замену CC все селлеры делают строго при предоставлении видео вбива

лектор: Видео должно начинаться с момента открытия CC от продавца в привноте, потом показать что носок/туннель у вас читый (check2ip.com) и закончиться либо удачным вбивом либо проблемами на сбросе вбв и т д)

лектор: дам линк на прогу для записи

лектор: http://rutracker.org/forum/viewtopic.php?t=5022971

лектор: Формат выдаваемых сс обычный, но плюс к этому в фуллке ДЕ идет

лектор: Габерстатум (кратко говоря ДОБ)

лектор: Kontonummer (номер счета от 7-10 цифр)

лектор: Servicenummer (не на все цц) номер банка куда звонить, но он редко требуется

лектор: Bankleitzahl (номер банка для других банков, обычно не просит его, так как он един в банке)

лектор: SC соотвестенно Секьюрити код, для нас он известен как ВББ, но очень большое НО, он в 70% случаях не нужен, так как в немецких банках СК сбрасывается автоматov каждые 30 дней

лектор: получается мы активируем СК каждый раз используя Kontonummer (номер счета), Габерстатум (доб), Gultigkeit(эскпирейшн дэйт) и Пруфзиффер(свв2 код – трехзначный код)

лектор: Вбиваем данные пассажира, вбиваем данные карты, меняем ВББ и если все получается, то радуемся. Если карта невалид, не хватает средств до обговоренного лимита, не дает изменить ВББ, ставим Бандикам на стоп, заливаем на sendspace, отправляем селлеру и ждем замены

лектор: а вот еще очень важный нюанс

лектор: Вчера в лекции по отелям я подробно говорил о сервисах типа booking.com

лектор: Напомню эти сервисы которые не имеют собственного мерча и просто передают ваши данные в АК и уже авиакомпания их обрабатывает

лектор: При этом Вы можете сами не видеть этого

лектор: То есть когда вы делаете бронь через агрегатор типа skyscanner то вы видете что перешли при оплате на другой сайт

лектор: А при бронировании на vayama вы никуда не переходите, но деньги снимает та авиакомпания чей рейс вы делаете!!!

лектор: По факту это прямой вбив со всеми вытекающими последствиями

лектор: Как тут разобраться:

лектор: метода тут два — вбивать тесты с ролки и смотреть кто списал деньги

лектор: Можно так же позвонить в АК и под видом внесения неких изменений все разузнать, но этот метод не 100% часто бывает так что в АК говорят «обращайтесь к агенту который выписал билет» хотя само списание денег произвела авиа компания!!!

лектор: Если вы сделали тикет через такой мерч то желательно сделать клиенту фейк доки на билет и обязательно предупредить о возможных проблемах

лектор: При таком вбиве НИКОГДА не бейте матом той страны куда летите!!!

лектор: Бывали случаи когда снимают на пересадке и начинают очень сильно терзать!!!

лектор: ледующий способ это вбив в агента формой оплаты

лектор: Тут все так же как с отелями

лектор: Только звоним агенту, придумываем историю почему мы не можем оплатить через интернет, запрашиваем форму, делаем отрисовку, прозваниваем и делаем тикет

лектор: Скажу сразу, очень немного агентов сейчас принимают оплату по форме, ну и делать тикеты на небольшие суммы тут конечно не интересно так как себестоимость высокая получается

лектор: Следующая тема – это реварды

лектор: Тут тоже самое что и по отелям, многое я вчера рассказал

лектор: Отмечу важную вещь – чаще всего программы лояльности как раз позволяют делать отели/авиа/авто то есть все для туриста

лектор: Остается совсем немного – найти)))

лектор: Мили от авиа компаний тоже весьма рабочая тема, хотя у крупных авиа компаний уже все удрочено, и тут я хочу отметить важный нюанс

лектор: Когда мы оплачиваем тикет милями – часто требуется доплата налогов и сборов деньгами, тут вбиваем СС, но так же требуется найти СС что бы чарж был максимально длительный

лектор: Сумма таксов и доплат обычно не большая 20-100 баксов на пассажира

лектор: Порой можно оплатить таксы с виртуальной карты типа КИВИ или ЯД, но почти везде это уже не работает

лектор: Самые побитые АК это бритишь, дельта, люфтганза...они ведут себя очень странно, могут и ссадить с рейса на пересадке, бывает что регают на рейс а в самолет не пускают)))

лектор: Это я все пишу к тому, что прежде чем кого то отправлять важно все оттестить

лектор: Активность телефона очень важна, я об этом говорил на прошлой лекции по отелям, если вчера кого то не было перечитайте логи

лектор: Так же есть мили не какой то конкретно АК а обьединения, типа SkyTeam и в некоторых возможен вбив по код-шерингу, то есть у вас есть мили авиакомпании А а вы используете их для рейса компании Б

лектор: Тут совет такой, не используйте мили русских авиакомпаний, и не используйте мили западных АК для рейсов русских АК

лектор: Аккаунты можем добывать следующими способами:

лектор: Брутим сами – Покупаем с логов – Покупаем в шопах аков

лектор: СЛЕДУЮЩИЙ СПОСОБ ИСПОЛЬЗОВАТЬ НЕ СОВЕТУЮ

лектор: Прямой вбив в ак, чаще всего вбить в ак никаких проблем не бывает, там и вбв нету, да и фрод не так лютует, все это потому что ак может всегда с вас денгьги взять через суд)

лектор: Вбив напрямую дело криминально и очень опасное, случаев когда АК отсуживают все деньги очень много, так что делать это не советую)))

лектор: Безопасность по авиа

лектор: Итак, если вы хотите воспользоваться такой услугой, выбирайте продавцов с хорошими отзывами, используйте гаранта при сделках

лектор: ВСЕГДА имейте деньги на оплату тикета налом!!!!

лектор: Никогда никому не говорите о происхождении билетов

лектор: НИКОГДА не имейте с собой электронных следов на ноутах телефоне и тд, все всегда шифруйте!!!

лектор: Не нужно прыгать выше жопы!!!

лектор: То есть если у вас нету кеша на всякий случай – то не нужно покупать тикеты на бизнес-класс

лектор: Если вы открываете сервис:

лектор: Убедитесь на 100% что ваша схема работает

лектор: Не работайте без оплаты

лектор: Не берите заказов, которые не можете исполнить

лектор: Всегда осторожно относитесь к заказам где куча народа с детьми

лектор: Никогда не бейте напрямую в ак и в ру мерчи

лектор: Всегда и обо всем договаривайтесь на берегу