Россия, 2018

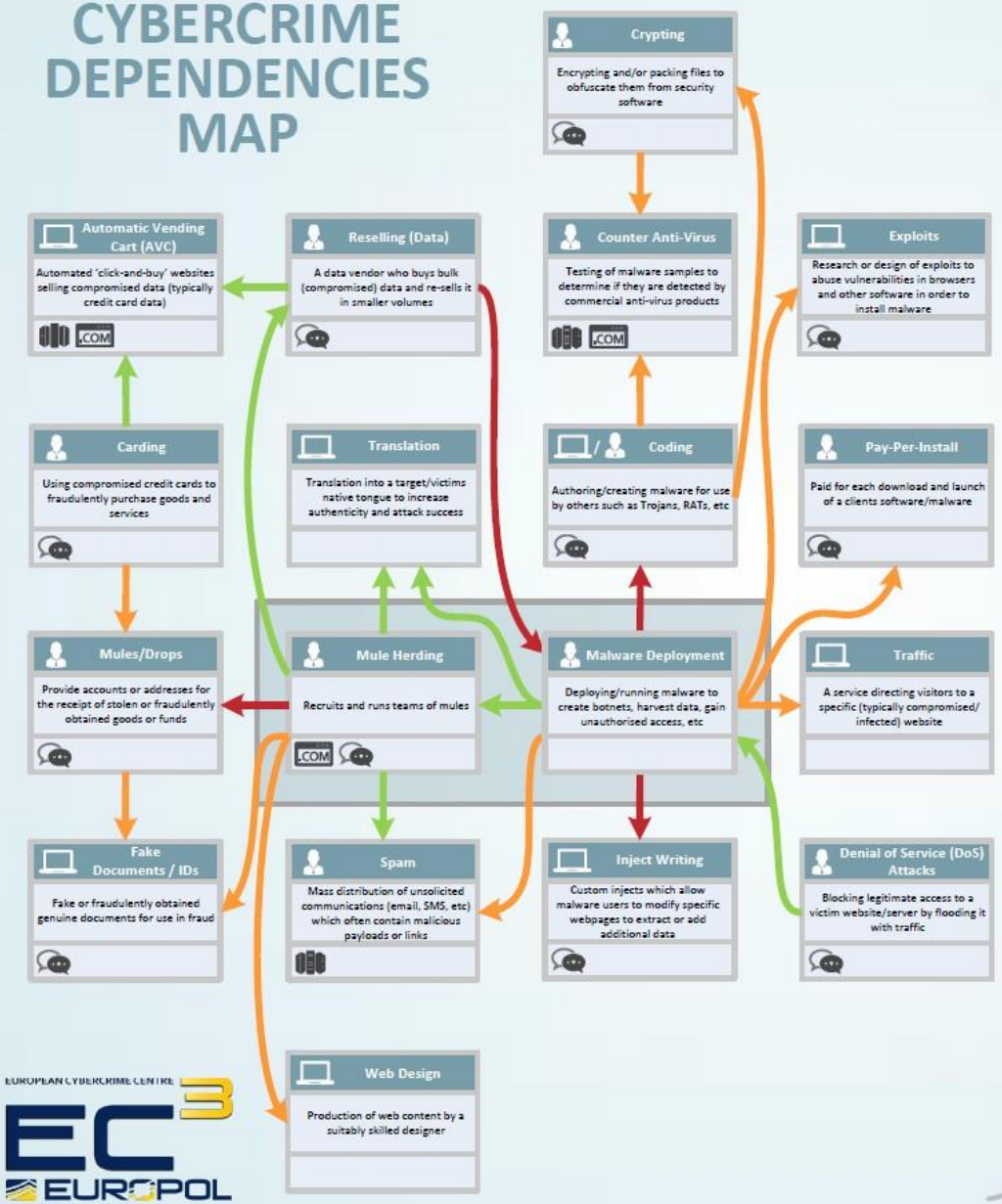
ПРОБЛЕМЫ, СВЯЗАННЫЕ С РАССЛЕДОВАНИЕМ И УГОЛОВНЫМ ПРЕСЛЕДОВАНИЕМ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В ДАРКНЕТЕ

«ПРЕСТУПЛЕНИЕ КАК-УСЛУГА»

- Огромное количество преступлений
- Необходимы специальные навыки, знания или инструменты
- Немногие могут выполнять множество различных действий
  - Специализируются в конкретной области
  - Когда им необходимы доступы или навыки, которых у них нет,
    - нужно КУПИТЬ доступ к следующему сервису: «ПРЕСТУПЛЕНИЕ КАК-УСЛУГА»
    - Каждый действующий субъект теневого киберпространства зависит от услуг, предоставляемых другими

Криминальная бизнес-модель

CYBERCRIME DEPENDENCIES MAP



Cross-Crime Factors

The **Cybercrime Dependencies Map** is designed to outline the key products and services within the digital underground and to highlight how and to what degree these products and services are *DEPENDENT* on each other to operate. For example, **Mule Herding** has a *HIGH DEPENDENCY* on the availability of **Mules.**

Several products or services are commonly required by many other services in order for them to operate. These have been collected under **Cross-Crime Factors.** Where one of these **Cross-Crime Factors** has been assessed as being of *HIGH* or *MEDIUM* importance to some of the key products/services it has been allocated an icon in order to annotate the appropriate product/ service.

Mouse over the arrows to see the level of dependency between products and/or services.

Europol Public Information

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

Зависимые продукты / услуги

Внедрение вредоносных программ

- Внедрение/ запуск вредоносных программ для создания бот-сетей, сбора данных...

Кодирование и написание внедряемых кодов

- Вредоносные программы, создаваемые путем Кодирования
- Настройка вредоносных программ
  - Выбор целей атаки, например, конкретного банка

Трафик и спам, а также оплата за установку и эксплойты

- Направляют жертв на зараженные сайты
- Отправляют вредоносные файлы или переадресовывают на вредоносные сайты
- Гарантируют установку вредоносного ПО на определенном количестве целевых систем
- Эксплойты, необходимые для установки вредоносного ПО на уязвимую целевую систему

"Выпас денежных мулов" и Перевод

- Внедрение вредоносных программ, в результате которого собираются скомпрометированные финансовые счета, которые необходимо обналичивать
- Может повысить эффективность кампаний по распространению вредоносных программ

«Выпас денежных мулов»

Набор команд «денежных мулов» и управление ими

«Денежные мулы»/Дропы

- Получают и / или передают незаконные средства

Разработка поддельных документов/удостоверений личности

- Создание банковских счетов или получение денежных переводов по поддельным документам
- Создание веб-сайтов, используемых в вербовке

Спам и Перевод, а также Перепродажа (данных)

- Распространение сообщений, предназначенных для вербовки
- Повышение эффективности вербовки путем адаптации языка кампании
- Перепродажа с целью получения списков адресов электронной почты, используемых для определения потенциальных мулов

«Денежные мулы»/Дропы

- МУЛЫ = деньги: Лица, завербованные с целью получения и перевода незаконно полученных денег между банковскими счетами и / или странами за комиссионное вознаграждение
  - Предоставляют счета или адреса для получения украденных средств
- ДРОПЫ = пакеты: Получают товары, заказанные мошенническим путем, и передают их клиентам

Поддельные документы/удостоверения

- Создание банковских счетов или получение денежных переводов под ложными именами

Мошенничество с платежными картами (кардинг)

- Использование скомпрометированных кредитных карт для покупки товаров и услуг

«Денежные мулы»/Дропы

- Для получения товаров, приобретенных обманным путем

Автоматизированные торговые авто

- Средства для получения скомпрометированных финансовых данных

Перепродажа (данных)

- Поставщик данных, который покупает скомпрометированные данные и перепродает их

Внедрение вредоносных программ

- Получение скомпрометированных данных в общей массе с целью дальнейшей перекомпоновки и перепродажи

Автоматизированные торговые автомат

- Средства для продажи скомпрометированных данных

Кодирование

- Разработка/создание вредоносных программ для использования другими лицами
  - Трояны, RAT-программы и др.

Программы обхода антивирусов и кр

- Проверяют, обнаруживается ли продукт коммерческими антивирусными программами
- Шифруют и / или упаковывают файлы для предотвращения обнаружения или анализа вредоносного кода с помощью программного обеспечения системы безопасности

Криптование

- Шифрование и / или упаковка файлов в целях сокрытия их от программного обеспечения системы безопасности

Программы обхода антивир

- Проверяют, обнаруживается ли упакованный/зашифрованный продукт коммерческими антивирусными программами

Атаки типа «отказ в обслуживании» (DDoS)

- Блокировка доступа к сайту/серверу путем заполнения его трафиком

Внедрение вредоносных программ

- Когда для проведения атаки требуется ботнет

Независимые товары / услуги

Автоматизированные торговые автоматы (AVC)

- Автоматизированные веб-сайты покупок «в один клик», продающие скомпрометированные данные
  - Данные кредитных карт

Программы обхода антивирусов

Тестирование образцов вредоносных программ с целью определения того, обнаруживаются ли они коммерческими антивирусными продуктами

Эксплойты

- Исследование или разработка эксплойтов с целью ненадлежащего использования уязвимостей для установки вредоносного ПО

Перевод

- На родной язык цели/жертвы для повышения достоверности и успеха атаки
- Плохой перевод часто является признаком того, что сообщение ложное

Оплата за установку

- Широко используется для распространения вредоносного ПО
- Плата за каждое скачивание и запуск клиентского программного обеспечения / вредоносного ПО

Трафик

- Сервис, направляющий посетителей на определенный (скомпрометированный / зараженный) веб-сайт

Написание внедряемых кодов

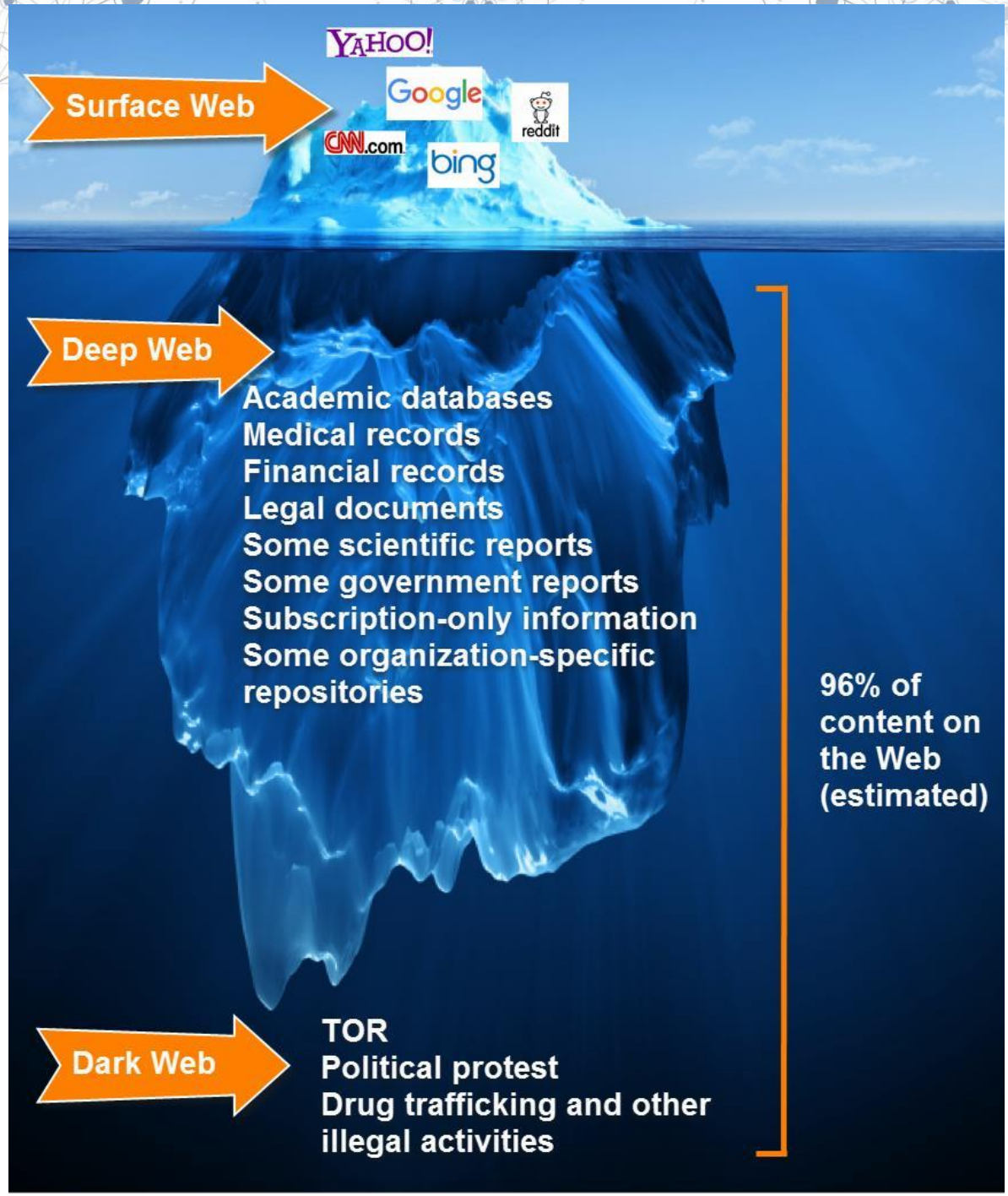
- Пользовательские внедряемые коды, которые позволяют пользователям вредоносных программ изменять определенные веб-страницы для извлечения или добавления дополнительных данных

Веб-разработка

- Создание веб-контента

Расследование и судебное преследование преступлений, совершенных в Даркнете и с криптовалютами

Методики расследования в Даркнете


YAHOO!
Google
reddit
CNN.com
bing
Surface Web
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories
96% of content on the Web (estimated)
Dark Web
TOR
Political protest
Drug trafficking and other illegal activities

Поверхностный интернет, Глубокий интернет и Даркнет

Поверхностный интернет

- Все, что можно найти с помощью обычной поисковой системы (Google Chrome, Safari и т. д.),

Глубокий интернет

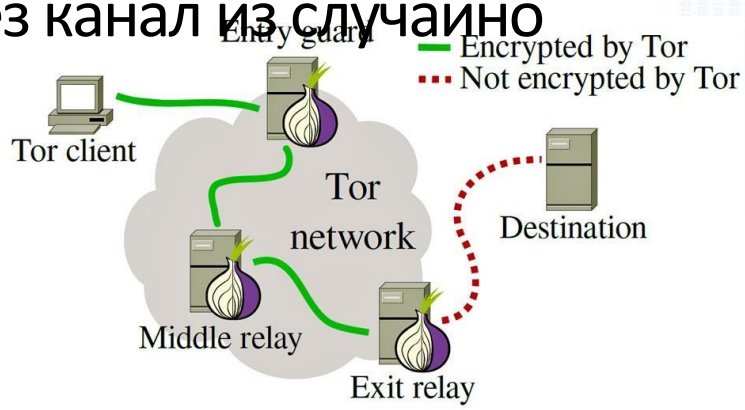
- Часть всемирной сети, недоступная поисковым системам
- Нет специальных инструментов, просто нужно знать, где искать
- То, что не может найти ваша обычная поисковая система (государственные базы данных, библиотеки и т. д.)

Темная паутина / Даркнет

- Вид сети, к которому невозможно получить доступ в нормальных режимах
- Небольшая часть глубокого интернета, которая скрыта умышленно
- Преднамеренно скрытая и недоступная через поисковые системы (сеть Tor, доступная только через браузер Tor)

Луковые сети

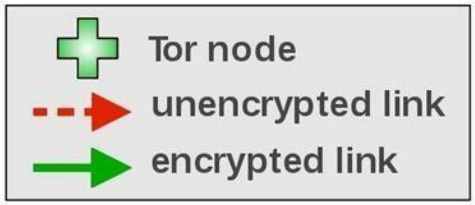
- Архитектура луковой сети первоначально была разработана военными - ВМС США
- Луковая маршрутизация осуществляется при помощи шифрования
- Наложение слоев шифра напоминает слои луковицы
- Tor несколько раз шифрует данные (в том числе назначение) и отправляет их через канал из случайно выбранных узлов сети Tor

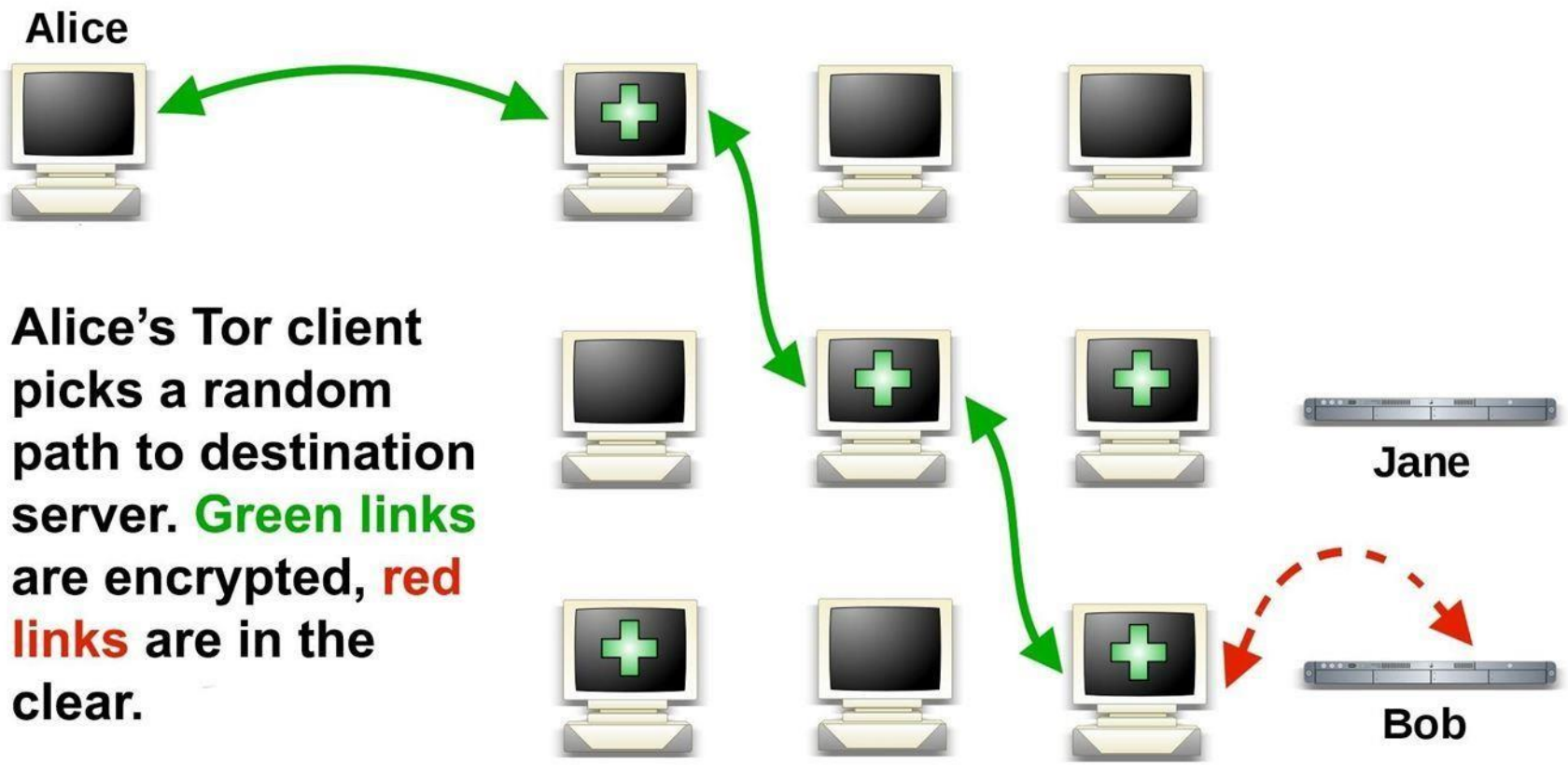


Луковые сети

- Во время доступа к поверхностному интернету ваш компьютер напрямую обращается к серверу, на котором размещен веб-сайт
- В луковой сети прямая связь нарушена, и данные проходят через ряд посредников, прежде чем достигнут цели
- Tor - это популярный луковый маршрутизатор, который достаточно удобен для анонимной связи и доступен для большинства операционных систем
- Может также использоваться для анонимного использования ресурсов поверхностного интернета

How Tor Works





Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Луковые сети

- Обеспечивают вашу анонимность в интернете
  - Как в отношении интернет-пользователей, так и в отношении издателей веб-сайтов
  - Правительственные учреждения теоретически способны отслеживать действия некоторых лиц
  - Очень сложно, необходимо огромное количество ресурсов
  - Не всегда успешно

Кто скрывается за тенями Даркнета?

Public

- Politically Oppressed
- Socially Disenfranchised
- Whistle Blowers
- Illicit Product/ Service Buyers

Government

- Agencies
- Contractors
- Researchers

Criminals

- Drug Cartels
- Organized Crime
- Human Trafficking

xHATs

- Script Kiddies
- White Hats
  - Vulnerability Researchers
  - Ethical Hackers
- Gray Hats
  - Hacktivists
- Black Hats
  - Botmasters
  - Financial Hackers
  - Hackers
  - Trolls

Terrorists

- Political Terrorists
- Environmental Terrorists
- Religious Terrorists

Использование Даркнета

- Военные, правительственные и правоохранительные организации входят в число основных пользователей
  - Используется посольствами правительств для отправки конфиденциальных писем и защиты разведданных
- Особенно популярны в странах с цензурой и тюремным заключением по политическим соображениям
  - Свобода от потенциального угнетения
  - Свобода от мониторинга средств связи
- Доступ к заблокированным интернет-сайтам, на которых действуют ограничения
  - Например. когда режим Мубарака в Египте закрыл доступ в Интернет, политические диссиденты использовали даркнет Tor для поддержания связи с остальным миром

Использование Даркнета

- Пользователи домашних ПК с целью защиты себя в интернете
- Активисты и революционеры создают организации, не опасаясь выдать свое положение правительствам
  - Активисты анонимно сообщают о нарушениях
- Террористы также используют его по тем же причинам, и поэтому наиболее известные пользователи даркнета - *преступники*

Использование Даркнета

- Место торговли запрещенными товарами
  - Наркотики
  - Огнестрельное оружие
  - Запрещенные эротические материалы
  - Контрафактные товары
  - Украденные кредитные карты
  - Программы-вымогатели
  - Наемные убийства
  - …
- Торговые площадки Alphabay, Silk Road 3, Dream Market, Valhalla …


LOADING 100%
BUSINESS
NETWORK
DAT BID
JAN € 241,00
FEB € 955,00
MAR € 116,00
APR € 262,00
MAY € 839,00
JUN € 706,00
AUG € 557,00
SEP € 50,00
LOADING 100%
NETWORK SEARCH

Криптовалюты, используемые в Даркнете

- Торговые площадки имели ключевое значение для развития криптовалют
  - Основываются на децентрализации и усиленных мерах безопасности
  - Конфиденциальность и анонимность криптовалют
- Bitcoin, Litcoin, Peercoin, Primecoin, Namecoin, Ripple, Quark, Freicoin, Mastercoin, Nxt, Auroracoin, Dogecoin и др.

Cryptocurrencies: **1610** • Markets: **10688** • Market Cap: **$458,909,198,682** • 24h Vol: **$30,933,152,407** • BTC Dominance: **36.0%**

#	Name
1	Bitcoin
2	Ethereum
3	Ripple
4	Bitcoin Cash
5	EOS
6	Cardano
7	Litecoin
8	Stellar
9	IOTA
10	NEO

Bitcoin (BTC)

$9,722.26 USD (5.52%)
1.00000000 BTC (0.00%)

Rank 1
Website
Website 2
Explorer
Explorer 2
Explorer 3
Message Board
Message Board 2
Source Code
Coin Mineable

Market Cap	Volume (24h)	Circulating Supply	Max Supply
$165,418,420,544 USD 17,014,400 BTC	$9,774,560,000 USD 1,006,160 BTC	17,014,400 BTC	21,000,000 BTC

Charts | Markets | Social | Tools | Historical Data

Bitcoin Charts

Linear Scale Log Scale

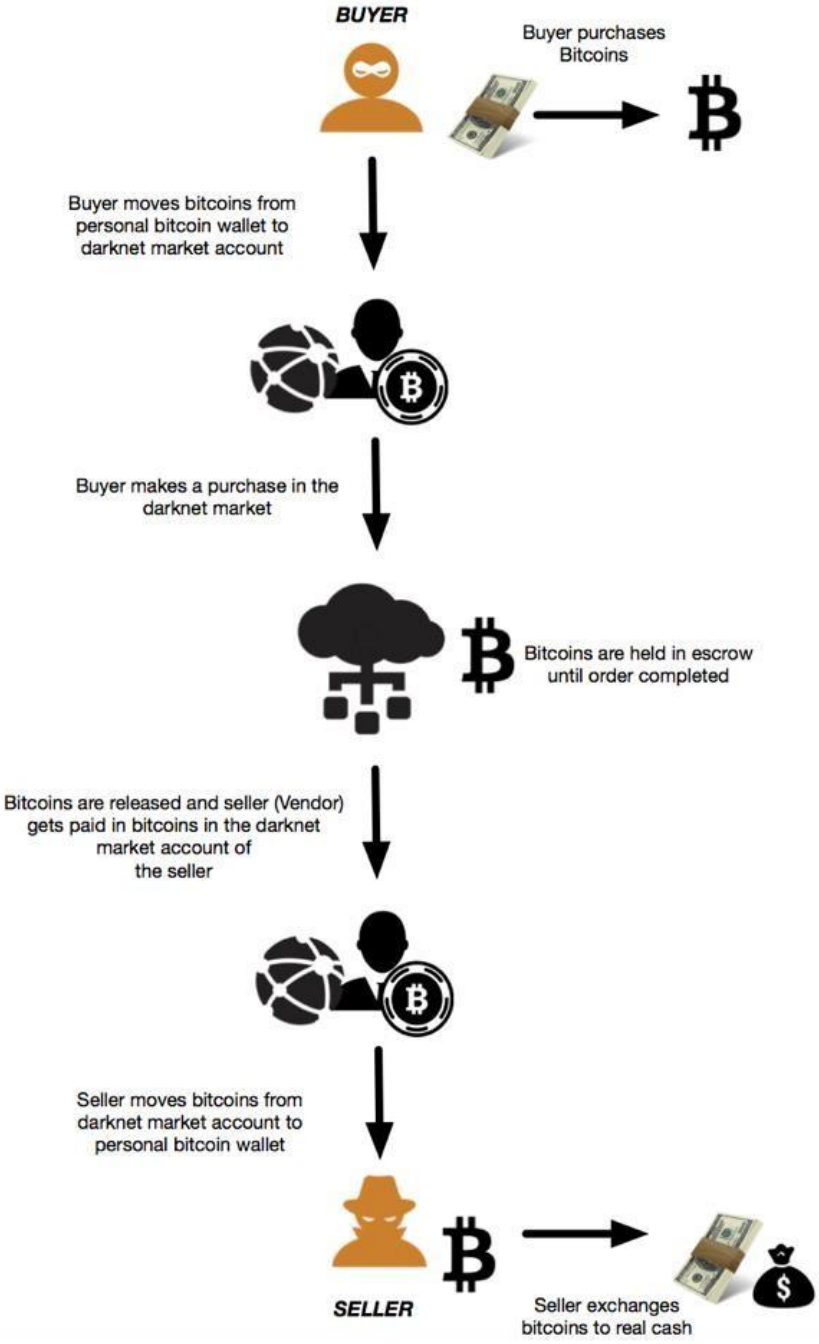
Zoom 1d 7d 1m 3m 1y YTD ALL From Apr 28, 2013 To May 4, 2018

Биткойн

- Биткойны используются для проведения анонимных операций
- И криптовалюты, и закрытые сети являются проектами с распределенной обработкой данных
  - Требуют, чтобы использовалась сеть из компьютеров, принадлежащих частным лицам, вместо одного мощного веб-сервера, принадлежащего компании

Биткойн

- Биткойн = виртуальные денежные средства
  - Форма денежных средств, которая объединяет одноранговый обмен файлами BitTorrent и шифрование с открытым ключом
  - Создана в качестве вознаграждения за вычислительную обработку данных = МАЙНИНГ
  - Пользователи проверяют и записывают платежи в публичный реестр = БЛОКЧЕЙН
    - Блокчейн содержит все операции, совершенные с биткойнами за все время
    - Новый блок генерируется каждые 10 минут = группа операций
    - Доступен всем, обновляется майнерами, контролируется всеми, не принадлежит никому
  - Выплаты совершаются не реальным людям, а на адреса
    - Доступны для всеобщего ознакомления в блокчейне


BUYER
Buyer purchases Bitcoins
Buyer moves bitcoins from personal bitcoin wallet to darknet market account
Buyer makes a purchase in the darknet market
Bitcoins are held in escrow until order completed
Bitcoins are released and seller (Vendor) gets paid in bitcoins in the darknet market account of the seller
Seller moves bitcoins from darknet market account to personal bitcoin wallet
SELLER
Seller exchanges bitcoins to real cash

Законность

- Все компоненты, используемые рынками даркнета (Tor, биткойн, VPN) являются законными
- Незаконные пакеты обычно проходят незамеченными
  - Разработаны таким образом, чтобы их не заметили
  - Почтовым службам и полиции запрещено законом открывать пакеты, которые не являются подозрительными
- Даже если власти конфискуют незаконный пакет, инструменты шифрования обеспечивают отсутствие легкого способа доказать в суде, что отправитель или получатель на самом деле совершил операцию
  - Что пакет не был просто случайно отправлен на неправильный адрес

Юрисдикция

- Серверы могут быть в любой точке мира
  - Кто имеет право доступа к данным?
- Поставщики и потребители в разных местах
  - Например, подростки в Перте могут в огромных количествах покупать запрещенные вещества у дилера в Сиднее
  - Сложная межгосударственная юрисдикция

Знания

- Интернет, глубокая паутина и темная паутина
- Луковые сети
- Криптовалюты
  - Биткойн
  - Блокчейн
- Методы шифрования
- Судебное право

Технология

- Сложное шифрование
- Инструменты обеспечения анонимности
- Миксеры

Исследование даркнета

- Даркнет мониторится правоохранительными органами
  - Владеют и управляют достаточным количеством узлов Tor для получения информации
  - Мониторинг социальных сайтов
    - Сайты темной паутины часто рекламируются на социальных сайтах
  - Получение снимков каждого нового сайта сразу после его обнаружения
  - Как только темный веб-сайт будет найден, необходимо загрузить и внести его в базу данных для будущего сематического анализа
    - Для сравнения
  - Агентствам безопасности следует создавать базы данных дилеров темной паутины
    - Дилеры переходят с рынка на рынок
  - Анализ веб-данных клиента с целью поиска подключений к нестандартным доменам
    - Контролируются только пункты назначения, а не те, кто к ним подключается

Исследование даркнета

- Сайты-ловушки Honeypot, предназначенные для поимки преступников
- При использовании сети Tor могут возникать утечки через надстройки
- Датская полиция внедрила методику поиска и судебного преследования продавцов на рынках даркнета
  - Анализ блокчейнов, а также методики идентификации клиентов и противодействия отмыванию денег и финансированию терроризма (ПОДФТ) с помощью обменников биткойнов
  - Анализ блокчейнов для подтверждения того, что адрес доставки указывает на конкретную операцию с биткойнами

Желаемые конечные точки

- Значения
- Даты
- Соединения с:
  - Другими адресами
  - Другими кошельками
- Субъекты реального мира
- Покупки в реальном мире

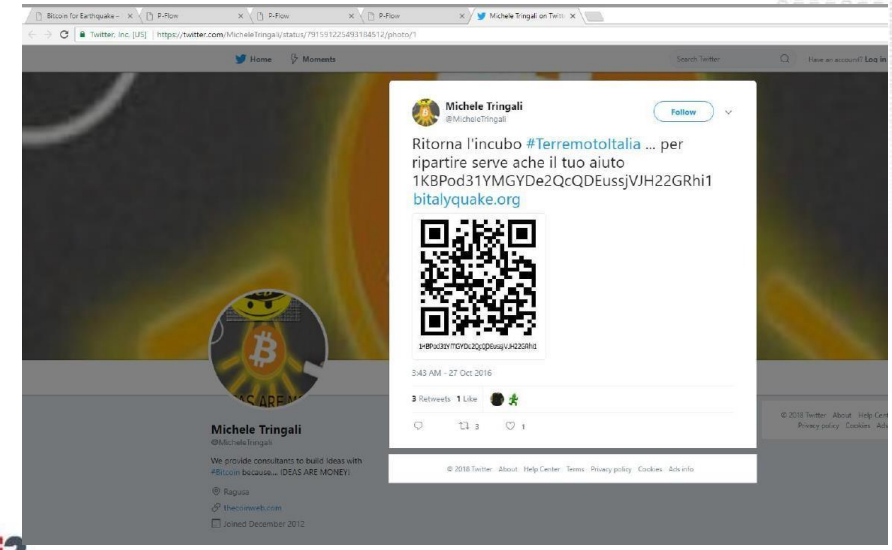
Исходные точки

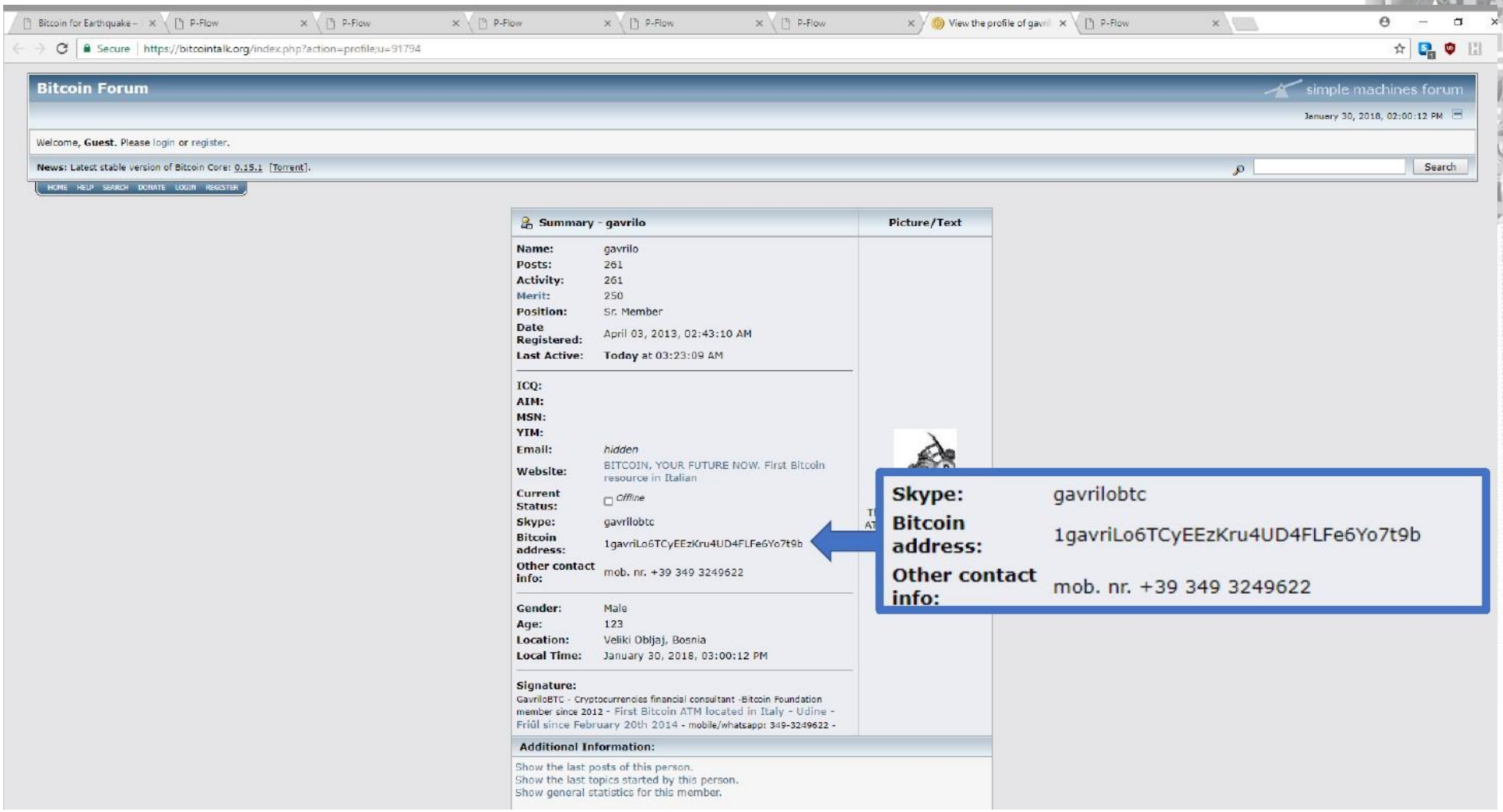
- Идентификатор адреса
- Идентификатор операции
- Значение
- Разведка на основе открытых источников (OSINT)

Source address	15VtCPFBKPPRNGk7F1aiB8ciYp87qXykHg
Destination address	19GL1k3i8K6u6wHfQSzaToM4ZRafVrsnwf
Transaction ID	141c19749e80326d48103dc9b106c6a63007435600b7ebdcb6a40677068b21fa

Где их найти

- Телефон/ноутбук
  - Установленный SPV-клиент
- Аппаратный кошелек
- Блог/форум пользователей
  - bitcoinTalk
  - BitcoinForum
- Блокнот, конверт, клейкие ли[illegible]
- ...




Bitcoin for Earthquake –
P-Flow
View the profile of gavri
Secure
https://bitcointalk.org/index.php?action=profile;u=91794
Bitcoin Forum
simple machines forum
January 30, 2018, 02:00:12 PM
Welcome, Guest. Please login or register.
News: Latest stable version of Bitcoin Core: 0.15.1 [Torrent].
Search
HOME HELP SEARCH DONATE LOGIN REGISTER
Summary - gavrilo
Picture/Text
Name: gavrilo
Posts: 261
Activity: 261
Merit: 250
Position: Sr. Member
Date Registered: April 03, 2013, 02:43:10 AM
Last Active: Today at 03:23:09 AM
ICQ:
AIM:
MSN:
YIM:
Email: hidden
Website: BITCOIN, YOUR FUTURE NOW. First Bitcoin resource in Italian
Current Status: Offline
Skype: gavrilobtc
Bitcoin address: 1gavriLo6TCyEEzKru4UD4FLFe6Yo7t9b
Other contact info: mob. nr. +39 349 3249622
Gender: Male
Age: 123
Location: Veliki Obljaj, Bosnia
Local Time: January 30, 2018, 03:00:12 PM
Signature:
GavriloBTC - Cryptocurrencies financial consultant -Bitcoin Foundation member since 2012 - First Bitcoin ATM located in Italy - Udine - Friûl since February 20th 2014 - mobile/whatsapp: 349-3249622 -
Additional Information:
Show the last posts of this person.
Show the last topics started by this person.
Show general statistics for this member.
Skype: gavrilobtc
Bitcoin address: 1gavriLo6TCyEEzKru4UD4FLFe6Yo7t9b
Other contact info: mob. nr. +39 349 3249622

Инструменты с открытым исходным кодом

- www.blockchaininfo.com
- www.walletexplorer.com
- www.bit-cluster.com
- www.blockseer.com
- …

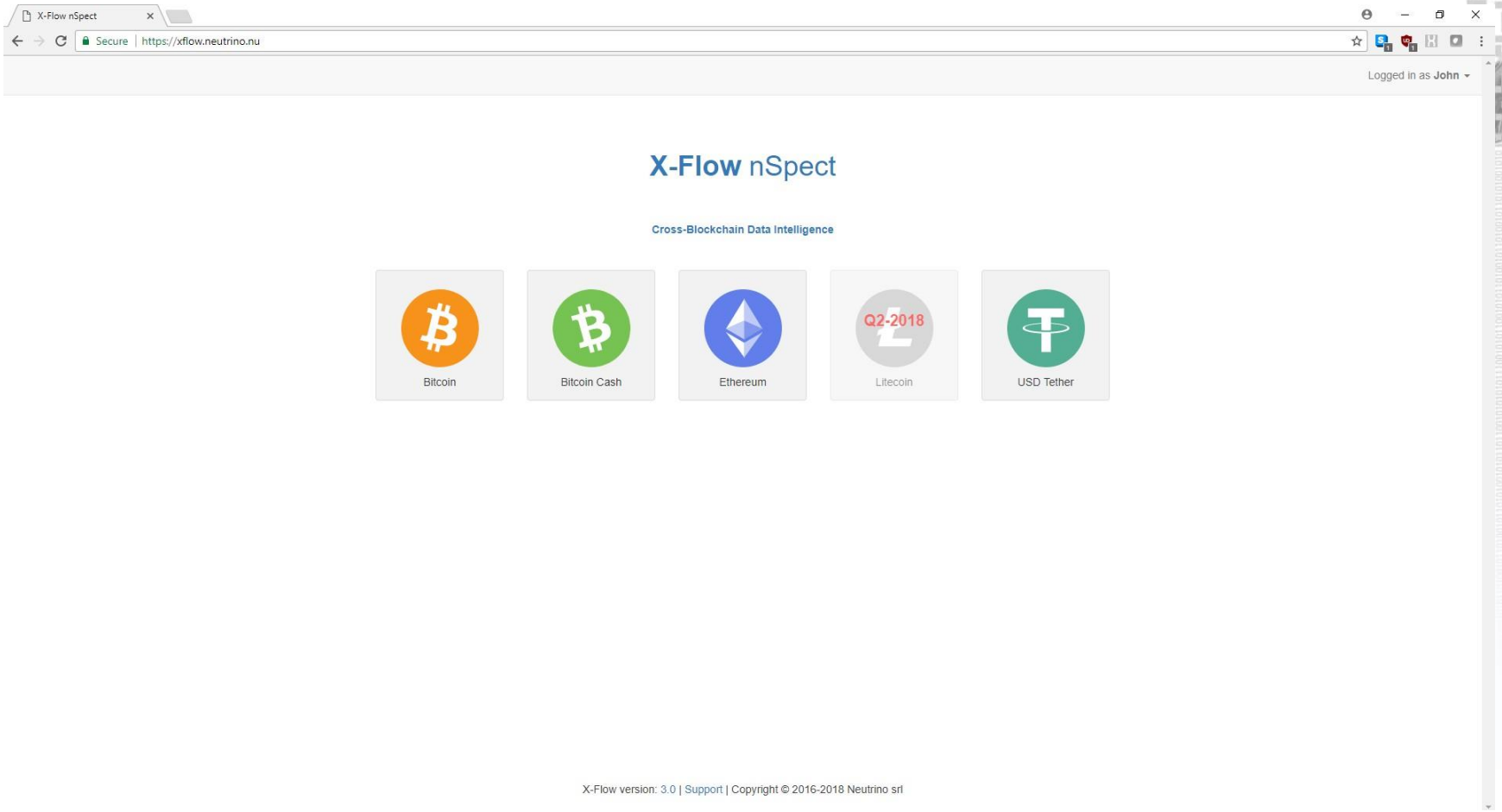
Обменники и поставщики кошельков

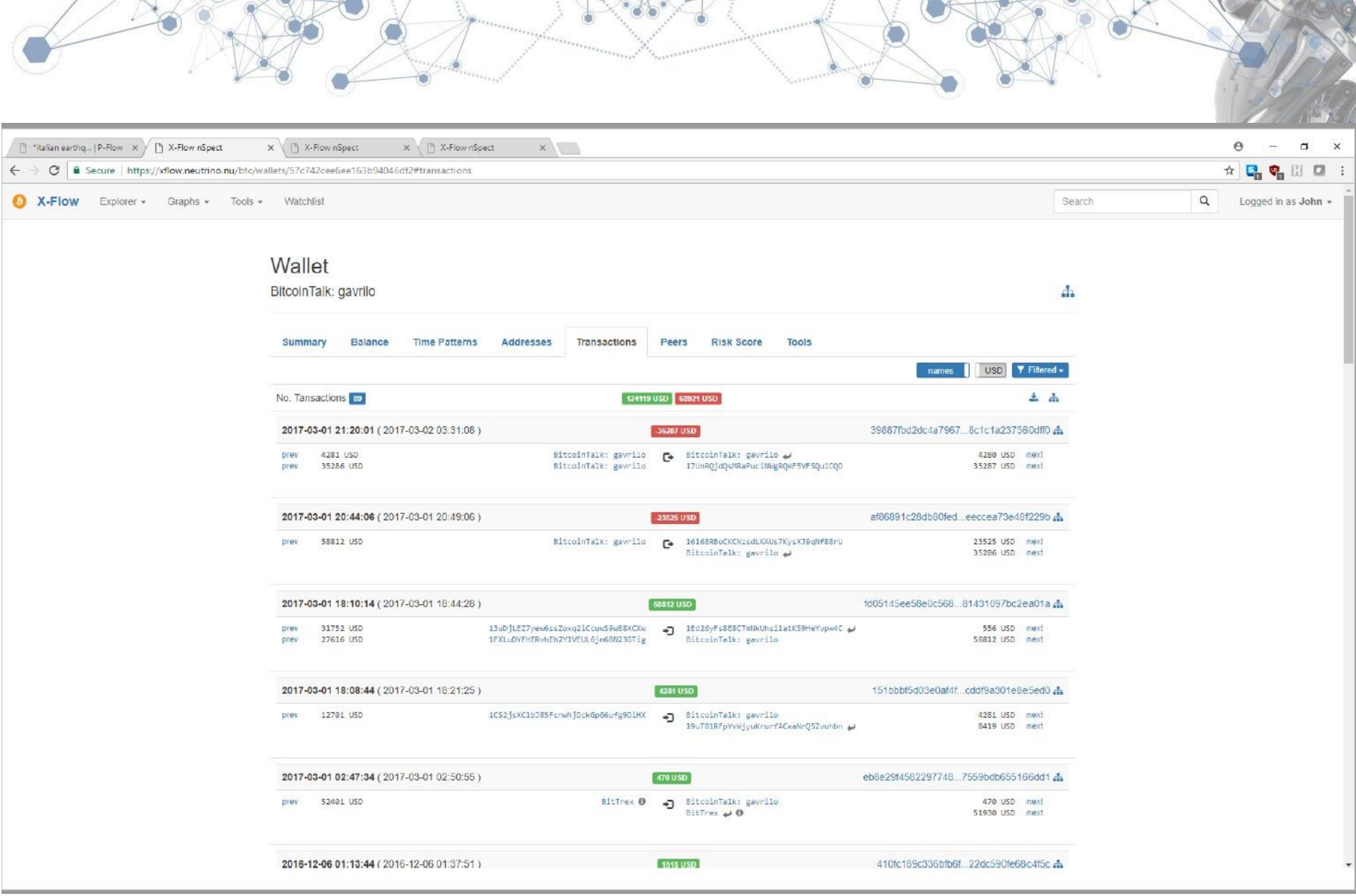
- В основном оценивают по уровню применяемой идентификации клиента (KYC)
  - KYC: удостоверяющий личность документ с фотографией, формы адресной информации ...
    - Контролируются (Хороший уровень KYC):

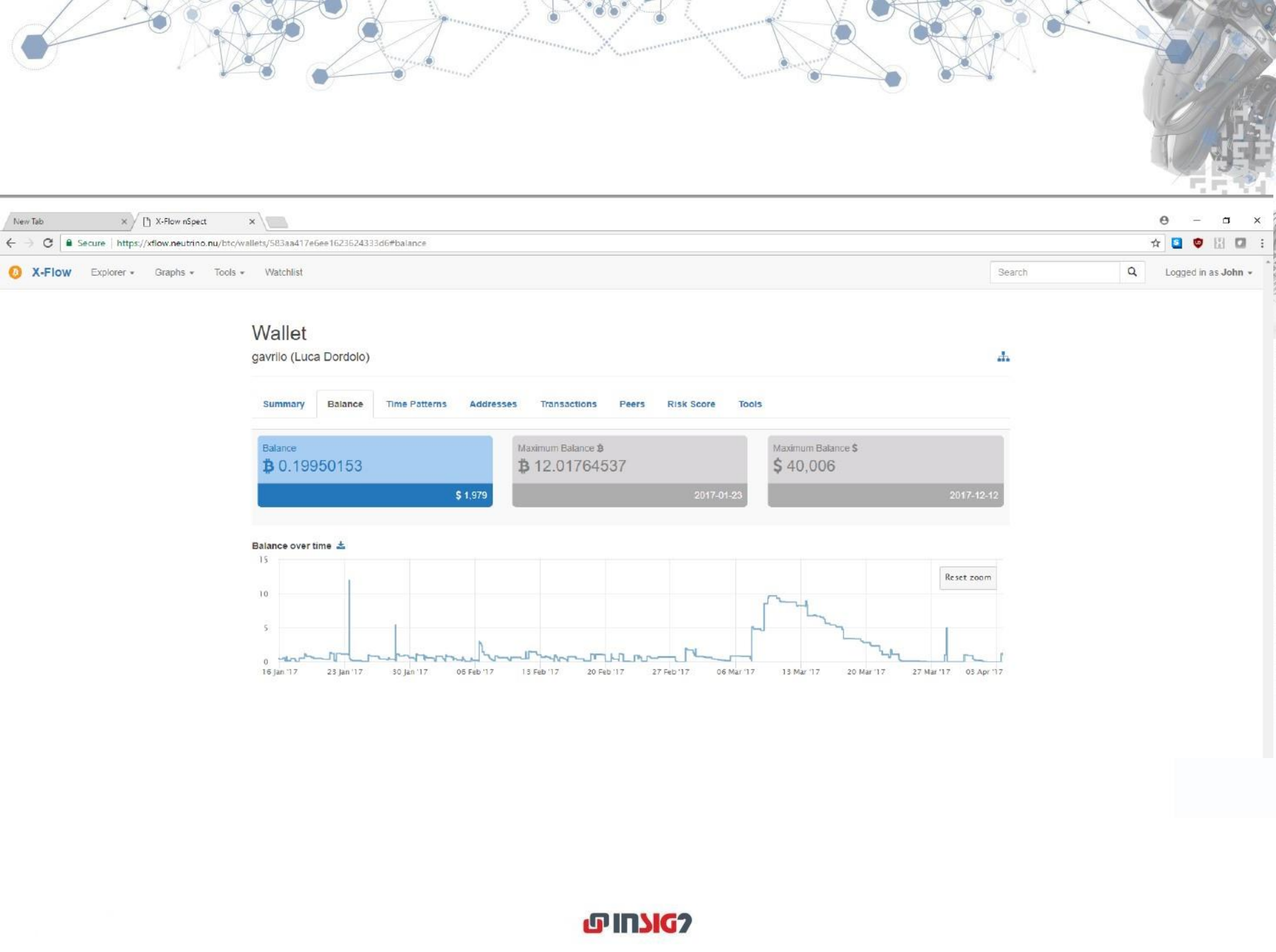
    coinbase, bitrex, cubits
  - NOKYC: адрес электронной почты
    - Не контролируются (Плохой уровень KYC):

    shapeshift, changelly

Операционная система Neutrino




*italian earthq... | P-Flow
X-Flow nSpect
X-Flow nSpect
X-Flow nSpect
Secure | https://xflow.neutrino.nu/btc/wallets/57c742cee6ee163b94046df2#transactions
X-Flow
Explorer
Graphs
Tools
Watchlist
Search
Logged in as John
Wallet
BitcoinTalk: gavrilo
Summary
Balance
Time Patterns
Addresses
Transactions
Peers
Risk Score
Tools
names
USD
Filtered
No. Tansactions 89
124119 USD
68921 USD
2017-03-01 21:20:01 (2017-03-02 03:31:08)
35287 USD
39887fbd2dc4a7967...8c1c1a237560dff0
prev 4281 USD BitcoinTalk: gavrilo BitcoinTalk: gavrilo 4280 USD next
prev 35286 USD BitcoinTalk: gavrilo 17UnRQjdQsNRaPuclNWgRQWF5VFSQu1CQD 35287 USD next
2017-03-01 20:44:06 (2017-03-01 20:49:06)
23525 USD
af86891c28db80fed...eeccea73e48f229b
prev 58812 USD BitcoinTalk: gavrilo 16168RBoCKCNzsdLKAUs7KysXJ9qNf88rU 23525 USD next
BitcoinTalk: gavrilo 35286 USD next
2017-03-01 18:10:14 (2017-03-01 18:44:26)
58812 USD
fd05145ee58e0c568...81431097bc2ea01a
prev 31752 USD 13uDjLEZ7yew6ssZoxq2iCcuwS9w88XCXw 1Ed26yFs8E8CTmNkUhs11atKS9HeYvpw4C 556 USD next
prev 27616 USD 1FXLuDYFHERvhEh2Y1VEUL6jm68N23GTig BitcoinTalk: gavrilo 58812 USD next
2017-03-01 18:08:44 (2017-03-01 18:21:25)
4281 USD
151bbbf5d03e0af4f...cddf9a301e8e5ed0
prev 12701 USD 1CS2jsXC1b385FcnwNjDckGpG6ufg9O1HX BitcoinTalk: gavrilo 4281 USD next
19uT81RFpYvWjyuKrurfACwaNrQ5Zvuhbn 8419 USD next
2017-03-01 02:47:34 (2017-03-01 02:50:55)
470 USD
eb8e29f4582297748...7559bdb655166dd1
prev 52401 USD BitTrex BitcoinTalk: gavrilo 470 USD next
BitTrex 51930 USD next
2016-12-06 01:13:44 (2016-12-06 01:37:51)
1518 USD
410fc189c336bfb6f...22dc590fe68c4f5c


New Tab
X-Flow nSpect
Secure | https://xflow.neutrino.nu/btc/wallets/583aa417e6ee1623624333d6#balance
X-Flow
Explorer
Graphs
Tools
Watchlist
Search
Logged in as John
Wallet
gavrilo (Luca Dordolo)
Summary
Balance
Time Patterns
Addresses
Transactions
Peers
Risk Score
Tools
Balance
฿ 0.19950153
$ 1,979
Maximum Balance ฿
฿ 12.01764537
2017-01-23
Maximum Balance $
$ 40,006
2017-12-12
Balance over time
Reset zoom
15
10
5
0
16 Jan '17
23 Jan '17
30 Jan '17
06 Feb '17
13 Feb '17
20 Feb '17
27 Feb '17
06 Mar '17
13 Mar '17
20 Mar '17
27 Mar '17
03 Apr '17

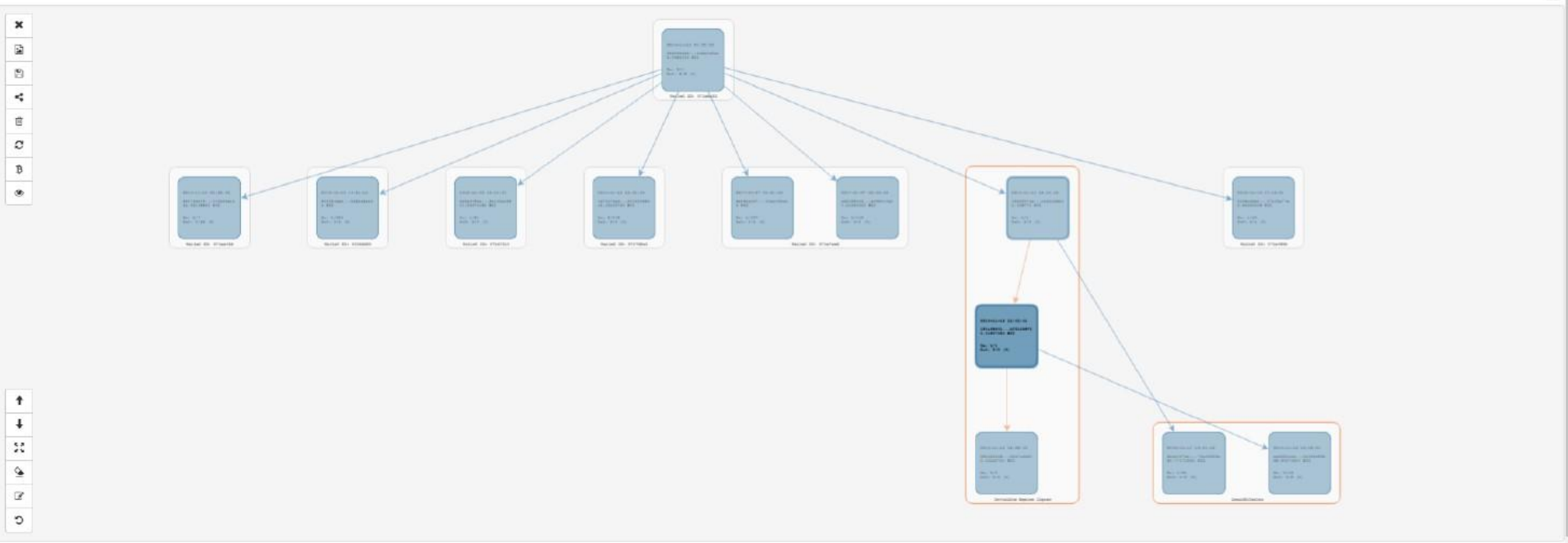
P–FLOW Explorer Graphs Tools Watchlist Search Logged in as demo fin

Summary Details Wallets Scripts Risk Score

2016-11-18 15:45:41 (2016-11-18 16:14:16) 120a69951f10c501355c7bb28e1e258d8b64528974ea44dcfcbef8ebf5189873 names BTC

In: 0.019773 BTC Fee: 0.00010285 BTC Out: 0.01967085 BTC

prev	0.019773 BTC	Invisible Empire Jigsaw	Invisible Empire Jigsaw LocalBitcoins	0.00367085 BTC 0.016 BTC	next next



PFlow version: 2.5 | Support | API | Copyright © 2016-2017 Neutrino srl

INSIG2

Криминалистическое расследование

- Проверить реестр
  - Путь к исполняемому файлу Tor-браузера
- Проверить pagefile.sys
  - Может содержать имя исполняемого файла Tor-браузера
- Проверить иконки
  - Значок логотипа с изображением лука
- Проверить Упреждающую выборку
  - Может содержать записи приложений Tor-браузера
- Пользовательский карвинг данных

Это сложные условия

- Зашифрованная инфор
- Псевдонимы
- Служит для обеспечени
- Непостоянство данных
  - Ежедневные изменения

Заключение

- Мониторинг темной паутины должен стать приоритетом
- Криптовалюты становятся основным центром внимания для подразделений по борьбе с киберпреступностью
- Правительства, террористы, правоохранительные органы и преступники являются одними из основных пользователей средств связи даркнета
- Легко получить доступ к даркнету и легко его использовать
- Использование Tor не противоречит закону, но вызывает подозрения
- Биткойны и даркнет затрудняют отслеживание потока денег

Как с этим бороться?

- Образование
  - У Интерпола есть давно действующие образовательные программы по даркнету, предлагающие обучение тому, как использовать темные рынки, взаимодействовать с отдельными лицами и отслеживать их, а также блокировать деятельность основных поставщиков
  - Профессиональные курсы, проводимые специализированными компаниями