Cybercrime In The Deep Web

Marco Balduzzi, Vincenzo Ciancaglini
HITB GSEC SG
15th Oct ‘15
About us

Dr. Marco BALDUZZI
- MSc in Computer Engineering
- Ph.D. in System Security with ~15 peer-reviewed papers
- 13+ years experience in IT Security -- Consultant, engineer and researcher
- Turned my hobby into my profession
- Sr. Research Scientist for Trend Micro
- Development of novel proof of concepts and complex systems

Dr. Vincenzo CIANCAGLINI
- M.Sc. in Telecommunication Engineering
- Ph.D. in Computer Networking, Peer to peer networks and next generations protocols
- 10+ years experience in R&D
- Sr. Research Scientist for Trend Micro
- Bridge scientific research and industry needs
- Veteran speaker in major conferences with 50+ talks
Roadmap

Introduction

Deep Web Analyzer (DeWA)
- Data collection
- Data enrichment
- Storage and indexing

Illegal Trading

Data Analysis

Malware

Conclusions
Deep Web: Internet not indexed by traditional search engines.

Dark Net: Private overlay network.

Dark Web: WWW hosted on Dark Nets.
The Deep Web is vast. Thousands of times larger than the surface web.

Alex Winter, Deep Web Documentary, 2015
The Deep Web is vast. Thousands of times larger than the surface web.

Alex Winter, Deep Web Documentary, 2015
Our research focus

- Infrastructure resilient to LE takedowns
- Marketplaces for cybercrime goods
- Safe haven for information exchange and coordination

Dark Web
- TOR
- I2P
- Freenet

Rogue TLDs
- Cesidian Root
- OpenNIC
- NewNations
- …

Custom DNS
- Namecoin
- Emercoin

Cesidian Root
Cyberterra Mean Time
Saturday 22 Kurosawa 2015 @ 535

name.space
the "dot everything people" since 1996
Oldest one: summer of 1999 (father of I2P)
Content distribution and discovery, no service hosting
Gossip protocol to lookup a resource (i.e. web page)
First beta in 2003
Full Dark Net, no anonymous browsing to the Surface Web
Garlic routing: multiple encrypted tunnels, multiple layers of encryption (transport, tunnel, path)
TOR

- First alpha in 2002
- Initially used to browse anonymously the Surface Web
- Hidden services -> effective Dark Web
- Onion routing: multihop routing with with host key encryption.

How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Dave

Alice

Bob

Jane

Tor node
unencrypted link
encrypted link
Namecoins, Emercoins

- Blockchain-based domain name server
- Think bitcoins, but instead of payment transactions, DNS register transaction

- Distributed
- Decentralised
- No regulating institution
rogueTLDs & privateDNSes

Plain old DNS, but with custom servers

Custom registrars

Custom domains
Roadmap

- Introduction
- **Deep Web Analyzer (DeWA)**
  - Data collection
  - Data enrichment
  - Storage and indexing
- Illegal Trading
- Data Analysis
- Malware
- Conclusions
System Overview

URLs Acquisition
- User data
- Scout feedback
- Pastebin
- Public sites
- TOR/I2P Gateways
- (DHT Monitor)
- Twitter

Indexing
- Events
- URLs
- URL Statistics
- Enriched Scouting Information

Page Scouting
- HTTP Headers
- Page Content
- Screenshot
- Links
- Emails, Bitcoins
- Port Scan

Enrichment
- Word Clusters
- Link Ratings
- Language Detection
- Translation

Qualitative Analytics
(Depth Web portal)
- System Monitoring
- Scouting Information
- Website Breakdown

Quantitative Analytics
(Kibana 4)
- Trend Analysis
- Aggregations
- Charts and Index Analytics
Data Sources

- User data
- Pastebin sites
- Twitter (1% feed)
- Reddit
- URL listing sites
- TOR gateways
- I2P host files
- Scouting feedback
Deep Web Gateway

- Privoxy + TOR anonymizer
- Polipo + TOR 64 instances
- I2P
- Freenet
- Squid transparent proxy
- Custom DNS resolver
- Namecoin DNS
- rogueTLD DNS
- Cesidian root
- Opennic
- NameSpace
- ...
Page Scouting

Headless browser

- HAR Log
- Page DOM
- Screen shot
- Title
- Text
- Metadata
- Raw HTML
- Links
- Email
- Bitcoin Wallets
Headless Browser

- Scrapyhub's Splash
  - QTWebkit browser
  - Dockerized
  - LUA scriptable
  - Full HTTP traces

- Crawler based on Python's Scrapy + multiprocessing + Splash access
  - Headers rewrite
  - Shared queue support
  - Har log -> HTTP redirection chain

- Extract links, emails, bitcoin wallets
Data Enrichment

Embedded links classification (WRS)
- Surface Web links
- Classification and categorisation

Page translation
- Language detection
- Non-English to English

Significant wordcloud
- Semantic clustering
- Custom algorithm
Significant Wordcloud

Page text

Tokenization

Filtering

Semantic distance matrix

Hierarchical clustering

Cluster label and popularity

Word cloud

Scrap text from HTML, clean up, strip spaces…

Create list of (word, frequency) pairs

Keep only substantives

How “far” are words from one another?

Group similar words

Label clusters, sum frequencies

Draw using summed frequencies
Example: Russian Forum

General information

<table>
<thead>
<tr>
<th>Title</th>
<th>Правила — Регистрация — Russian Silkroad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page MD5</td>
<td>3707c80ccd99134678d6ad611bdee86f</td>
</tr>
<tr>
<td>Page size</td>
<td>6911</td>
</tr>
</tbody>
</table>

Wordcloud (Top 20 words)

- moscow
- substance
- trading
- resource
- service
- news
- administration
- store
- forum
- seller
- rules
- customers
- registration
terms
- center
- platform
- silkroad
- ready
- seller
- registration
terms
- center
- platform
- silkroad
- ready
- seller

Russian Silkroad

Анонимная автоматическая торговая площадка

Форум | Правила | Регистрация | Вход

Вы не вошли. Пожалуйста, войдите или зарегистрируйтесь.

Новости

Futurama - Bender’s Game. Угадай курс биткоина и получи приз от магазина!
Kushman's Ganja - Москва - Шильки Royal Canadian Haze - один из любимых сортов Snoop Dogg и Dr. Dre. Готовые клады в центре Москвы.
Night City Light's - Москва - Амфетамины. Готовые клады.

Внимание - Приглашаем продавцов ПАВ с качественным товаром. Для тех, кто уже работает на других площадках, специальные условия. По вопросам открытия магазина пишите в личку RusSilk

Russian Silkroad → Регистрация → Правила

Регистрация на Russian Silkroad

Для регистрации необходимо согласиться с правилами форума ниже.

Правила ресурса

Форум и его сервисы полноценно работают без использования JavaScript.

Продажи происходят через систему автогаранта, требуется от продавцов её использование. Для покупателей услуга бесплатна.

Данный ресурс предназначен для покупок/продаж любых товаров, кроме явно запрещенных.

При помощи партнерской программы любой участник ресурса может зарабатывать на привлечении покупателей, получая в последствии процент с каждой совершенной покупки привлечённым рефералом.

Запрещено

1. Реклама межнациональной вражды.
2. Вынос информации из закрытых разделов форума.
3. Политика в любом ее проявлении.
4. Попытка продаж одного ПАВ под видом другого.
5. Оставление отзывов без реальной покупки через торговую систему площадки.
6. Регистрация провокационных, а также схожих с никами администрации и других пользователей.
7. Оскорбление других пользователей. Провоцирование ругани (троллинг в любых вариантах).
8. Обсуждение действий администрации ресурса и его правил.

Торговля разрешена всем, кроме:
Indexing

- Free text search
- Structured queries:
  - i.e. url.query.parameter:xu
- Analytics
- Data exploration

Elasticsearch

- URL Index
- URL Stats Index
- Scouting data Index
- Quantitative analysis
  - Kibana
- Qualitative analysis
  - Deepweb Portal
Collected Data

Running since **11/2013 (~2 years)**

- 40.5 M Events
- 611,000 URLs
- 20,500 domains

### Collected Data

<table>
<thead>
<tr>
<th>Source</th>
<th># events/hour</th>
<th># events/day</th>
<th>total events</th>
<th>first seen</th>
<th>last seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scouter</td>
<td>649</td>
<td>649</td>
<td>36,578,152</td>
<td>2014-06-06, 16:09</td>
<td>2015-10-12, 10:22</td>
</tr>
<tr>
<td>TOR Gateways</td>
<td>21,228</td>
<td>21,228</td>
<td>779,169</td>
<td>2015-05-08, 13:00</td>
<td>2015-10-11, 18:10</td>
</tr>
<tr>
<td>I2P Registries</td>
<td>1,280</td>
<td>1,280</td>
<td>368,015</td>
<td>2015-05-08, 15:58</td>
<td>2015-10-11, 18:10</td>
</tr>
<tr>
<td>SPN data</td>
<td>48</td>
<td>456</td>
<td>341,333</td>
<td>2013-11-12, 18:29</td>
<td>2015-10-12, 10:53</td>
</tr>
<tr>
<td>Reddit</td>
<td>543</td>
<td>543</td>
<td>15,466</td>
<td>2015-05-07, 20:03</td>
<td>2015-10-12, 10:54</td>
</tr>
<tr>
<td>Twitter</td>
<td>1</td>
<td>5</td>
<td>70</td>
<td>2015-05-08, 20:00</td>
<td>2015-10-11, 18:10</td>
</tr>
</tbody>
</table>
Demo time!
Roadmap

◎ Introduction

◎ Deep Web Analyzer (DeWA)
  ○ Data collection
  ○ Data enrichment
  ○ Storage and indexing

◎ Illegal Trading

◎ Data Analysis

◎ Malware

◎ Conclusions
### Guns

**UK Guns and Ammo Store**

#### Guns

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
<th>Buy now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glock 19 - 9mm - new and unused</td>
<td>£1.418</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>Walther P99 - 9mm - new and unused</td>
<td>£1.843</td>
<td>1</td>
<td>Buy now</td>
</tr>
</tbody>
</table>

#### Ammo

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
<th>Buy now</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 x 9mm Bullets for Glock 19</td>
<td>£0.142</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>100 x 9mm Bullets for Walther P99</td>
<td>£0.142</td>
<td>1</td>
<td>Buy now</td>
</tr>
</tbody>
</table>
Drugs! Drugs! Drugs!

CRISTAL METH 7g
$1.61
BUY

COKE From PERU 93%, 7 gram, FINALIZE EARLY
$2.37
BUY

COKE From PERU 93%, 3 gram
$1.27
BUY

Crystal Meth - 2g
$0.85
BUY

SHOW STIMULANTS CATEGORY

LSD Anonymous 140µg, 50 blotters
$1.1
BUY

1 OZ Super Stong Mushrooms
$0.59
BUY

1oz Cubensis Mushrooms
$0.61
BUY

!! SPECIAL OFFER 1oz DRY PSILOCYBIN CUBENSIS SHROOMS!!
$0.42
BUY
# Passports and Fake IDs

<table>
<thead>
<tr>
<th>Country</th>
<th>Price for Passport</th>
<th>Price for Passport + Driving License</th>
<th>Price for Passport + ID Card</th>
<th>Price for Passport + Driving License + ID Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>600 Euro</td>
<td>700 Euro</td>
<td>700 Euro</td>
<td>800 Euro</td>
</tr>
<tr>
<td>Belgium</td>
<td>500 Euro</td>
<td>600 Euro</td>
<td>600 Euro</td>
<td>700 Euro</td>
</tr>
<tr>
<td>Brazil</td>
<td>400 Euro</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Canada</td>
<td>600 Euro</td>
<td>700 Euro</td>
<td>700 Euro</td>
<td>800 Euro</td>
</tr>
<tr>
<td>Ireland</td>
<td>500 Euro</td>
<td>600 Euro</td>
<td>600 Euro</td>
<td>700 Euro</td>
</tr>
<tr>
<td>Italia</td>
<td>550 Euro</td>
<td>650 Euro</td>
<td>650 Euro</td>
<td>750 Euro</td>
</tr>
<tr>
<td>Finland</td>
<td>500 Euro</td>
<td>600 Euro</td>
<td>600 Euro</td>
<td>700 Euro</td>
</tr>
<tr>
<td>France</td>
<td>600 Euro</td>
<td>700 Euro</td>
<td>700 Euro</td>
<td>800 Euro</td>
</tr>
<tr>
<td>Germany</td>
<td>600 Euro</td>
<td>700 Euro</td>
<td>700 Euro</td>
<td>800 Euro</td>
</tr>
<tr>
<td>Netherlands</td>
<td>600 Euro</td>
<td>700 Euro</td>
<td>700 Euro</td>
<td>800 Euro</td>
</tr>
<tr>
<td>Norway</td>
<td>650 Euro</td>
<td>750 Euro</td>
<td>750 Euro</td>
<td>850 Euro</td>
</tr>
<tr>
<td>Poland</td>
<td>500 Euro</td>
<td>600 Euro</td>
<td>600 Euro</td>
<td>700 Euro</td>
</tr>
<tr>
<td>Portugal</td>
<td>500 Euro</td>
<td>600 Euro</td>
<td>600 Euro</td>
<td>700 Euro</td>
</tr>
<tr>
<td>Spain</td>
<td>550 Euro</td>
<td>650 Euro</td>
<td>650 Euro</td>
<td>800 Euro</td>
</tr>
<tr>
<td>Switzerland</td>
<td>650 Euro</td>
<td>750 Euro</td>
<td>750 Euro</td>
<td>850 Euro</td>
</tr>
<tr>
<td>Sweden</td>
<td>550 Euro</td>
<td>650 Euro</td>
<td>650 Euro</td>
<td>750 Euro</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>650 Euro</td>
<td>750 Euro</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>USA</td>
<td>700 Euro</td>
<td>800 Euro</td>
<td>800 Euro</td>
<td>900 Euro</td>
</tr>
</tbody>
</table>

For some countries we have an unique option to register passports in official government department databases. To get more details please contact with our manager: documents.service@safe-mail.net

<table>
<thead>
<tr>
<th>Additional service</th>
<th>Price for one unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents duplicating</td>
<td>extra 100 Euro</td>
</tr>
<tr>
<td>Visa/stamps affixion</td>
<td>extra 25-110 Euro</td>
</tr>
</tbody>
</table>

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.
Counterfeit Money

20 CNY BILLS

5000 CNY (250 bills) $1.35 BUY NOW
7500 CNY (375 bills) $1.80 BUY NOW
10000 CNY (500 bills) $2.26 BUY NOW

15000 CNY (750 bills) $3.14 BUY NOW
20000 CNY (1000 bills) $3.93 BUY NOW
50000 CNY (2500 bills) $8.64 BUY NOW

50 CNY BILLS
Credit Cards

Higher balance = higher price

<table>
<thead>
<tr>
<th>Credit Card</th>
<th>Balance</th>
<th>Daily Withdraw Limit</th>
<th>Amount</th>
<th>BTC Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA VISA</td>
<td>$2,000</td>
<td>$500</td>
<td>0</td>
<td>0.4001 BTC</td>
</tr>
<tr>
<td>USA VISA</td>
<td>$5,000</td>
<td>$1,000</td>
<td>0</td>
<td>0.7557 BTC</td>
</tr>
<tr>
<td>EU VISA</td>
<td>€5,000</td>
<td>€1,000</td>
<td>0</td>
<td>0.9335 BTC</td>
</tr>
</tbody>
</table>
Paypal & Ebay Stolen Accounts

We get new lists every day!
80%+ working guarantee, we will replace if more than 20% don't work!

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 PayPal accounts</td>
<td>100 USD = 0.434 $</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>100 Ebay accounts</td>
<td>100 USD = 0.434 $</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>100 CCs with CVV2</td>
<td>150 USD = 0.652 $</td>
<td>1</td>
<td>Buy now</td>
</tr>
</tbody>
</table>
# Assassins

## SELECT VICTIM's LOCATION:

### EUROPE

<table>
<thead>
<tr>
<th>Name</th>
<th>Confirm Victims</th>
<th>Age</th>
<th>Gender</th>
<th>Extended Suffering</th>
<th>Photo/Video</th>
<th>CONTINENT</th>
<th>HIRE Price</th>
<th>Email/Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklord</td>
<td>(100+)</td>
<td>16+</td>
<td>ANY</td>
<td>+</td>
<td>+</td>
<td>EUROPE, ASIA, AFRICA</td>
<td>5000 €/person</td>
<td></td>
</tr>
<tr>
<td>K2</td>
<td>(70+)</td>
<td>20+</td>
<td>ANY</td>
<td>+</td>
<td>+</td>
<td>EUROPE, ASIA, AFRICA</td>
<td>7500 €/person</td>
<td><a href="mailto:K2@mail2tor.com">K2@mail2tor.com</a></td>
</tr>
<tr>
<td>HITMAN</td>
<td>(70+)</td>
<td>ANY</td>
<td>ANY</td>
<td>+</td>
<td>+</td>
<td>EUROPE, ASIA</td>
<td>3000 €/person</td>
<td></td>
</tr>
<tr>
<td>Rodger D.</td>
<td>(20+)</td>
<td>16+</td>
<td>ANY</td>
<td>+</td>
<td>+</td>
<td>EUROPE, ASIA</td>
<td>10000 €/person</td>
<td></td>
</tr>
</tbody>
</table>
Crowdfunding evil

The concept is simple:

1. Someone adds a name to the list with background information.
2. People add money to the dead pool to entice would be assassins.
3. Assassins and speculators predict when the person will die, but the content of the prediction stays hidden until after the fact.
4. Correct predictions get the pool.

The List

<table>
<thead>
<tr>
<th>Name</th>
<th>Country</th>
<th>Status</th>
<th>Pool Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barack Hussein Obama II</td>
<td>United States of America</td>
<td>Alive</td>
<td>$0</td>
</tr>
<tr>
<td>Ben Shalom Bernanke</td>
<td>United States of America</td>
<td>Alive</td>
<td>$0</td>
</tr>
<tr>
<td>Hugh Grant (business executive)</td>
<td>United States of America</td>
<td>Alive</td>
<td>$0</td>
</tr>
<tr>
<td>Justin Drew Bieber</td>
<td>United States of America</td>
<td>Alive</td>
<td>$0</td>
</tr>
</tbody>
</table>
Roadmap

◎ Introduction
◎ Deep Web Analyzer (DeWA)
  ○ Data collection
  ○ Data enrichment
  ○ Storage and indexing
◎ Illegal Trading
◎ Data Analysis
◎ Malware
◎ Conclusions
Protocols (no HTTP/S)

By publicly sourced URLs

Protocol breakdown:

Legend:
- irc
- ircs
- magnet
- gopher
- xmpp
- telnet
- ftp
- git
- mailto
- news
- rhttp
- webcal
- imap
- mumble
- pop
- smtp
- 80
- 6,667

172
17
7
#freeanons 15 [+Cnt] This channel is created to support arrested Anons and act with solidarity in Anons. No MoneyFags, No Famefags, No PowerManiacs, No LeaderFags! Another Anons was arrested in France: http://www.ladepeche.fr/article/2015/10/10/2194982-enquete-de-la-dgsi-sur-du-piratage-informatique.html

<table>
<thead>
<tr>
<th>IRC</th>
<th>IRCS</th>
<th>SSH</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>31</td>
<td>855</td>
</tr>
</tbody>
</table>
Languages per domain

Language breakdown domains

Legend:
- English
- Russian
- French
- German
- Catalan
- Portuguese
- Italian
- Polish
- Spanish
- Finnish
- Bulgarian
- Japanese
- Dutch
- Danish
- Chinese
- Swedish
- Spanish; Castilian
- Romanian
- Other
交易区规则

一、一些简单的规则，待完善
1. 严禁发布反人类的物品，如尸体、排泄物等。
2. 所有交易一律使用比特币（BTC），按照当天的汇率换算。
3. 所有交易请不要使用真实的邮箱，请勿留下除了邮箱以外的任何联系方式，如QQ、手机等。
4. 所有的实体物品交易请不要当面进行，违者后果自负。
5. 所有的虚拟物品交易请谨慎防骗子，如发现骗子，请及时汇报。

二、一些简单的建议，待完善
1. 推荐使用匿名邮箱，如 mail2tor.com 等，勿使用真实的互联网邮箱。
2. 推荐使用比特币交易，可在各个国内外网站购买，购买后请尽快存到自己的比特币钱包，请不要使用国内的网站进行交易。
3. 千万不要在论坛泄露自己的真实信息，包括但不限于QQ、手机、身份等。

管理员邮箱：nzyoung@mail2tor.com
暗网中文论坛
Pages Embedding Suspicious Links

Mr. TwoFaces
Newbie

7 Cracked Paid Keyloggers
« on: November 25, 2014, 05:03:09 pm »

[h]Collection of Cracked Paid Keyloggers[/h]

I'd like to present to you my list of cracked paid Keyloggers. Please PM me if any download link isn't working, I will provide a new one for you.

Format:

Name (Thread Design)
Download Link

Predator Pain v1.4 (http://www.predatorpain.com/bronxfiles/iI9hX2b.png)
https://mega.co.nz/#!/yQAQFjzC!cf_NyRyGY_jgjByfOZi27o_AM9K5IMNSF6Tak85feE

Autologger 2.0 (http://i1.minus.com/ibfxq2rWiKVyjr.jpg)
http://adfoqc.us/22069339665199

Hades Logger (https://i.imgur.com/ice0pyQ.jpg)
http://adfl.ly/rvnpl

Galaxy Logger & Stealer (https://i.imgur.com/9DQRD0j.jpg)
https://mega.co.nz/#!/2zOQQDha!GP8hd4dmL0Rt8z7RNaltHr3Gt9r4fkkK802mZuQ4CE

Tasty Logger (https://pup.sh/4FatG.png)
https://mega.co.nz/#!/HRQFQTJY!GgoeZ0rNxO...rpidpoUviC8
Password: http://DeceptiveEngineering.info
Eis algumas pizzas que foram APROVADAS hoje (01/03/2015)...

---

BANDEIRA: Mastercard
TIPO DO CARTAO: Platinum / Itau Unibanco
NUMERO DO CARTAO: 541555018763XXXX
DATA DE VALIDADE: 10/16
CODIGO DE SEGURANCA: 953
NOME NO CARTAO: Humberto Alcantara
DATA DE NASCIMENTO: 26/10/1964
TELEFONE:
CPF: 440.645.528-06
STATUS: Debitado

BANDEIRA: Mastercard
TIPO DO CARTAO: Gold / Itau Unibanco
nullCoder, eu clico no +1 (vaaaras vezes) mas não acontece nada. clico clico clico clico mas nada Man!! TOTAL!! Queria te dar +9999 mas não ta indo.

Se ainda tiver um pedaço pra mim... tive que sair rapidinho da net e só voltei agora.

Outra coisa, alguns sites que tentei pedem o endereço. Como eu chuto qualquer endereço, acho que é por isso que alguns não vão!

Lá em cima do seu navegador possui um ícone S com um bloqueio, habilite-o temporariamente que você consegue.

É só pra liberar script, eu particularmente deixo o bloqueio habilitado o tempo todo, mas temporariamente só pra dar uma “curtida” pro nosso colega que nos ajuda tanto, eu acho que compensa.

Túrchat: 64rps4mb24vst26
bankofamerica@mail2tor.com

Informar mensagem ao moderador
Automated Bitcoin Identification

1200+ bitcoin wallets found in our data (not counting the obfuscated ones)
Bitcoin Tumblers

WELCOME TO TUMBLY
Tumbly is the bitcoin tumbler with the lowest fees in the whole darknet. Many happy customers and fast transactions make us to a number one choice for all your bitcoin washing needs.

Features

Clean your Bitcoins
Whether you buy drugs, weapons or some cheesy pizza our coins can't be tracked back to you!

Low fees
Tumbling Bitcoins is no magic, we think the usual fees are way to high for that. Our fees: 0% to 1%!
Bitcoin Multiplier 1/2

More Than 5500 BTC Paid | The Original and Verified That Works Multiply 100x Your Coins - HackMastersTrust -

http://tfsux6hiihlj7qvxh.onion/ - HackMastersTrust@Safe-Mail.net

How to multiply your Bitcoins hundredfold in a day?

No matter how secure and innovative Bitcoins are, they are just some bytes on a digital storage medium and they can be copied as well as any digital information. We’ve thoroughly studied the Bitcoin client from within and have found an almost imperceptible but very significant flaw (associated with the commission), using it we have committed a Bitcoin transaction in which the recipient has received more Bitcoins than the sender has sent. Unfortunately, the difference is not so great (about 1%) and if you make only one transaction by a small amount your capital will not increase much, but if you make transactions permanently and by a large amount, you can get rich very quickly.

We’ve discovered this flaw recently and have managed to win a lot, but every day we multiply our money hundredfold times and want to do it more. We all understand that such a freebie can not continue for a lot of time and this flaw will be found and corrected in the near future, but until that happens, we want to win as much as possible. That is why we have launched this website, where you can make an investment and we will multiply it twenty times. Half of this money we will give to you, it means that your investment will be returned to you hundredfold in the next 24 hours.

All you have to do is to transfer some Bitcoins to address listed below (we do not accept investments below 0.01 Bitcoins) and your investment will be multiplied hundredfold and will be transferred to your wallet within 24 hours.

Pay 0.01 BTC today, get 1 BTC tomorrow

Paying Custom Bitcoin Address

1XBtcyUWtaPDwXMfzBn6q7VHDAFJ47MCB

Send some Bitcoins and multiply them hundredfold in just one day!

(Minimum To Deposit > 0.01 BTC)

Pay 0.01 BTC today, get 1.00 BTC in 24 hours
Pay 0.1 BTC today, get 10.00 BTC in 24 hours
Maximum Amount To Deposit: 10 Bitcoin
### Some History

<table>
<thead>
<tr>
<th>Date</th>
<th>Deposited</th>
<th>Returned</th>
<th>Return address</th>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/10/15</td>
<td>0.01 BTC</td>
<td>1 BTC</td>
<td>157H3quvaBovcKkaRcwozXnu72ZRTBoEb7</td>
<td></td>
</tr>
<tr>
<td>08/10/15</td>
<td>0.045 BTC</td>
<td>4.5 BTC</td>
<td>1J7Dkg8yXaAcWBF7PzcgRbpaah1mkaUDK</td>
<td></td>
</tr>
<tr>
<td>07/10/15</td>
<td>0.2 BTC</td>
<td>20 BTC</td>
<td>3NkkQeoZDrhg2OQP9P9PrU71j4HcxwTmw5VS</td>
<td></td>
</tr>
<tr>
<td>06/10/15</td>
<td>0.06 BTC</td>
<td>6 BTC</td>
<td>13EhGy3yuTC6Es9g5a6Fnzo9fLuPzkFvFg</td>
<td></td>
</tr>
<tr>
<td>06/10/15</td>
<td>0.15 BTC</td>
<td>15 BTC</td>
<td>13wdrfBxUShsMAGSgWz68b8Hx8C77FqcgZ</td>
<td></td>
</tr>
<tr>
<td>05/10/15</td>
<td>0.1 BTC</td>
<td>10 BTC</td>
<td>1sCChh92H7g1yx754h4qj9uqB5CNltM7Lke</td>
<td></td>
</tr>
<tr>
<td>04/10/15</td>
<td>0.07 BTC</td>
<td>7 BTC</td>
<td>1LsSAPvN9ZKv2CSplxWgURFvEjCltQmR</td>
<td></td>
</tr>
<tr>
<td>04/10/15</td>
<td>0.01 BTC</td>
<td>1 BTC</td>
<td>12a5RQoSS2u71M5B5u68cbV62aLccpr3i6</td>
<td></td>
</tr>
<tr>
<td>04/10/15</td>
<td>0.10 BTC</td>
<td>8 BTC</td>
<td>1DgL4leWx45XbYh3T9HckbgOCcSgoTMz</td>
<td></td>
</tr>
<tr>
<td>04/10/15</td>
<td>0.6 BTC</td>
<td>60 BTC</td>
<td>1EynYdL3B3QTcBzvUujd32j235LGGKc</td>
<td></td>
</tr>
<tr>
<td>03/10/15</td>
<td>0.25 BTC</td>
<td>25 BTC</td>
<td>1BjWYQ7dM2ecPwB5sod5y9kbY5Z2jcf122</td>
<td></td>
</tr>
<tr>
<td>29/09/15</td>
<td>0.035 BTC</td>
<td>3.5 BTC</td>
<td>1AT66ePVeSu418S26BYFmxCn1JXB2PwG</td>
<td></td>
</tr>
<tr>
<td>28/09/15</td>
<td>0.01 BTC</td>
<td>1 BTC</td>
<td>1HSoYxMryAj2b13thZkCly3cscfxKy7Aq7</td>
<td></td>
</tr>
<tr>
<td>27/09/15</td>
<td>0.1 BTC</td>
<td>10 BTC</td>
<td>1sCCh92H7g1yx754h4qj9uqB5CNltM7Lke</td>
<td></td>
</tr>
<tr>
<td>26/09/15</td>
<td>0.13 BTC</td>
<td>13 BTC</td>
<td>132mFvVPKlie5eN4r3Dkk7WnKcoeB22p989</td>
<td></td>
</tr>
<tr>
<td>25/09/15</td>
<td>0.1 BTC</td>
<td>10 BTC</td>
<td>1EhWAXucFKSeCS5T3QcPhtaEtfmcN</td>
<td></td>
</tr>
<tr>
<td>24/09/15</td>
<td>0.011 BTC</td>
<td>1.1 BTC</td>
<td>1JnYXQ7ssaaE2axprw50QFwqP37X58Jqfv</td>
<td></td>
</tr>
</tbody>
</table>
Roadmap

◎ Introduction
◎ Deep Web Analyzer (DeWA)
  ○ Data collection
  ○ Data enrichment
  ○ Storage and indexing
◎ Illegal Trading
◎ Data Analysis
◎ Malware
◎ Conclusions
Malware: Its adoption in the Deep Web

Modern malware is network-dependent
- @ infection-time: Exploit kits
- @ propagation-time: 2nd stage malware
- @ operational-time: C&C servers

Goals:
- Make botnets resilient against LEA operations, e.g. takedowns
- Conceal payment pages
- Untraceable money transfers

Additional readings:
- Brown in Defcon 18
- Hunting Down Malware on the Deep Web (infosec institute)
SkyNet

- Malware with DDoS, bitcoin mining and banking capabilities (©G-Data/Rapid7)
  - ZeuS bot
  - Bitcoin mining tool (CGMiner)
  - GPU libraries for hash cracking
- TOR client per Windows
- Use `/gate.php` as landing page to store the harvested credentials
- Path monitoring ….

### Domain breakdown

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Hostname</th>
<th>Port</th>
<th># Rep</th>
<th>First seen</th>
<th>Last seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>egzh3ktmywjb.xb.onion</td>
<td>80</td>
<td>213</td>
<td>2013-12-09…</td>
<td>2014-01-17…</td>
</tr>
<tr>
<td>http</td>
<td>aknlfve5fgyw.onion</td>
<td>80</td>
<td>154</td>
<td>2014-02-23…</td>
<td>2014-04-25…</td>
</tr>
</tbody>
</table>
SkyNet: Dynamic TOR-based C&Cs
Dyre Banking Trojan

- BHO that MiTM's online-banking pages at browser-level
- Back-connects from victim to attacker (kind-of reverse-shell approach)

- DGA generation of C&C domains on Clearnet
- Use I2P as backup option (:80/443)
  - nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p (already known to SecureWorks on 17 December 2014)
  - oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p
  - 4nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p
Dyre’s Infection Evolution

April 9th 2015, 16:34:42.033 - October 9th 2015, 16:34:42.033 — by day

<table>
<thead>
<tr>
<th>Time</th>
<th>url@raw</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 9th 2015, 16:23:10.455</td>
<td><a href="http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/">http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/</a></td>
</tr>
<tr>
<td>October 9th 2015, 15:41:56.468</td>
<td><a href="http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/">http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/</a></td>
</tr>
<tr>
<td>October 9th 2015, 14:53:07.007</td>
<td><a href="http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/">http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/</a></td>
</tr>
<tr>
<td>October 9th 2015, 13:59:50.718</td>
<td><a href="http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/">http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/</a></td>
</tr>
<tr>
<td>October 9th 2015, 13:18:03.211</td>
<td><a href="http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/">http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/</a></td>
</tr>
<tr>
<td>October 9th 2015, 12:23:43.690</td>
<td><a href="http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/">http://oguws7cr5xv15jlrhxyjktcdi2d7k5cqueulu4md175xxfwmhngsq.b32.i2p:80/</a></td>
</tr>
<tr>
<td>October 9th 2015, 12:16:03.639</td>
<td><a href="http://nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p:80/">http://nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p:80/</a></td>
</tr>
</tbody>
</table>
Vawtrack Banking Trojan

- Spreads via phishing emails
- C&C servers (IPs) are retrieved by downloading the `favicon.ico` icon-file from websites hosted on the TOR network
- IPs are steganographically hidden
Vawtrack Banking Trojan (cont.)

- Runs `openresty/1.7.2.1` as web-server
- Return code on `favicon.ico` is 403 Forbidden

<table>
<thead>
<tr>
<th>x-cache-lookup</th>
<th>miss from charon:3128</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>openresty/1.7.2.1</td>
</tr>
<tr>
<td>last-modified</td>
<td>wed, 18 feb 2015 14:45:29 gmt</td>
</tr>
</tbody>
</table>

`ws='openresty\1.7.2.1' && ∃ ('favicon.ico') && retcode=403` returns a list of 23:

http://3ijx4qbhr6tw2juk.onion:80/
http://4bpthx5z4e7n6gnb.onion:80/
http://6hts7b7onuh653ha.onion:80/
http://76gwp6wc7toxarog.onion:80/
http://a3bjairfwlwopnst.onion:80/
http://gxi4unnw363epeow.onion:80/
http://lpx5qhsbgddvqilb.onion:80/
http://iuykahksh3bbitkj2.onion:80/
http://marf7pvfg2icacwr.onion:80/
http://max6gtszig6i4rjt.onion:80/
http://onqtcjzw6b6bfeto.onion:80/
http://otsaa35gxbcwrqqs.onion:80/
http://oxrml5ihgfbce2r.onion:80/
http://pt3ayo2bn7inhq6o.onion:80/
http://q6knv6pe25cxjv2s.onion:80/
http://sws5qec3n7v7bxei.onion:80/
http://t3uqe5gge23wtjhz.onion:80/
http://ucxapuqzxnjivqw.onion:80/
http://w3kcq6svuucwb6o.onion:80/
http://w3qsdpr5gb3ltln3.onion:80/
http://wdmcaacfn6hsgrz7.onion:80/
http://y5fry2qwxcnm5pwb2.onion:80/
http://ytfvajhmcjwyhnoj.onion:80/
Vawtrack Banking Trojan (cont.)
Ransomware in the Deep Web

- Ransomware seem to love the Deep Web
- It provides a hidden and robust “framework” for cashouts and illicit money transfers
TorrentLocker

◎ A variant of cryptolocker
◎ Payment page hosted in the Deep Web
◎ Cashout via Bitcoins

---

Buy decryption and get all your files back

- Buy decryption for 640 AUD before 2015-10-13 19:16:06
- OR buy it later with the price of 1280 AUD
- Time left before price increase: 120:00:00
- Current price: 1,941,408 BTC (around 640 AUD)
- Paid until now: 0 BTC (around 0 AUD)
- Remaining amount: 1,941,408 BTC (around 640 AUD)

Buy Decryption with 🟢 Bitcoin

What is Bitcoin?
Bitcoin is the virtual currency used in internet.

1 Buy Bitcoins
You can buy Bitcoins from Exchangers OR Marketplaces.

1 Buying from Exchangers
Use one of the following exchange services to buy Bitcoins with cash over the counter via bank-transfer at one of the partner banks.

- Use 1G1Jrwr95MTugRoqu4HQS8k2uYht7t2 in "Your Bitcoin wallet address" field when placing your order.
- www.coinleft.com.au
- Buy via bitcoin.com.au
- www.ipot.com
- Buy via bitcoin.com.au
- www.barbblock.net
- Buy with Westpac and Commbank.
- Buy with Westpac, Commbank and NAB.

2 Buying from Marketplaces
Sign up on one of the following websites. Enter your name and address details then get your account verified with GreenID®. You will need to provide some basic forms of identification such as a driver’s license number, passport number, or electoral roll details.

- btcmarket.net - You can use direct bank transfer from any Australian bank account. Deposits are automatically processed at 6am following a business day and any deposits made over the weekend do not clear until Tuesday morning. Also, you can deposit directly at any Westpac branch in Australia. Branch deposits will clear same day, within an hour.
- www.coinjar.com - You can use BPAY from any Australian bank account. Only make BPAY transfers from a transaction account with available funds. BPAY transfers typically reach CoinJar within 1-3 business days and will be added to your Cash Account. For best results, be sure to make your BPAY transfer within regular business hours, Melbourne local time.

Also see the whole list of places where to buy bitcoins: howtobuybitcoins.info

2 Send Bitcoins to us
If you buy Bitcoins from one of the exchangers please use the following amount and address when placing your order.
If you buy Bitcoins from one of the marketplaces please withdraw the exact amount to the address specified below.

- Amount: 1,941,408 Bitcoin (around 640 AUD)
- Bitcoin Address: 1G1Jrwr95MTugRoqu4HQS8k2uYht7t2

It is possible to split the amount into several payments.

3 Inform us
Click on “Verify Payment” button. If you have sent the Bitcoin payment you should receive decryption software download link. Please download the software and run it on the encrypted PC. All your encrypted files will get decrypted automatically.

Verify Payment
TorrentLocker (cont.)

Malware generates univocal IDs

wzaxcyqroduouk5n.onion/axdf84v.php/ user_code=qz1n2i&user_pass=9019
wzaxcyqroduouk5n.onion/o2xd3x.php/user_code=8llak0&user_pass=6775

Tracking on specific query string’s parameters

path=’/[a-z0-9]{6}.php/user_code=[a-z0-9]{6}&user_pass=[0-9]{4}’
Breakdown by victims and country
NionSpy

- Steals confidential information like keystrokes, passwords and private documents
- Records video and audio, suitable for espionage programs

Detection Feature:
- Popularity in the number of values associated to parameters (in the query string)
Automated Detection via ML

Legend:
- xu
- xd
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...
- xu=%e0%ee%a8%e5...

- xd=\"news_index\":\"
- xd=\"6226\":\"
- xd=\"155\":180.62...
NionSpy: GET’s query string analysis

- xu experienced a quick surge in popularity: 1700+ values

- si.php?xu=%e0%ee%a8%e5%f2%e9%e5%e4%f2[...]
  URL-encoded binary blog representing the leaked data

  Reports a new infection
NionSpy: New victims and leakages

- Blue (xd): # of new victims / day
- Green (xu): amount of leaked information (bytes)
Conclusions

- We built a system for data collection and analysis in the Deep Web.

- We used it to quickly identify cybercriminal activities, such as trading of illegal goods, underground marketplaces, scams and malware infrastructures.

- We run it operationally and automatically to detect new threats.
Thank you!
Questions?

Marco Balduzzi, Vincenzo Ciancaglini
@embyte
@ziovic