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

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
- Development of novel proof of concepts and complex systems
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
TOR

- First alpha in 2002
- Initially used to browse anonymously the Surface Web
- Hidden services -> effective Dark Web
- Onion routing: multihop routing with host key encryption.
I2P

- 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)
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)
Namecoins, Emercoins

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

- Distributed
- Decentralised
- No regulating institution
RogueTLDs & PrivateDNSes

Plain old DNS, but with custom servers

Custom registrars

Custom domains

Cesidian Root
Cyberterra Mean Time
Saturday 22 Kurosawa 2015 @ 535
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/2P 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

Charon
- 64 TOR Instances
- 12P Gateway
- Freenet Instance
- RogueTLD DNS Resolver
- Transparent Proxy

Qualitative Analytics (Deep 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
  - ...

16
Page Scouting

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

- Scrapinghub'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

1. **Page text**: Scrap text from HTML, clean up, strip spaces…
2. **Tokenization**: Create list of (word, frequency) pairs
3. **Filtering**: Keep only substantives
4. **Semantic distance matrix**: How “far” are words from one another?
5. **Hierarchical clustering**: Group similar words
6. **Cluster label and popularity**: Label clusters, sum frequencies
7. **Word cloud**: Draw using summed frequencies
Правила — Регистрация — Russian Silkroad

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 - Шишки Royal Canadian Haze - один из любимых сортов Snoop Dogg и Dr. Dre. Готовые клады в центре Москвы.
Night City Lights - Москва - Амфетамин. 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.

Регистрация на Russian Silkroad

Для регистрации необходимо согласиться с правилами форума ниже.

Правила ресурса

Форум и его сервисы полноценно работают без использования JavaScript.

Продажи производятся через систему автогаранта, требуйте от продавцов её использование. Для покупателей услуга бесплатна.

Данный ресурс предназначен для покупки/продажи 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 привлечённых рефералом.

Запрещено

1. Разжигание межнациональной вражды.
2. Вынос информации из закрытых разделов форума.
3. Политика в любом ее проявлении.
4. Попытки продажи 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 ругань (троллоло в любых вариантах).
8. Обсуждение действий администрации ресурса и его правил.

Торговля разрешена всем, кроме:
Collected Data

Running since 11/2013 (2 years)

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

<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>38,578,152</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
Drugs! Drugs! Drugs!
## Passports and Fake IDs

### Pricing

<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>Malaysia</td>
<td>450 Euro</td>
<td>550 Euro</td>
<td>550 Euro</td>
<td>650 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

### Additional services

- Documents duplicating: extra 100 Euro
- Visa/stamps affixon: extra 25-110 Euro

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

HQER - High Quality Euro Replicas / Counterfeits

Counterfeit 50 Euro Bills

Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessary security features to be spent at most retailers.

FREE EXPRESS SHIPPING! We are shipping from France!

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 x 50 Euro Bills</td>
<td>1.128</td>
<td>1</td>
</tr>
<tr>
<td>60 x 50 Euro Bills</td>
<td>2.256</td>
<td>1</td>
</tr>
<tr>
<td>120 x 50 Euro Bills</td>
<td>4.286</td>
<td>1</td>
</tr>
</tbody>
</table>
Credit Cards

Higher balance = higher price

USA VISA CREDIT CARD BALANCE $2,000
Accepted at ATM worldwide
$500 daily withdraw limit

USA VISA CREDIT CARD BALANCE $5,000
Accepted at ATM worldwide
$1,000 daily withdraw limit

EU VISA CREDIT CARD BALANCE €5,000
Accepted at ATM worldwide
€1,000 daily withdraw limit

Please enter the amount you wish to purchase below and fill in the form.
(BTC value updates periodically via BTPAY)
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>Buy now</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 PayPal accounts</td>
<td>100 USD = 0.434 $</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>100 Ebay accounts</td>
<td>100 USD = 0.434 $</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>100 CCs with CVV2</td>
<td>150 USD = 0.652 $</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
## Doxing

<table>
<thead>
<tr>
<th>Bill and Hillary Clinton</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOB:</strong> 02/11/1964</td>
</tr>
<tr>
<td><strong>Phone Number:</strong></td>
</tr>
<tr>
<td><strong>Address:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>William J. Clinton</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOB:</strong> 10/26/1947</td>
</tr>
<tr>
<td><strong>Address:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sarah Palin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOB:</strong> 02/01/1964</td>
</tr>
<tr>
<td><strong>Phone Number:</strong></td>
</tr>
<tr>
<td><strong>Address:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hillary Clinton</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOB:</strong> 10/26/1947</td>
</tr>
<tr>
<td><strong>Address:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Joseph R Biden Jr</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOB:</strong> 11/20/1942</td>
</tr>
<tr>
<td><strong>Phone Number:</strong></td>
</tr>
<tr>
<td><strong>Address:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Previous Addresses:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1600 Pennsylvania Ave Washington, DC 20599</td>
</tr>
<tr>
<td>PO Box 2741 Little Rock, AR 72203</td>
</tr>
<tr>
<td>1600 Pennsylvania Ave NW # 214 Washington, DC 20006</td>
</tr>
<tr>
<td>1600 Pennsylvania Ave NW Washington, DC 20500</td>
</tr>
</tbody>
</table>
Assassins

ASSASSIN’s COMMUNITY

SELECT VICTIM’s LOCATION:

Europe • North America • Asia • South America • Australia • Africa

EUROPE

5000 € / person  HIRE

Blacklord
Confirmed Victims: (100+)

Age: 16+
Gender: ANY
Extended Suffering: +
Photo/Video: +
CONTINENT: EUROPE, ASIA, AFRICA

7500 € / person  HIRE

K2
Confirmed Victims: (70+)

Age: 20+
Gender: ANY
Extended Suffering: +
Photo/Video: +
CONTINENT: EUROPE, ASIA, AFRICA

3000 € / person  HIRE

HITMAN
Confirmed Victims: (70+)

Age: ANY
Gender: ANY
Extended Suffering: +
Photo/Video: +
CONTINENT: EUROPE, ASIA

10000 € / person  HIRE

Rodger D.
Confirmed Victims: (20+)

Age: 16+
Gender: ANY
Extended Suffering: +
Photo/Video: +
CONTINENT: EUROPE, ASIA
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
**Active Portscan**

<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>

* - We are based on anarchistic control so nobody haz power certainly not power over the servers or domains who ever says that this or that person haz power here, are trolls and mostly agents of factions
* - that haz butthurt about the concept or praxis where the CyberGuerrilla Anonymous Nexus stands for.

#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](http://www.ladepeche.fr/article/2015/10/10/2194982-enquete-de-la-dgsi-sur-du-piratage-informatique.html)
Languages per domain
Languages per domain (2)
**French forum: Weapon sale**

---

<table>
<thead>
<tr>
<th>Le Trollodôme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vous n’êtes pas identifié(e).</td>
</tr>
</tbody>
</table>

**Annonce**

Le trollodôme est un espace de discussion libre, sans modération ni censure et entièrement anonyme.

L’inscription n’est pas nécessaire.

Merci de poster dans la bonne section, votre message pourrait être supprimé sans préavis.

Vous seule faites évoluer le trollodôme

---

**Accueil > SHOP > Vente arme + billet de banque**

**Pages : 1**

**2015-04-28 22:23:18** #1

**Lord of war**

**Invité**

**Reputation: 12**

Bonsoir à tous, compagnons du trollodrome.

Je me permet de reboîter sur une réponse donnée sur un fil pour faire une promotion.

**Niveau arme**

Je met en vente un Colt .45 1911.

Fonctionnel mais rouillé et chien cassé (pièce que je peux réparer).

Niveau rouillé je peux tremper les pièces dans un bain de vinaigre puis le polir (ponceuse entourée de vieux vêtements + blanc d’espagnole)

200 munitions

**Billets**

- 20 euros (pas trop mauvaise facture)
- 50 euros (pour les plus tatillons, ils font foirés !)

Je connais mal le deep, mais je propose de passer par un escrow d’un site reconnu ici (de votre choix).

Annonce sérieuse, et *mini prix*

**contact:** h12q3af1q2ks2dc@torbox3uot6wchz.onion

tchao

---

L’administrateur du forum a désactivé l'usage du système de réputation pour le membre de ce groupe.
<table>
<thead>
<tr>
<th>Name (Thread Design)</th>
<th>Download Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predator Pain v1.4</td>
<td><a href="http://www.predatorpain.com/bronxfiles/ll9bX2b.png">Link</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://mega.co.nz/%21yQADFjzC!cf_NyRyGY_jg%5DBf0XZi27o_AM9K5IMNSF6Tak85feE">https://mega.co.nz/%21yQADFjzC!cf_NyRyGY_jg]Bf0XZi27o_AM9K5IMNSF6Tak85feE</a></td>
</tr>
<tr>
<td>Autologger 2.0</td>
<td><a href="http://i1.minus.com/ibfxq2rWiKVyi.png">http://i1.minus.com/ibfxq2rWiKVyi.png</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://adfoc.us/22069339665199">http://adfoc.us/22069339665199</a></td>
</tr>
<tr>
<td>Hades Logger</td>
<td><a href="https://i.imgur.com/ice0pyQ.png">https://i.imgur.com/ice0pyQ.png</a></td>
</tr>
<tr>
<td>Galaxy Logger &amp; Stealer</td>
<td><a href="https://i.imgur.com/9DQRD0j.png">https://i.imgur.com/9DQRD0j.png</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://mega.co.nz/%212zoQDha!GP8hd4dmL0Rt8z7RNaltHR3Gt9r4fkK8o2mZuQ4CE">https://mega.co.nz/%212zoQDha!GP8hd4dmL0Rt8z7RNaltHR3Gt9r4fkK8o2mZuQ4CE</a></td>
</tr>
<tr>
<td>Tasty Logger</td>
<td><a href="https://puu.sh/4FatG.png">https://puu.sh/4FatG.png</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://mega.co.nz/%21HRQFQTjY!GgoeZ0rnX0...rdpdoUviC8">https://mega.co.nz/%21HRQFQTjY!GgoeZ0rnX0...rdpdoUviC8</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://DeceptiveEngineering.info">http://DeceptiveEngineering.info</a></td>
</tr>
</tbody>
</table>

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.
Email Identification

Legend:
- zenow@riseup.net
- odim@safemail.com
- ***@onionmail.in
- kay.sievers@vrfy.org
- TriPh0rce@riseup.net
- pozabankowe@gmail.com
- zzz@mail.i2p
- 48596@qq.com
- Jokerv@safemail.net
- doublec@epwvnhpjl6.org
- admin@soylentnews.org
- kytv@mail.i2p
- username@i2pmail.org
- username@mail2tor.com
- username@torbox3ui.org
- username@ruggedinbox.com
- spw@wolomin.sr.gov.pl
- konrad.wojciechowski@riseup.net
- username@safemail.net
- killyourtv@i2pmail.org
- philipk1ick@riseup.net
- t0xicp0ison@yahoo.com
- mail@rospavosudie.com
- bankofamerica@mail2tor.com
- format at www.floridas...
- myjob@ruggedinbox.com
- themightybuzzard@so...

...
Eis algumas pizzas que foram APROVADAS hoje (01/03/2015)...

---

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

BANDEIRA: Mastercard
TIPO DO CARTÃO: Gold / Itau Unibanco
NullCoder, eu clico no +1 (várias vezes) mas não acontece nada. clico clico clico clico mas nada Man!! TOTAL!! Quem.

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

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 um ajuda tanto, eu acho que compensa.

Torchat: 64rpss4mb24vsfz6
bankofamerica@mail2tor.com
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 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://tfsux6hiihj7qvxh.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

Custom Bitcoin Deposit Addresses

1XBTcyUW7aPdOwXMF2Bn6q7VHDAFj47MCB

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
## Bitcoin Multiplier 2/2

<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><strong>0.01</strong> BTC</td>
<td>1 BTC</td>
<td>157H3quvaBovcKkaRcwozNnxu72ZRTBoEb7</td>
<td>a42c37ad189f07cd5405e433fb1eb6c88a4e05f8761</td>
</tr>
<tr>
<td>08/10/15</td>
<td><strong>0.045</strong> BTC</td>
<td>4.5 BTC</td>
<td>1J7Dkq8yXaAcWBF7PzczGrbpaSh1mkaUDK</td>
<td>4d0d5c800039e68034e7bde622478b5edc778bbd6c</td>
</tr>
<tr>
<td>07/10/15</td>
<td><strong>0.2</strong> BTC</td>
<td>20 BTC</td>
<td>3NKKQeZDRhg2QK99pRU71j4HcwXTmww5VS</td>
<td>7e2de327913b8b3c664afbab0d4c2ea68e7c1492718a</td>
</tr>
<tr>
<td>06/10/15</td>
<td><strong>0.06</strong> BTC</td>
<td>6 BTC</td>
<td>13EhGy3yuTC6Es9g5a6Fnzo9fLuP2kFvFg</td>
<td>6261d13329f19f0f4d1fb96a0ad3e9ef95d5b86f3899</td>
</tr>
<tr>
<td>06/10/15</td>
<td><strong>0.15</strong> BTC</td>
<td>15 BTC</td>
<td>13wdrfBxUShsMASGxGwZ68bH8Xc7XrCqzc</td>
<td>8c86c0e8107286eb1b696c5a5d198cdd10ae3cfc3436</td>
</tr>
<tr>
<td>05/10/15</td>
<td><strong>0.1</strong> BTC</td>
<td>10 BTC</td>
<td>1sCChh9zH7g1yx7S4h4q9uqzCDLNm7Lke</td>
<td>fc766fc6c180ae162a5cc845d8a4f156ffe988b667f0c</td>
</tr>
<tr>
<td>04/10/15</td>
<td><strong>0.07</strong> BTC</td>
<td>7 BTC</td>
<td>1LSAPNm9ZkPv2CSpx6wgUFRXvEjC1rQmR</td>
<td>366c0da3ad9bd2b8fda43baca2d6799252dee492b268</td>
</tr>
<tr>
<td>04/10/15</td>
<td><strong>0.01</strong> BTC</td>
<td>1 BTC</td>
<td>12a5RQOssS1u71MeS6Bu68cbV62aLcppr3l6</td>
<td>767c8c51c63b00520e930596dee0a64411c398765951</td>
</tr>
<tr>
<td>04/10/15</td>
<td><strong>0.10</strong> BTC</td>
<td>8 BTC</td>
<td>1DgDiL4weX45XbyH3rT9HckbgDCC5goTMz</td>
<td>aa23f7d56ac53b4f585670225fd70681e7de685eb1d</td>
</tr>
<tr>
<td>04/10/15</td>
<td><strong>0.6</strong> BTC</td>
<td>60 BTC</td>
<td>1EmYzDnLBQCTezbuzvUuj4d32j235LgKtC</td>
<td>db157cb915b8e01da6d8cc5ca5b5be22a796c146a35035b</td>
</tr>
<tr>
<td>03/10/15</td>
<td><strong>0.25</strong> BTC</td>
<td>25 BTC</td>
<td>1BJWYQ7dM2ecPw5eodY9ik8Y52JGf122</td>
<td>4637cfbd20d862cd5156991d327cc18ccbf4a7aded70</td>
</tr>
<tr>
<td>29/09/15</td>
<td><strong>0.035</strong> BTC</td>
<td>3.5 BTC</td>
<td>1AT66aPVe5u418S26BYXFrmXcn1XJB2PWg</td>
<td>4da13ece015a49c8765cd27c3a4009bea73df5a11e3f</td>
</tr>
<tr>
<td>28/09/15</td>
<td><strong>0.01</strong> BTC</td>
<td>1 BTC</td>
<td>1H5oYxMrMyAj2b13tuZkCLy3cscfyyKx7Aq7</td>
<td>f2af8b3bc57dae2c8c7853b5b8564c65e5fcd38e7cacf</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 etc.

<table>
<thead>
<tr>
<th>Domain breakdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td>http</td>
</tr>
</tbody>
</table>
SkyNet: Dynamic TOR-based C&Cs
Dyre Banking Trojan

- BHO that MiTM 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)
  - oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnqsq.b32.i2p
  - 4nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p
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://a3bjairfwlwopn.onion:80/
- http://gxi4unnw363epeow.onion:80/
- http://lp5qhsgddvqilb.onion:80/
- http://iuykahksh3bbtkj2.onion:80/
- http://marf7pvfg2icacwr.onion:80/
- http://max6gtszigr6i4rj.onion:80/
- http://onqtcjzw66bfeto.onion:80/
- http://otsaa35gxbcwrq.onion:80/
- http://oxrml5ihgifbce2.onion:80/
- http://pt3ayo2bn7inhq6o.onion:80/
- http://q6knv6pe25cxjv2s.onion:80/
- http://sws5qec3n7v7bx.onion:80/
- http://t3uqe5gge23wtjhem.onion:80/
- http://ucxapuqzxnajvqw.onion:80/
- http://w3kjcq6svuucwb6o.onion:80/
- http://w3qsdpr5gb3ltln3.onion:80/
- http://wdmcadcfn6hsrgz7.onion:80/
- http://y5fry2qwxcem5pwb2.onion:80/
- http://ytvajhmjwyhouj.onion:80/
Vawtrack Banking Trojan (cont.)

Vawtrack traffic

Legend
- marf7pvfg2icacwr.onion
- t3uqe5gee23wtjihq.onion
- pt3ayo2bn7inhq6o.onion
- otsaa35gxbcwrqs.oni...
- 4bpthx5z4e7n6g6b.on...
- y5fry2qwxc5m5pwb2.o...
- onqtcjzw6b6bfeto.onion
- a3bjairfwlwpnsto.onion
- iuykakhk3bbtkj2.onion
- ucxapuqzxanjivqw.onion
- ytfvajhmcjwyhnoj.onion
- 6hts7b7onuh653ha.on...
- 76gwp6wc7toxorog.o...
- wdmcadcfn6hsrc7.on...
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.
A variant of cryptolocker

Payment page hosted in the Deep Web

Cashout via Bitcoins

 TorrentLocker

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-teller at one of the partner banks.

- Use 1G1fEr95MYTugRoqu4Hq58ik2uvYf37K in "Your Bitcoin wallet address" field when placing your order.
- Visit www.hardblock.net - Buy Bitcoins with Westpac, Cmmbank 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 drivers license number, passport number, or electoral roll details.

- Visit www.coinmarkers.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.
- Visit 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: 1G1fEr95MYTugRoqu4Hq58ik2uvYf37K

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
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

Legend:
- English
- Turkish
- French
- Chinese
- Italian
- 6o4xqbd4cpmumytk.o...
- xf7kegtgykjoom.onion
- ndvgtf27xkhdezr.onion
- 3xo7axbmkttd4qlx.onion
- ergdzsjgpvsc5rvj.onion
- gumuj7unxtiai2a3.onion
- bica3zjnv6fxkqf.onion
- wzaxcyqroduouk5n.on...
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
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 blob 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)
Black Hat Sound Bytes

- 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.
Thanks! Q&A time...

Marco Balduzzi -- @embyte
Vincenzo Ciancaglini -- @ziovic