Cybercrime in the Deep Web

Dr. Marco Balduzzi

HackInBo, 14th May 2016

TREND MICRO™

HACK IN BO

Spring 2016 Edition

embyte:~$ whoami

- Underground and ‘hackish’ subculture since the early 2000s
- M.Sc. + Ph.D. in System Security

- Turned hobby into profession
- Sr. Research Scientist at *Trend Micro*
  - Bridge scientific research and industry needs

- Veteran speakers in major conferences and wide presence in review boards

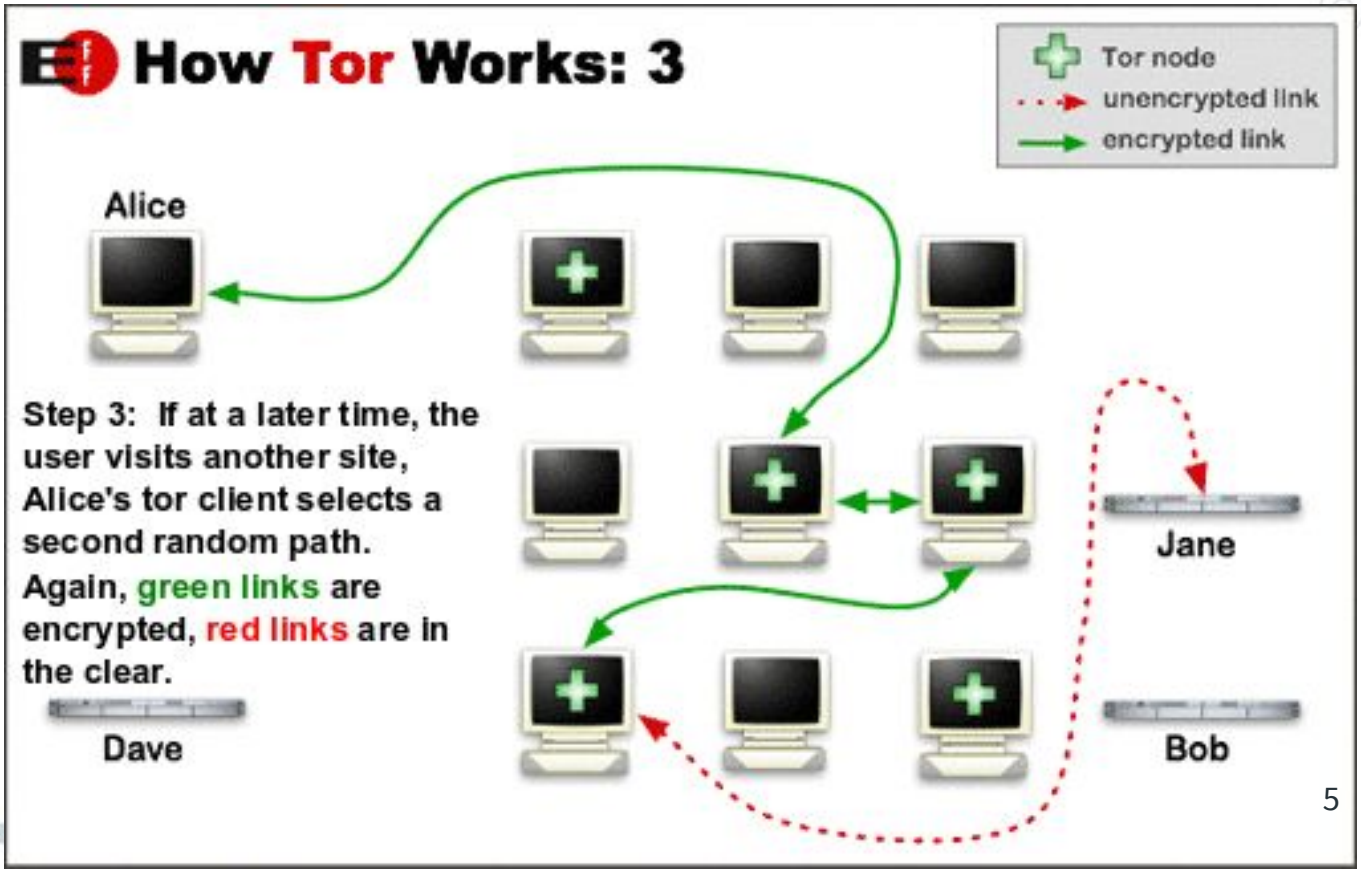
The Deep Web

Deep, dark, what?

- Deep Web: the Internet not indexed by traditional search engines (e.g., private forums)
- Dark Net: Private overlay network (e.g., TOR)
- Dark Web: WWW hosted on Dark Nets

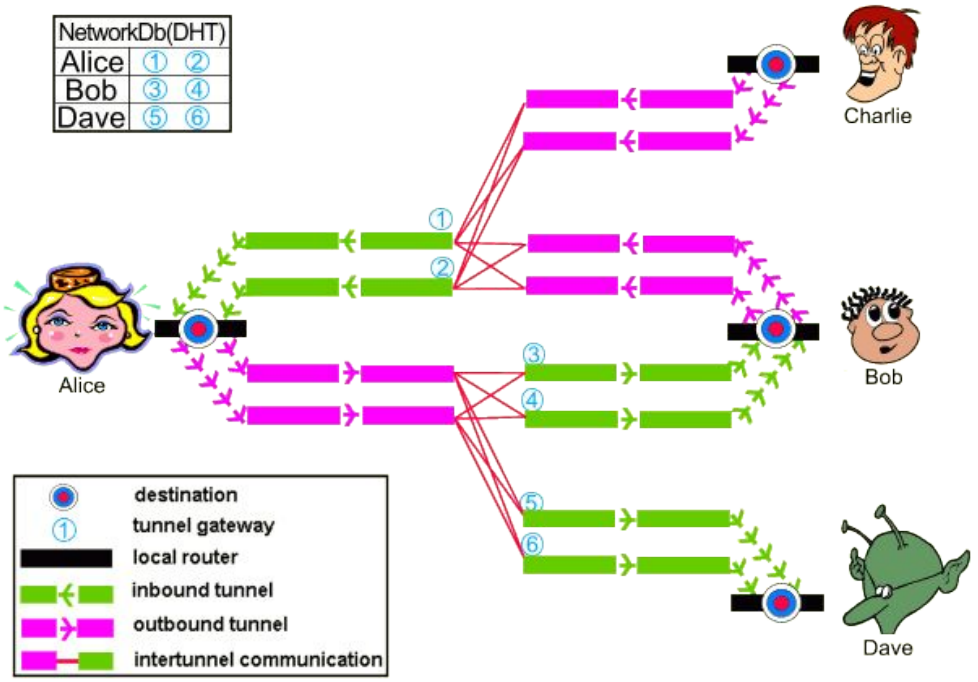
TOR

- 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.



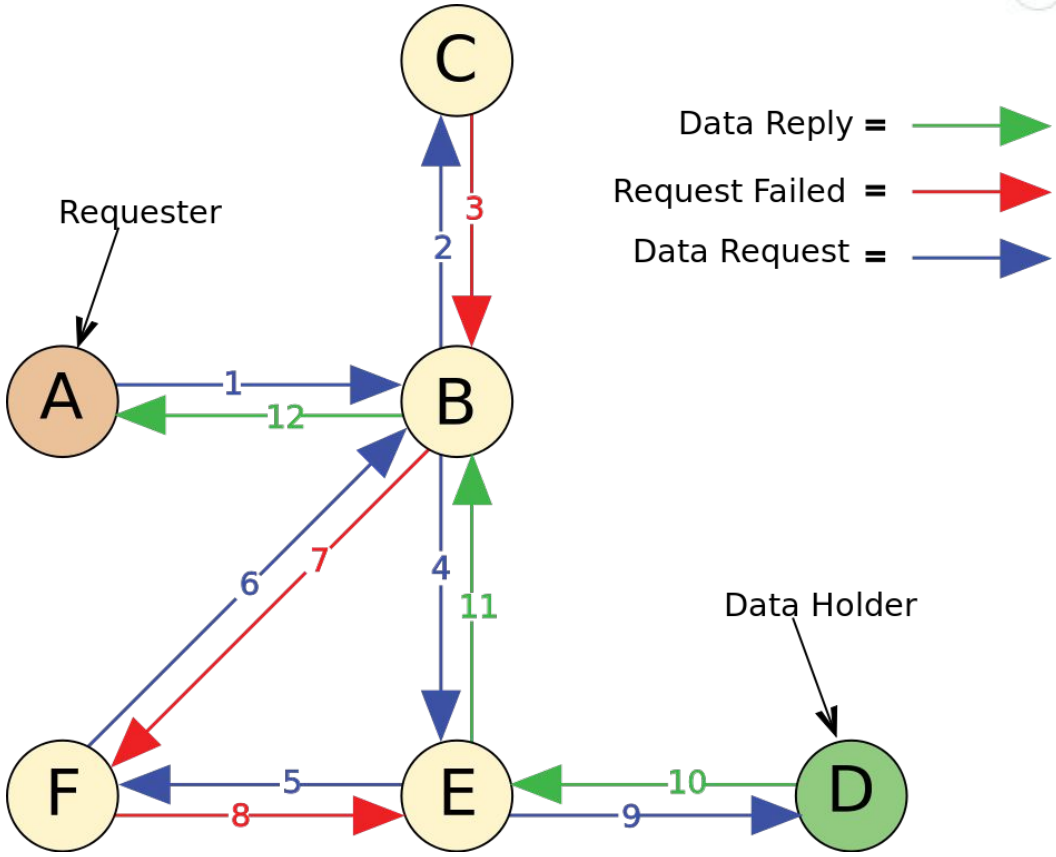
I2P

- 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)



Freenet

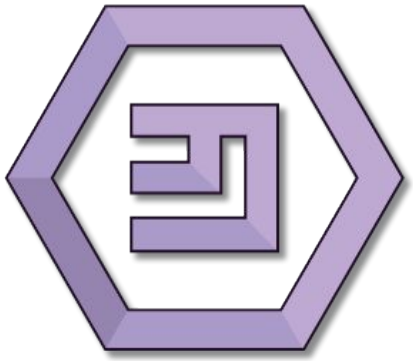
- Oldest one: summer of 1999 (father of I2P)
- Content distribution and discovery, no service hosting
- Gossip protocol to lookup a resource (i.e. web page)



Namecoins, Emercoins

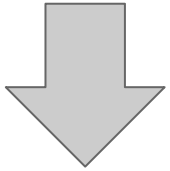
- Blockchain-based domain name server
- Think bitcoins, but instead of payment transactions, DNS registrar transaction

- Distributed
- Decentralised
- No regulating institution

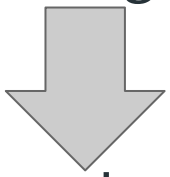


RogueTLDs & PrivateDNSes

Plain old DNS, but with custom servers



Custom registrars



Custom domains

Cesidian Root

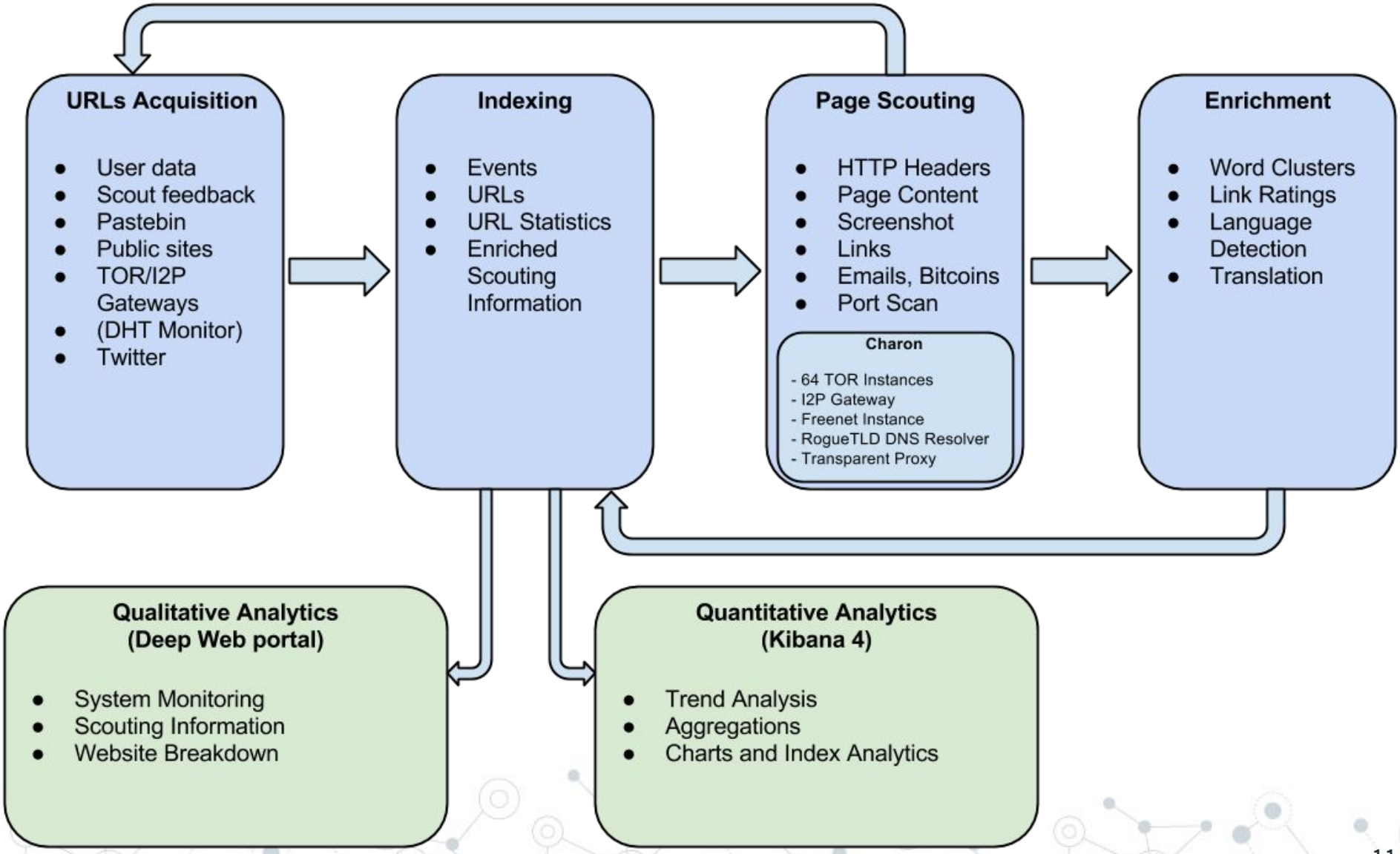
Cyberterra Mean Time
Saturnday 22 Kurosawa 2015 @ 535

nic

name.space
the "dot everything people" since 1996

DeWA (Deep Web Analyzer)

System Overview



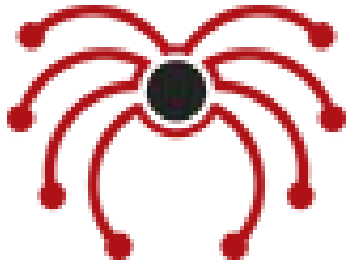
Data Sources

User transactions	Pastebin-like sites	Twitter 1% feed	Reddit
URL listing sites	TOR gateways	I2P host files	Scouting feedback

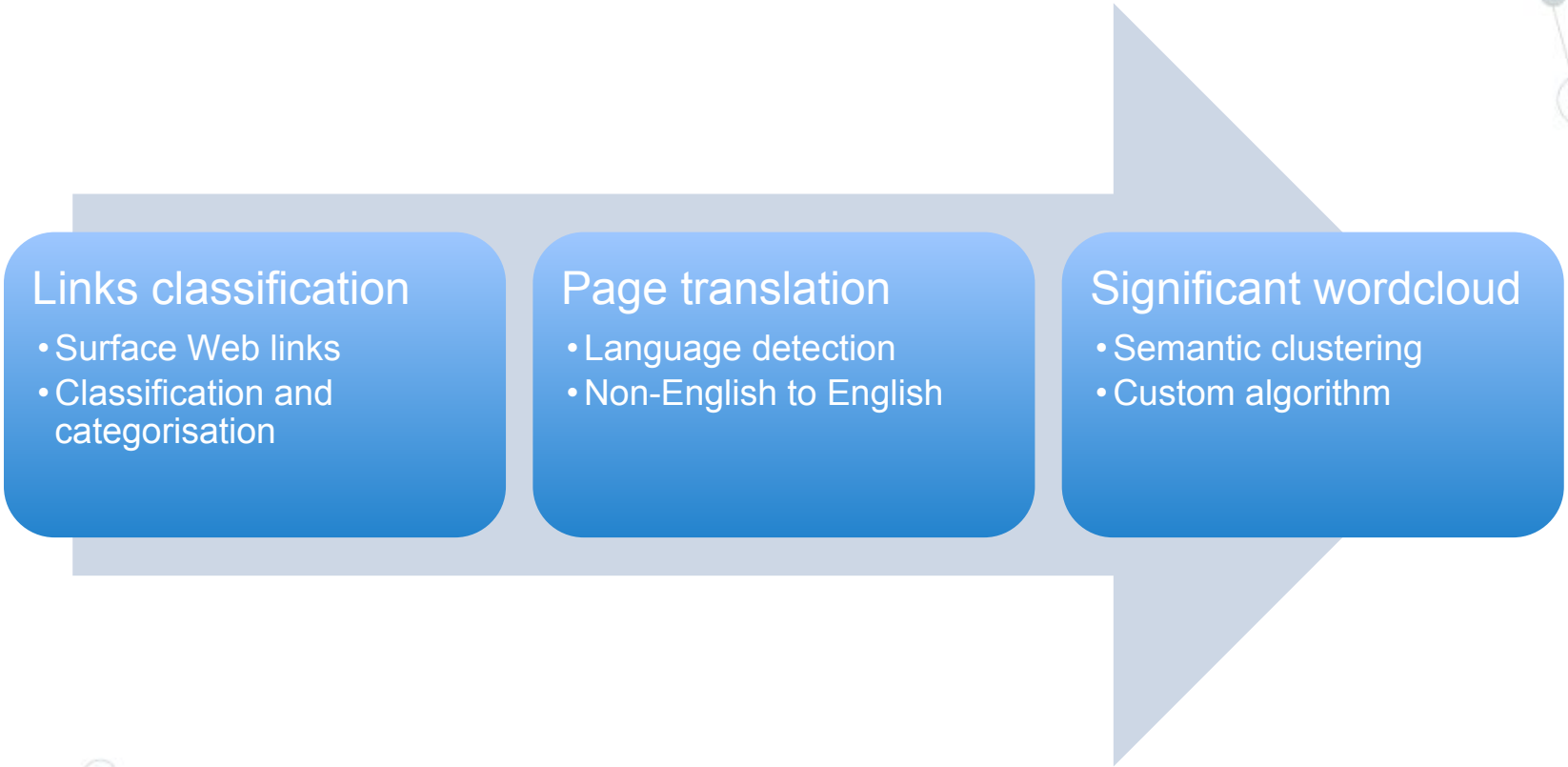
Page Scouting

Headless Browser

- Scrapinghub's Splash
  - QTWebkit browser
  - Dockerized
  - LUA scriptable
  - Full HTTP traces
- Crawler based on Python's Scrapy + multiprocess + Splash access
  - Headers rewrite
  - Shared queue support
  - Har log -> HTTP redirection chain
- Extract links, emails, bitcoin wallets



Data Enrichment

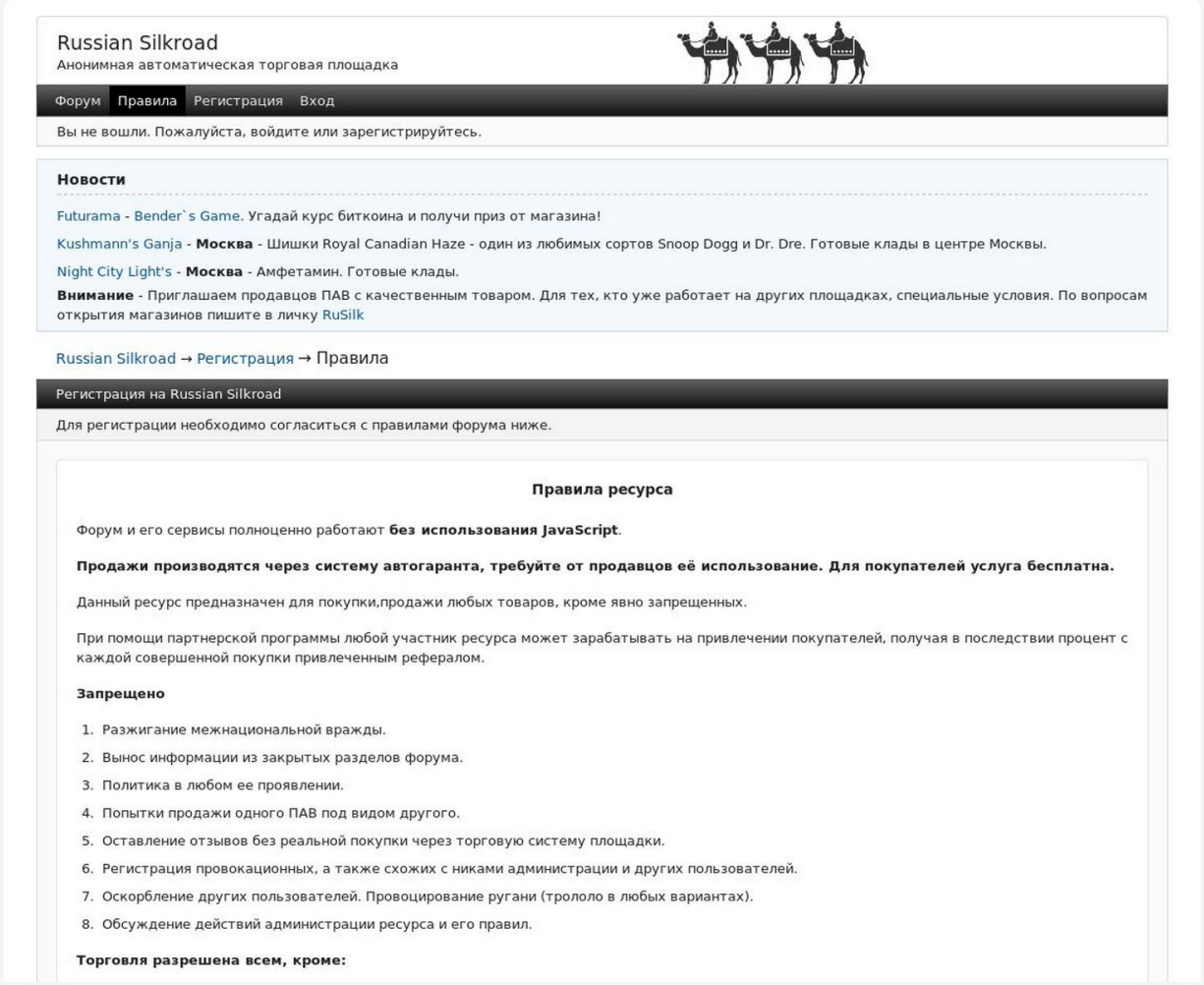


Example: Russian Forum

General information

Title	Правила — Регистрация — Russian Silkroad
Page MD5	3707c80ccd99134678d6ad611bdee86f
Page size	6911

Wordcloud (Top 20 words)



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!

Kushmann's Ganja - **Москва** - Шишки Royal Canadian Haze - один из любимых сортов Snoop Dogg и Dr. Dre. Готовые клады в центре Москвы.

Night City Light's - **Москва** - Амфетамин. Готовые клады.

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

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 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 привлеченным 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 ругани (трололо в любых вариантах).
8. Обсуждение действий администрации ресурса и его правил.

Торговля разрешена всем, кроме:

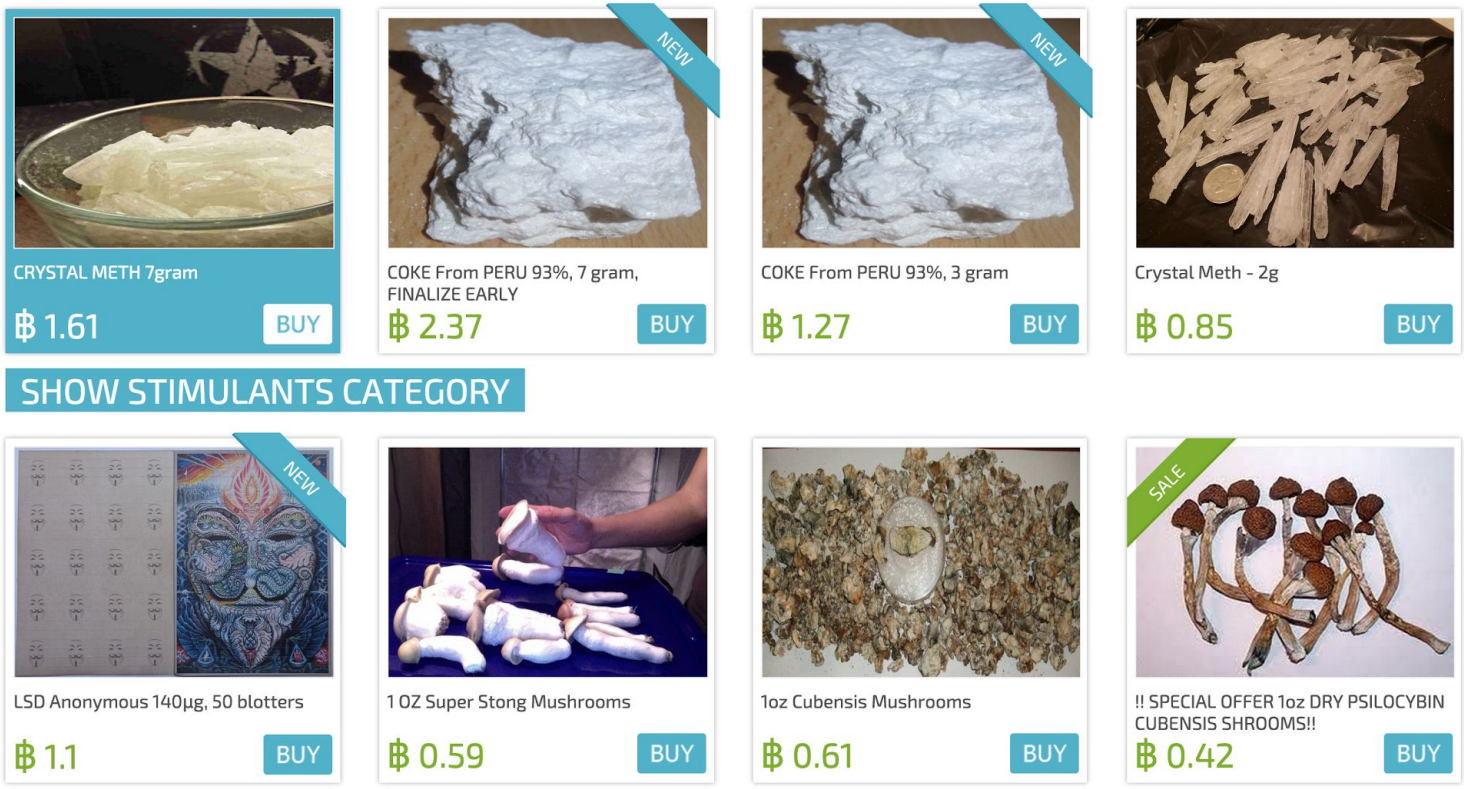
Collected Data

- Running since **Nov. 2013**
- **42.5 M** Events
- **624,000** URLs
- **35,500** domains

Source	# events/hour	# events/day	total events	first seen	last seen
Scouter	2	16	38,683,447	2014-06-06, 16:09	2016-02-11, 02:30
TOR Gateways	2,560	2,560	1,565,905	2015-05-08, 13:00	2016-03-05, 18:05
I2P Registries	6,500	6,500	883,325	2015-05-08, 15:58	2016-03-05, 18:28
SPN data	60	429	352,569	2013-11-12, 18:29	2015-11-03, 09:56
Reddit	55	2,805	17,728	2015-05-07, 20:03	2015-10-12, 14:14
Pastebin	1	27	16,685	2013-11-19, 15:32	2015-05-11, 07:48
manual	12,685	12,685	12,685	2016-02-09, 17:05	2016-02-09, 17:19
Twitter	1	7	443	2015-05-08, 20:00	2016-04-01, 21:09

Illegal Trading

Drugs! Drugs! Drugs!



Guns

UK Guns and Ammo Store

Products | Info | Login | Registration

Guns

Product	Price	Quantity
Glock 19 - 9mm - new and unused	1.418 ฿	1 X Buy now
Walther P99 - 9mm - new and unused	1.843 ฿	1 X Buy now

Ammo

Product	Price	Quantity
100 x 9mm Bullets for Glock 19	0.142 ฿	1 X Buy now
100 x 9mm Bullets for Walther P99	0.142 ฿	1 X Buy now

Passports and Fake IDs

FakeID®

Main | News | Services | Samples | faq | Order | Contacts

Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

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	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	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.

Passports:

Counterfeit Money

HQER - High Quality Euro Replicas / Counterfeits

Products | Info | Login | Register

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 necessery security features to be spent at most retailers.
FREE EXPRESS SHIPPING! We are shipping from france!

Product	Price	Quantity
25 x 50 Euro Bills	1.128 ฿	1 X Buy now
60 x 50 Euro Bills	2.256 ฿	1 X Buy now
120 x 50 Euro Bills	4.286 ฿	1 X Buy now

HQER

Credit Cards

- Higher balance = higher price

Please enter the amount you wish to purchase below and fill in the form.
(BTC value updates periodically via BTPAY)

USA VISA CREDIT CARD BALANCE $2,000

Accepted at ATM worldwide
$500 daily withdraw limit

$90 (0.4001 BTC)

amount 0

USA VISA CREDIT CARD BALANCE $5,000

Accepted at ATM worldwide
$1,000 daily withdraw limit

$170 (0.7557 BTC)

amount 0

EU VISA CREDIT CARD BALANCE €5,000

Accepted at ATM worldwide
€1,000 daily withdraw limit

$210 (0.9335 BTC)

amount 0

Paypal & Ebay Stolen Accounts

We get new lists every day!
80%+ working guarantee, we will replace if more than 20% dont work!

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.434 ฿	1 X Buy now
100 Ebay accounts	100 USD = 0.434 ฿	1 X Buy now
100 CCs with CVV2	150 USD = 0.652 ฿	1 X Buy now

Doxing

Post Entry | Old Archive Fail |

Bill and Hillary Clinton
[redacted]

William J. Clinton
[redacted]

Sarah Palin
DOB: 02/11/1964
Phone Number's: [redacted]
Address: [redacted]

Previous Addresses:
[redacted]

Hillary Clinton
DOB: 10/26/1947
Address: [redacted]

Previous Addresses:
1600 Pennsylvania Ave Washington, DC 20599
PO Box 2741 Little Rock, AR 72203
[redacted]
1600 Pennsylvania Ave NW # 214 Washington, DC 20006
1600 Pennsylvania Ave NW Washington, DC 20500

Joseph R Biden Jr
DOB: 11/20/1942
Phone Number: [redacted]
Address: [redacted]

Previous Addresses:
1. [redacted]
2. [redacted]

Assassins

ASSASSIN's COMMUNITY

KILLERS LIST ABOUT INFO CONTACT Logout

SELECT VICTIM's LOCATION:

Europe · North America · Asia · South America · Australia · Africa

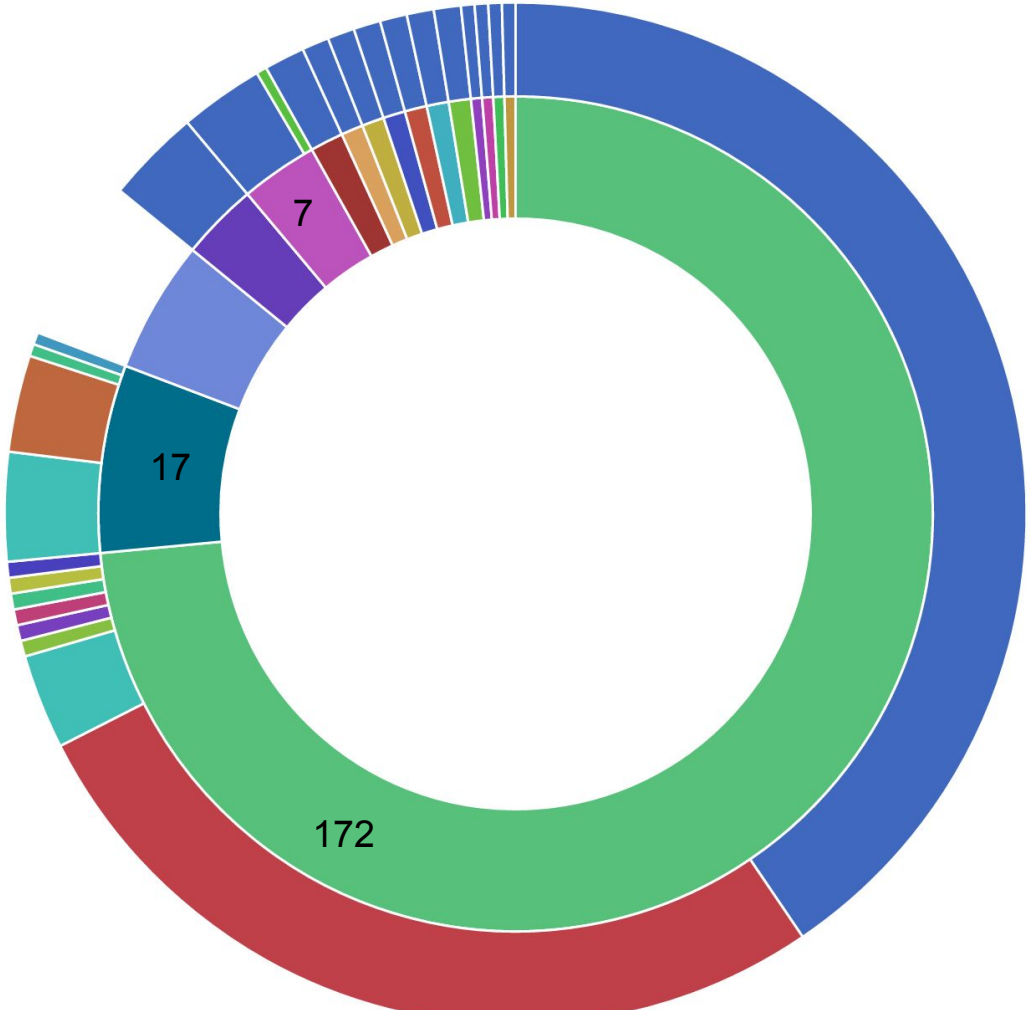
EUROPE

5000 € / person HIRE	7500 € / person HIRE	3000 € / person HIRE	10000 € / person HIRE
	K2		
Blacklord	K2	HITMAN	Rodger D.
Confirmed Victims: (100+)	K2@mail2tor.com Confirmed Victims: (70+)	Confirmed Victims: (70+)	Confirmed Victims: (20+)
Age: 16+	Age: 20+	Age: ANY	Age: 16+
Gender: ANY	Gender: ANY	Gender: ANY	Gender: ANY
Extended Suffering: +	Extended Suffering: +	Extended Suffering: +	Extended Suffering: +
Photo/Video: +	Photo/Video: +	Photo/Video: +	Photo/Video: +
CONTINENT: EUROPE, ASIA, AFRICA	CONTINENT: EUROPE, ASIA, AFRICA	CONTINENT: EUROPE, ASIA	CONTINENT: EUROPE, ASIA
POLITICIANS	POLITICIANS	POLITICIANS	POLITICIANS
(TOP-10) -	(TOP-10) -	(TOP-10) -	(TOP-10) -
(TOP-100) -	(TOP-100) -	(TOP-100) -	(TOP-100) -

Data Analysis

Protocols (HTTP/S+)

- By publicly sourced URLs



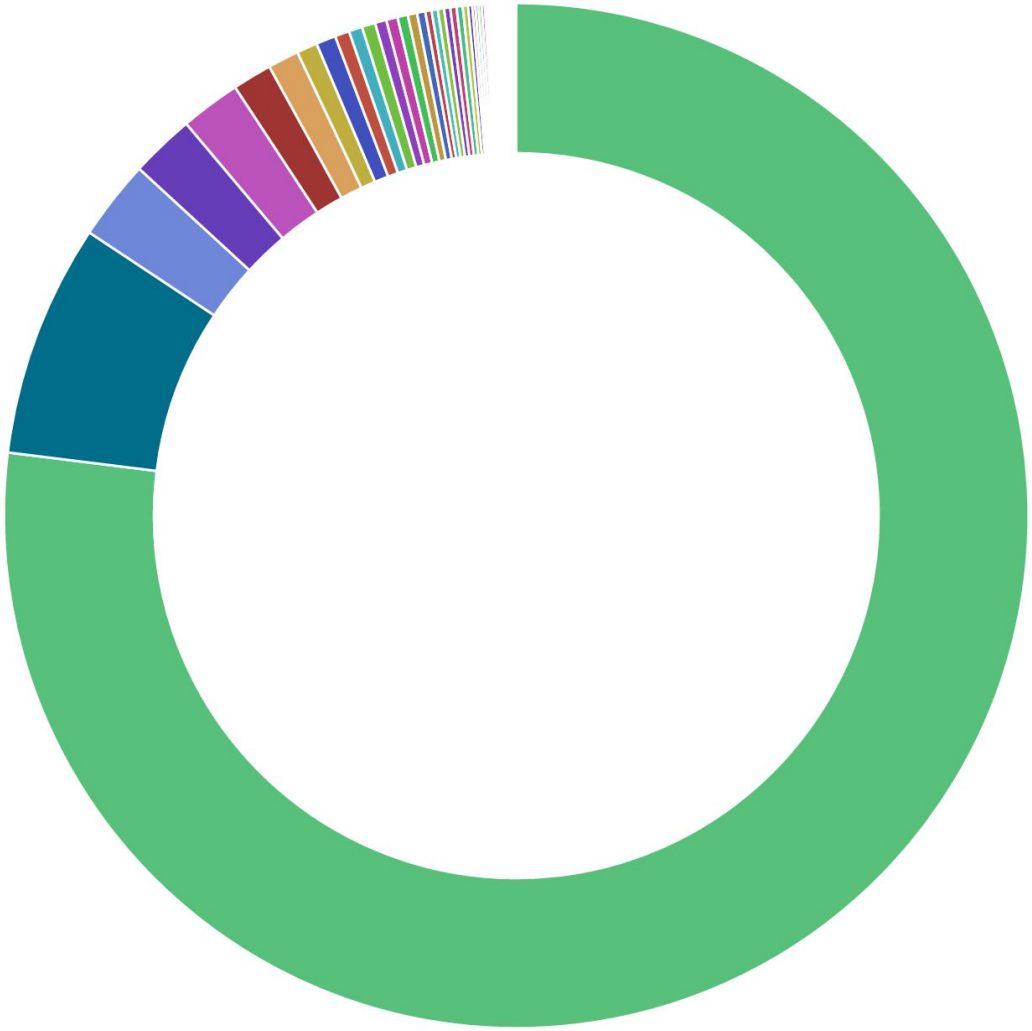
Active Portscan

IRC	IRCS	SSH
49	31	855

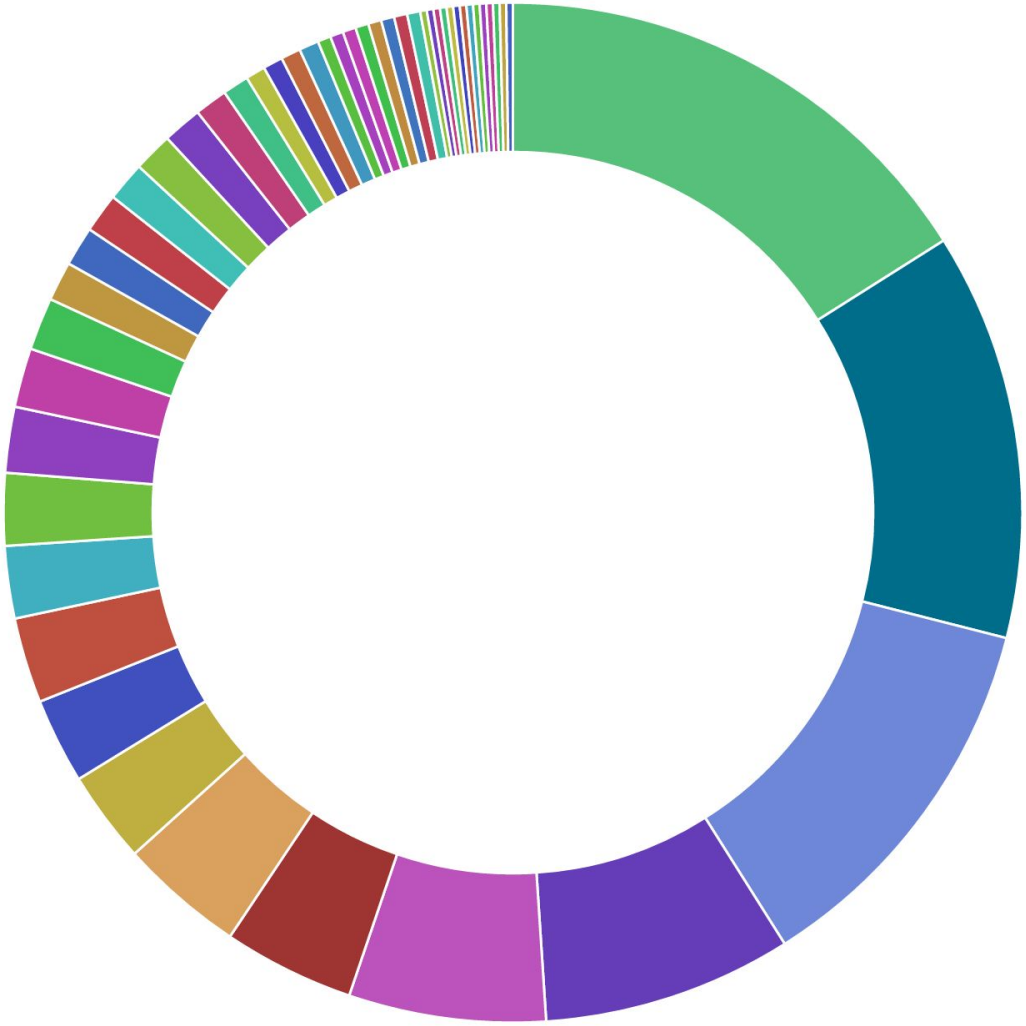
** - We are based on anarchistic control so nobody haz power certainly not power over the servers or*
** - domains who ever says that this or that person haz power here, are trolls and mostly agents of factions*
** - that haz butthurt about the concept or praxis where the CyberGuerrilla Anonymous Nexus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

Languages per domain



Languages per domain (2)



French forum: Weapon sale

Le Trollodrôme

Accueil | Liste des membres | Recherche | Inscription | Identification

Vous n'êtes pas identifié(e). Contributions : Récentes | Sans réponse

Annonce

Le trollodrôme 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 seuls faites évoluer le trollodrôme

Accueil » SHOP » Vente arme + billet de banque

Pages : 1

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

Lord of war
Invité

Réputation: 12

Bonsoir à tous, compagnons du trollôdrome.
Je me permet de rebondir sur une réponse donnée sur un fil pour faire une promotion.

Niveau arme je met en vente un colt .45 1911.
Fonctionel mais rouillé et chien cassé (piece que je peux réparer).
Niveau rouille je peux tremper les pièces dans un bain de vinaigre puis le polir (ponceuse entourée de vieux vêtement + blanc d'espgane)
200 munitions

Billets
- 20 euros (pas trop mauvaise facture)
- 50 euros (pour les plus téméraires, 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"

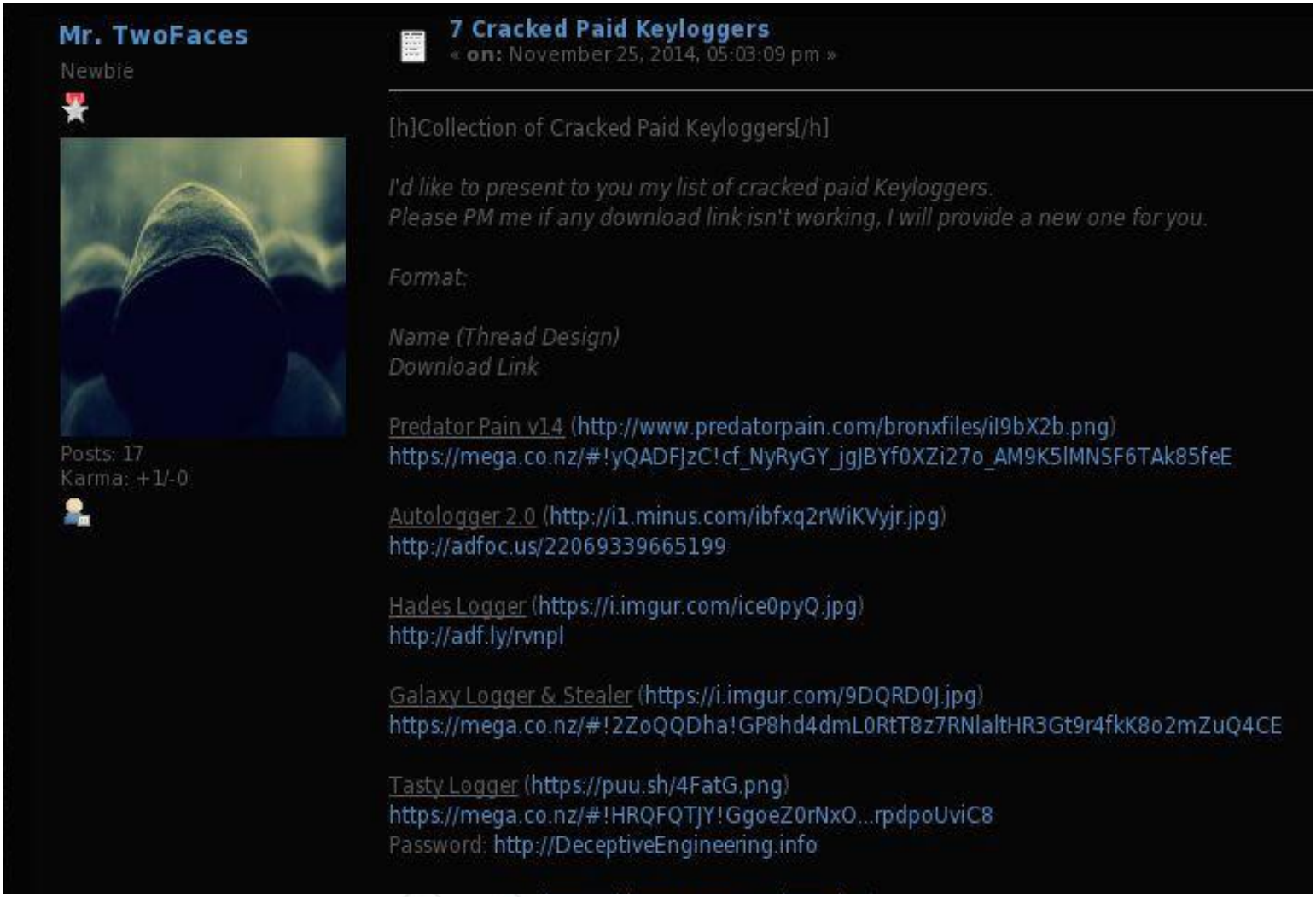
contact: h12g3af1q2ks2dc@torbox3uiot6wchz.onion

tchao

0

L'administrateur du forum a désactivé l'usage du système de réputation pour le membre de ce groupe.

Pages Embedding Suspicious Links



Mr. TwoFaces
Newbie

Posts: 17
Karma: +1/-0

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 v14 (http://www.predatorpain.com/bronxfiles/iI9bX2b.png)
https://mega.co.nz/#!yQADFJzC!cf_NyRyGY_jgJBYf0XZi27o_AM9K5lMN5F6TAk85feE

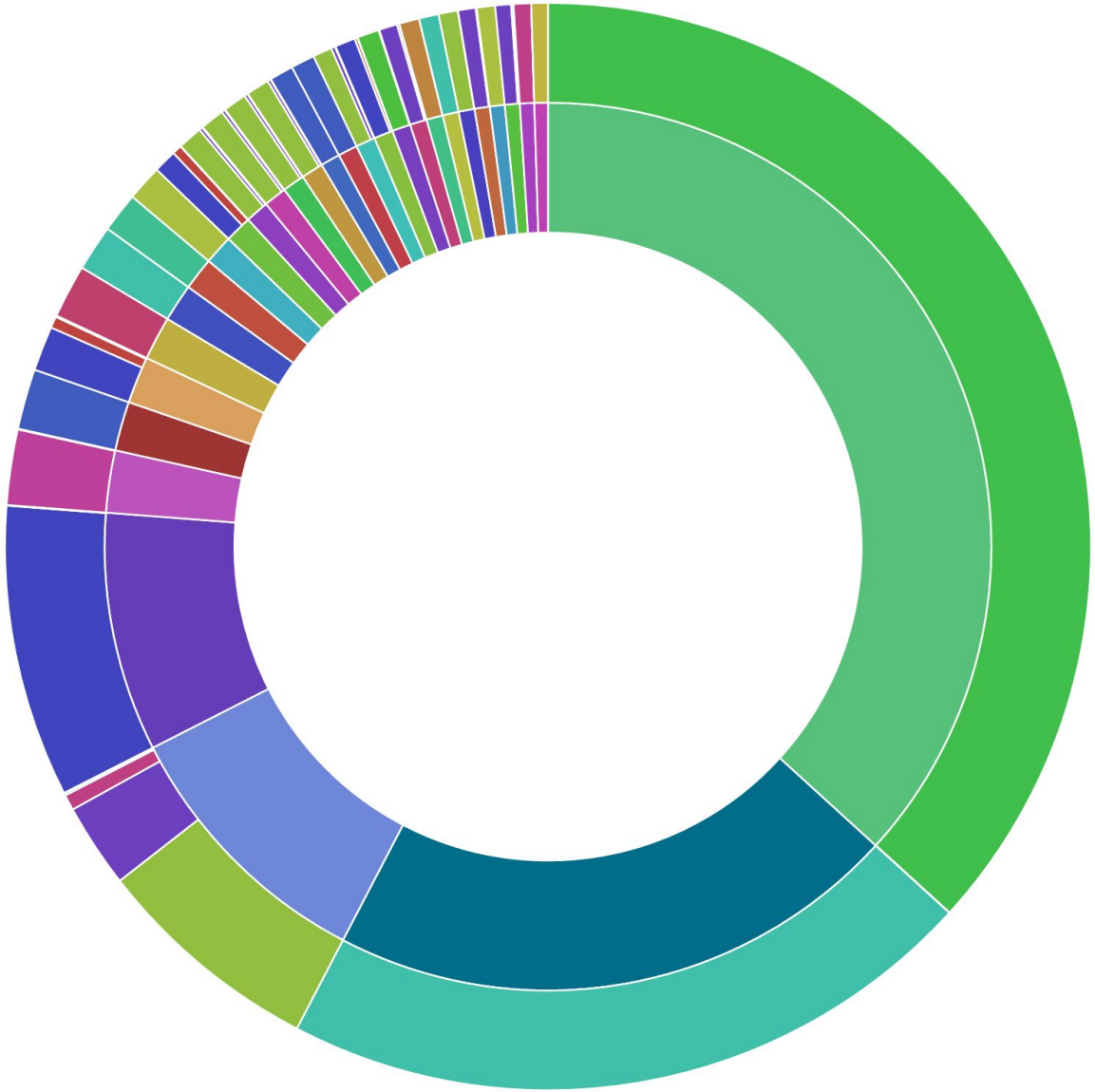
Autologger 2.0 (http://i1.minus.com/ibfxq2rWiKVyjr.jpg)
http://adfoc.us/22069339665199

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

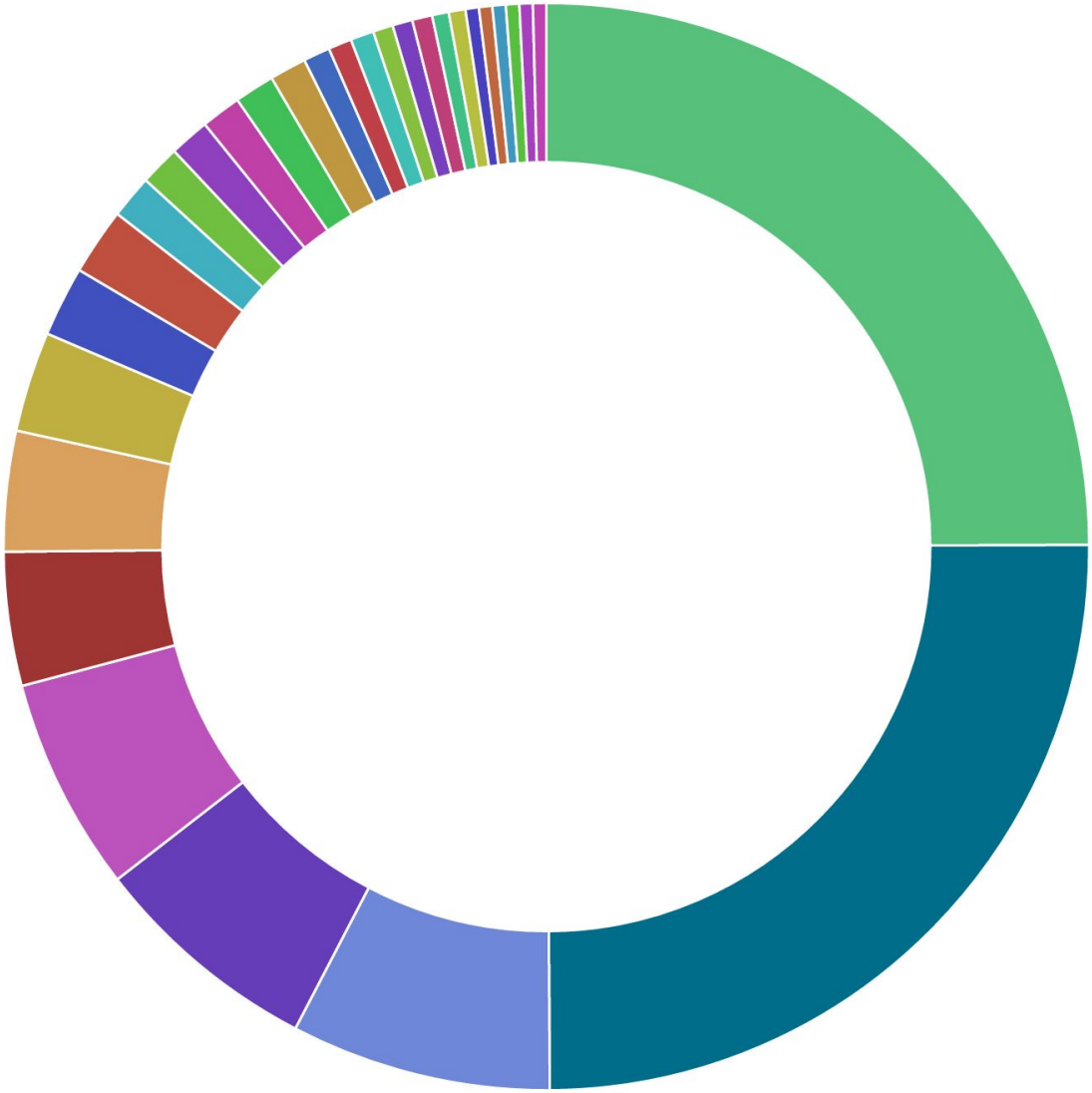
Galaxy Logger & Stealer (https://i.imgur.com/9DQRD0J.jpg)
https://mega.co.nz/#!2ZoQQDha!GP8hd4dmL0RtT8z7RNlaltHR3Gt9r4fkK8o2mZuQ4CE

Tasty Logger (https://puu.sh/4FatG.png)
https://mega.co.nz/#!HRQFQTJY!GgoeZ0rNxO...rpdpoUviC8
Password: http://DeceptiveEngineering.info

Email Identification



bankofamerica@mail2tor



Exilio forum 1/2

Pizzas gratis [NullCode - 0x00] [mensagem #4246]

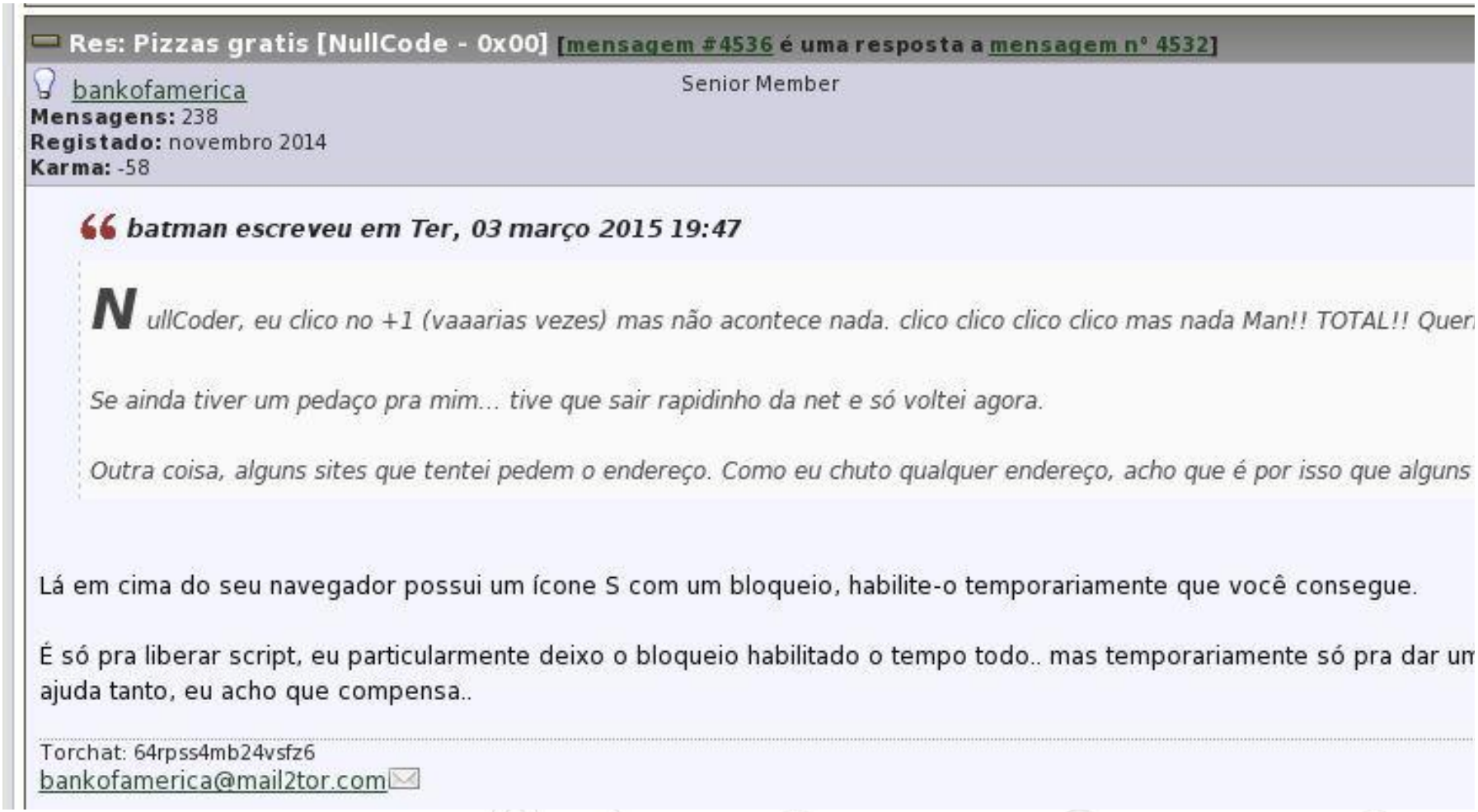
NullCode — Senior Member
Mensagens: 433
Registado: fevereiro 2015
Karma: 120

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

BANDEIRA: Mastercard
TIPO DO CARTAO: Platinum / Itau Unibanco
NUMERO DO CARTAO: 5415550187 63XXXX
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

Exilio forum 2/2



Res: Pizzas gratis [NullCode - 0x00] [mensagem #4536 é uma resposta a mensagem nº 4532]

bankofamerica — Senior Member
Mensagens: 238
Registado: novembro 2014
Karma: -58

> **batman escreveu em Ter, 03 março 2015 19:47**
>
> *NullCoder, eu clico no +1 (vaaarias vezes) mas não acontece nada. clico clico clico clico mas nada Man!! TOTAL!! Quer*
>
> *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.

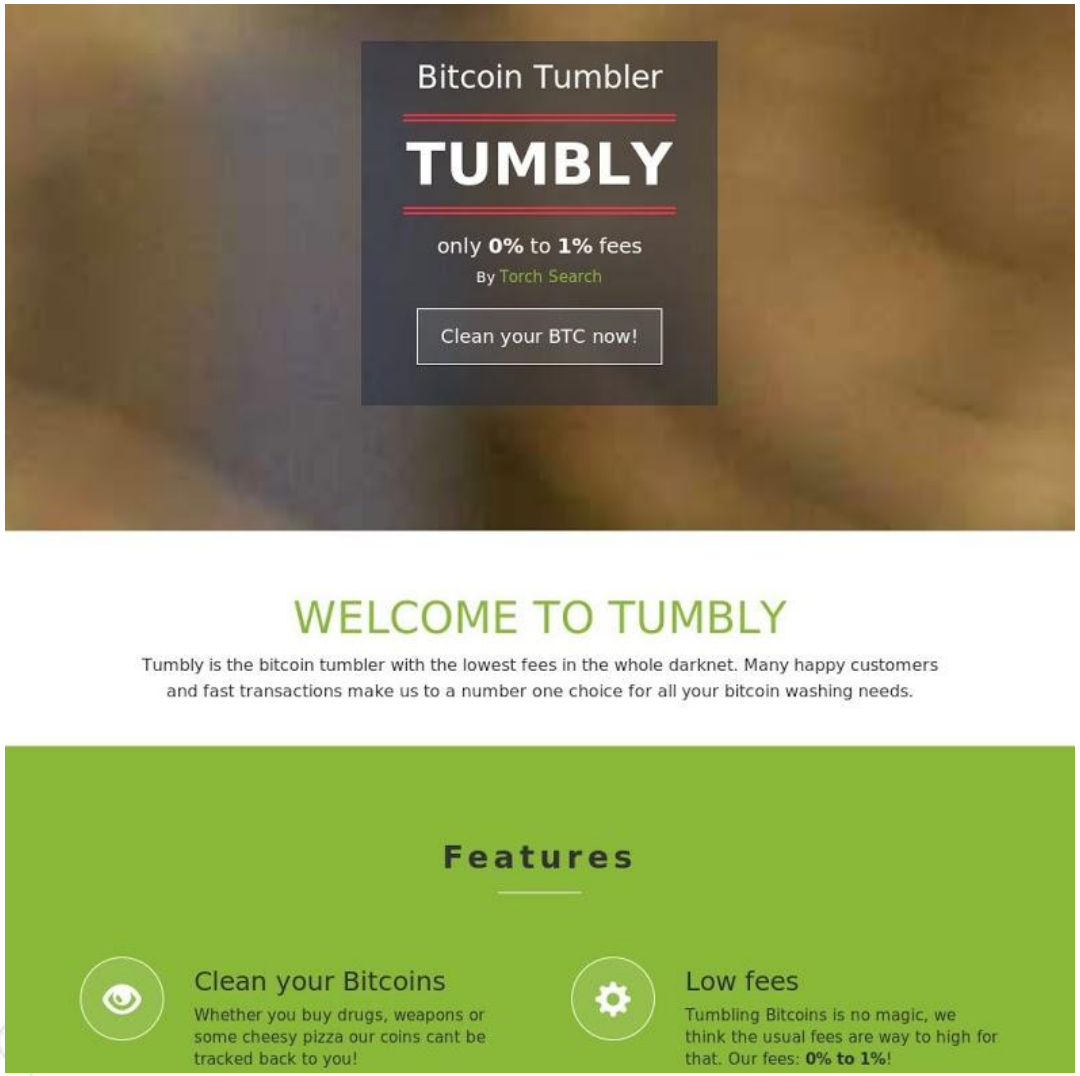
É só pra liberar script, eu particularmente deixo o bloqueio habilitado o tempo todo.. mas temporariamente só pra dar um ajuda tanto, eu acho que compensa..

Torchat: 64rpss4mb24vsfz6
bankofamerica@mail2tor.com

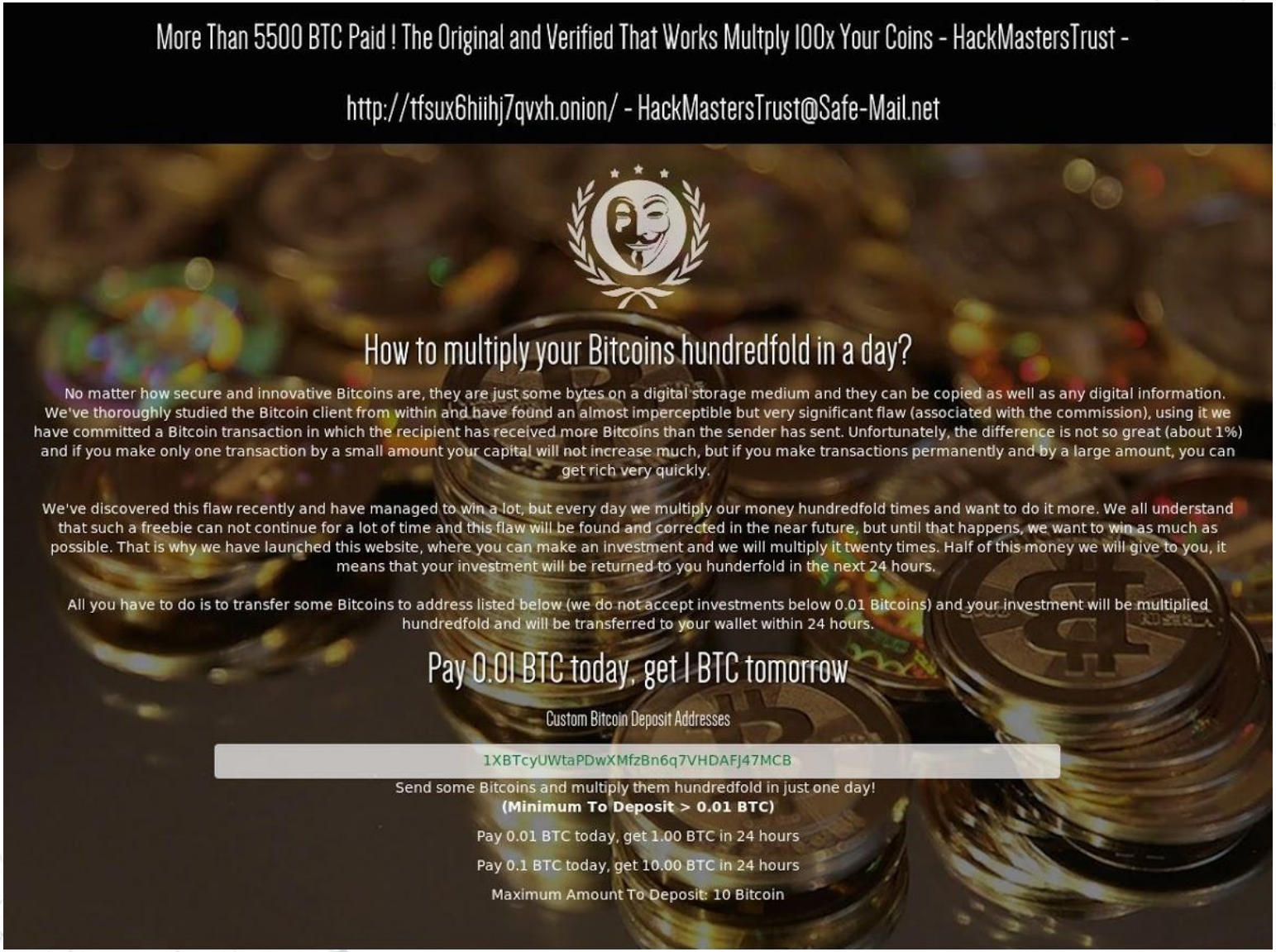
Automated Bitcoin Identification

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

Bitcoin Tumblers



Bitcoin Multiplier 1/2



Bitcoin Multiplier 2/2

Some History

Date	Deposited	Returned	Return address	Transaction
08/10/15	**0.01** BTC	**1** BTC	157H3quvaBovcKkaRcwozNxu72ZRTBoEb7	a42c37ad189f07cd5405e433fb1ebb6c88a4e05f8761
08/10/15	**0.045** BTC	**4.5** BTC	1J7Dkq8yXaAcWBF7PpzcGrbpsah1mkaUDK	4d0d5c800039e68034e7bdbe622478b5eadc778bbdc
07/10/15	**0.2** BTC	**20** BTC	3NKkQeZDrhgzQKP99pRU71j4HcwXTmw5VS	7e2de327913b8b3c644afbab0d4c2ea68e7c1492718a
06/10/15	**0.06** BTC	**6** BTC	13EhGy3yuTC6Es9g5a6Fnzo9fLuPzkFvFg	6261d13329f19f0f44d1fb96a0ad3e9ef95d5b86f3899
06/10/15	**0.15** BTC	**15** BTC	13wdrfBxUShsMASGxGwZ68bH8XC7XrCqzC	8c86c0e8107286eb1b696c5a5d198cdd10aeb3cf343b
05/10/15	**0.1** BTC	**10** BTC	1sCHh9zH7g1yx7S4h4qJ9uqxCDLNm7Lke	fc766fc6c180ae162a5cc845d8a4f156ffe988b667fdc
04/10/15	**0.07** BTC	**7** BTC	1LsSAPNm9ZkPv2CSpx6wgUFRVxEJC1rQmR	366cfda3ad9bd2b8fda43baca2d6799252dee492b268
04/10/15	**0.01** BTC	**1** BTC	12a5RQoSs2u71MeSBu68cbV62aLccpr3i6	767c8c51c63b00520e930596dfe0a64411c39876595b
04/10/15	**0.10** BTC	**8** BTC	1DgDiL4weX45XbyH3rT9HckbgDCcSgoTMz	aa23f7d56ac53b4f585670225fd70681e7de0685eb1d
04/10/15	**0.6** BTC	**60** BTC	1EmYzDnLB3QCTebzuvUuJ4d32j235LGKtC	db157cb915b8ea1dd8cc5ca5b5be22a796c146a35039
03/10/15	**0.25** BTC	**25** BTC	1BJWYQ7dM2ecPWbB5eodY9ikBY52JGf122	4637cfbd20d862cd5156991d327cc18ccbf4a7aded70
29/09/15	**0.035** BTC	**3.5** BTC	1AT66aPVe5u418S26BYFXRmxCn1XJB2PWg	4da13ece015a49c8765cd27c3a4009bea73df5a11e3f
28/09/15	**0.01** BTC	**1** BTC	1H5oYxmRyAJ2b13tuZkCLy3cscfyKx7Aq7	f2af8b3bc57dae2c8c7853b5b8564c65e5fcd38e7caf

Malware

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

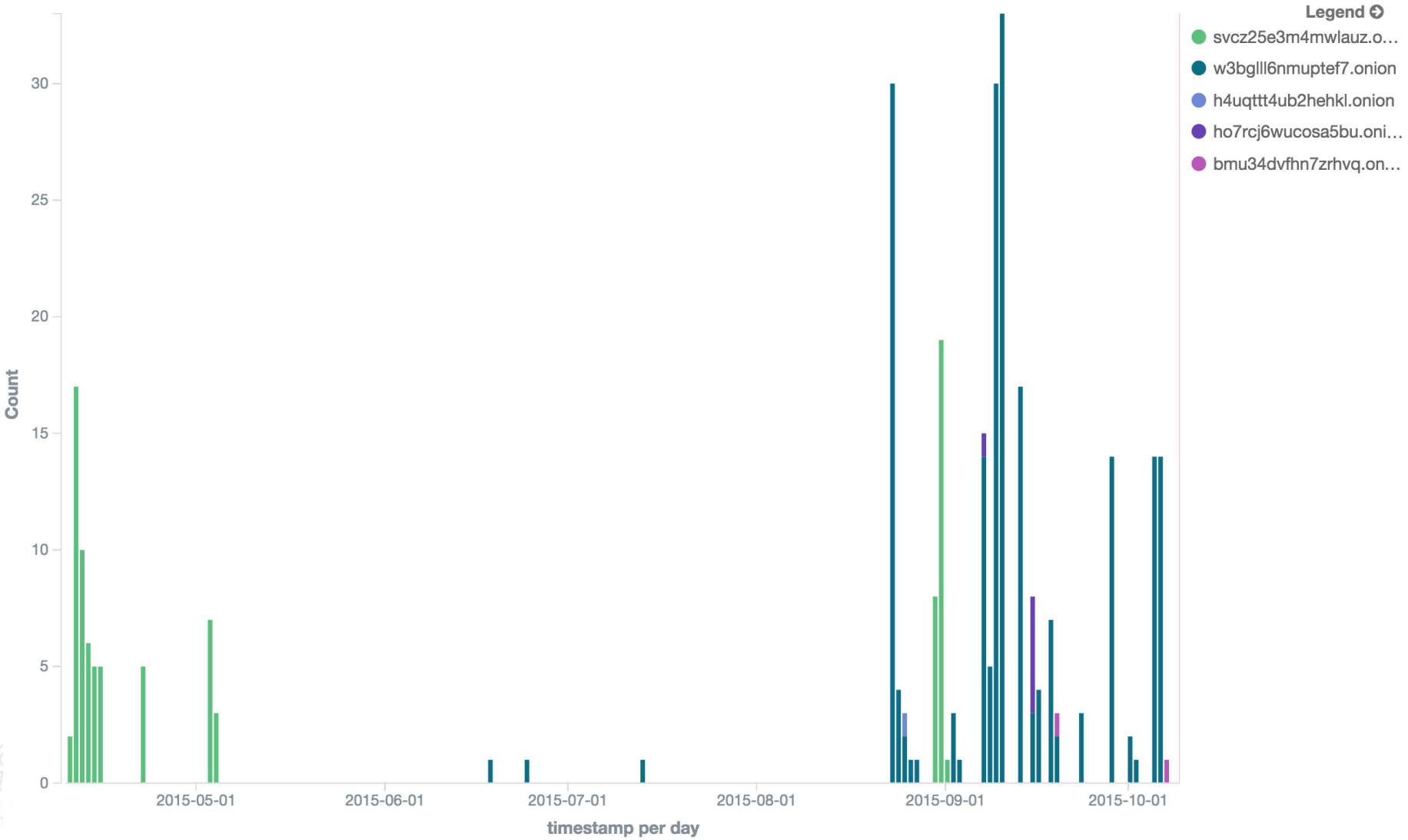
- Malware with DDoS, bitcoin mining and banking capabilities (©G-Data/Rapid7)
  - ZeuS bot
  - Bitcoin mining tool (CGMiner)
  - GPU libraries for hash cracking
- TOR client per Windows
- Use `/gate.php` as landing page to store the harvested credentials
- Path monitoring ….

⊖	/gate.php	367	2013-12-09	2014-04-25

Domain breakdown

Scheme	Hostname	Port	# Rep	First seen	Last seen
-	egzh3ktnywjwabxb.onion	80	213	2013-12-09...	2014-01-17...
http	akrnfve5eifqygwr.onion	80	154	2014-02-23...	2014-04-25...

SkyNet: Dynamic TOR-based C&Cs

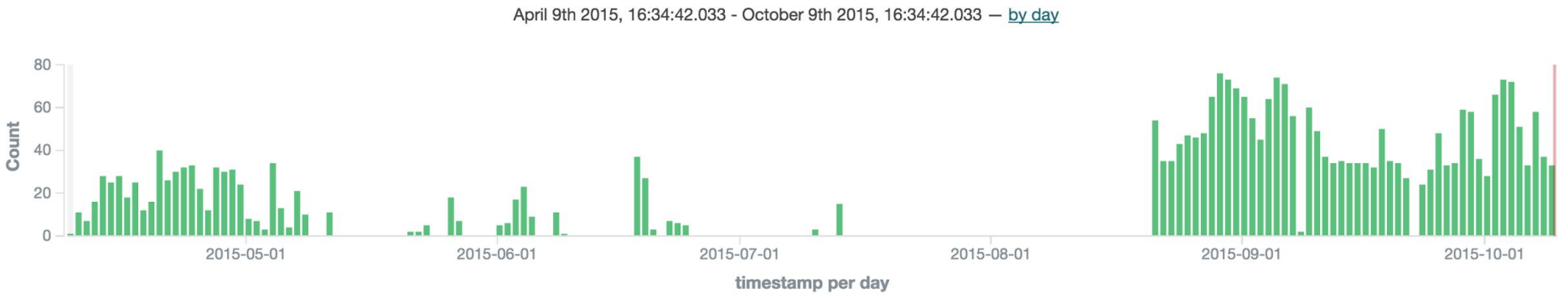


Dyre Banking Trojan

- BHO that MiTMs 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

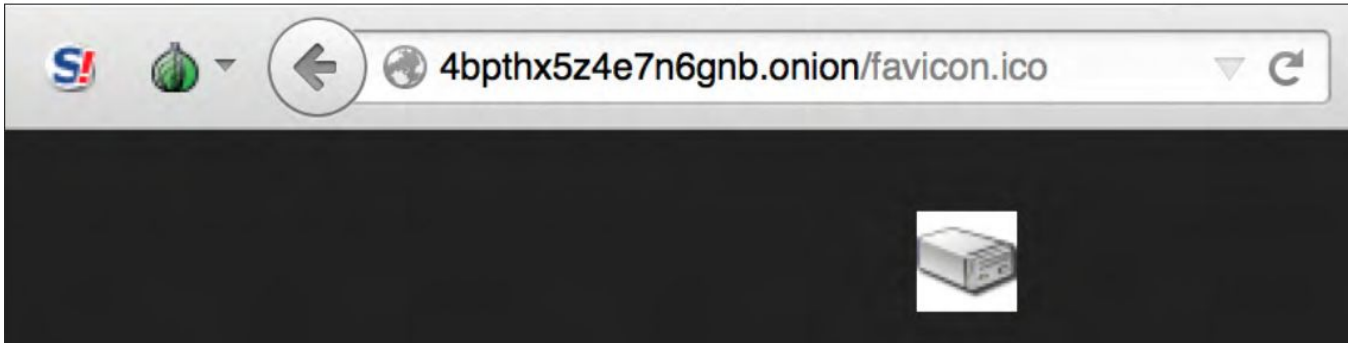
Dyre's Infection Evolution



Time	url.@raw
October 9th 2015, 16:23:10.455	http://oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p:80/
October 9th 2015, 15:41:56.468	http://oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p:80/
October 9th 2015, 14:53:07.007	http://oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p:80/
October 9th 2015, 13:59:50.718	http://oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p:80/
October 9th 2015, 13:18:03.211	http://oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p:80/
October 9th 2015, 12:52:27.011	http://nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p:80/
October 9th 2015, 12:23:43.690	http://oguws7cr5xvl5jlrhyxjktcdi2d7k5cqeulu4mdl75xxfwmhgnsq.b32.i2p:80/
October 9th 2015, 12:16:03.639	http://nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p:80/

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.)

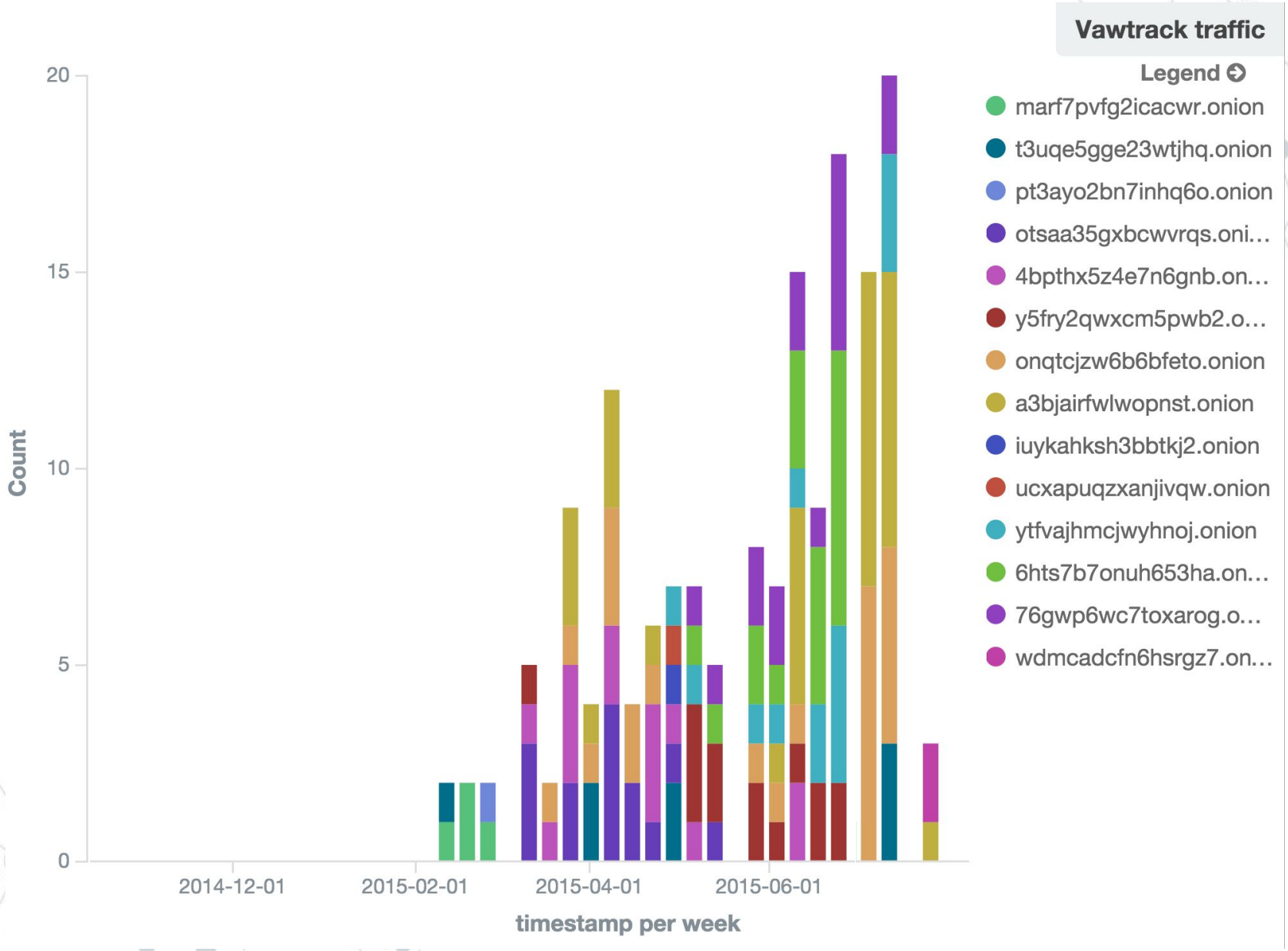
- Runs ‘`openresty/1.7.2.1`’ as web-server
- Return code on ‘`favicon.ico`’ is 403 Forbidden

x-cache-lookup	miss from charon:3128
server	openresty/1.7.2.1
last-modified	wed, 18 feb 2015 14:45:29 gmt

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

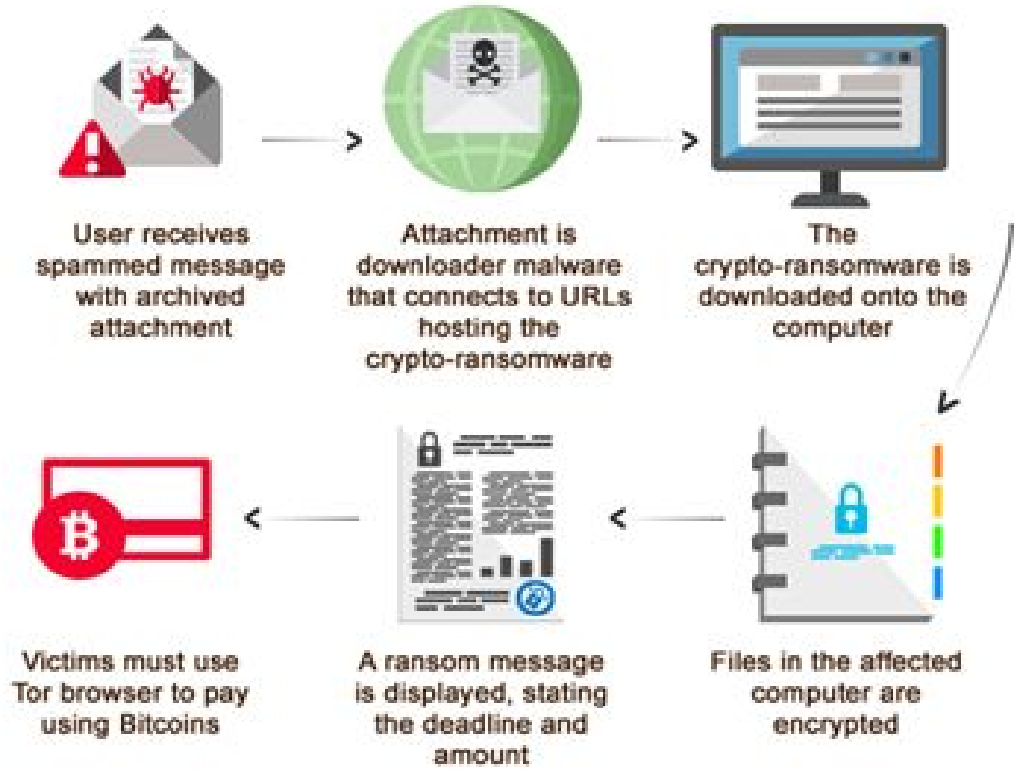
http://3jjx4qbhr6tw2juk.onion:80/	http://iuykahksh3bbtkj2.onion:80/	http://sws5qec3n7v7bxei.onion:80/
http://4bpthx5z4e7n6gnb.onion:80/	http://marf7pvfg2icacwr.onion:80/	http://t3uqe5gge23wtjhq.onion:80/
http://6hts7b7onuh653ha.onion:80/	http://max6gtszig6i4rjt.onion:80/	http://ucxapuqzxanjivqw.onion:80/
http://76gwp6wc7toxarog.onion:80/	http://onqtcjzw6b6bfeto.onion:80/	http://w3kjcq6svuucwb6o.onion:80/
http://a3bjairfwlwopnst.onion:80/	http://otsaa35gxbcwvrqs.onion:80/	http://w3qsdpr5gb3ltln3.onion:80/
http://gxi4unnw363epeow.onion:80/	http://oxrml5ihgfibce2r.onion:80/	http://wdmcadcfn6hsrgz7.onion:80/
http://ipx5qhsbgddvqilb.onion:80/	http://pt3ayo2bn7inhq6o.onion:80/	http://y5fry2qwxcm5pwb2.onion:80/
	http://q6knv6pe25cxjv2s.onion:80/	http://ytfvajhmcjwyhnoj.onion:80/

Vawtrack Banking Trojan (cont.)



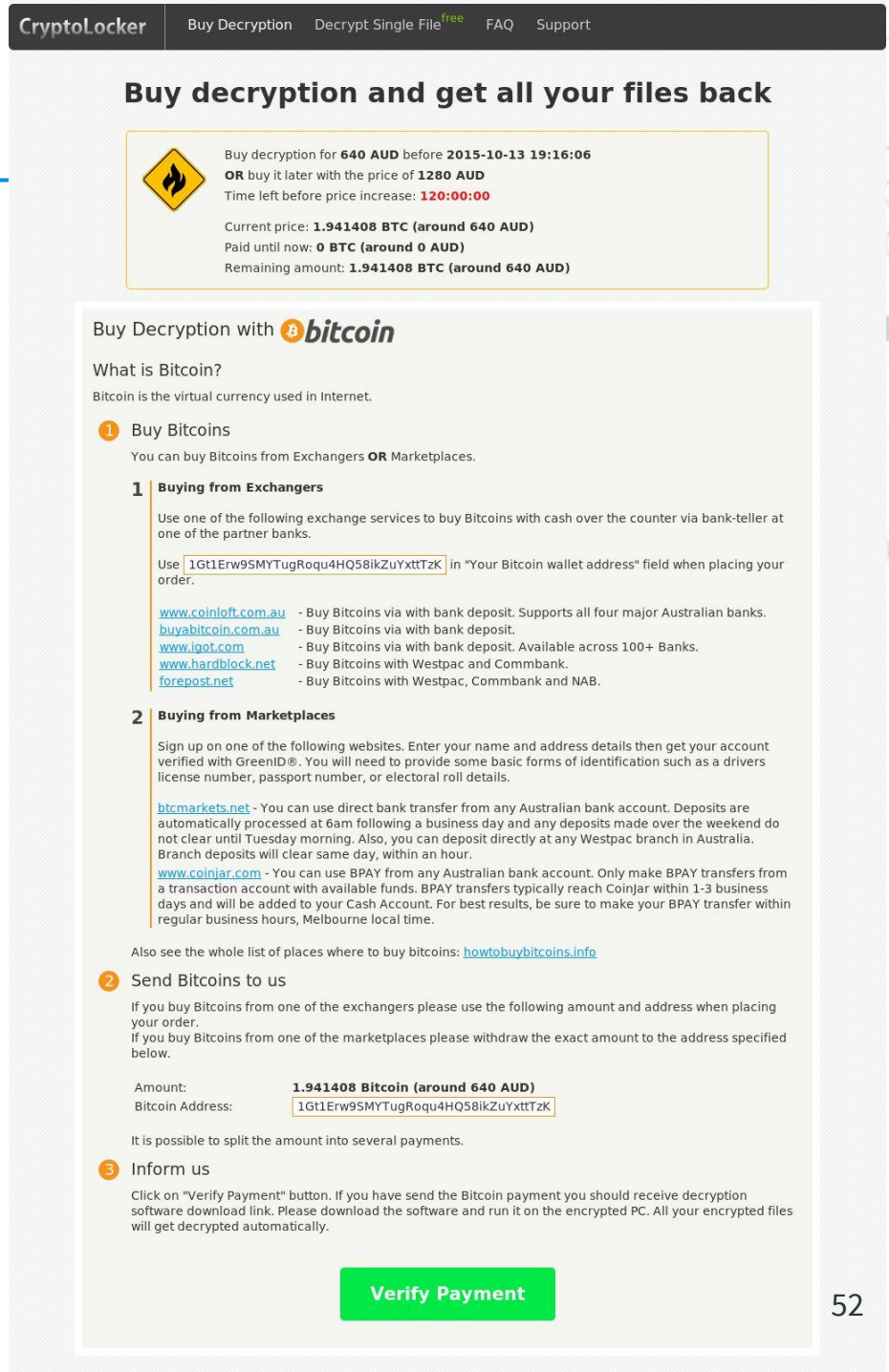
Ransomware

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



TorrentLocker

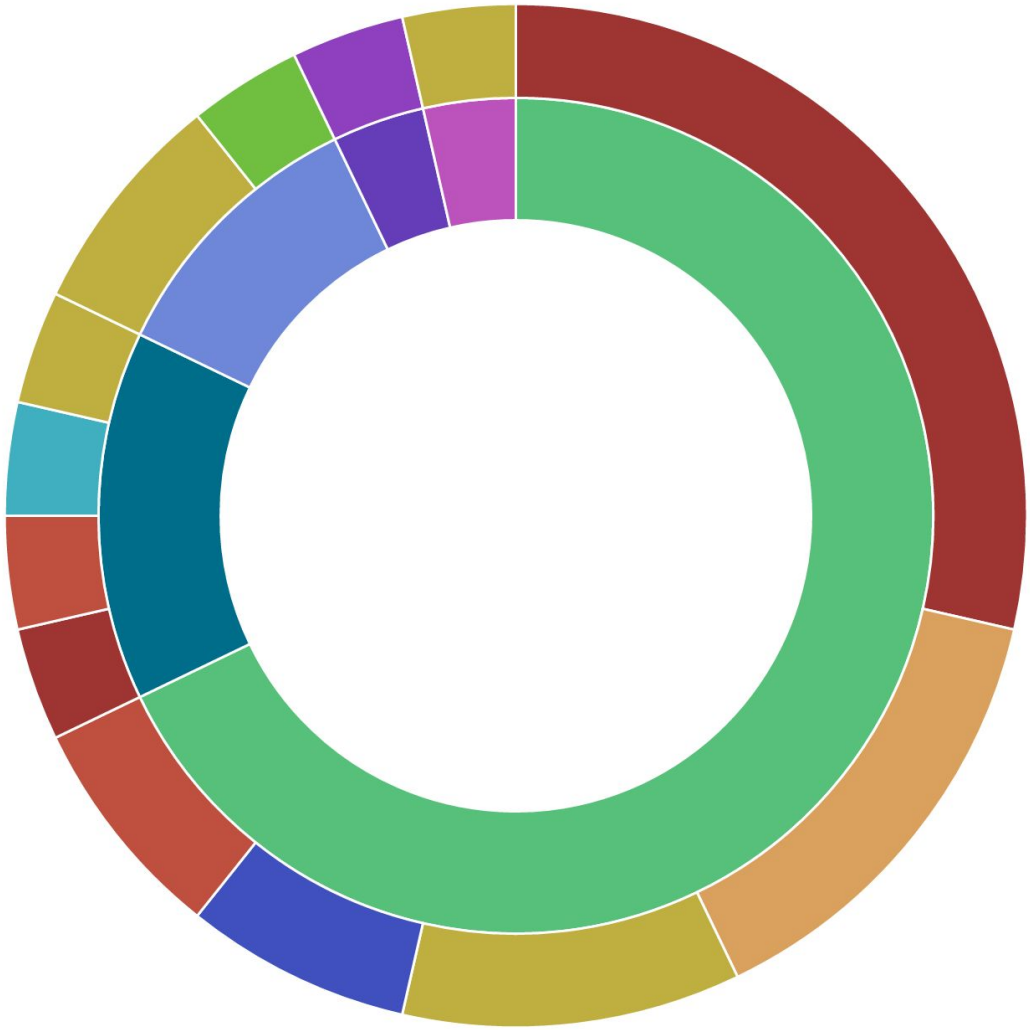
- A variant of cryptolocker
- Payment page hosted in the Deep Web
- Cashout via Bitcoins



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

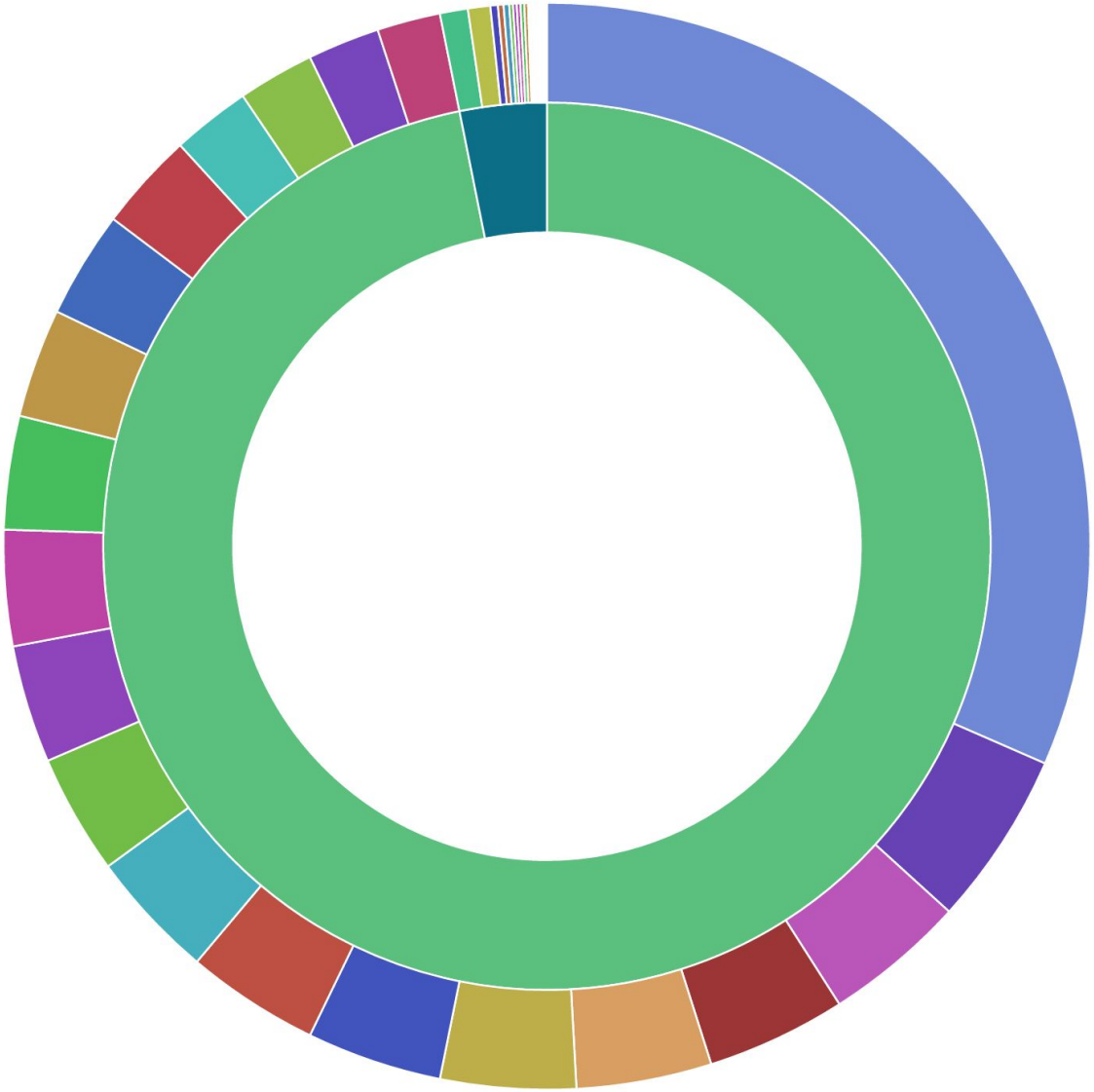


NionSpy

- 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



NionSpy: GET's query string analysis

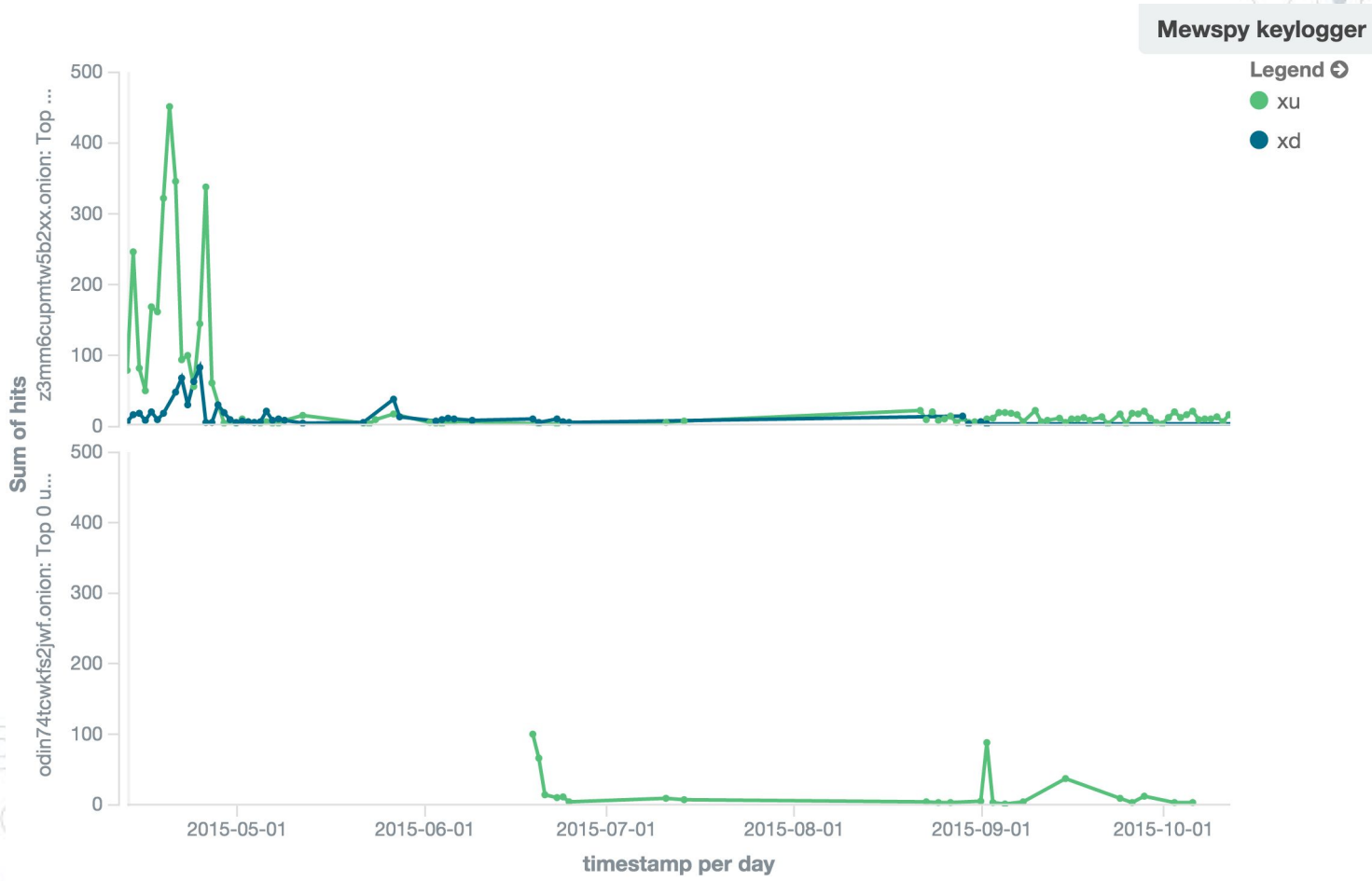
- `xu` experienced a quick surge in popularity: 1700+ values

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

- `si.php?xd={"f155":"MACHINE_IP", "f4336": "MACHINE_NAME","f7035":"5.9.1.1","f1121": "windows","f2015":"1"}`
- Reports a new infection

NionSpy: New victims and leakages

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



Thank you!

Dr. Marco Balduzzi
@embyte