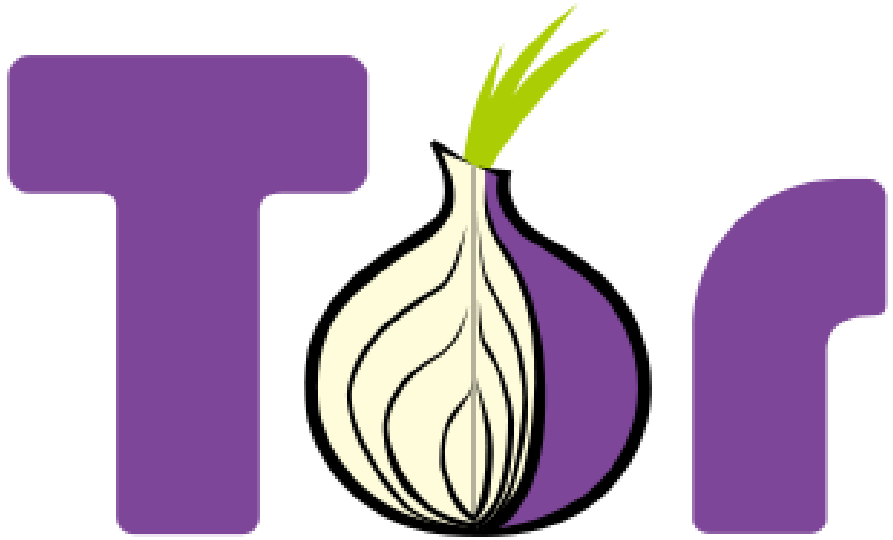
{codemotion}

POWER OF OPPORTUNITY

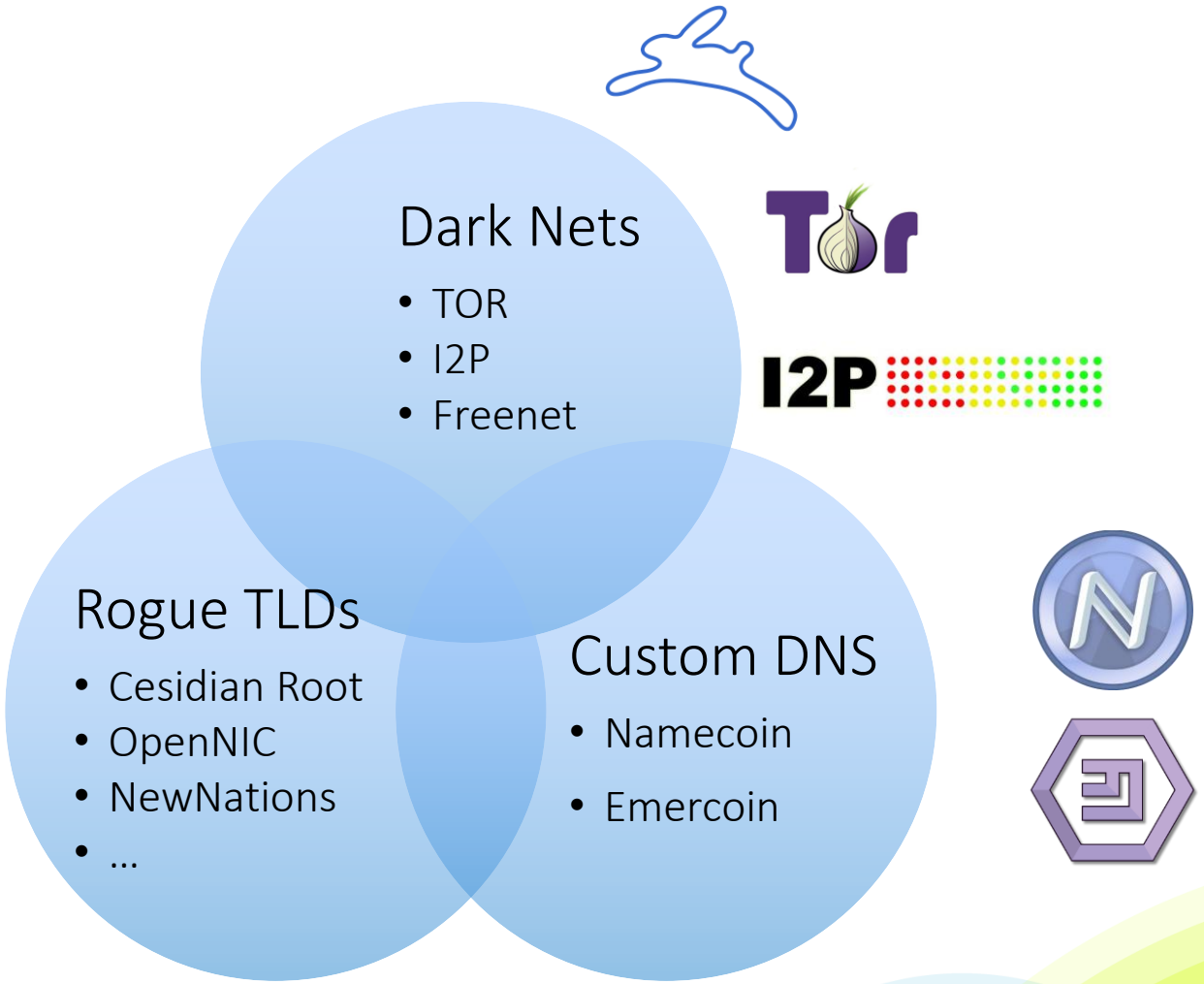
Cybercrime and Attacks in the Dark Side of the Web

Dr. Marco Balduzzi*
Senior Researcher at Trend Micro
http://www.madlab.it @embyte

*With the cooperation of Mayra Rosario and Vincenzo Ciancaglini


Tor

The Dark Ecosystem



Cesidian Root

Cyberterra Mean Time
Saturnday 22 Kurosawa 2015 @ 535

nic

name.space
the "dot everything people" since 1996

A perfect platform for Cybercrime

Our Investigative System: DEMO

timestamp:[2015\-01\-01 TO 2015\-12\-31] AND title:marketplace

Collected Data

Source	# events/hour	# events/day	total events	first seen	last seen
Scouter	13	13	23,103,904	2014-06-06, 16:09	2017-07-01, 00:13
TOR Gateways	928	928	2,211,114	2015-05-08, 13:00	2017-10-04, 00:02
SPN data	129	3,418	1,492,602	2013-11-12, 18:29	2017-10-04, 12:20
I2P Registries	104	104	890,699	2015-05-08, 15:58	2017-09-30, 00:00
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

Website breakdown

10 records per page | Last month | Active | Inactive | Malicious | Search: | Search

	Hostname	# URLs	First seen	Last seen
⊕	hss3uro2hsxfogfq.onion	2	2017-05-17 06:30:03	2017-10-04 00:02:37
⊕	yfka3g2webemzg2z.onion	1	2017-05-31 00:02:27	2017-10-04 00:02:08

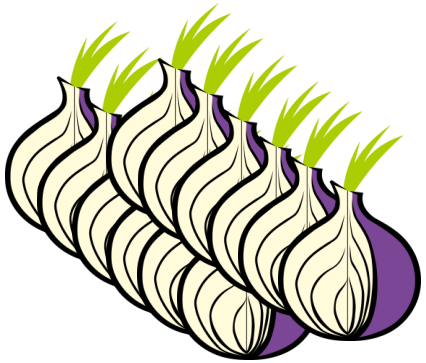
Our Gateway to the Dark Internet

Privoxy + TOR anonymizer

Squid transparent proxy

Polipo + TOR 64 instances

Custom DNS resolver (DNSMASQ)



Namecoin DNS

rogueTLD DNS

Cesidian root

Opennic

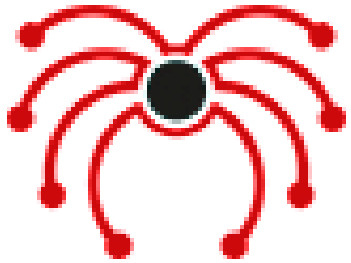
NameSpace

...

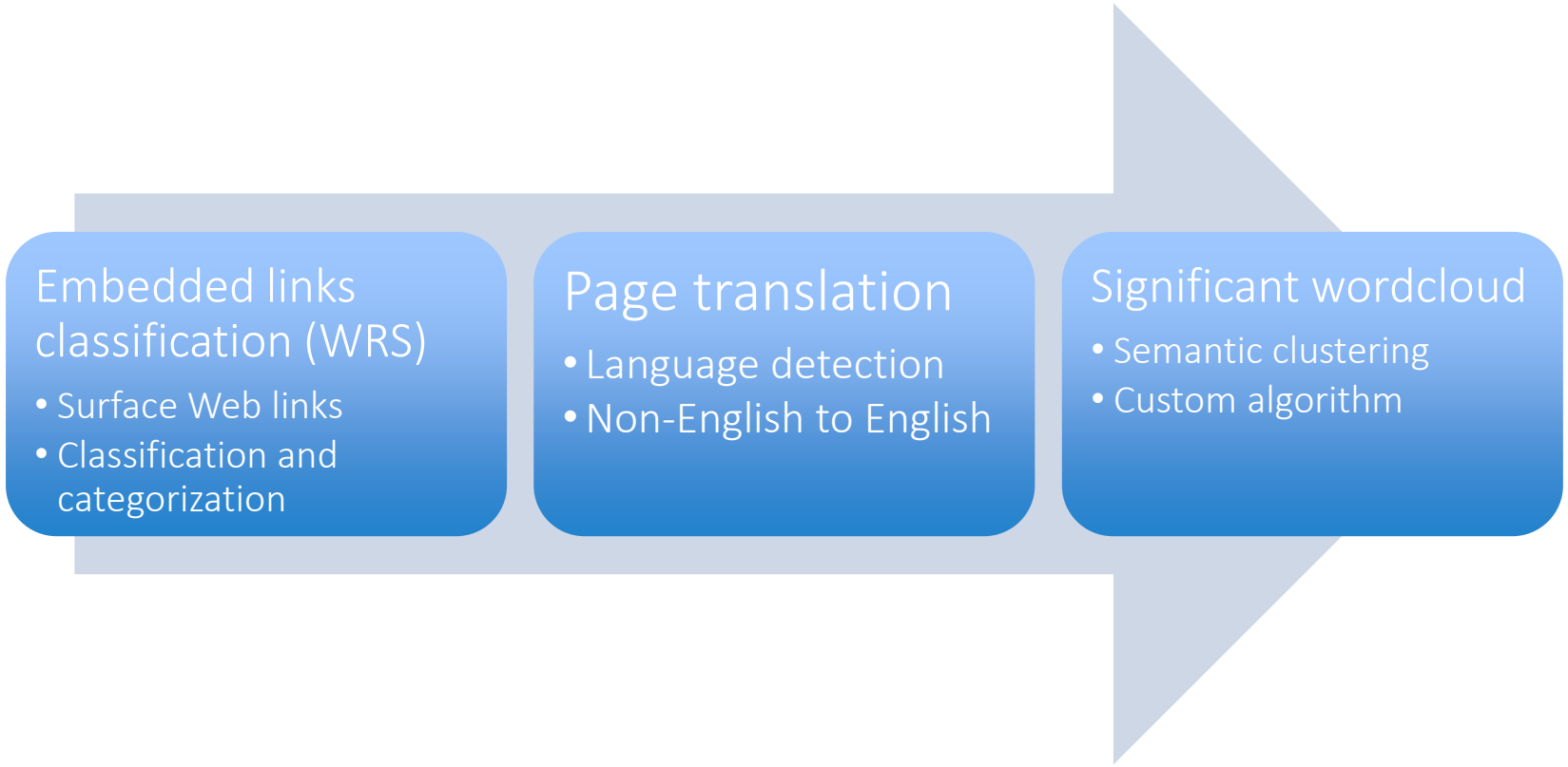
Data Exploration

Headless Browser

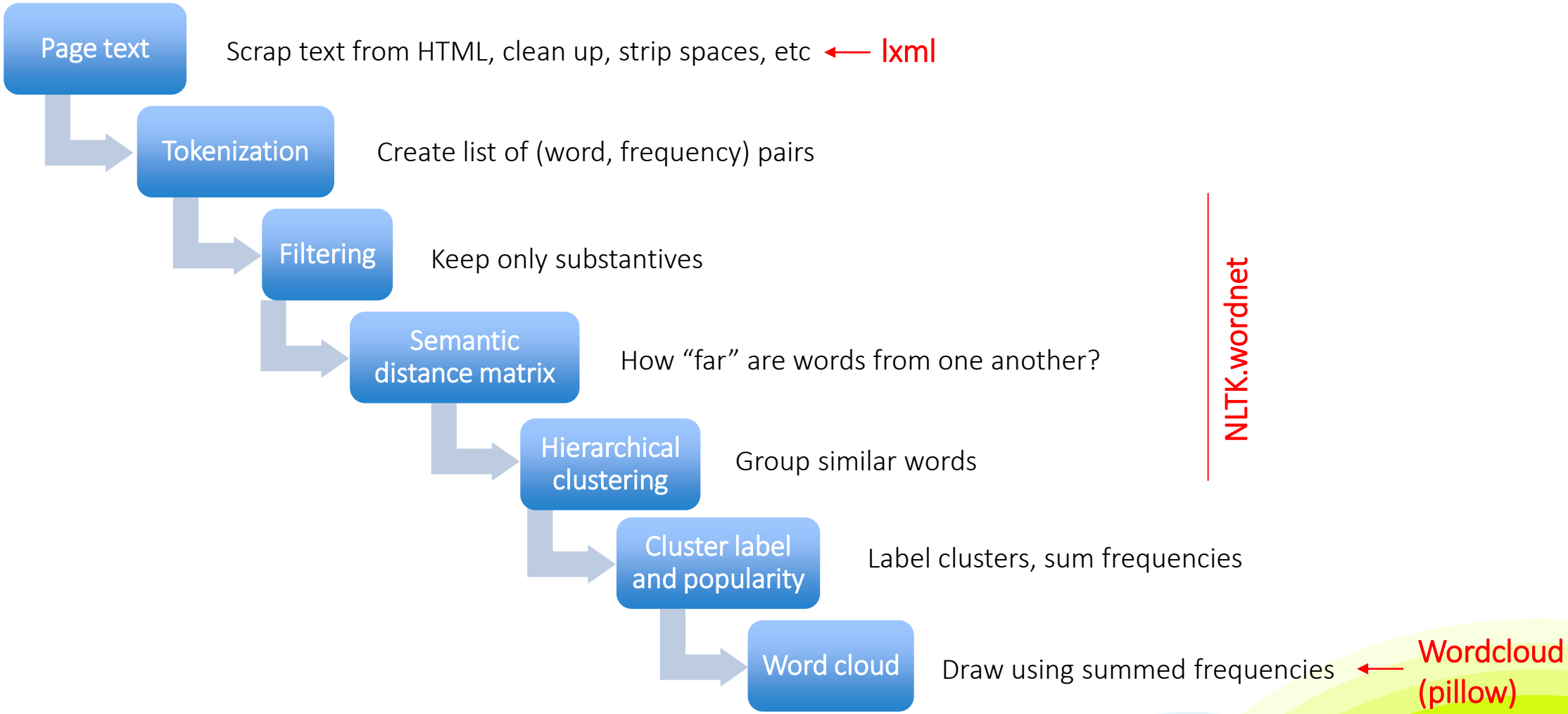
- Scrapinghub's Splash
  - QTWebkit browser, Dockerized, LUA scriptable
  - Full HTTP traces
- Crawler based on Python's Scrapy + multiprocess + Splash access
  - Headers rewrite
  - Shared queue support
  - Har log -> HTTP redirection chain
- Extract links, emails, bitcoin wallets



Data Analysis



Significant Wordcloud

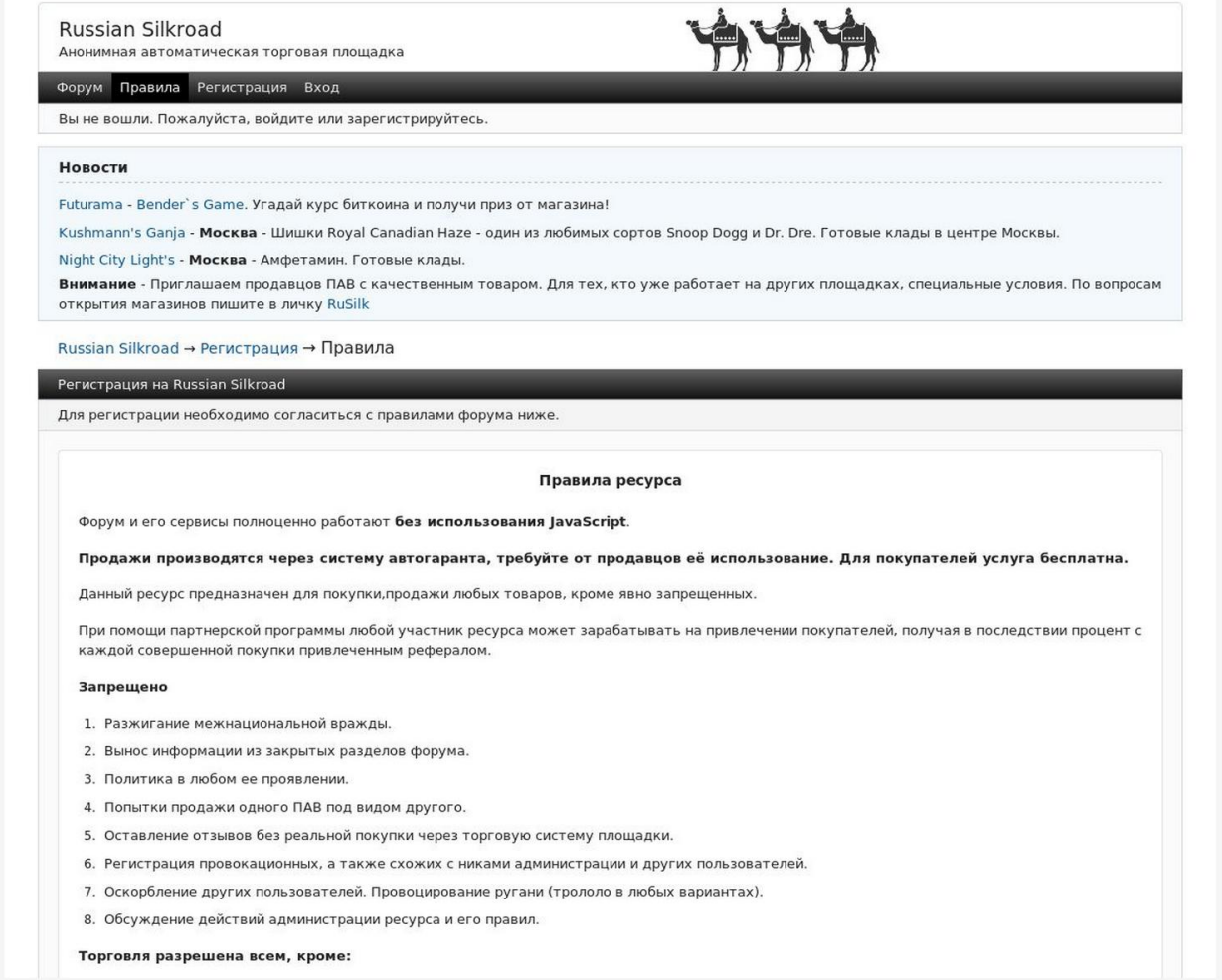


The Dark Portal

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:

Bootstrap

jQuery

{codemotion}

Examples

Guns

Identities and Passports

6 Identity Scans from Iraq

Iraq - 6 scans, all are passport scans These 6 scans are part of my Mega Scans Pack, to just buy these 6 scans order here. To buy the Full Mega Scans Pack Which Includes these scans and many other scans go to -

[redacted]

Sold by [redacted] - *0* sold since *May 31, 2016* Vendor Level 5 Trust Level 4

	Feature		Feature
Product class	Digital	**Origin country**	Worldw
Quantity left	Unlimit	**Ships to**	Worldw
Ends in	Never	**Payment**	Escrow

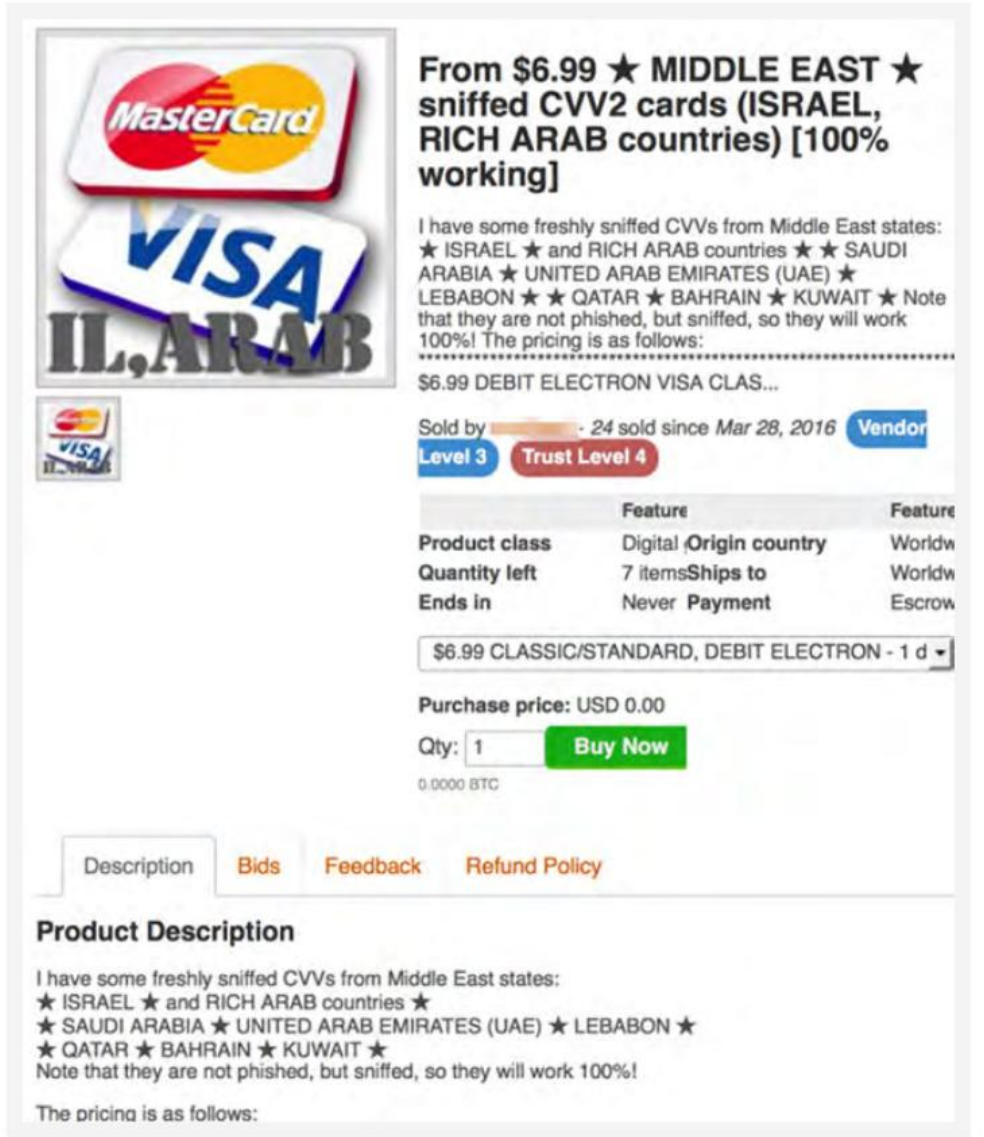
Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty: 1 Buy Now

0.0034 BTC

Credit Cards



Accounts, e.g. Israeli Paypal

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

Product	Price
100 PayPal accounts	100 USD =
100 Ebay accounts	100 USD =
100 CCs with CVV2	150 USD =

طلب حسابات بايبال اسرائيليه

السلام عليكم

مطلوب حسابات بايبال اسرائيلية وحصرا اسرائيلية بالشروط التالية

1-اذا في باسورد الايميل فيشترط انو مايكون جيميل بسعر $2.5 بنكوبن للحساب الواحد . واذا الحساب فيه بالانس كبير في سعر خاص .

2-اذا مافي باسورد الايميل فيشترط ان لايكون هوتميل وياهو بسعر $1 للحساب .

وطبعا يكون مربوط مع الحساب فيزا ووجود الاي بي .

الرجاء بلي ماعجبو السعر مايعلق تعليقات فارغه .

==========

سبحان الله وبحمده سبحان الله العظيم

==========

اقتباس

Cashout services

Country/ Region	Seller Item	Purchase Method	Price
Egypt	Sony Xperia Z2 D6503	BTC	$210–250
Jordan	Apple iPad mini Retina	Amazon Gift Card	$125
Iraq	Samsung 8-piece Surround Sound System	Escrow, BTC	$450 (including shipping)
MENA	10 Pieces Samsung Galaxy S8 64GB	BTC, credit card	$6,000
MENA	5 Pieces Apple iPhone 7 Plus 32GB	BTC, credit card	$2,600

Bulletproof Hosting Providers

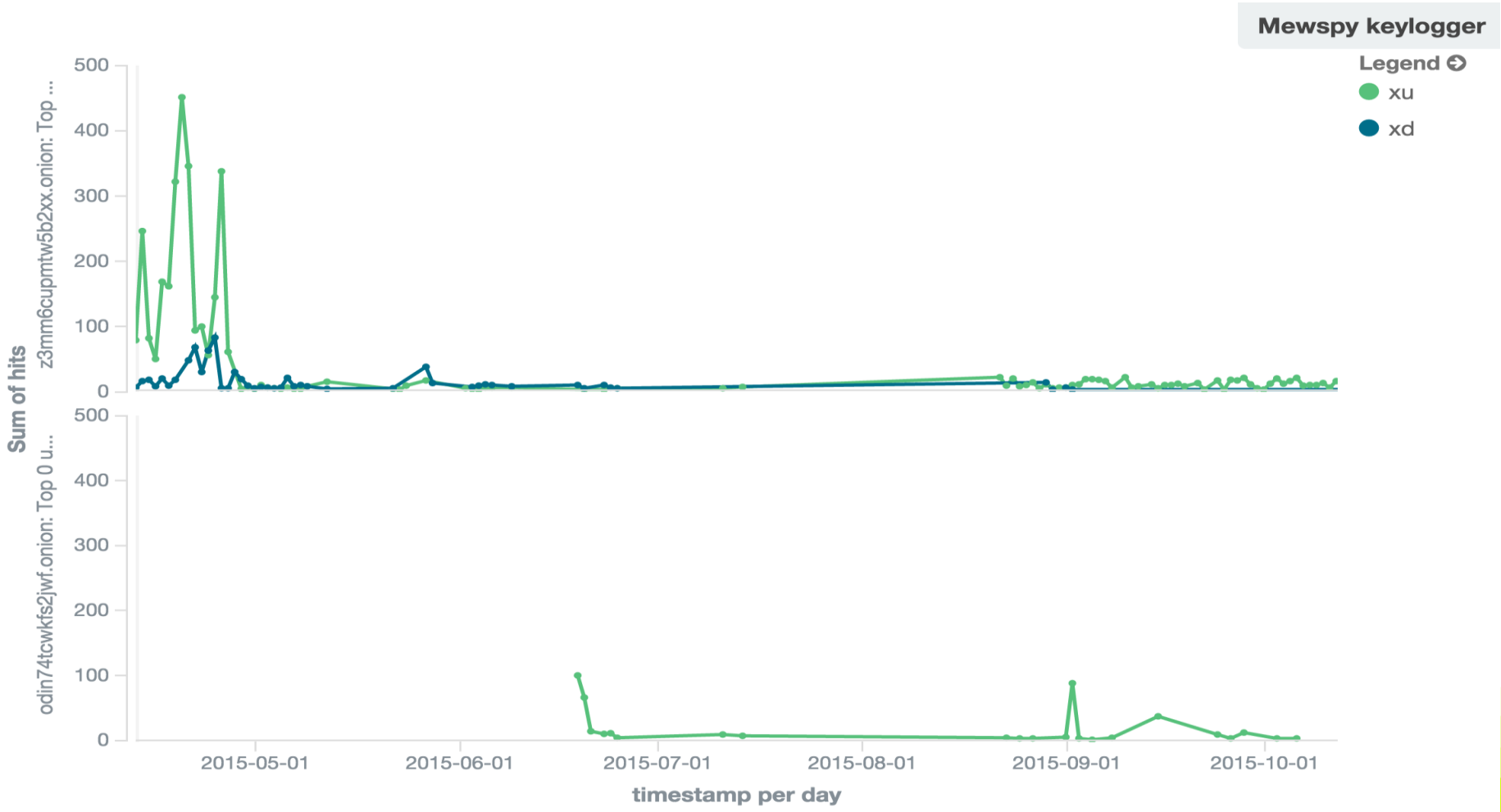
Impact on organizations

- Dark Web traffic is difficult to be detected by traditional systems (IDS)
- Resilient and stealth malware
- Persistence and monitoring (APT)

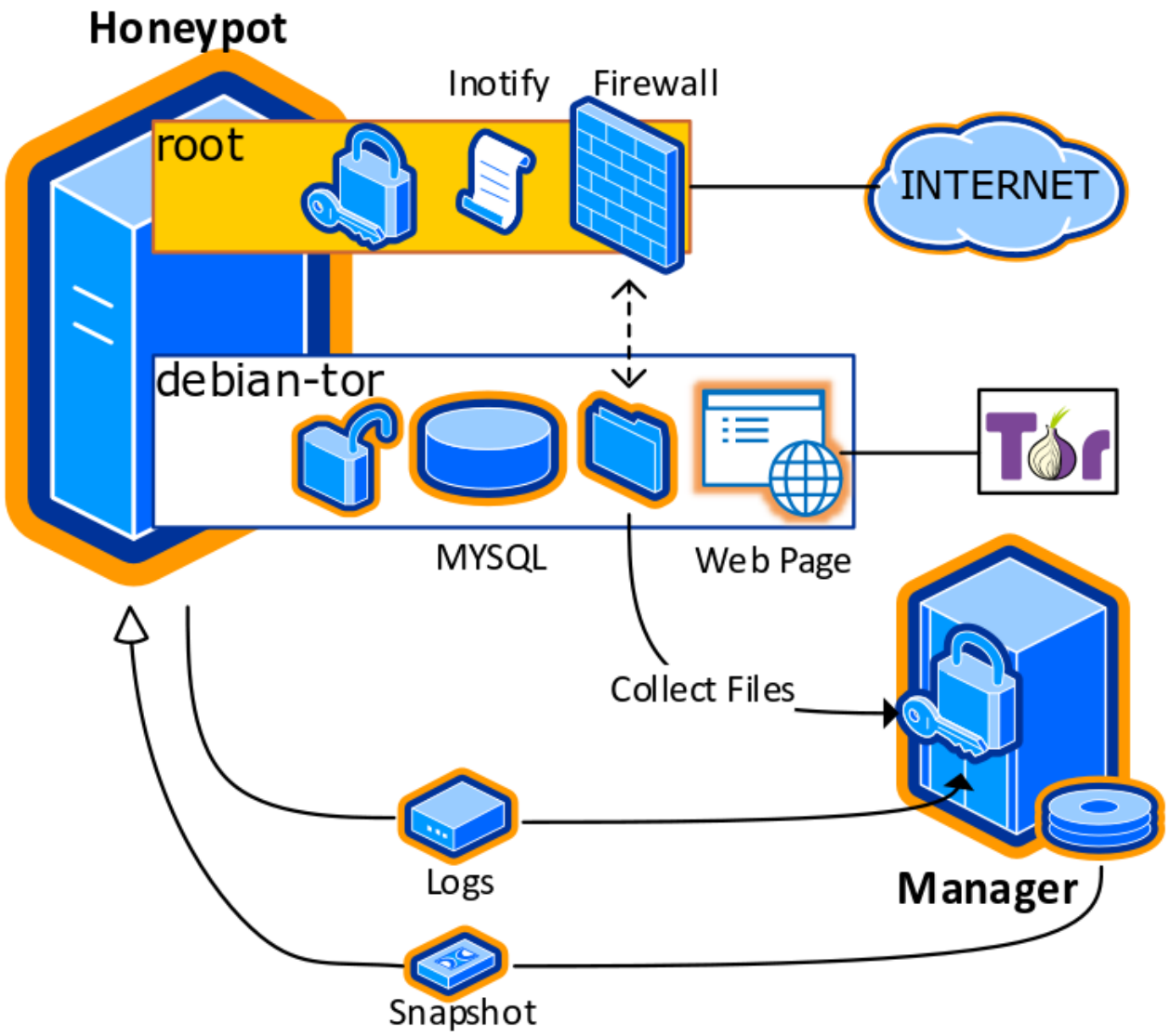
Ransomware

- TorrentLocker, i.e. variant of CryptoLocker
- Payment page hosted in TOR
  - wzaxcyqroduouk5n.onion/axdf84v.php/user_code=qz1n2i&user_pass=9019
  - wzaxcyqroduouk5n.onion/o2xd3x.php/user_code=8llak0&user_pass=6775
- Cashout via BITCOINS

Keylogger


Mewspy keylogger
Legend
xu
xd
Sum of hits
z3mm6cupmtw5b2xx.onion: Top ...
odin74tcwkfs2jwf.onion: Top 0 u...
500
400
300
200
100
0
2015-05-01
2015-06-01
2015-07-01
2015-08-01
2015-09-01
2015-10-01
timestamp per day

Organized Attacks



We simulated a cybercriminal installation in the Dark Web

Honeypot

I. Black Market
II. Hosting Provider
III. Underground Forum
IV. Misconfigured Server (FTP/SSH/IRC)

Technology

I. Wordpress + Shells
II. OsCommerce
III. Custom Web App
IV. Custom OS (Linux)

A private forum for our VIPs

VIP Forum

Home

What do you want to know more, it is here. We are more than just a forum, we are a community. Our member's privacy is our highest priority. Unless you choose to reveal it, we work hard to keep it anonymous.

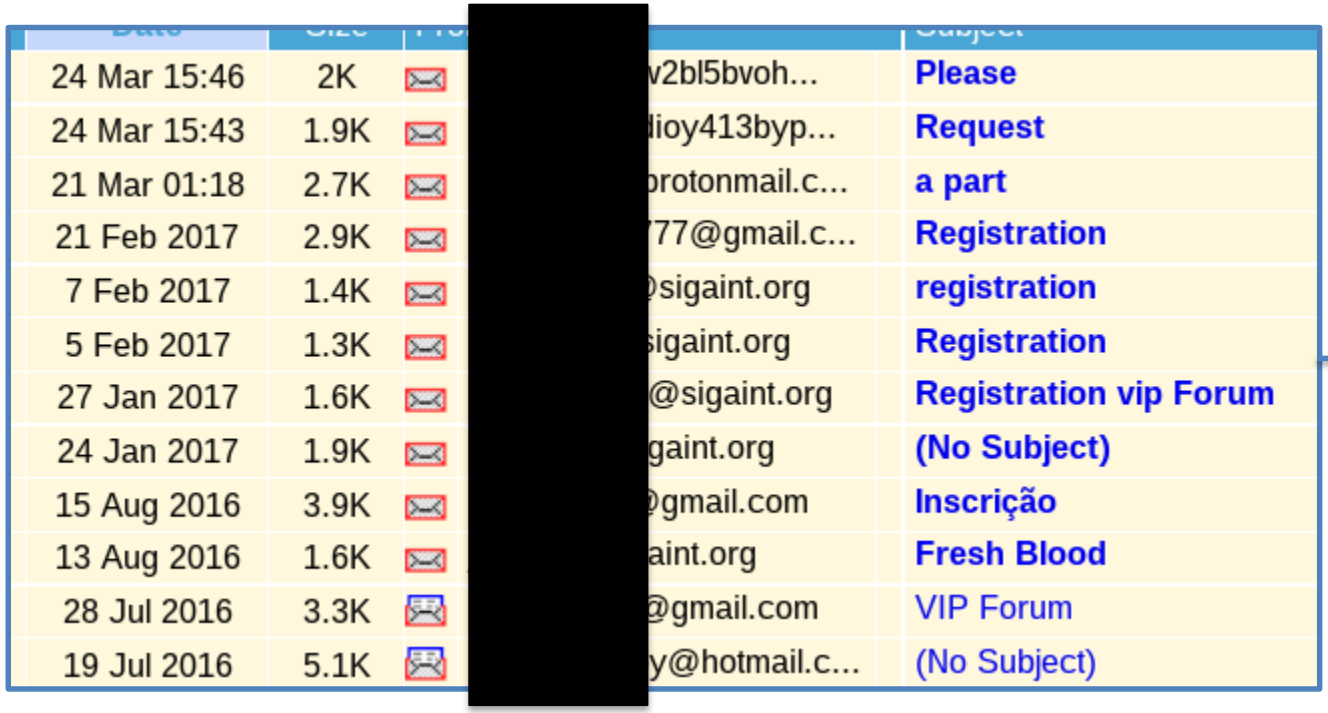
About us

We are a community that shares any kind of information, and by any... we mean anything!

Home .....
Login .....
Contact us .....

Please contact us with your reference for registration by clicking here.

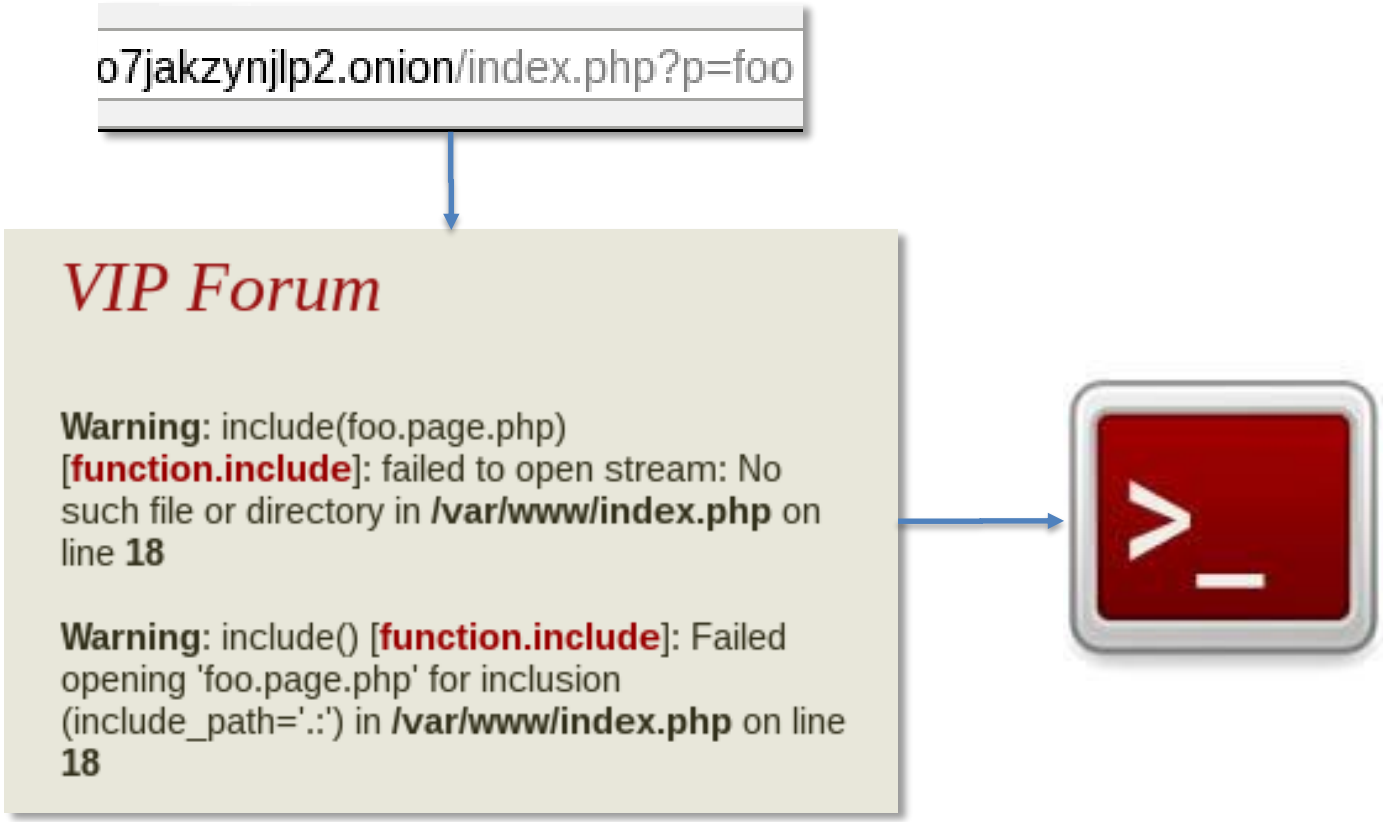
Registration-Only Forum



24 Mar 15:46	2K		v2bl5bvoh...	**Please**
24 Mar 15:43	1.9K		lioy413byp...	**Request**
21 Mar 01:18	2.7K		rotonmail.c...	**a part**
21 Feb 2017	2.9K		77@gmail.c...	**Registration**
7 Feb 2017	1.4K		sigaint.org	**registration**
5 Feb 2017	1.3K		igaint.org	**Registration**
27 Jan 2017	1.6K		@sigaint.org	**Registration vip Forum**
24 Jan 2017	1.9K		gaint.org	**(No Subject)**
15 Aug 2016	3.9K		gmail.com	**Inscrição**
13 Aug 2016	1.6K		aint.org	**Fresh Blood**
28 Jul 2016	3.3K		@gmail.com	VIP Forum
19 Jul 2016	5.1K		y@hotmail.c...	(No Subject)

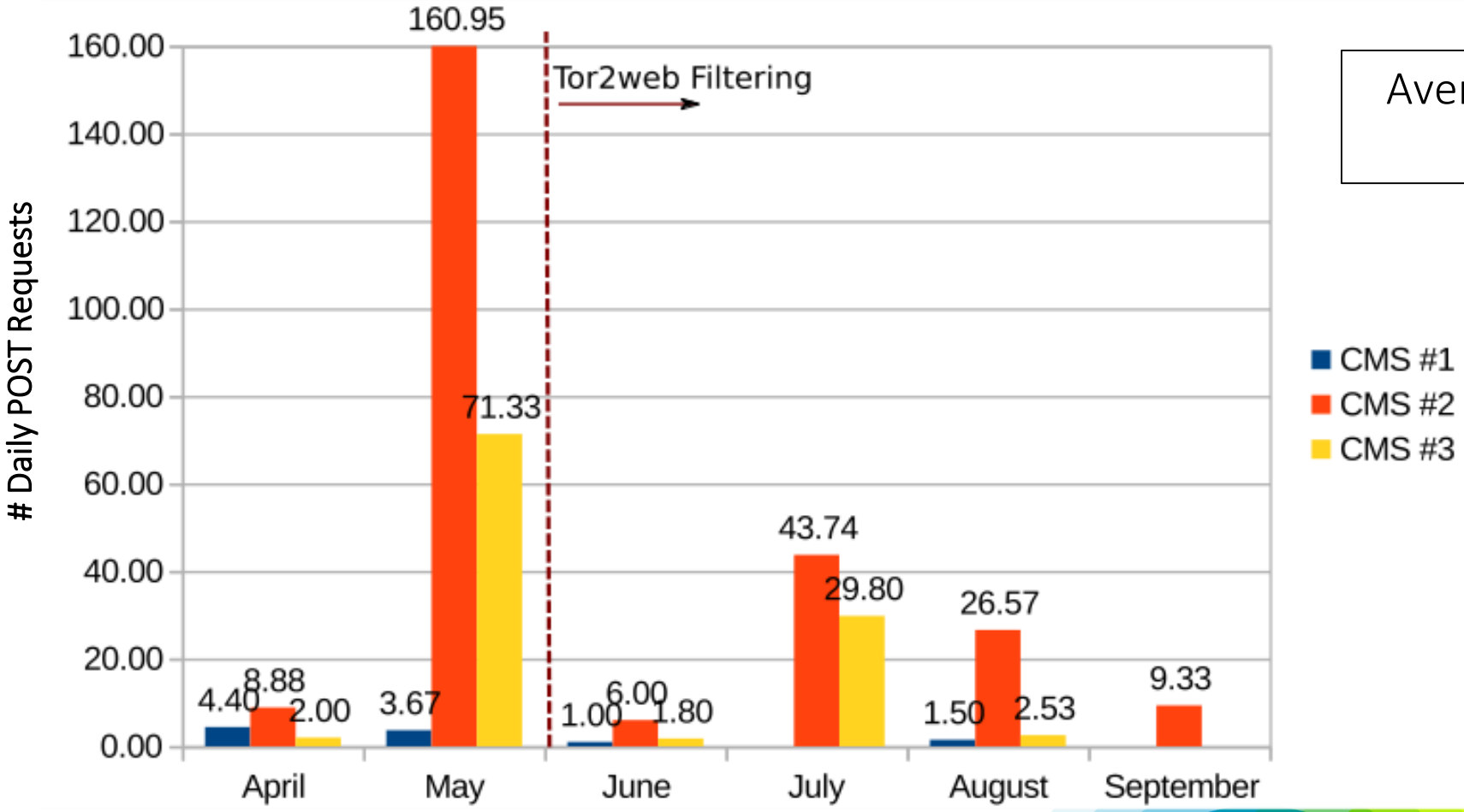
Hi , bro im new on tor .... b4 i use forums carding , hacking ... omerta , infraud ecc . i want to become member in your forum .
thx i wait permision to become member ...

Exposes a *Local File Inclusion*



A 7-months experiment

- Month 1: Different advertisement strategies to honeypot #1



Average of 1.4 malicious uploads per day

Manual VS Automated Attacks

- Pre-installed web shells attracted the most of “visitors”
- CMS #1-2 reached via Google Dorks (on Tor2Web), CMS #3 no because custom
- CMS #2 reached via TOR’s search engine’s query *“Index of /files/images/”* (http://hss3uro2hsxfogfq.onion)

	CMS #1 (OsCommerce)	**CMS #2** (Shells & WordPress)	**CMS #3** (Custom Vuln.)
Tor2web	115 (8 days)	1,930 (23 days)	0
TOR	0	2,146 (79 days)	689 (5 days)

Attacks

Days with Attacks

{codemotion}

Traditional Web Attacks

```
darkweb3/02_08_16/log/apache2/modsec_audit.log:Message: Warning. Pattern match "\\/etc\\/" at ARGS
:p. [file "/usr/share/modsecurity-crs/base_rules/modsecurity_crs_40_generic_attacks.conf"] [line "
221"] [id "958700"] [rev "2.2.0"] [msg "Remote File Access Attempt"] [data "/etc/"] [severity "CRI
TICAL"] [tag "WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI
/6.5.4"]
```

```
darkweb3/30_06_16_extra2/log/apache2/modsec_audit.log:Message: Pattern match "(fromcharcode|alert|
eval)\\s*\\(" at ARGS_NAMES:<script>alert(1)</script>. [file "/usr/share/modsecurity-crs/base_rule
s/modsecurity_crs_41_xss_attacks.conf"] [line "646"] [id "973307"] [rev "2.2.0"] [msg "XSS Attack
Detected"] [data "alert("]
```

```
darkweb3/04_08_16/log/apache2/modsec_audit.log:Apache-Error: [file "mod_cgi.c"] [line 209] [level
3] PHP Warning:  include() [<a href='function.include'>function.include</a>]: Failed opening 'cont
act&amp;quot; or (1,2)=(select*from(select name_const(CHAR(111,108,111,108,111,115,104,101,114),1),nam
e_const(CHAR(111,108,111,108,111,115,104,101,114),1))a) -- &amp;quot;x&amp;quot;=&amp;quot;x.page.php' for inc
lusion (include_path='.:') in /var/www/index.php on line 18
```

```
darkweb2/24_07_16/log/apache2/modsec_audit.log:GET /axis2/services/Version?xsd=../../../../../../.
./../../../../etc/passwd HTTP/1.1
darkweb2/24_07_16/log/apache2/modsec_audit.log:GET /pdf.php?module=1&pdf=../../../../../../../../.
./../../../../etc/passwd%00 HTTP/1.1
```

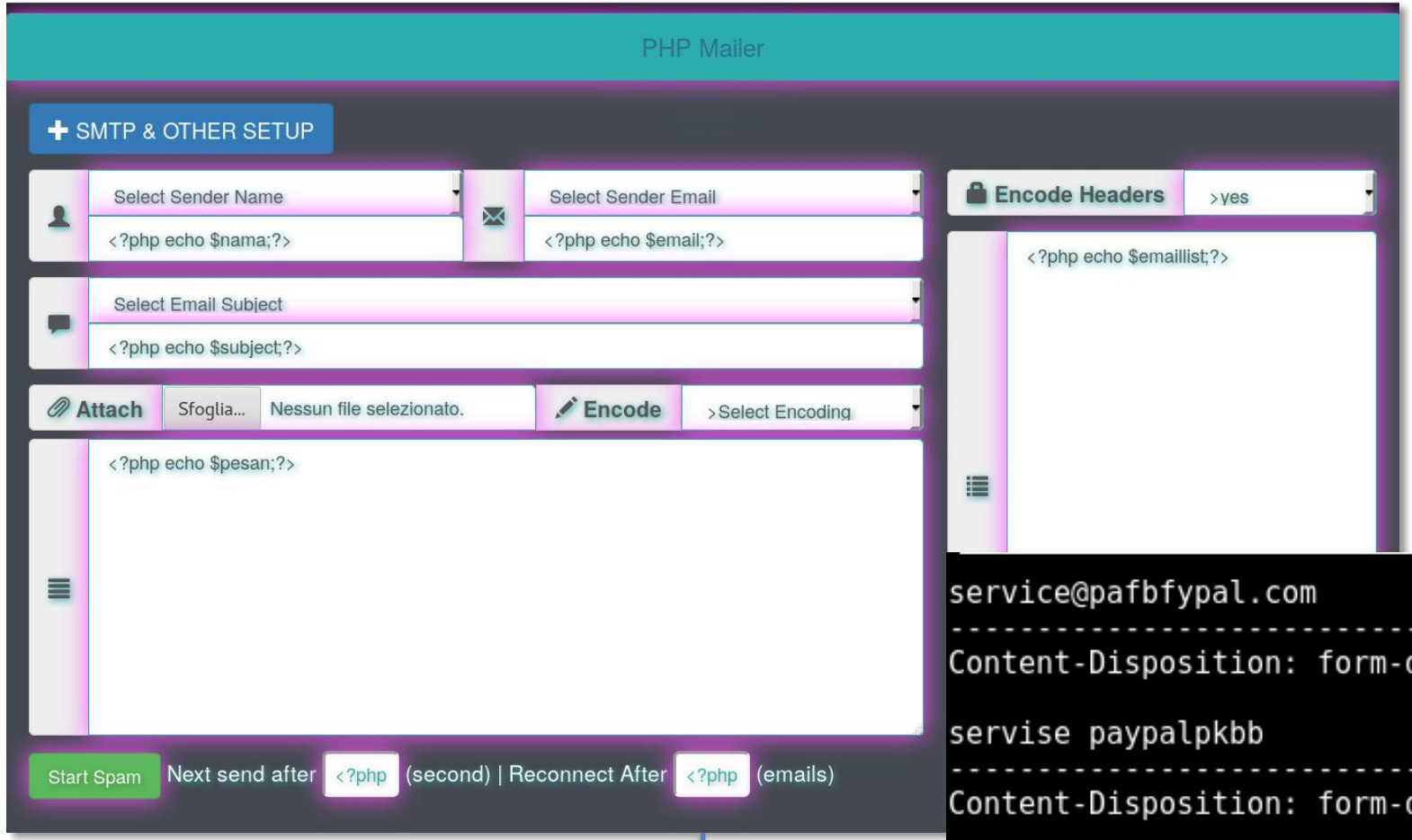
Password-protected Shells

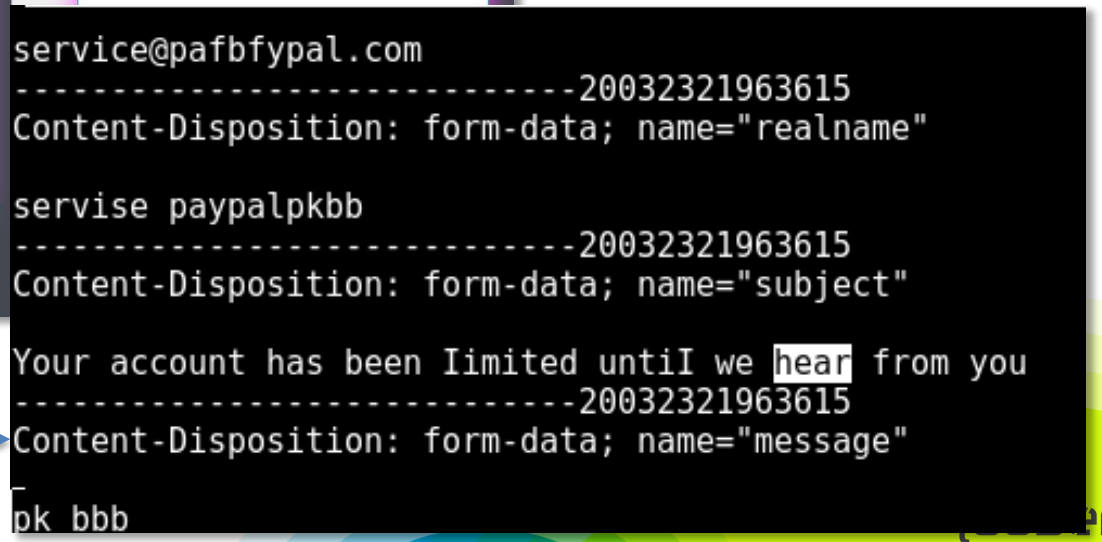
```
//PASSWORD CONFIGURATION

@$pass = $_POST['pass'];
$chk_login = true;
$password = "ha   i";

//END CONFIGURATION

if($pass == $password)
{
 $_SESSION['nst'] = "$pass";
}

if($chk_login == true)
{
 if(!isset($_SESSION['nst']) or $_SESSION['nst'] != $password)
 {
 die("
```

Smart use of Obfuscation

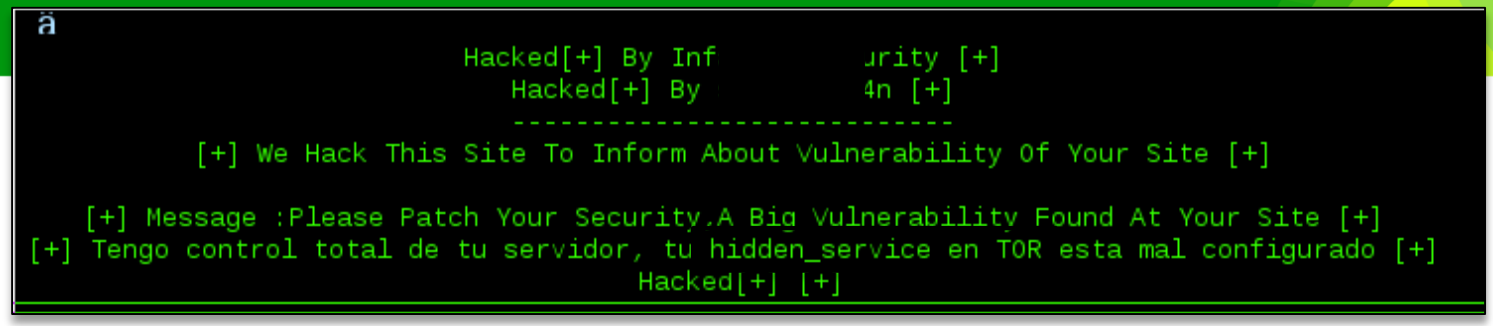
Abuse of Tor for Anonymized Attacks

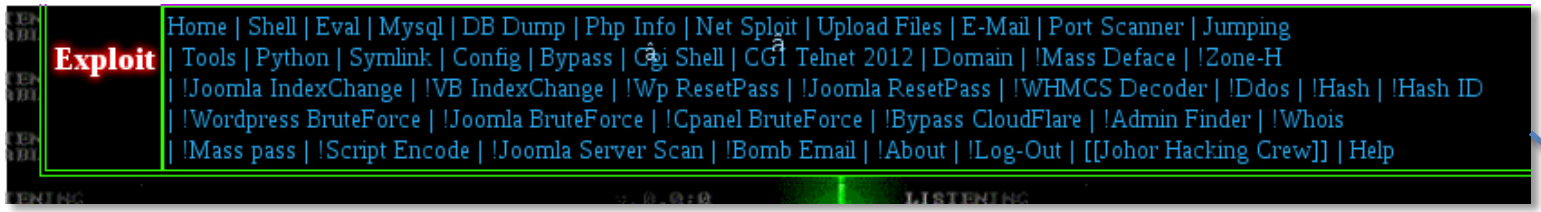
(Anonymized) Phishing Campaign



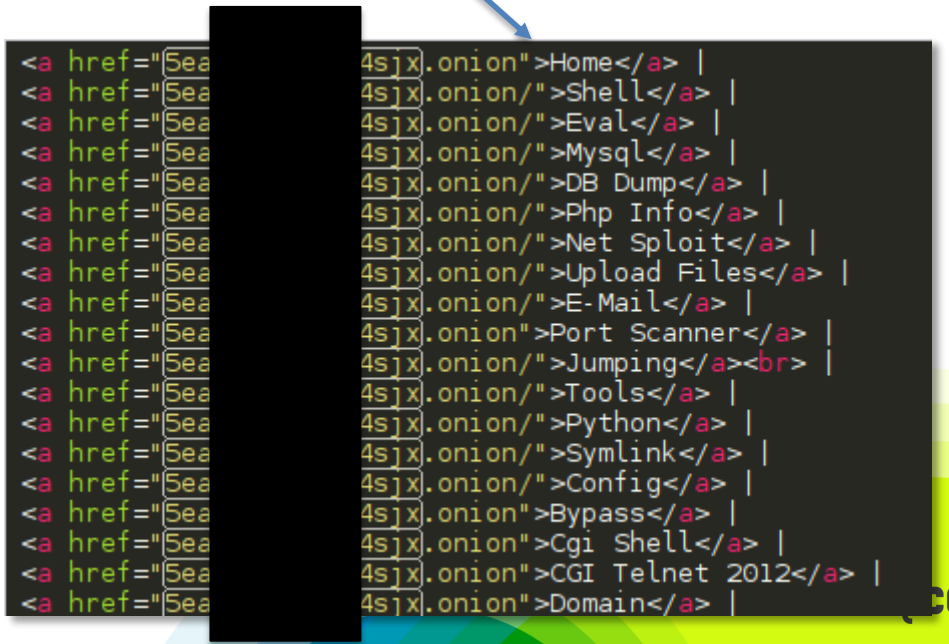


Rival Gangs



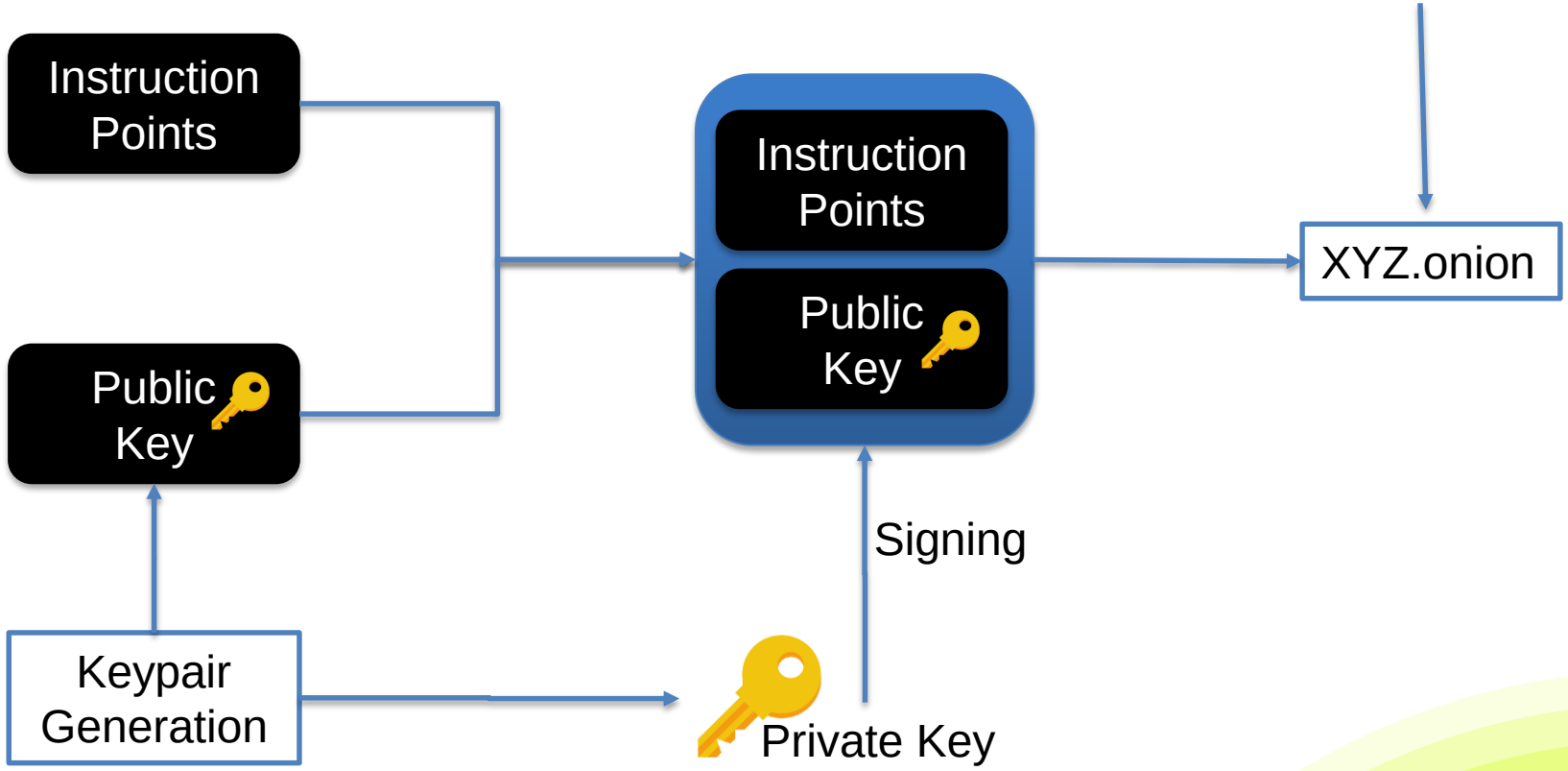


- Cyber-criminal gangs compromising opponents
- Self-promoting their "business"



(TOR Keys)

- Used to compute the *hidden service descriptor*



HS’ Private Key theft

```
[21/Aug/2016:20:58:29 +0200] "GET /private_key HTTP/1.1" 200 1096 "-" "Go 1.1 package http"
[22/Aug/2016:07:03:01 +0200] "GET /private_key HTTP/1.1" 200 1096 "-" "curl/7.47.0"
[22/Aug/2016:20:50:22 +0200] "GET /private_key HTTP/1.1" 200 1096 "-" "Go 1.1 package http"
- [22/Aug/2016:06:51:40 +0200] "GET /private_key HTTP/1.1" 200 1096 "-" "Go 1.1 package http"
[22/Jan/2017:14:11:51 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[22/Jan/2017:14:21:28 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[22/Jan/2017:14:26:57 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[22/Jan/2017:14:49:18 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[23/Jan/2017:22:00:16 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[24/Jan/2017:15:01:53 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[24/Jan/2017:18:11:35 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
[24/Jan/2017:18:12:46 +0100] "GET /private_key HTTP/1.1" 200 1151 "-" "Mozilla/5.0 (X11; Ubuntu;
[24/Jan/2017:18:17:28 +0100] "GET /private_key HTTP/1.1" 200 1095 "-" "Mozilla/5.0 (Windows NT 6.
```

- 400+ attacks
- MiTM, hijack and decryption

Lessons Learned

- Dark Web as “corner case” of the Internet… NO!

- Active and Dynamic Underground Market
- Motivated and Knowledgeable Attackers
- Manual and Targeted Attacks
- Modern and Sophisticated Threats

*With the cooperation of Mayra Rosario and Vincenzo Ciancaglini

Thank You!

Dr. Marco Balduzzi*
Senior Researcher at Trend Micro
http://www.madlab.it @embyte

{codemotion}