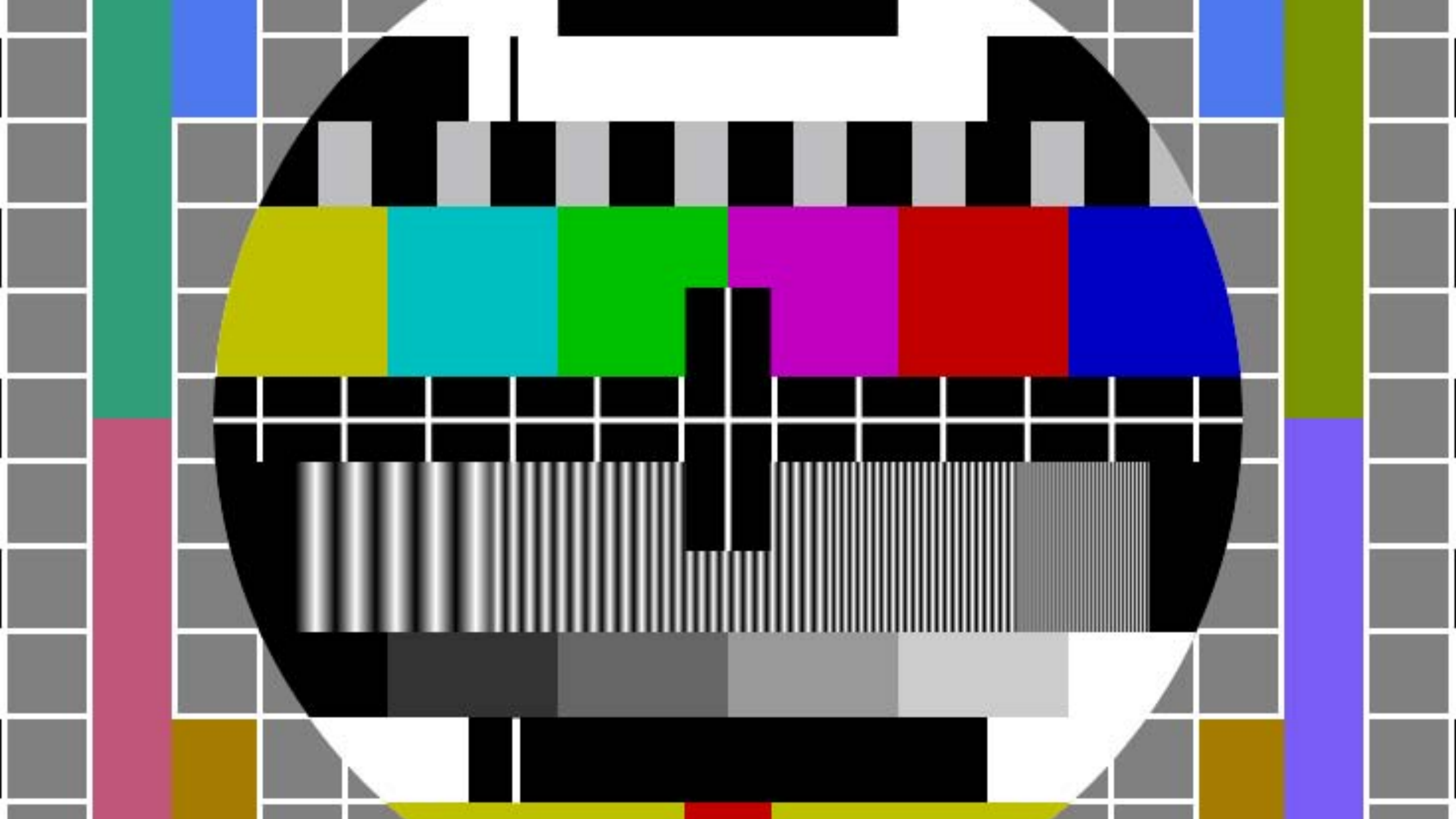


Hunting Malware Like a Sir

mlw.re

50 SHADES OF CRIMEWARE

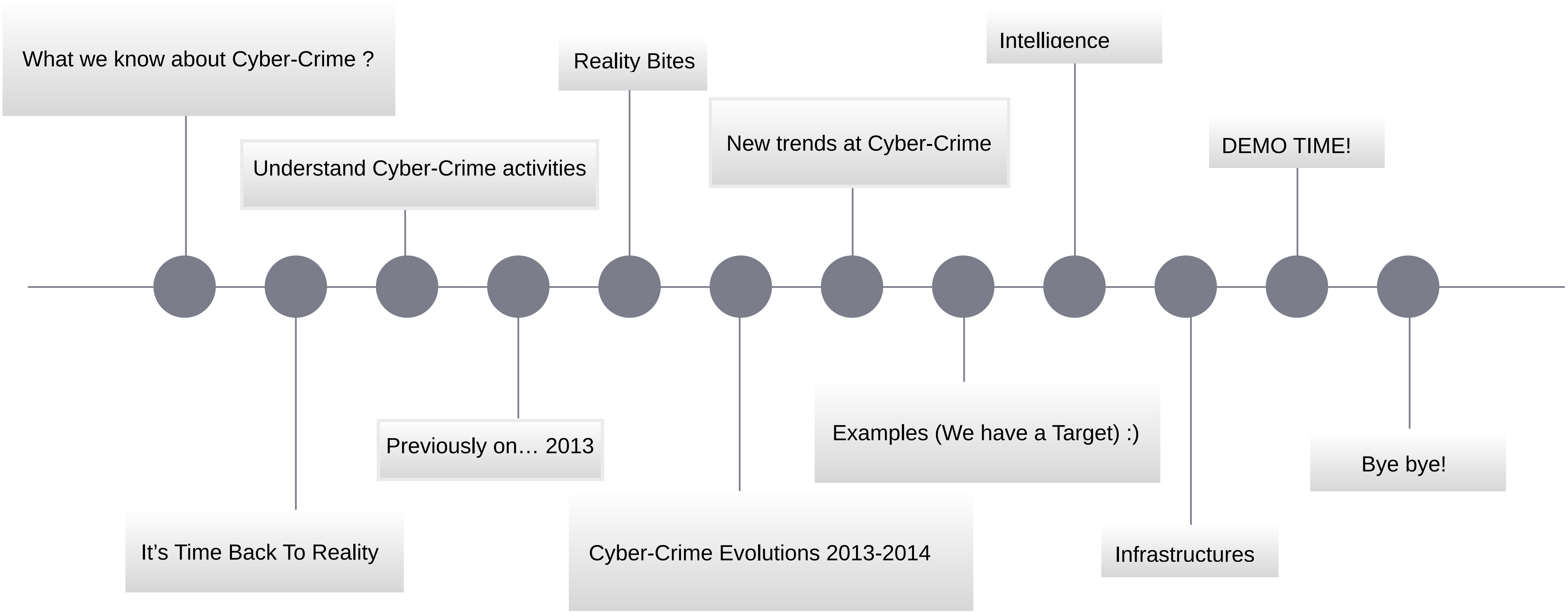
Manu Quintans // Frank Ruiz

ABOUT US

Frank Ruiz - Threat Intelligence Analyst at **Fox IT y miembro de la organización sin animo de lucro mlw.re.**

Manu Quintans - Threat Intelligence Manager at Buguroo / Deloitte, miembro fundador de la organización sin anímo de lucro **mlw.re** focalizada en combatir amenazas en Internet.

Index



What we know about Cyber-Crime ?

It's Time Back To Reality

Understand Cyber-Crime activities

Previously on… 2013

Reality Bites

Cyber-Crime Evolutions 2013-2014

New trends at Cyber-Crime

Examples (We have a Target) :)

Intelligence

Infrastructures

DEMO TIME!

Bye bye!

Hunting Malware Like a Sir

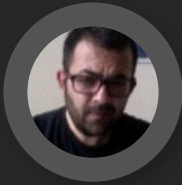
mlw.re

WHAT WE KNOW ABOUT **CYBER-CRIME?**

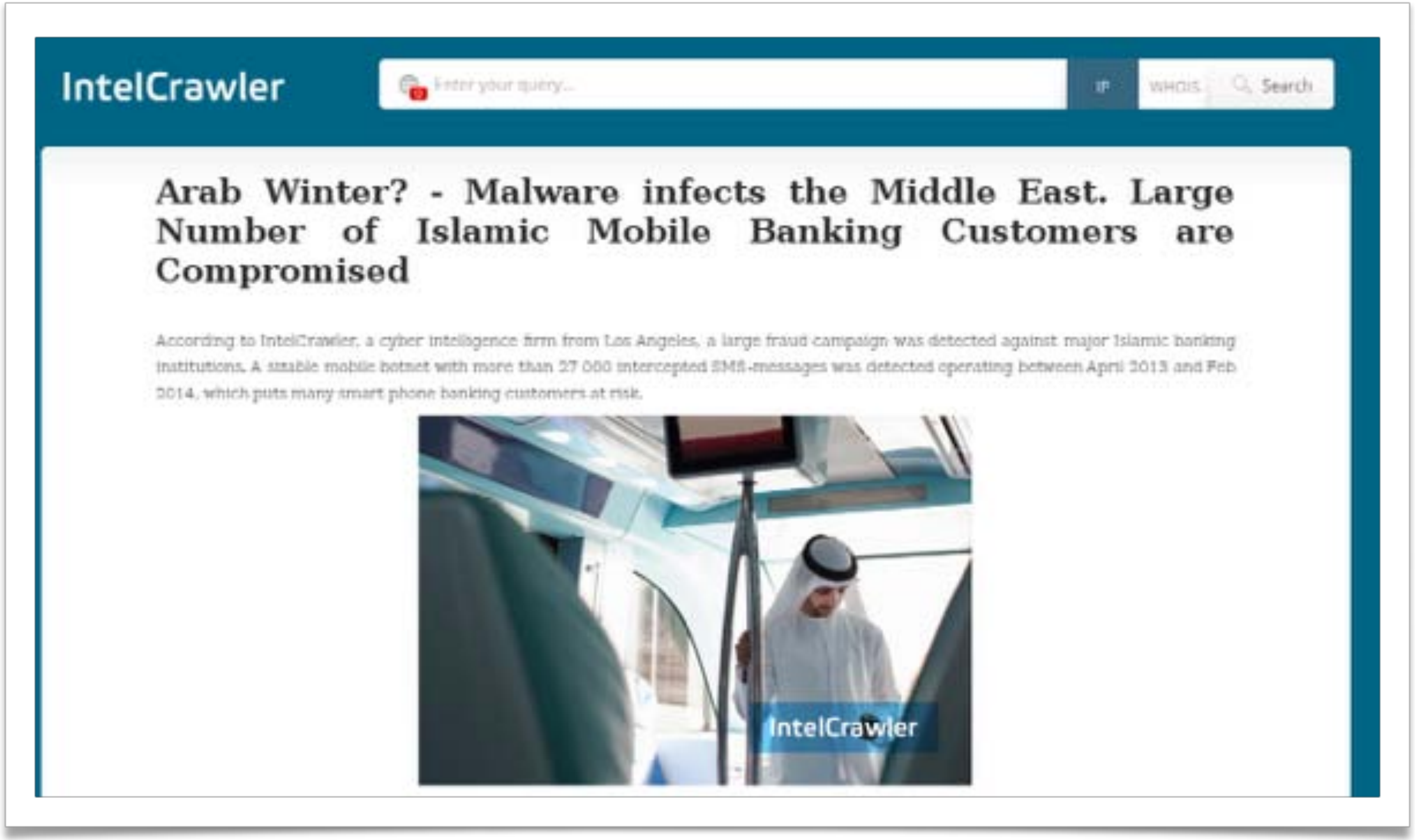
Conventions

ciber-. 1. Elemento compositivo prefijo, creado por acortamiento del adjetivo **cibernético**, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la r**ealidad virtual.**

SEÑORA! Soy un T800, he venido del futuro a robarle la tarjeta monedero….



WHAT WE KNOW ABOUT CYBER-CRIME?



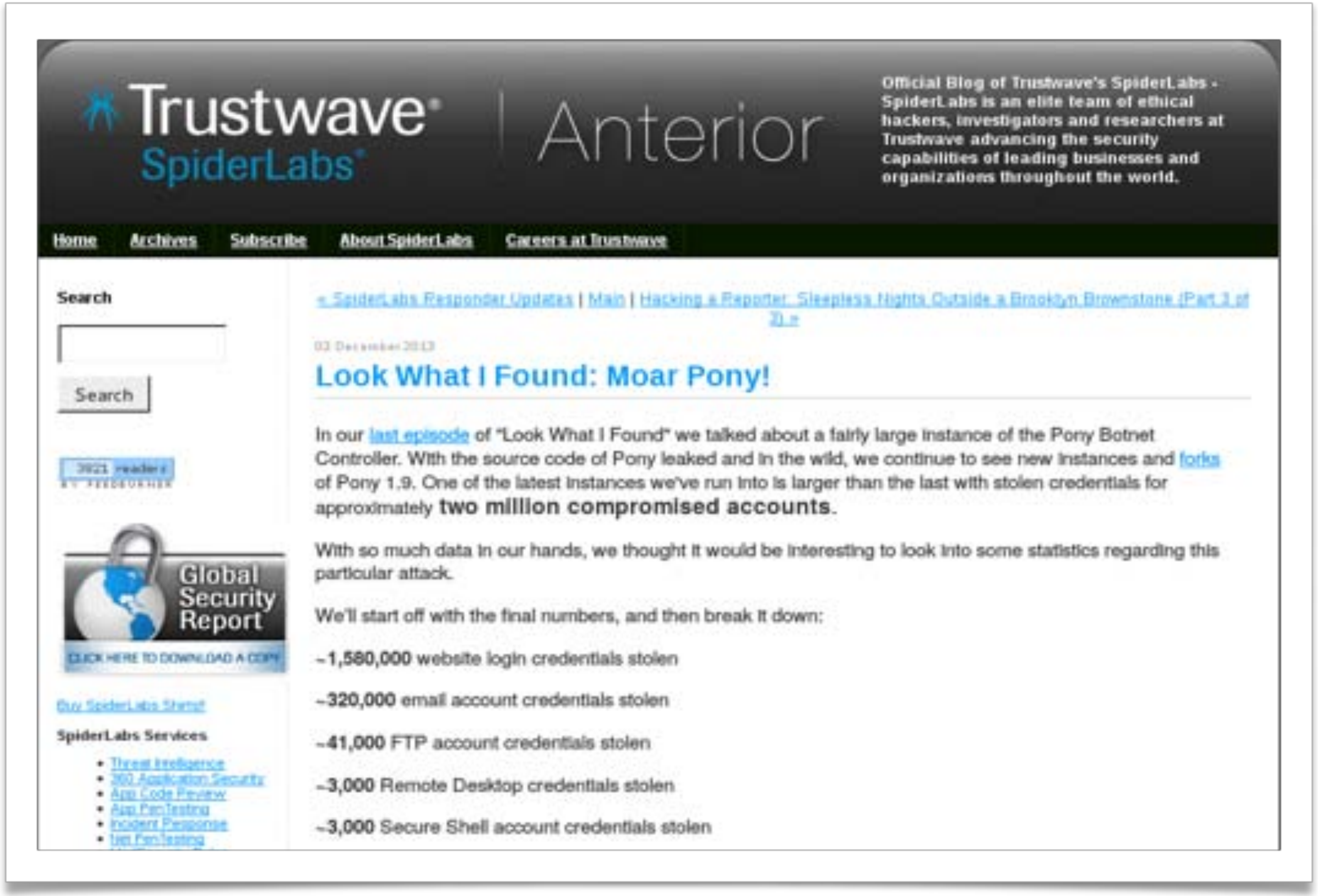
Arab Winter? - Malware infects the Middle East. Large Number of Islamic Mobile Banking Customers are Compromised

According to IntelCrawler, a cyber intelligence firm from Los Angeles, a large fraud campaign was detected against major Islamic banking institutions. A sizable mobile botnet with more than 27 000 intercepted SMS-messages was detected operating between April 2013 and Feb 2014, which puts many smart phone banking customers at risk.

ARAB WINTER

27.000 SMS INTERCEPTADOS

WHAT WE KNOW ABOUT CYBER-CRIME?



Trustwave SpiderLabs | Anterior

Official Blog of Trustwave's SpiderLabs - SpiderLabs is an elite team of ethical hackers, investigators and researchers at Trustwave advancing the security capabilities of leading businesses and organizations throughout the world.

Home | Archives | Subscribe | About SpiderLabs | Careers at Trustwave

Search

Search

3921 readers BY FEEDBURNER

Global Security Report

CLICK HERE TO DOWNLOAD A COPY

Buy SpiderLabs Shirts!

SpiderLabs Services

- Threat Intelligence
- 360 Application Security
- App Code Review
- App PenTesting
- Incident Response
- Net PenTesting

« SpiderLabs Responder Updates | Main | Hacking a Reporter: Sleepless Nights Outside a Brooklyn Brownstone (Part 3 of 3) »

03 December 2013

Look What I Found: Moar Pony!

In our last episode of "Look What I Found" we talked about a fairly large instance of the Pony Botnet Controller. With the source code of Pony leaked and in the wild, we continue to see new instances and forks of Pony 1.9. One of the latest instances we've run into is larger than the last with stolen credentials for approximately **two million compromised accounts.**

With so much data in our hands, we thought it would be interesting to look into some statistics regarding this particular attack.

We'll start off with the final numbers, and then break it down:

~**1,580,000** website login credentials stolen

~**320,000** email account credentials stolen

~**41,000** FTP account credentials stolen

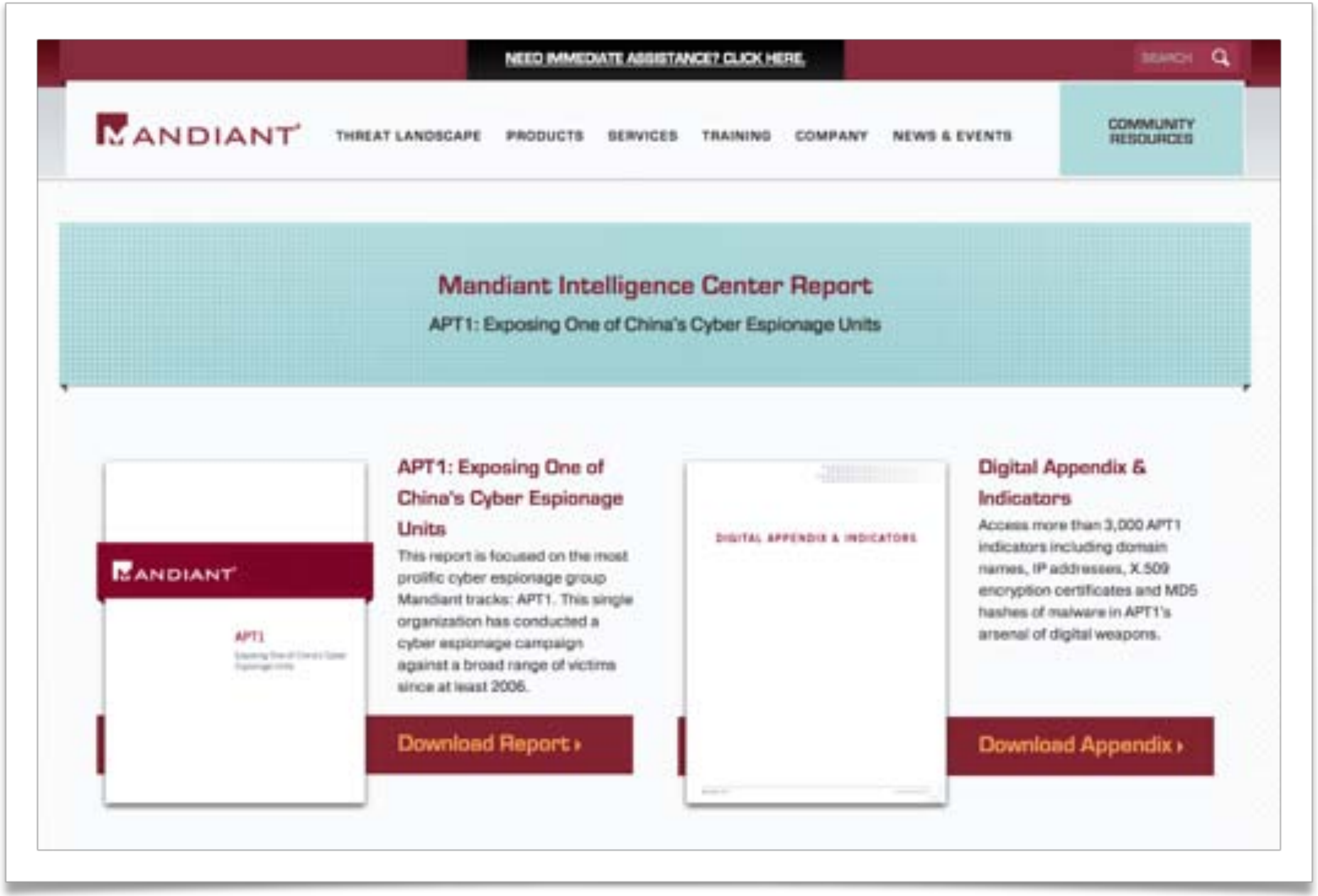
~**3,000** Remote Desktop credentials stolen

~**3,000** Secure Shell account credentials stolen

MOAR PONY!

- **1.580,00 WEBSITE LOGIN CREDENTIALS**
- **320,000 EMAIL ACCOUNTS**
- **41,000 FTP ACCOUNT CREDENTIALS**
- **3.000 RDP**
- **3.000 SSH ACCESS**

WHAT WE KNOW ABOUT CYBER-CRIME?



Mandiant Intelligence Center Report

APT1: Exposing One of China's Cyber Espionage Units

APT1: Exposing One of China's Cyber Espionage Units

This report is focused on the most prolific cyber espionage group Mandiant tracks: APT1. This single organization has conducted a cyber espionage campaign against a broad range of victims since at least 2006.

Digital Appendix & Indicators

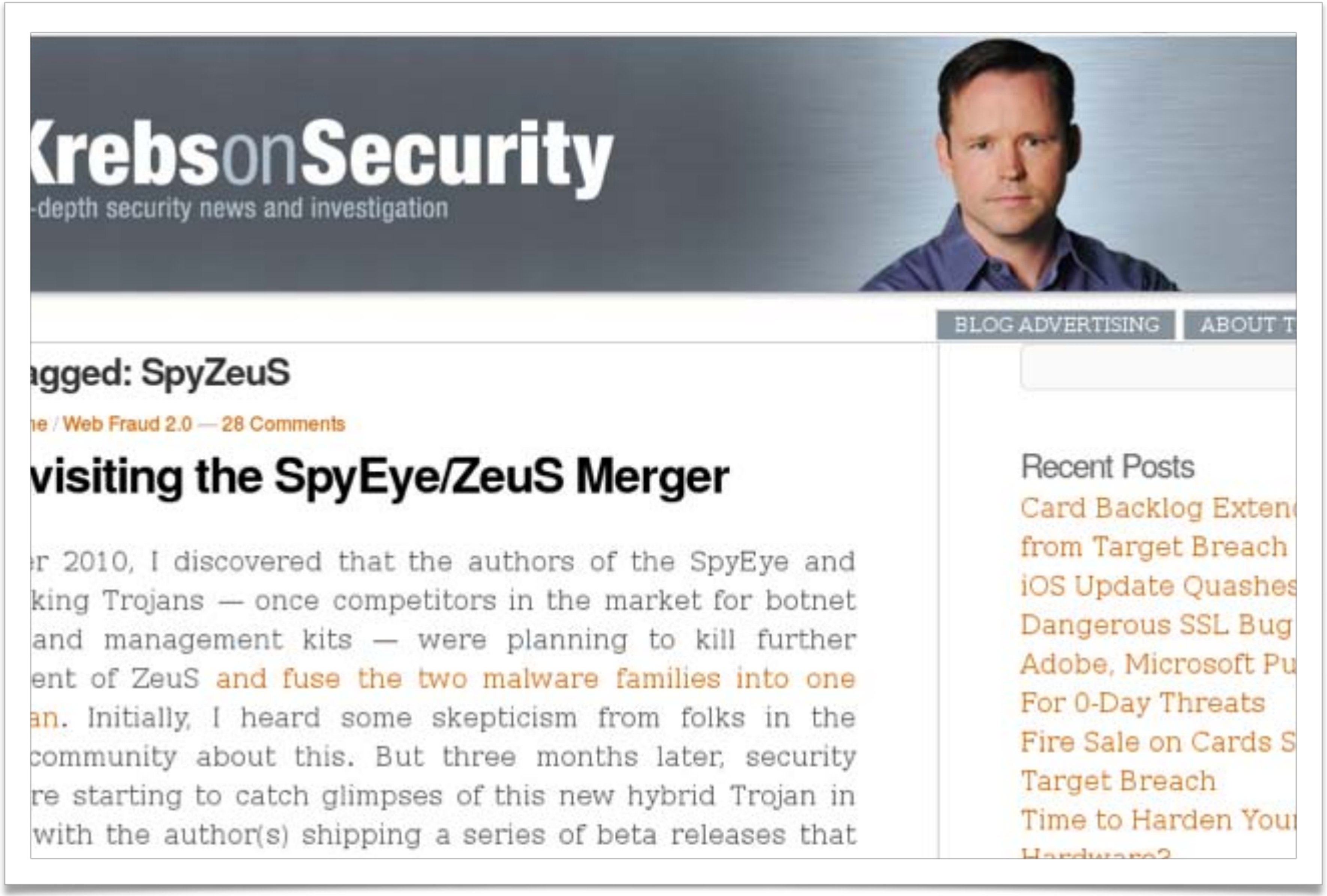
Access more than 3,000 APT1 indicators including domain names, IP addresses, X.509 encryption certificates and MD5 hashes of malware in APT1's arsenal of digital weapons.

APT1

- Obama runs first law about cybersecurity.
- CISPA (Cyber Intelligence Sharing and Protection Act) is runing again
- Mandiant, presents at RSA Conference new SOC.

Securestate talk at 2005 about this group and there tools…

WHAT WE KNOW ABOUT CYBER-CRIME?



agged: SpyZeuS

e / Web Fraud 2.0 — 28 Comments

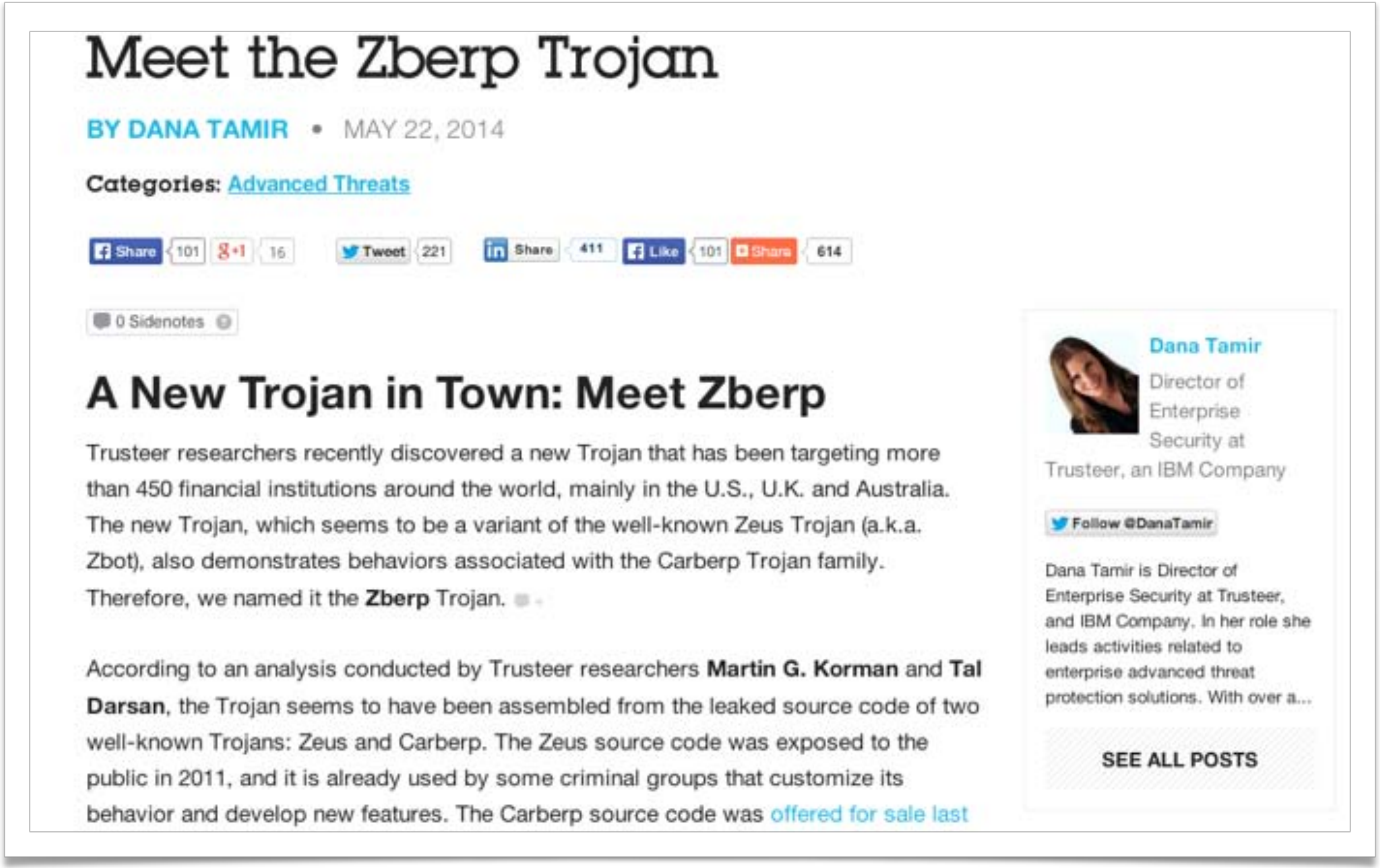
visiting the SpyEye/ZeuS Merger

r 2010, I discovered that the authors of the SpyEye and king Trojans — once competitors in the market for botnet and management kits — were planning to kill further ent of ZeuS and fuse the two malware families into one an. Initially, I heard some skepticism from folks in the community about this. But three months later, security re starting to catch glimpses of this new hybrid Trojan in with the author(s) shipping a series of beta releases that

Recent Posts

- Card Backlog Exten from Target Breach
- iOS Update Quashes Dangerous SSL Bug
- Adobe, Microsoft Pu For 0-Day Threats
- Fire Sale on Cards S Target Breach
- Time to Harden You Hardware?

WHAT WE KNOW ABOUT CYBER-CRIME?



Meet the Zberp Trojan

BY DANA TAMIR • MAY 22, 2014

Categories: Advanced Threats

A New Trojan in Town: Meet Zberp

Trusteer researchers recently discovered a new Trojan that has been targeting more than 450 financial institutions around the world, mainly in the U.S., U.K. and Australia. The new Trojan, which seems to be a variant of the well-known Zeus Trojan (a.k.a. Zbot), also demonstrates behaviors associated with the Carberp Trojan family. Therefore, we named it the **Zberp** Trojan.

According to an analysis conducted by Trusteer researchers **Martin G. Korman** and **Tal Darsan**, the Trojan seems to have been assembled from the leaked source code of two well-known Trojans: Zeus and Carberp. The Zeus source code was exposed to the public in 2011, and it is already used by some criminal groups that customize its behavior and develop new features. The Carberp source code was offered for sale last

Dana Tamir

Director of Enterprise Security at Trusteer, an IBM Company

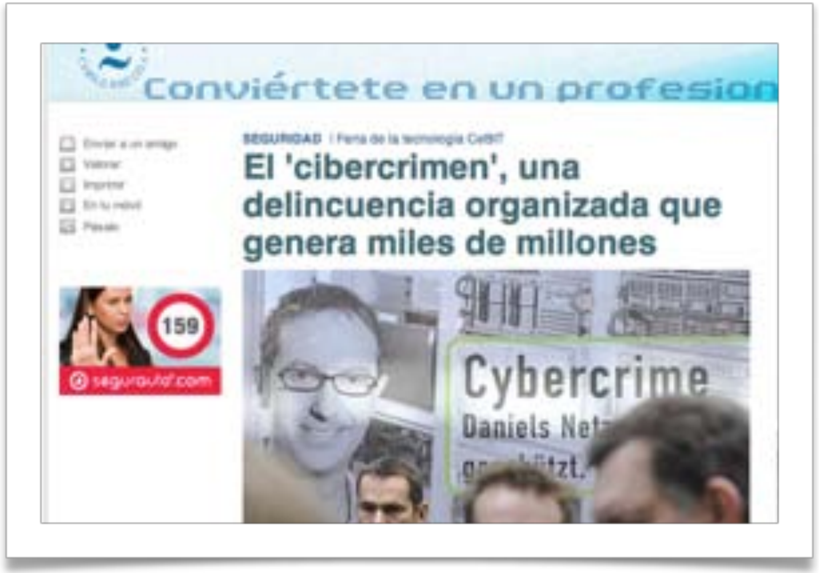
Dana Tamir is Director of Enterprise Security at Trusteer, and IBM Company. In her role she leads activities related to enterprise advanced threat protection solutions. With over a...

Hunting Malware Like a Sir

mlw.re

It’s time back to **“reality”**

It’s time back to “reality”

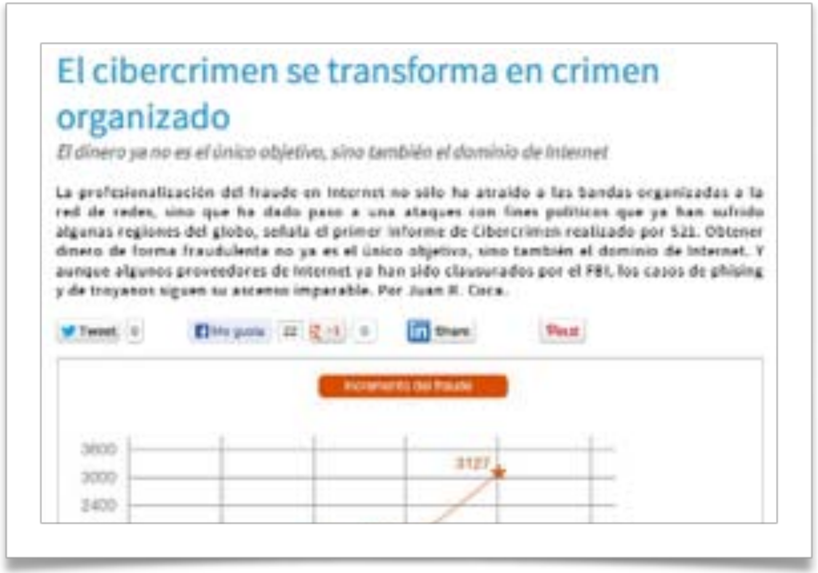


Conviértete en un profesion

□ Enviar a un amigo
□ Valorar
□ Imprimir
□ En tu móvil
□ Pásalo

SEGURIDAD | Feria de la tecnología CeBIT

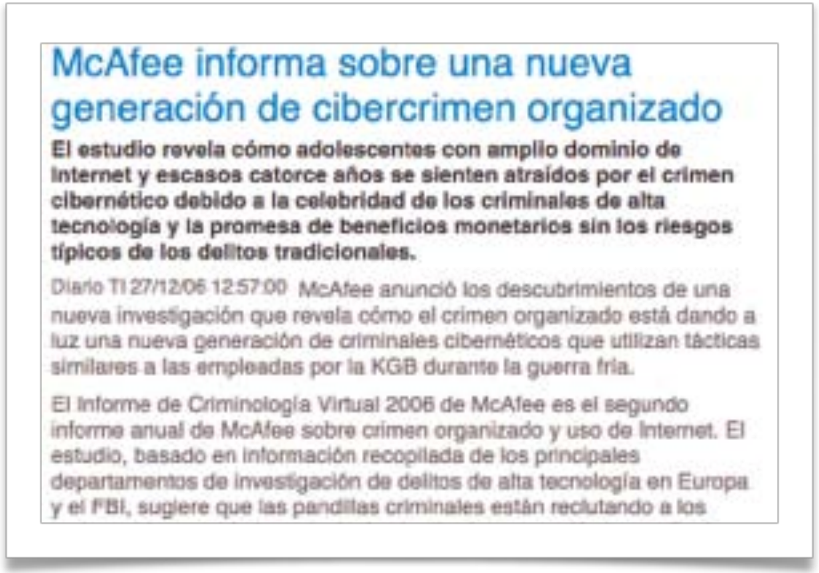
El 'cibercrimen', una delincuencia organizada que genera miles de millones



El cibercrimen se transforma en crimen organizado

El dinero ya no es el único objetivo, sino también el dominio de Internet

La profesionalización del fraude en Internet no sólo ha atraído a las bandas organizadas a la red de redes, sino que ha dado paso a una ataques con fines políticos que ya han sufrido algunas regiones del globo, señala el primer Informe de Cibercrimen realizado por S21. Obtener dinero de forma fraudulenta no ya es el único objetivo, sino también el dominio de Internet. Y aunque algunos proveedores de Internet ya han sido clausurados por el FBI, los casos de phising y de troyanos siguen su ascenso imparable. Por Juan R. Coca.



McAfee informa sobre una nueva generación de cibercrimen organizado

El estudio revela cómo adolescentes con amplio dominio de Internet y escasos catorce años se sienten atraídos por el crimen cibernético debido a la celebridad de los criminales de alta tecnología y la promesa de beneficios monetarios sin los riesgos típicos de los delitos tradicionales.

Diario TI 27/12/06 12:57:00 McAfee anunció los descubrimientos de una nueva investigación que revela cómo el crimen organizado está dando a luz una nueva generación de criminales cibernéticos que utilizan tácticas similares a las empleadas por la KGB durante la guerra fría.

El Informe de Criminología Virtual 2006 de McAfee es el segundo informe anual de McAfee sobre crimen organizado y uso de Internet. El estudio, basado en información recopilada de los principales departamentos de investigación de delitos de alta tecnología en Europa y el FBI, sugiere que las pandillas criminales están reclutando a los

It’s time back to “reality”

It’s time back to “reality”

DOC! TENEMOS QUE VOLVER AL PASADO!
Y EVITAR QUE LOS PADRES DE BRIAN KREBS SE CONOZCAN!
TOWN
GUATERMARQ

Hunting Malware Like a Sir

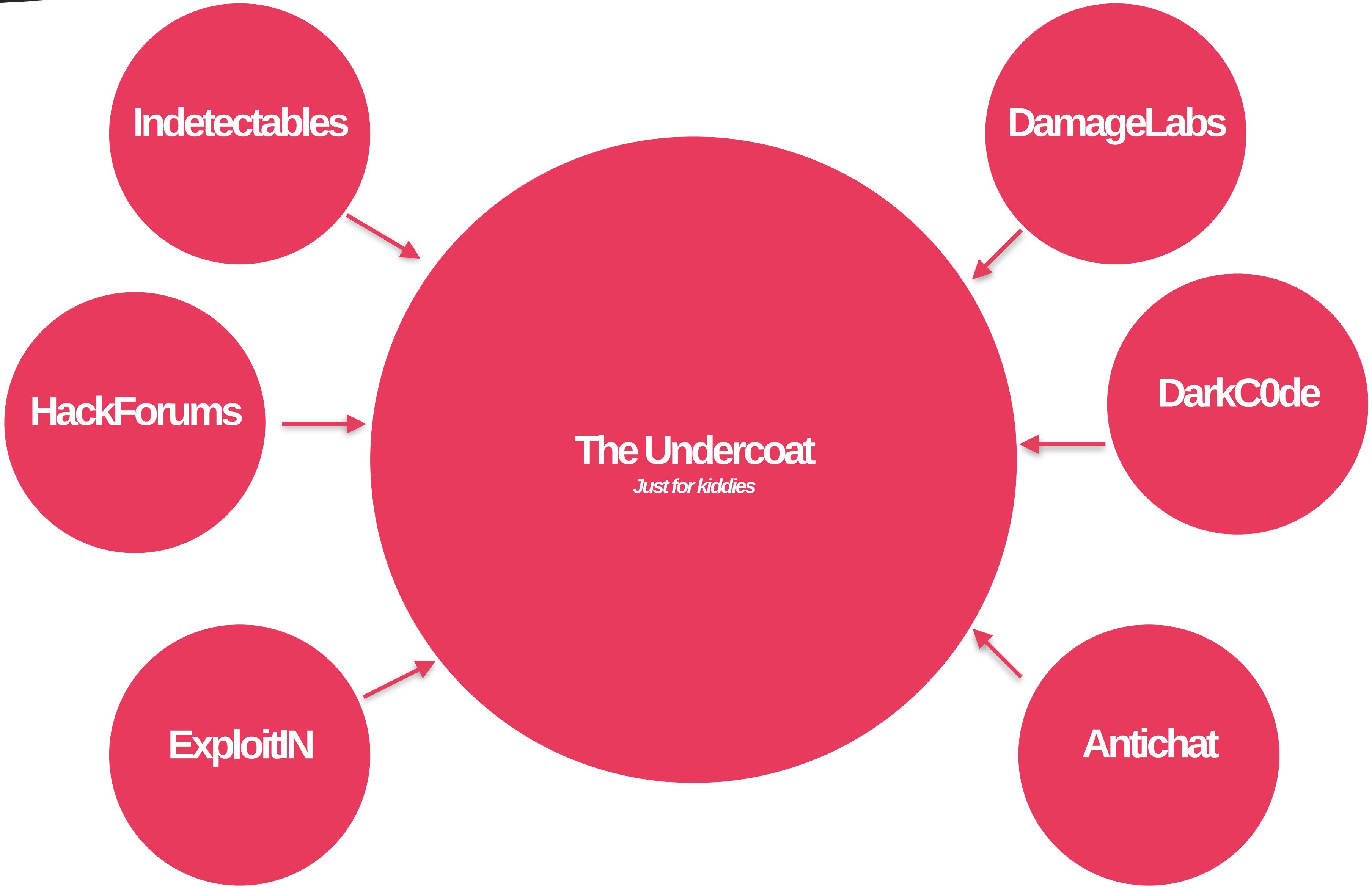
mlw.re

Understand

Cyber-Crime activities

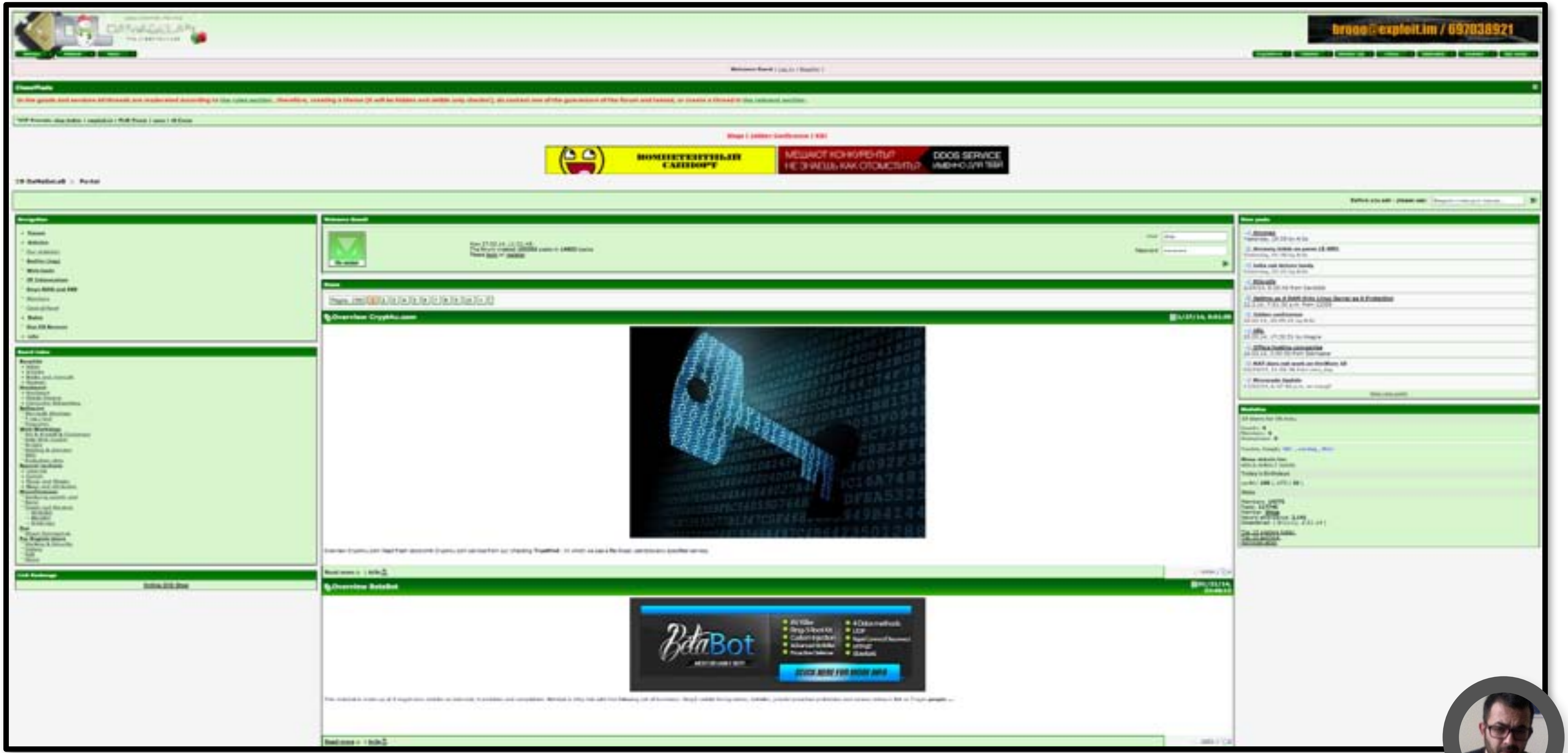
Understand Cyber-Crime activities

LAYER #1



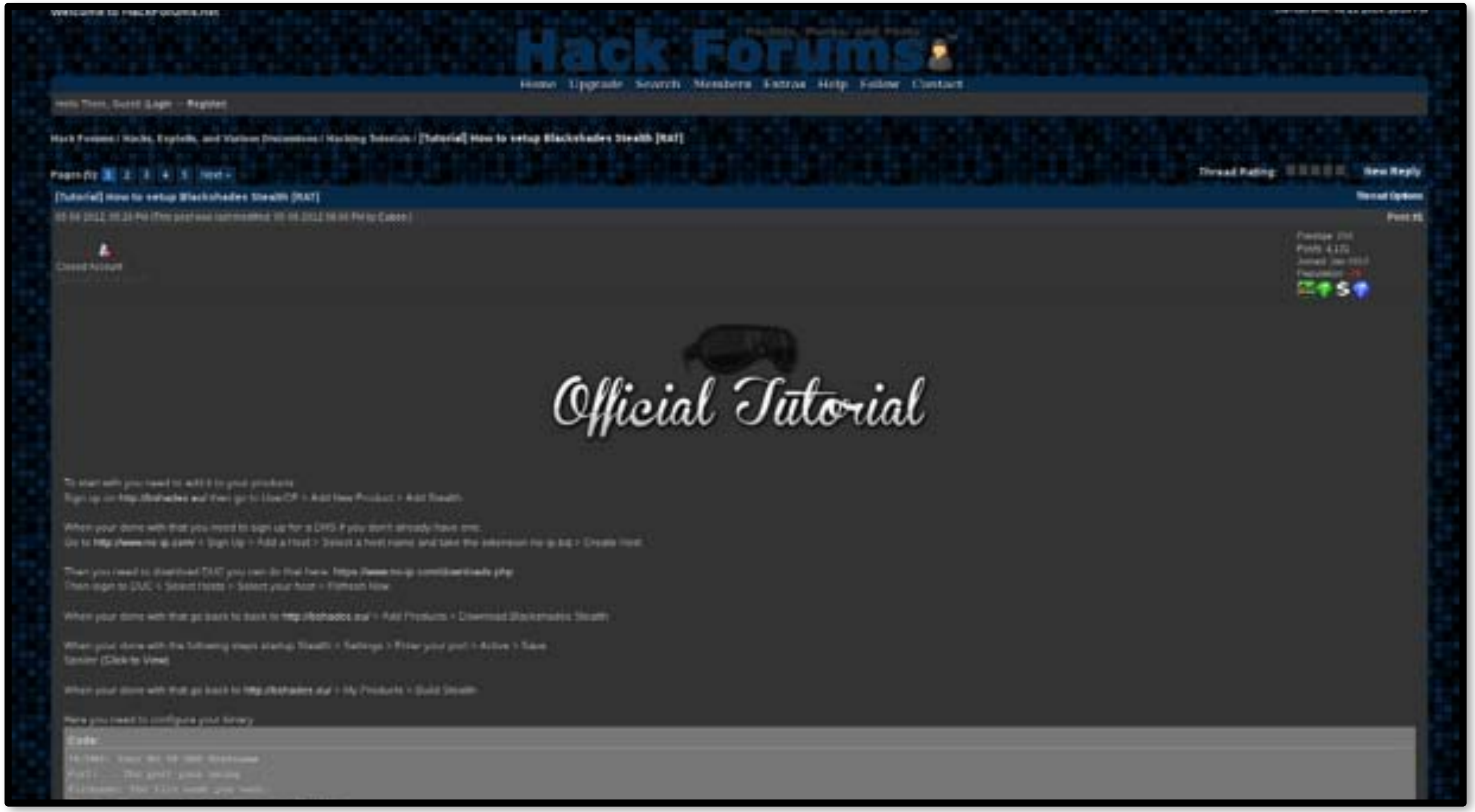
Understand Cyber-Crime activities

LAYER #1



Understand Cyber-Crime activities

LAYER #1



Welcome to HackForums.net

Hack Forums

Home Upgrade Search Members Extras Help Follow Contact

Hello There, Guest (Login — Register)

Hack Forums / Hacks, Exploits, and Various Discussions / Hacking Tutorials / [Tutorial] How to setup Blackshades Stealth [RAT]

Pages (5): 1 2 3 4 5 Next »

Thread Rating: New Reply

[Tutorial] How to setup Blackshades Stealth [RAT] Thread Options

05-04-2012, 05:25 PM (This post was last modified: 05-06-2012 08:00 PM by Cubon.) Post: #1

Closed Account

Prestige: [illegible]
Posts: [illegible]
Joined: [illegible]
Reputation: [illegible]

Official Tutorial

To start with you need to add it to your products
Sign up on http://bshades.eu/ then go to UserCP > Add New Product > Add Stealth

When your done with that you need to sign up for a DNS if you don't already have one.
Go to http://www.no-ip.com/ > Sign Up > Add a Host > Select a host name and take the extension no-ip.biz > Create Host

Then you need to download DUC you can do that here: https://www.no-ip.com/downloads.php
Then login to DUC > Select Hosts > Select your host > Refresh Now

When your done with that go back to back to http://bshades.eu/ > Add Products > Download Blackshades Stealth

When your done with the following steps startup Stealth > Settings > Enter your port > Active > Save
Spoiler (Click to View)

When your done with that go back to http://bshades.eu/ > My Products > Build Stealth

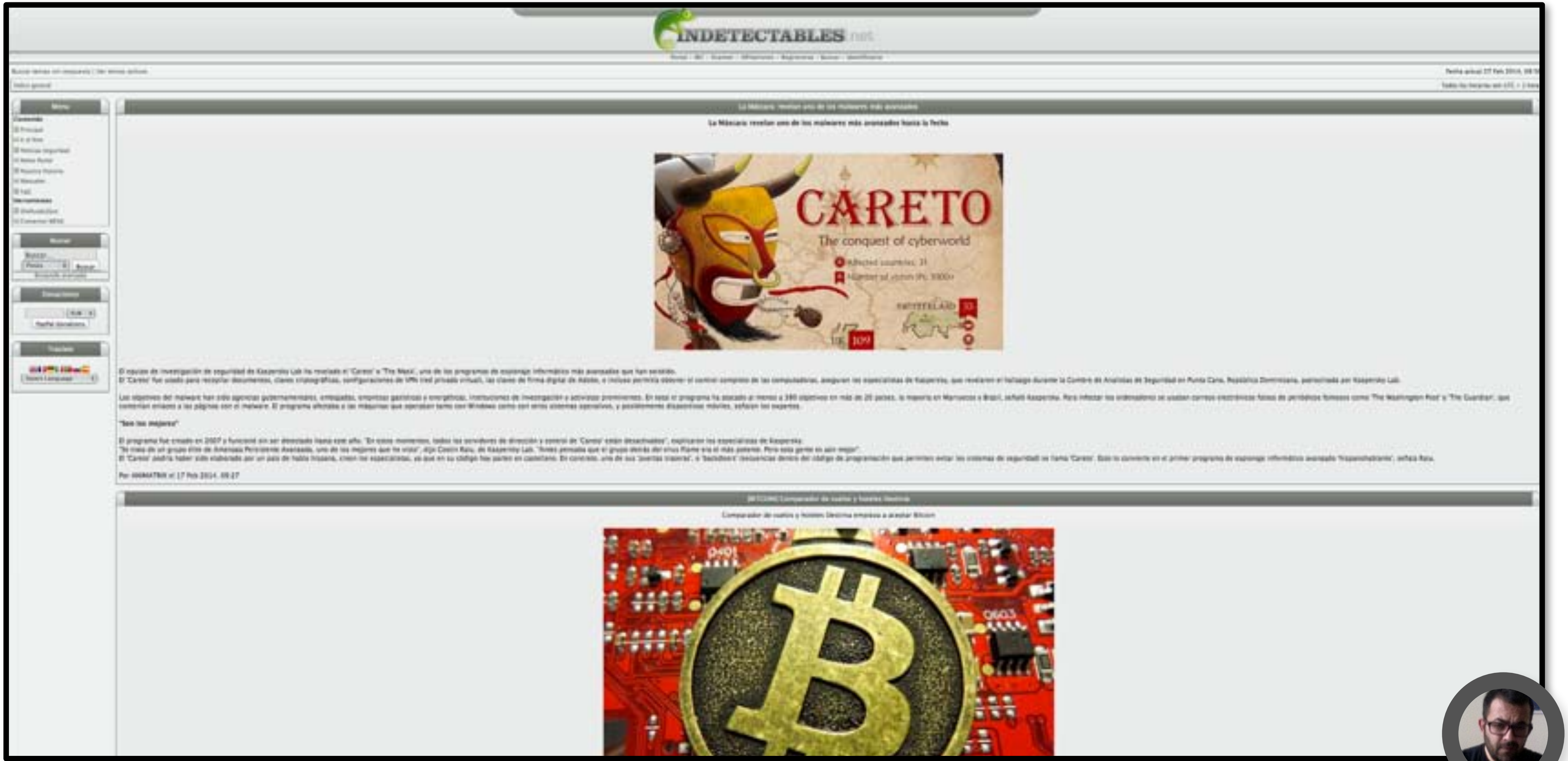
Here you need to configure your binary

Code:

```
IP/DNS: Your no-ip DNS Hostname
Port:    The port you setup
Filename: The file name you want...
```

Understand Cyber-Crime activities

LAYER #1



INDETECTABLES.net

La Máscara: revelan uno de los malwares más avanzados

La Máscara revelan uno de los malwares más avanzados hasta la fecha

El equipo de investigación de seguridad de Kaspersky Lab ha revelado el 'Careto' o 'The Mask', uno de los programas de espionaje informático más avanzados que han existido. [illegible]

[illegible]

"Son los mejores"

[illegible]

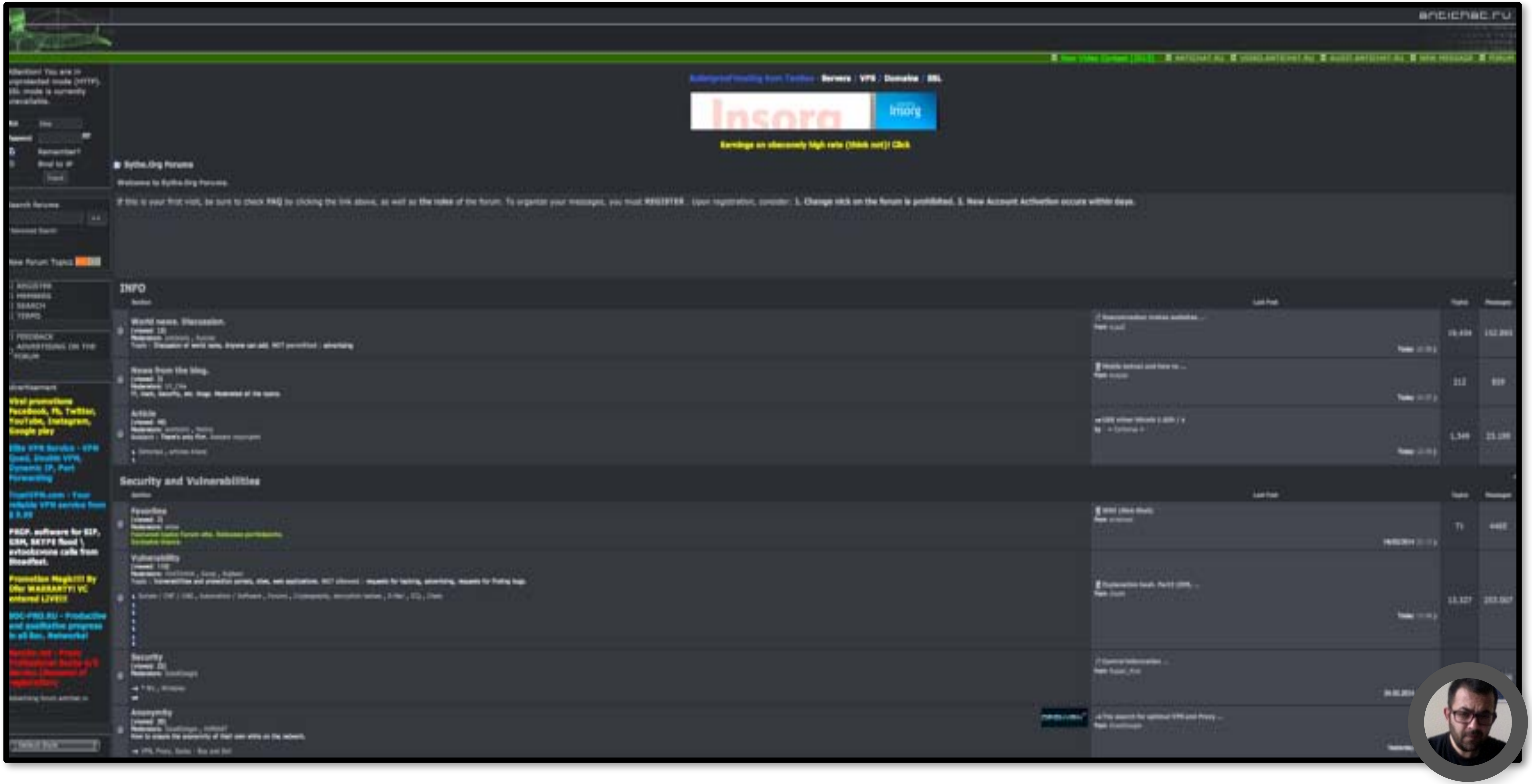
Por [illegible] el 17 Feb 2014, 09:27

BITCOINS Comparador de vuelos y hoteles Destinia

Comparador de vuelos y hoteles Destinia empieza a aceptar Bitcoin

Understand Cyber-Crime activities

LAYER #1



anticnat.ru

Servers | VPS | Domains | SSL

Earnings on obscenely high rate (think not)! Click

Sythe.Org Forums

Welcome to Sythe.Org Forums.

If this is your first visit, be sure to check FAQ by clicking the link above, as well as the rules of the forum. To organize your messages, you must REGISTER . Upon registration, consider: 1. Change nick on the forum is prohibited. 2. New Account Activation occurs within days.

Attention! You are in unprotected mode (HTTP). SSL mode is currently unavailable.

Remember?

Search forums

New Forum Topics

REGISTER
MEMBERS
SEARCH
TERMS

FEEDBACK
ADVERTISING ON THE FORUM

Advertisement

Viral promotions Facebook, fb, Twitter, YouTube, Instagram, Google play

PROF. software for SIP, GSM, SKYPE flood \ avtoobzvona calls from Bloodfast.

Promotion Magik!!! By Offer WARRANTY! VC entered LIVE!!!

INFO

World news. Discussion.

News from the blog.

Article

Security and Vulnerabilities

Favorites

Vulnerability

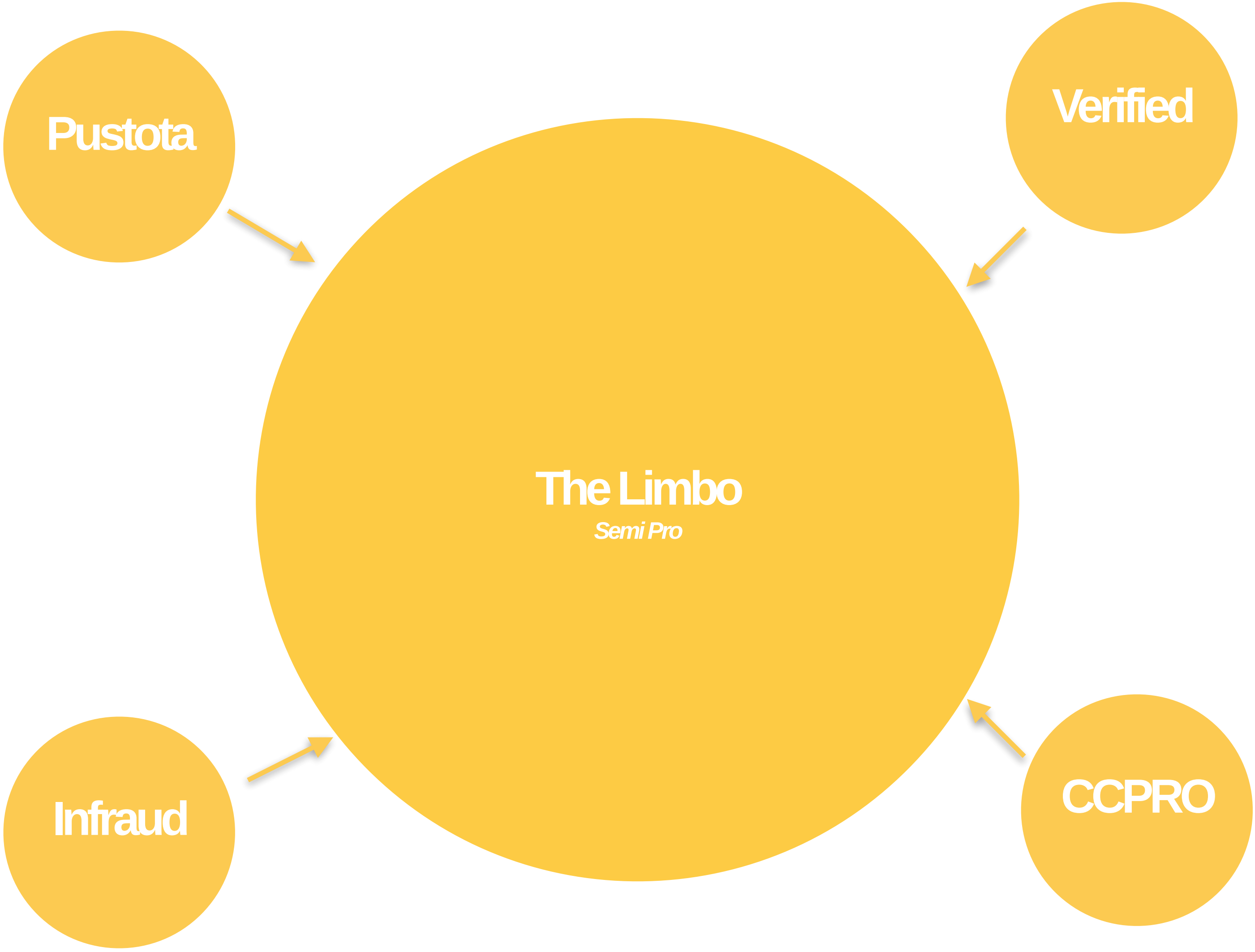
Security

Anonymity

How to ensure the anonymity of their own entity on the network.

Understand Cyber-Crime activities

LAYER #2



Pustota

Verified

The Limbo

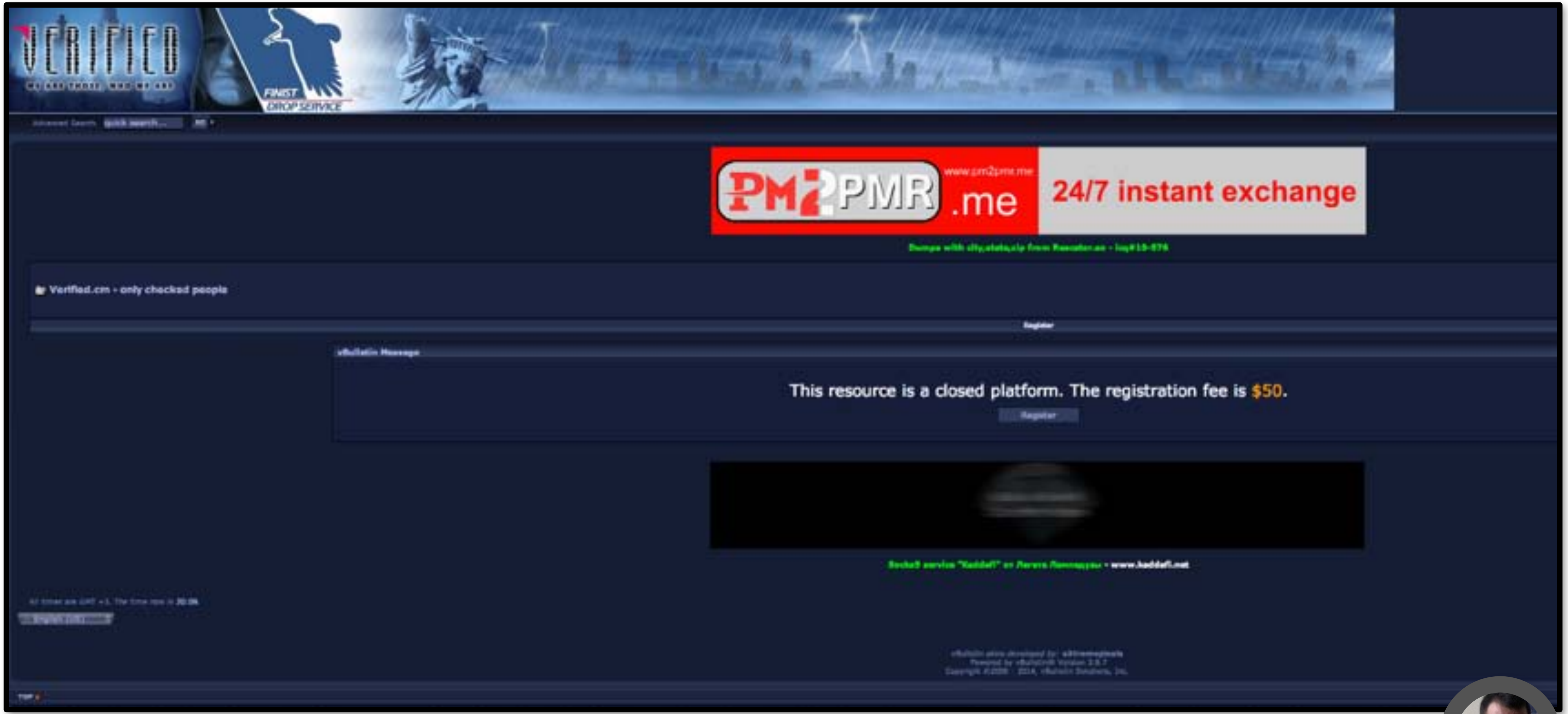
Semi Pro

Infraud

CCPRO

Understand Cyber-Crime activities

LAYER #2



Dumps with city,state,zip from Rescator.so - log#13-876

Verified.cm - only checked people

Register

vBulletin Message

This resource is a closed platform. The registration fee is $50.

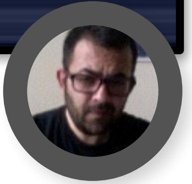
Register

Socks5 service "Kaddafi" on [illegible] - www.kaddafi.net

All times are GMT +3. The time now is 20:06.

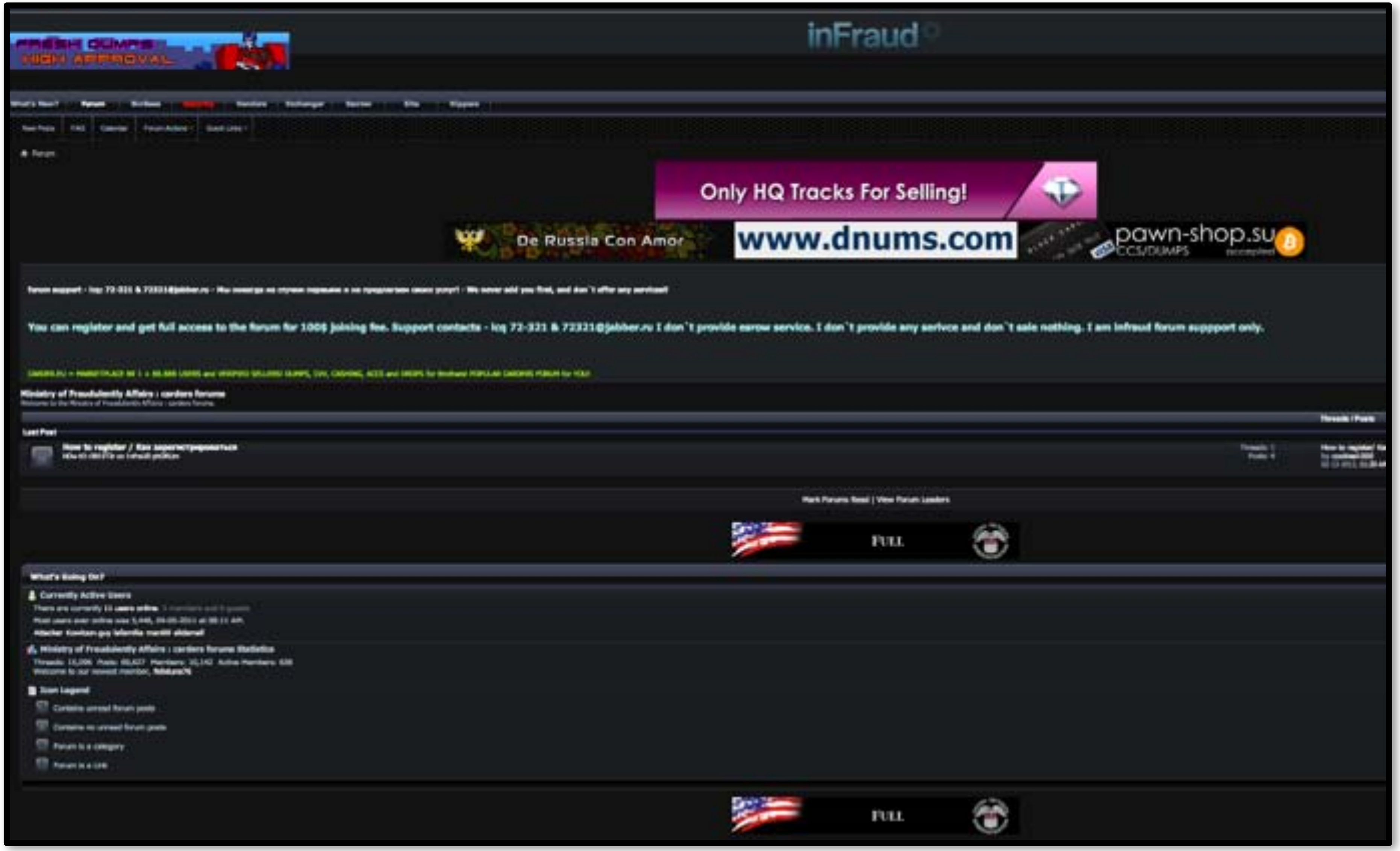
vBulletin skins developed by: [illegible]
Powered by vBulletin® Version 3.8.7
Copyright ©2000 - 2014, vBulletin Solutions, Inc.

TOP



Understand Cyber-Crime activities

LAYER #2


FRESH DUMPS HIGH APPROVAL
inFraud
What's New? Forum [illegible]
New Posts FAQ Calendar Forum Actions Quick Links
Forum
Only HQ Tracks For Selling!
De Russia Con Amor
www.dnums.com
pawn-shop.su CCS/DUMPS
FULL

Forum support - Icq 72-321 & 72321@jabber.ru - [illegible] - We never add you first, and don`t offer any services!

You can register and get full access to the forum for 100$ joining fee. Support contacts - Icq 72-321 & 72321@jabber.ru I don`t provide escrow service. I don`t provide any serivce and don`t sale nothing. I am infraud forum suppport only.

[illegible]

Ministry of Fraudulently Affairs : carders forums
Welcome to the Ministry of Fraudulently Affairs : carders forums.

Threads / Posts
Last Post

How to register / Как зарегистрироваться
[illegible]

Mark Forums Read | View Forum Leaders

What's Going On?

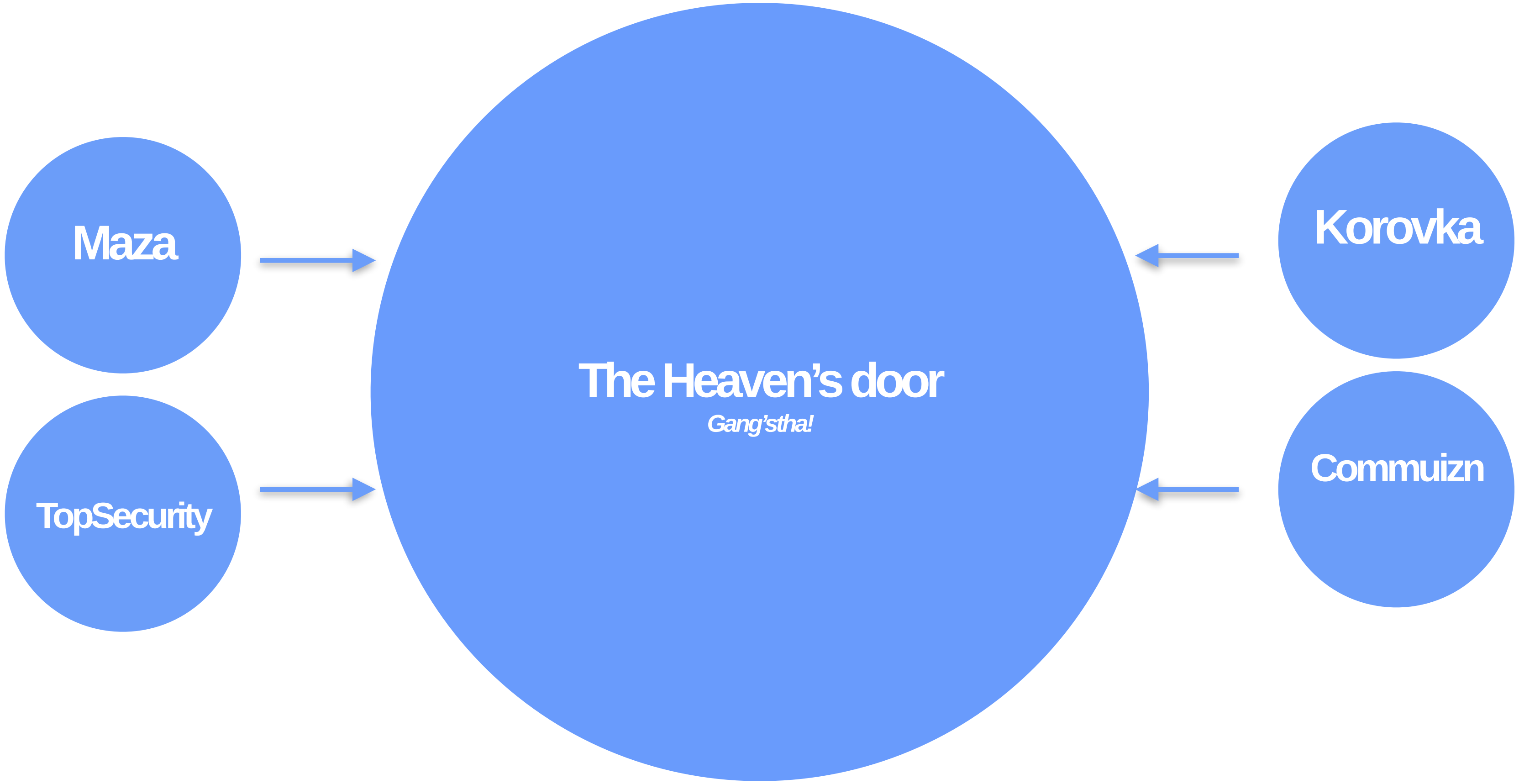
Currently Active Users
There are currently [illegible] users online. [illegible]
Most users ever online was [illegible]
[illegible]

Ministry of Fraudulently Affairs : carders forums Statistics
Threads: [illegible] Posts: [illegible] Members: [illegible] Active Members: [illegible]
Welcome to our newest member, [illegible]

Icon Legend
Contains unread forum posts
Contains no unread forum posts
Forum is a category
Forum is a Link

Understand Cyber-Crime activities

LAYER #3



Maza

TopSecurity

The Heaven’s door

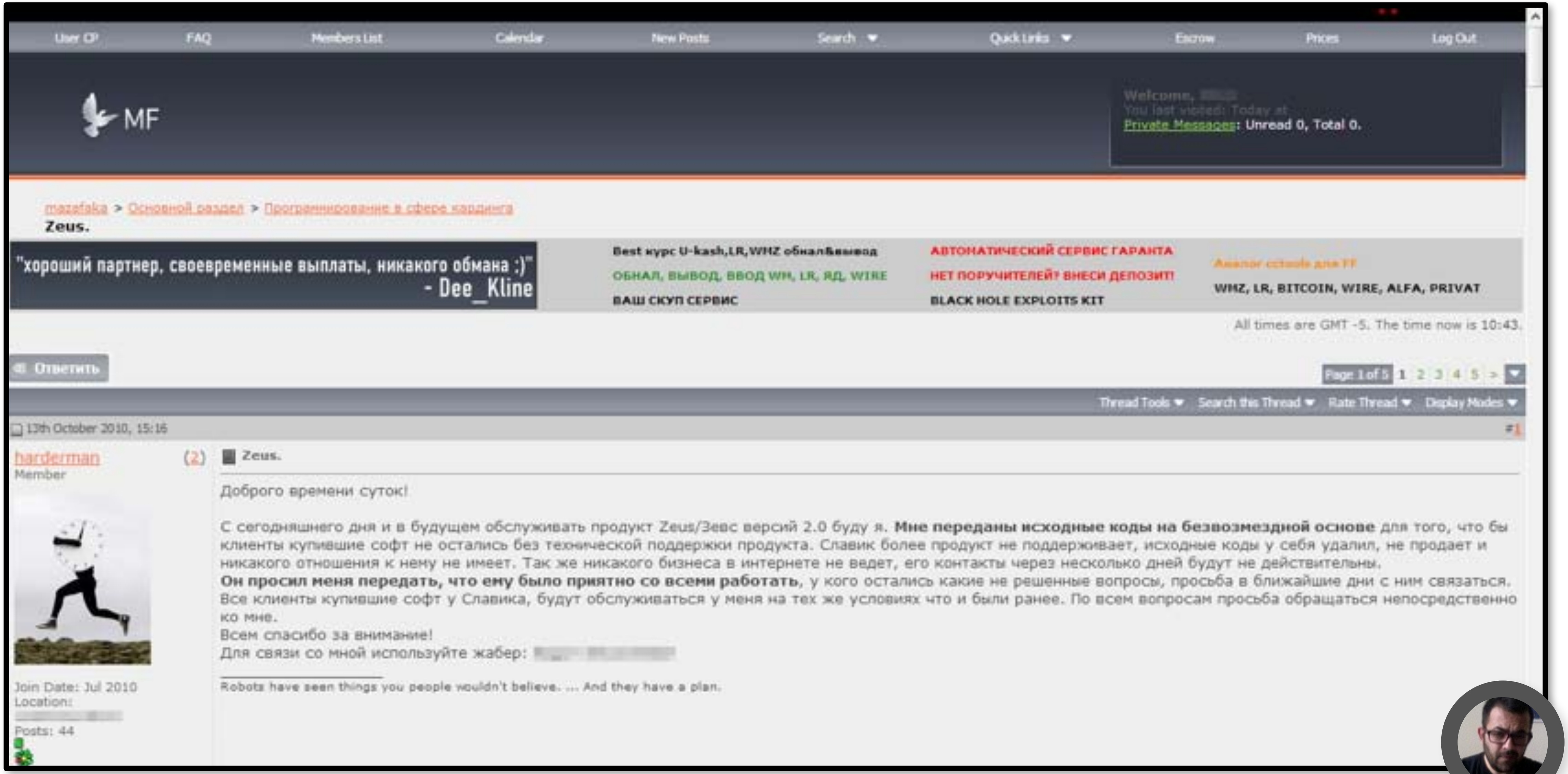
Gang’stha!

Korovka

Commuizn

Understand Cyber-Crime activities

LAYER #3



Welcome, [redacted]
You last visited: Today at
Private Messages: Unread 0, Total 0.

mazafaka > Основной раздел > Программирование в сфере кардинга
Zeus.

"хороший партнер, своевременные выплаты, никакого обмана :)"
- Dee_Kline

Best курс U-kash,LR,WMZ обнал&вывод
ОБНАЛ, ВЫВОД, ВВОД WM, LR, ЯД, WIRE
ВАШ СКУП СЕРВИС

АВТОМАТИЧЕСКИЙ СЕРВИС ГАРАНТА
НЕТ ПОРУЧИТЕЛЕЙ? ВНЕСИ ДЕПОЗИТ!
BLACK HOLE EXPLOITS KIT

Аналог cctools для FF
WMZ, LR, BITCOIN, WIRE, ALFA, PRIVAT

All times are GMT -5. The time now is 10:43.

13th October 2010, 15:16 #1

harderman (2)
Member

Join Date: Jul 2010
Location: [redacted]
Posts: 44

Zeus.

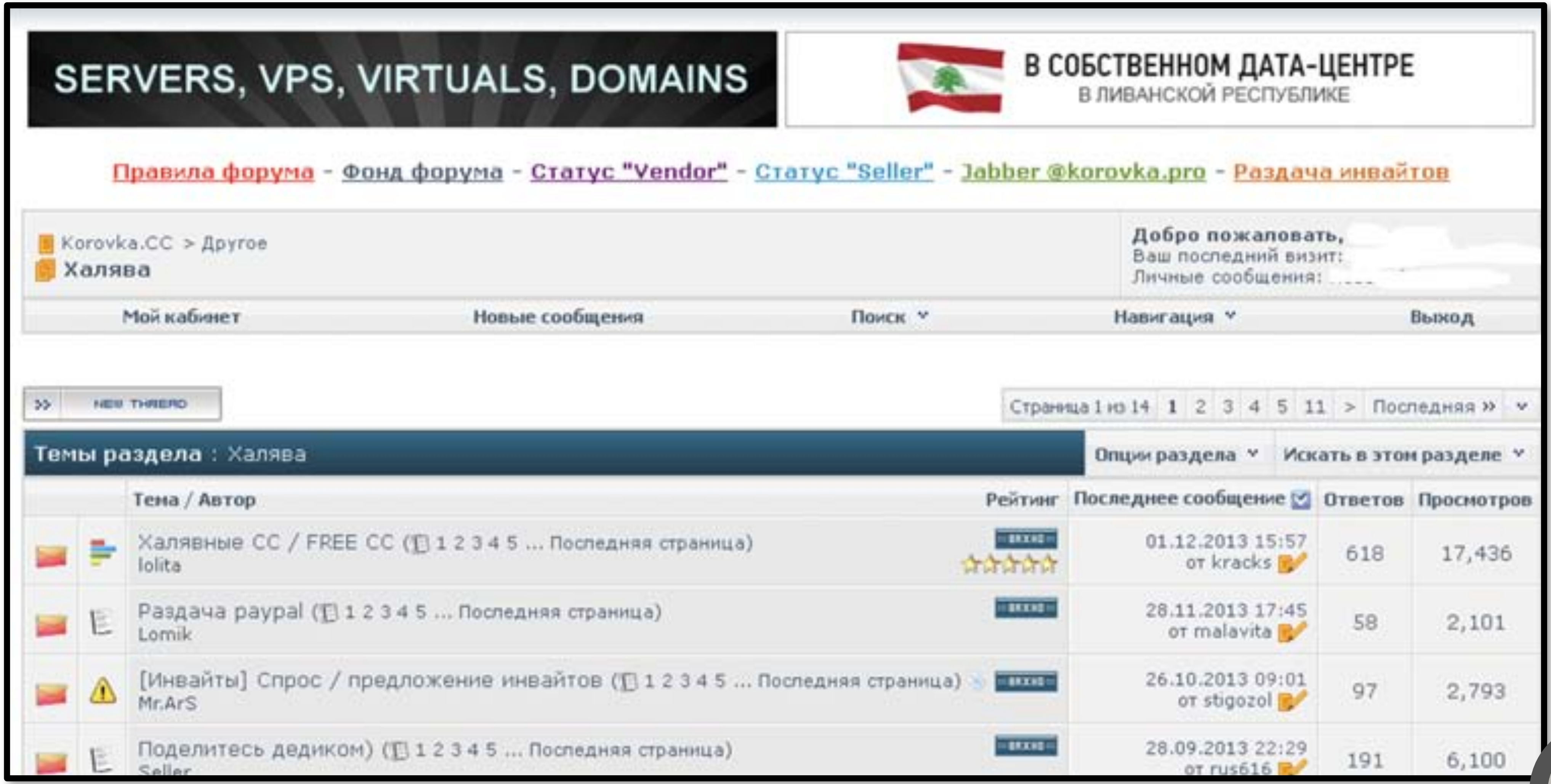
Доброго времени суток!

С сегодняшнего дня и в будущем обслуживать продукт Zeus/Зевс версий 2.0 буду я. **Мне переданы исходные коды на безвозмездной основе** для того, что бы клиенты купившие софт не остались без технической поддержки продукта. Славик более продукт не поддерживает, исходные коды у себя удалил, не продает и никакого отношения к нему не имеет. Так же никакого бизнеса в интернете не ведет, его контакты через несколько дней будут не действительны.
Он просил меня передать, что ему было приятно со всеми работать, у кого остались какие не решенные вопросы, просьба в ближайшие дни с ним связаться.
Все клиенты купившие софт у Славика, будут обслуживаться у меня на тех же условиях что и были ранее. По всем вопросам просьба обращаться непосредственно ко мне.
Всем спасибо за внимание!
Для связи со мной используйте жабер: [redacted]

Robots have seen things you people wouldn't believe. ... And they have a plan.

Understand Cyber-Crime activities

LAYER #3



SERVERS, VPS, VIRTUALS, DOMAINS

В СОБСТВЕННОМ ДАТА-ЦЕНТРЕ
В ЛИВАНСКОЙ РЕСПУБЛИКЕ

Правила форума - Фонд форума - Статус "Vendor" - Статус "Seller" - Jabber @korovka.pro - Раздача инвайтов

Korovka.CC > Другое
Халява

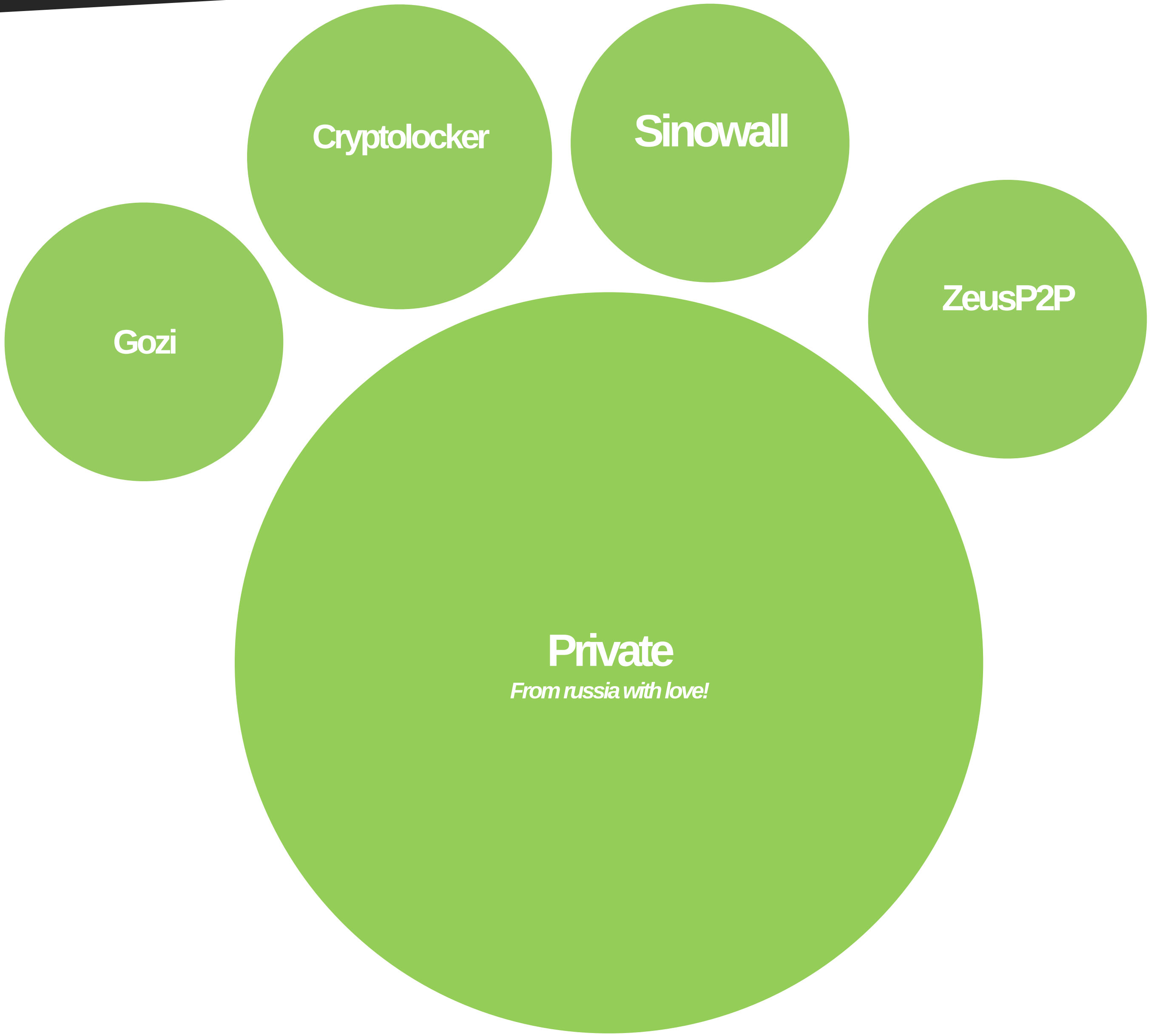
Добро пожаловать, [redacted]
Ваш последний визит:
Личные сообщения:

Темы раздела : Халява

Тема / Автор	Рейтинг	Последнее сообщение	Ответов	Просмотров
Халявные CC / FREE CC (1 2 3 4 5 ... Последняя страница) lolita	☆☆☆☆☆	01.12.2013 15:57 от kracks	618	17,436
Раздача paypal (1 2 3 4 5 ... Последняя страница) Lomik		28.11.2013 17:45 от malavita	58	2,101
[Инвайты] Спрос / предложение инвайтов (1 2 3 4 5 ... Последняя страница) Mr.ArS		26.10.2013 09:01 от stigozol	97	2,793
Поделитесь дедиком) (1 2 3 4 5 ... Последняя страница) Seller		28.09.2013 22:29 от rus616	191	6,100

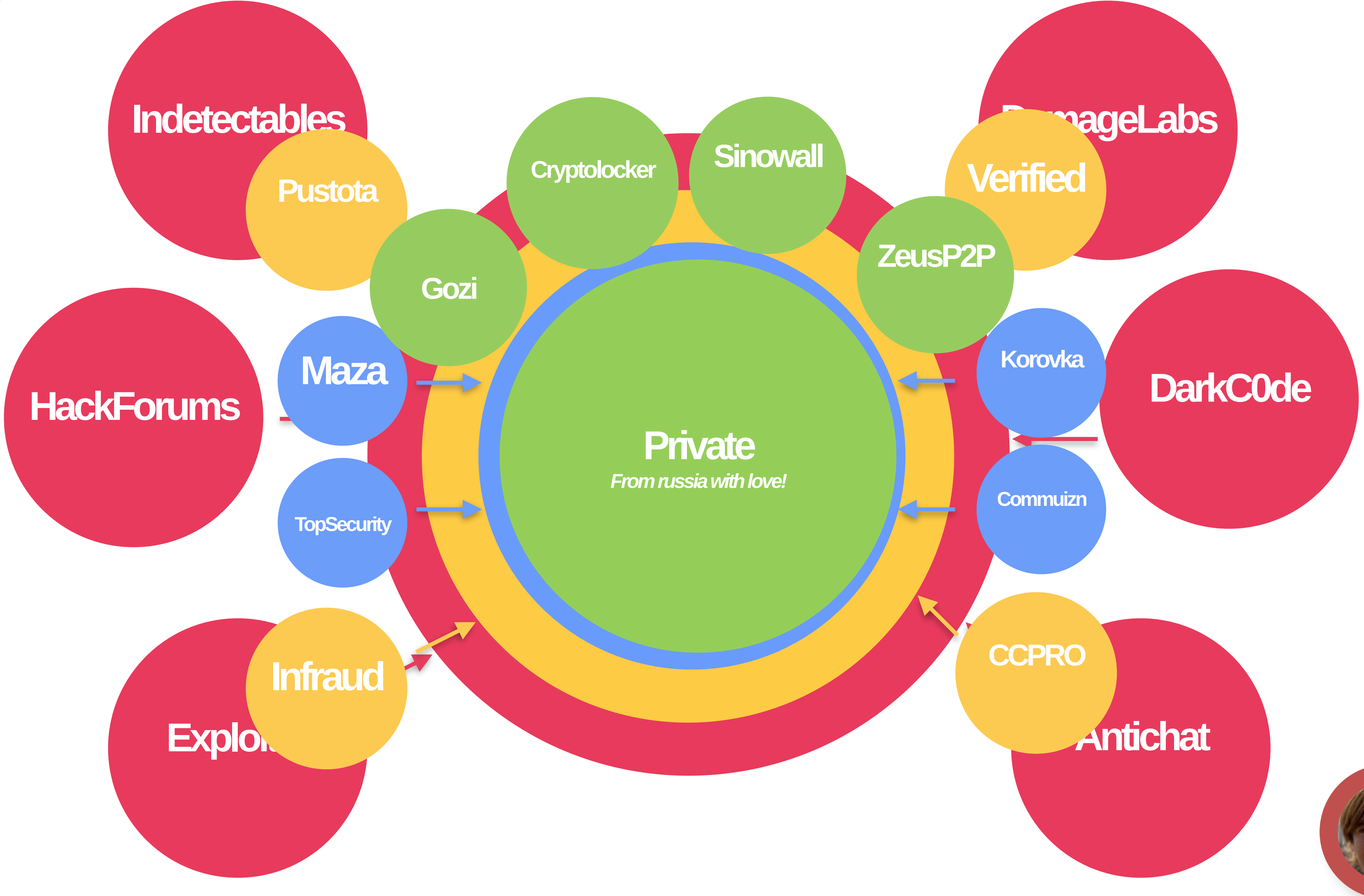
Understand Cyber-Crime activities

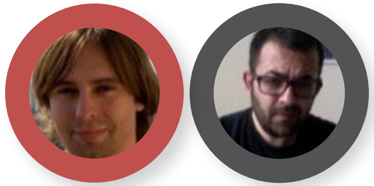
LAYER #4



WHAT WE KNOW ABOUT CYBER-CRIME?

FINAL SCENARIO





Hunting Malware Like a Sir

mlw.re

Previously on...

Previously

Previously on…

- First year, without new Banking Trojans. (Except’s KINS aka Kasper)
- Symlink Arrested (January)
- Paunch Arrested (BlackHole Exploit Kit) (OCTOBER)
- FBI shut down SilkRoad and they arrest Ross Willian Ulbrich. (OCTOBER)
- Target Breach. :-) – (NOVEMBER/DECEMBER)
- FBI With Spanish Police Cooperation take’s down Liberty Reserver and arrest CEO.– (MAY 2013)
- ZeusP2P (Game Over) and CryptoLocker Take down. - (MAY/JUN 2014)

Previously

Has been a special year in the volition of the industry of cyber-Crime

- The feeling of impunity begins to disappear.
- Groups midlevel begin to close and professionalize their assets.
- Ironically, the vetted gang’s start to show some gaps.

Previously

These Changes are due to

- Detentions.
- Proliferation of bloggers / twitters 'investigating' cybercrime scene. *(Pr0n stars)*
- Insider Researchers.
- Leaks (Pasties, services…)

Conclusions

The "industry" of Cyber-Crime, now are more than closed than ever.

Hunting Malware Like a Sir

mlw.re

New trends

OUR SERVICES

New Trends at Cyber-Crime Industry

01 POS

POS Malware - POINT OF SALES SYSTEM

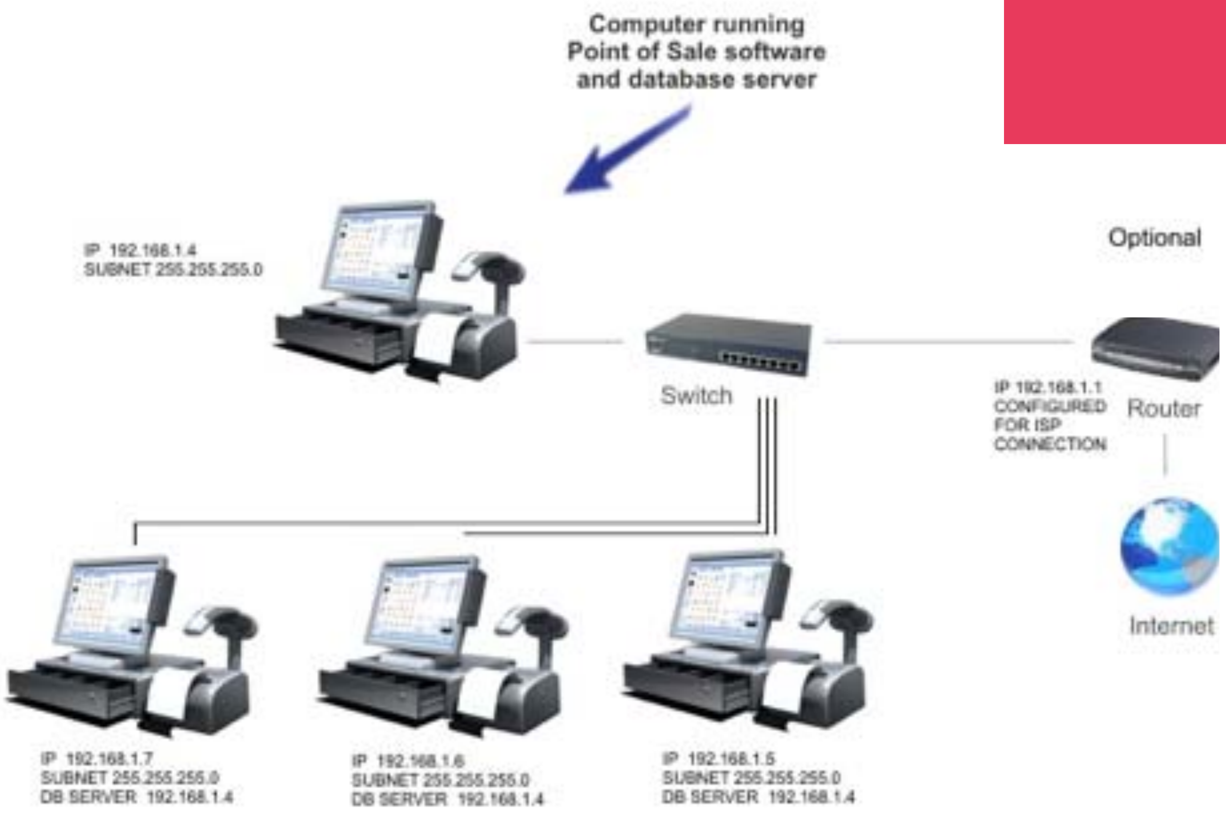
02 TOR BASED

NEW MOBILE MALWARE (EG: TOR BASED)

03 CRYPTOCURRENCIES

Bitcoin, Litecoin, DogeCoin just Crypto Malware Miners!

POS POINT OF SALE, *BUT WHY?*



The lack of a Banking Trojan for sale and the large increase in demand for cards has moved many players in this business.

Citadel users move there business to this new system.

Grows offer POS malware sales.

POS POINT OF SALE,

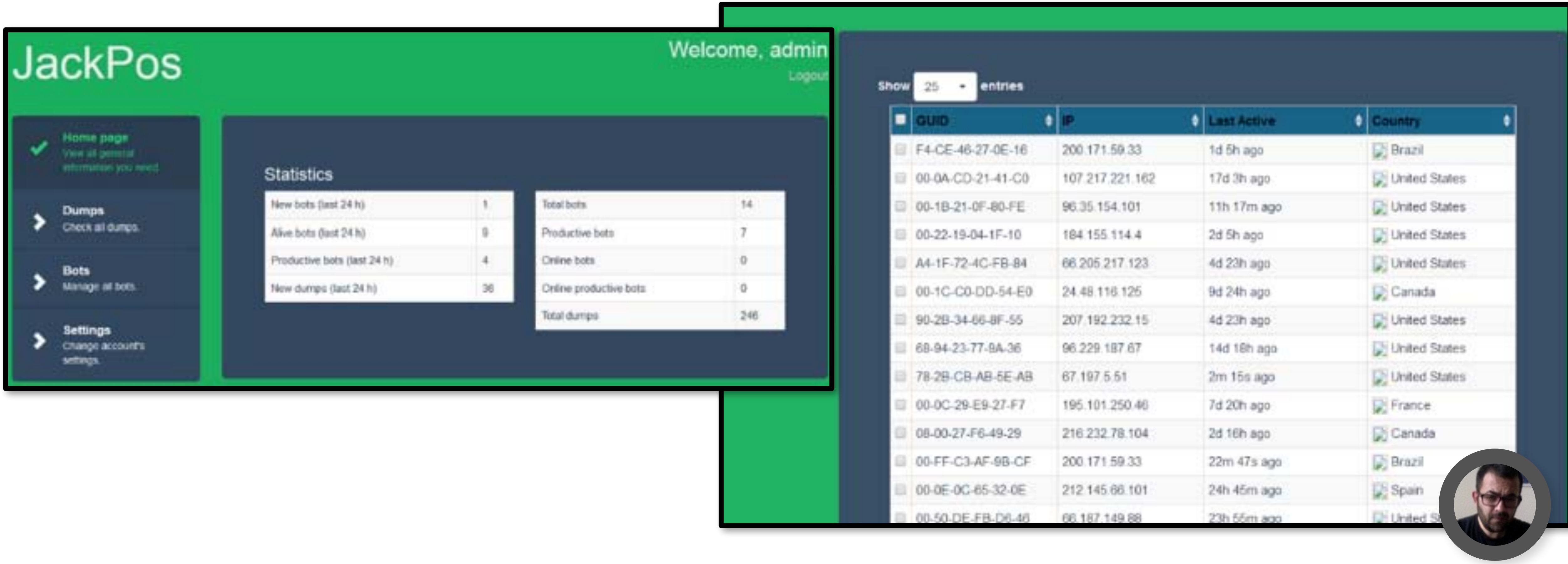
What we found on markets?

- 01 Alina Malware
- 02 Dexter Malware
- 03 BlackPos
- 04 Soraya

**The Beauty,
the Bad,
the Ugly
and
Guest start**

POS POINT OF SALE,

Sofware as Service? of course!



JackPos

Welcome, admin

Logout

✓ Home page
View all general information you need
Dumps
Check all dumps.
Bots
Manage all bots.
Settings
Change account's settings.

Statistics

New bots (last 24 h)	1
Alive bots (last 24 h)	9
Productive bots (last 24 h)	4
New dumps (last 24 h)	36

Total bots	14
Productive bots	7
Online bots	0
Online productive bots	0
Total dumps	246

Show 25 entries

□	GUID	IP	Last Active	Country
□	F4-CE-46-27-0E-16	200.171.59.33	1d 5h ago	Brazil
□	00-0A-CD-21-41-C0	107.217.221.162	17d 3h ago	United States
□	00-1B-21-0F-80-FE	96.35.154.101	11h 17m ago	United States
□	00-22-19-04-1F-10	184.155.114.4	2d 5h ago	United States
□	A4-1F-72-4C-FB-84	66.205.217.123	4d 23h ago	United States
□	00-1C-C0-DD-54-E0	24.48.116.125	9d 24h ago	Canada
□	90-2B-34-66-8F-55	207.192.232.15	4d 23h ago	United States
□	68-94-23-77-8A-36	96.229.187.67	14d 18h ago	United States
□	78-2B-CB-AB-5E-AB	67.197.5.51	2m 15s ago	United States
□	00-0C-29-E9-27-F7	195.101.250.46	7d 20h ago	France
□	08-00-27-F6-49-29	216.232.78.104	2d 16h ago	Canada
□	00-FF-C3-AF-9B-CF	200.171.59.33	22m 47s ago	Brazil
□	00-0E-0C-65-32-0E	212.145.66.101	24h 45m ago	Spain
□	00-50-DE-FB-D6-46	66.187.149.88	23h 55m ago	United S

Mobile Malware

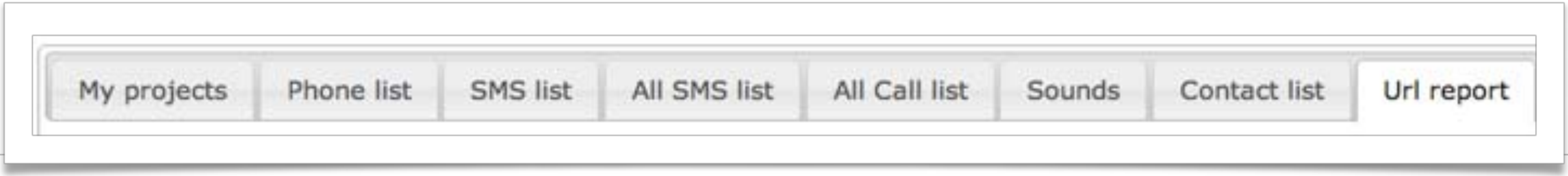
Uses new resources like TOR.

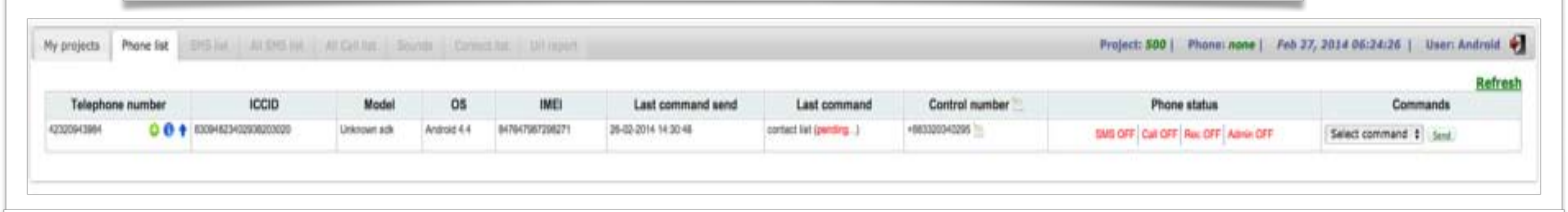
Increase of injections with support for mobile malware.

Mobile malware for sale:

- iBanking (as Service).
- Perkele

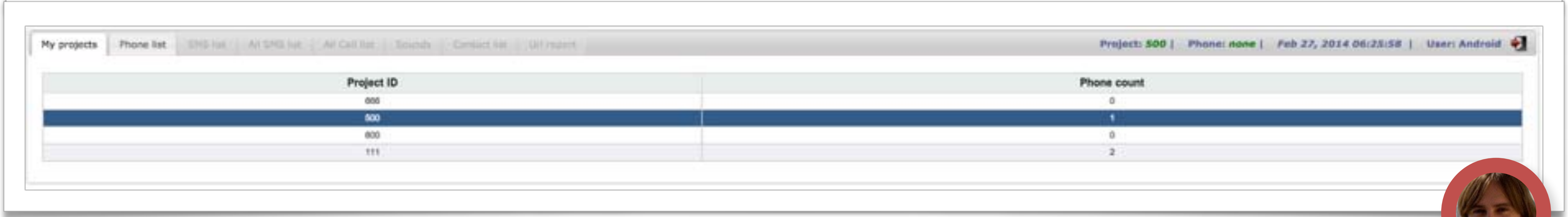
IBanking Malware





Project: 500 | Phone: none | Feb 27, 2014 06:24:26 | User: Android

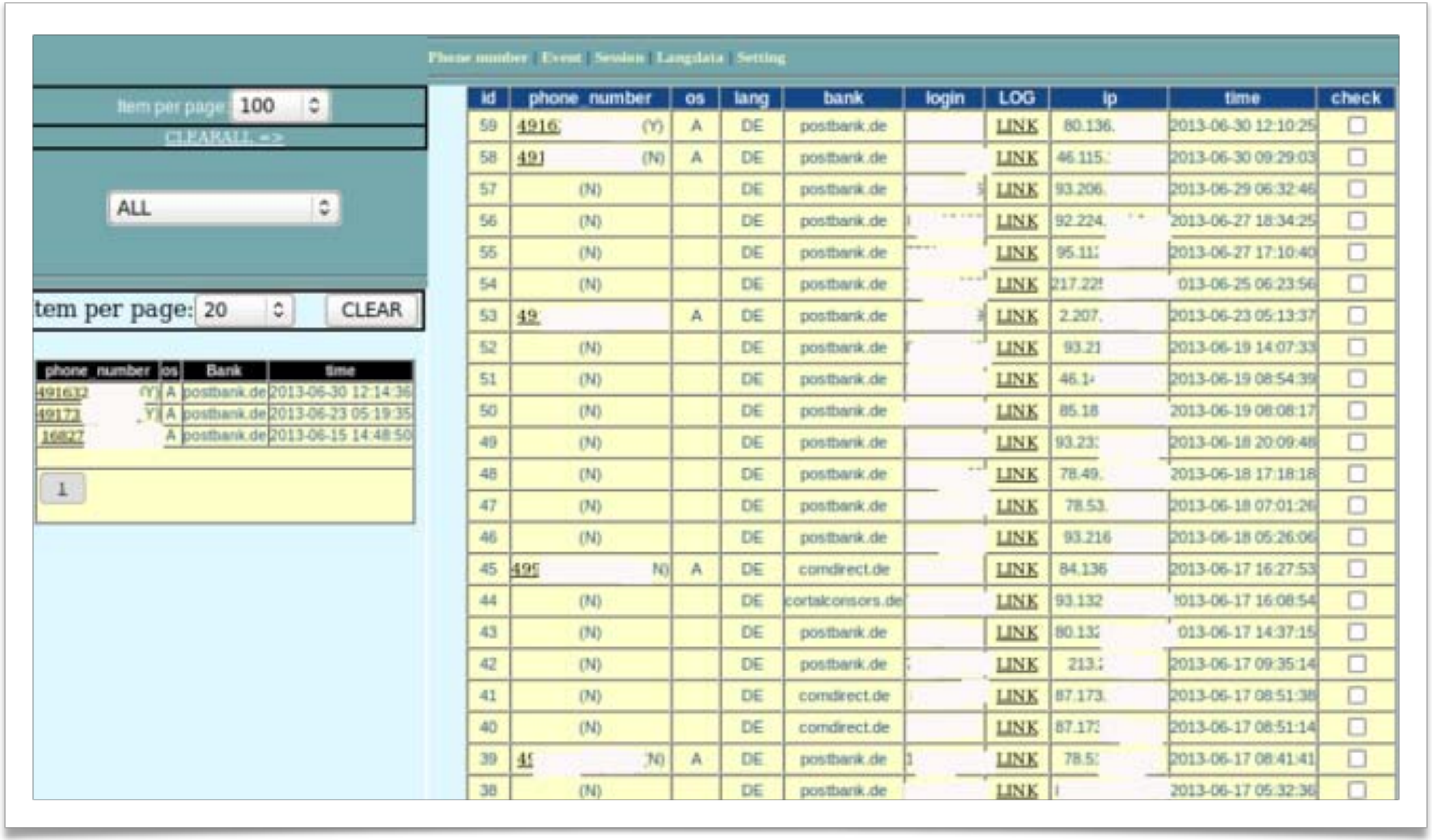
Telephone number	ICCID	Model	OS	IMEI	Last command send	Last command	Control number	Phone status	Commands
42320943984	8309462340290820302	Unknown sdk	Android 4.4	847647967298271	26-02-2014 14:30:48	contact list (pending...)	+883320043295	SMS OFF | Call OFF | Rec OFF | Admin OFF	Select command Send



Project: 500 | Phone: none | Feb 27, 2014 06:25:58 | User: Android

Project ID	Phone count
666	0
500	1
600	0
111	2

Perkele Malware



Phone number | Event | Session | Langdata | Setting

Item per page: 100

CLEARALL =>

ALL

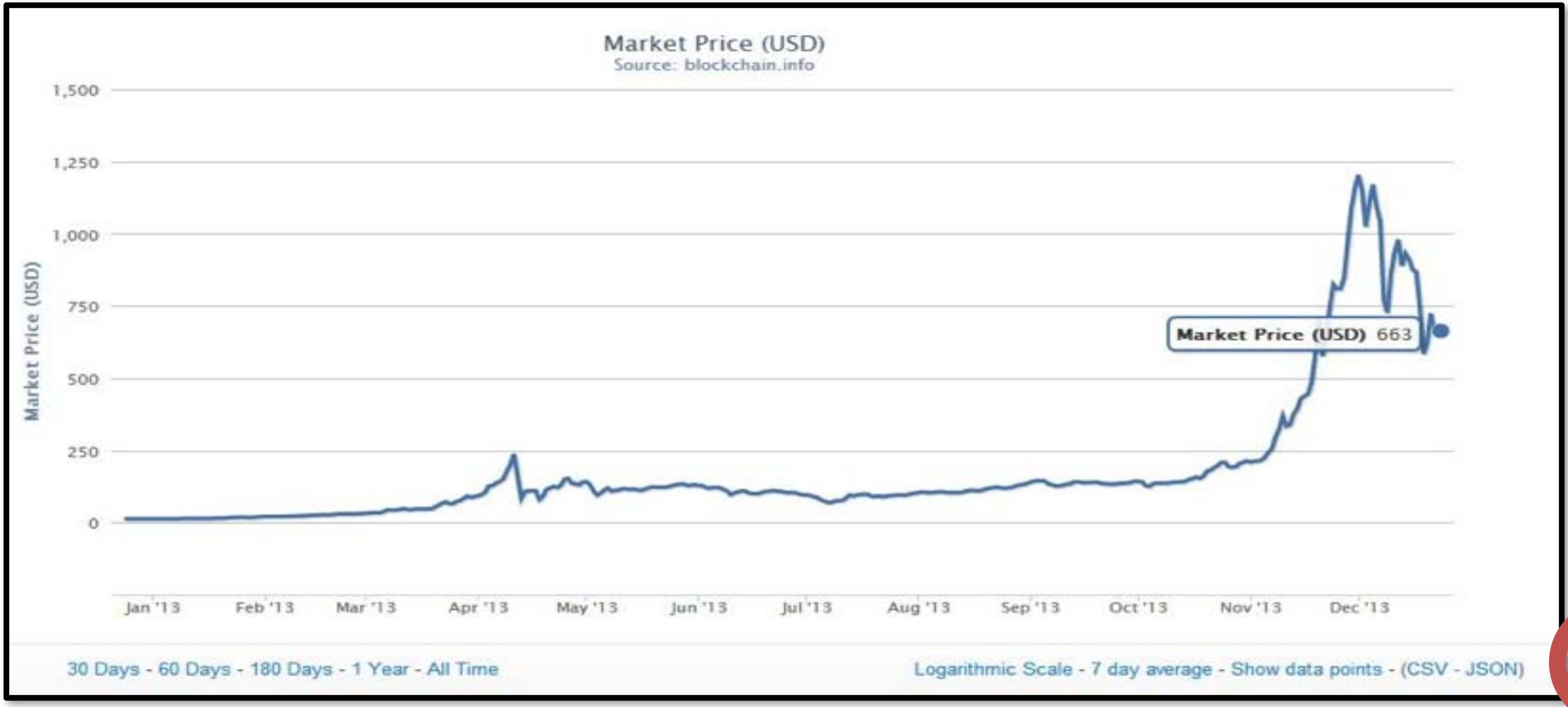
Item per page: 20 CLEAR

phone_number	os	Bank	time
491632 (Y)	A	postbank.de	2013-06-30 12:14:36
49173 Y)	A	postbank.de	2013-06-23 05:19:35
16827	A	postbank.de	2013-06-15 14:48:50

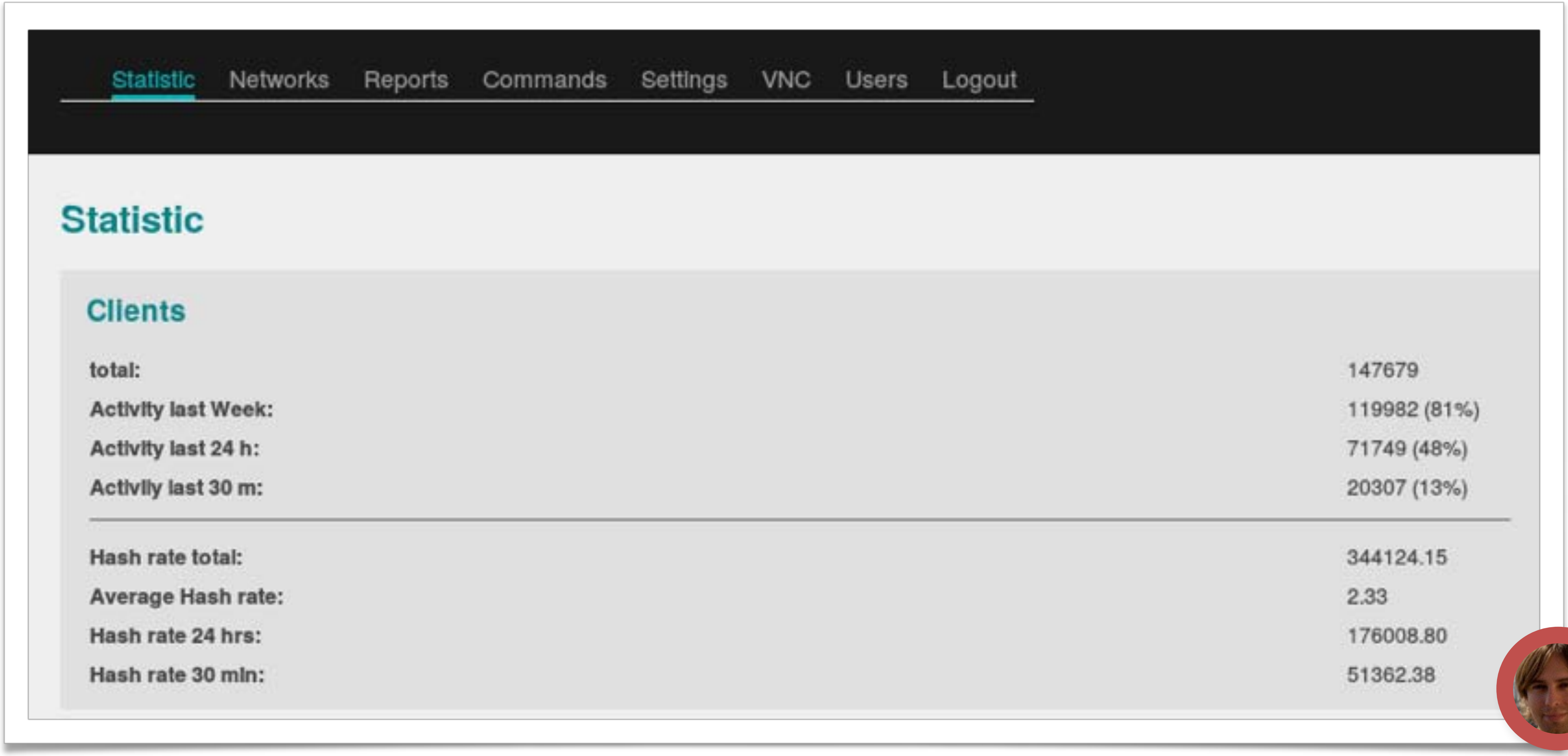
1

id	phone_number	os	lang	bank	login	LOG	ip	time	check
59	4916 (Y)	A	DE	postbank.de		LINK	80.136.	2013-06-30 12:10:25	□
58	491 (N)	A	DE	postbank.de		LINK	46.115.	2013-06-30 09:29:03	□
57	(N)		DE	postbank.de		LINK	93.206.	2013-06-29 06:32:46	□
56	(N)		DE	postbank.de		LINK	92.224.	2013-06-27 18:34:25	□
55	(N)		DE	postbank.de		LINK	95.11	2013-06-27 17:10:40	□
54	(N)		DE	postbank.de		LINK	217.22	013-06-25 06:23:56	□
53	49	A	DE	postbank.de		LINK	2.207.	2013-06-23 05:13:37	□
52	(N)		DE	postbank.de		LINK	93.21	2013-06-19 14:07:33	□
51	(N)		DE	postbank.de		LINK	46.1	2013-06-19 08:54:39	□
50	(N)		DE	postbank.de		LINK	85.18	2013-06-19 08:08:17	□
49	(N)		DE	postbank.de		LINK	93.23	2013-06-18 20:09:48	□
48	(N)		DE	postbank.de		LINK	78.49.	2013-06-18 17:18:18	□
47	(N)		DE	postbank.de		LINK	78.53.	2013-06-18 07:01:26	□
46	(N)		DE	postbank.de		LINK	93.216	2013-06-18 05:26:06	□
45	495 N)	A	DE	comdirect.de		LINK	84.136	2013-06-17 16:27:53	□
44	(N)		DE	cortalconsors.de		LINK	93.132	013-06-17 16:08:54	□
43	(N)		DE	postbank.de		LINK	80.13	013-06-17 14:37:15	□
42	(N)		DE	postbank.de		LINK	213.	2013-06-17 09:35:14	□
41	(N)		DE	comdirect.de		LINK	87.173.	2013-06-17 08:51:38	□
40	(N)		DE	comdirect.de		LINK	87.17	2013-06-17 08:51:14	□
39	45 N)	A	DE	postbank.de		LINK	78.5	2013-06-17 08:41:41	□
38	(N)		DE	postbank.de		LINK		2013-06-17 05:32:36	□

CryptoCurrencies



CryptoCurrencies

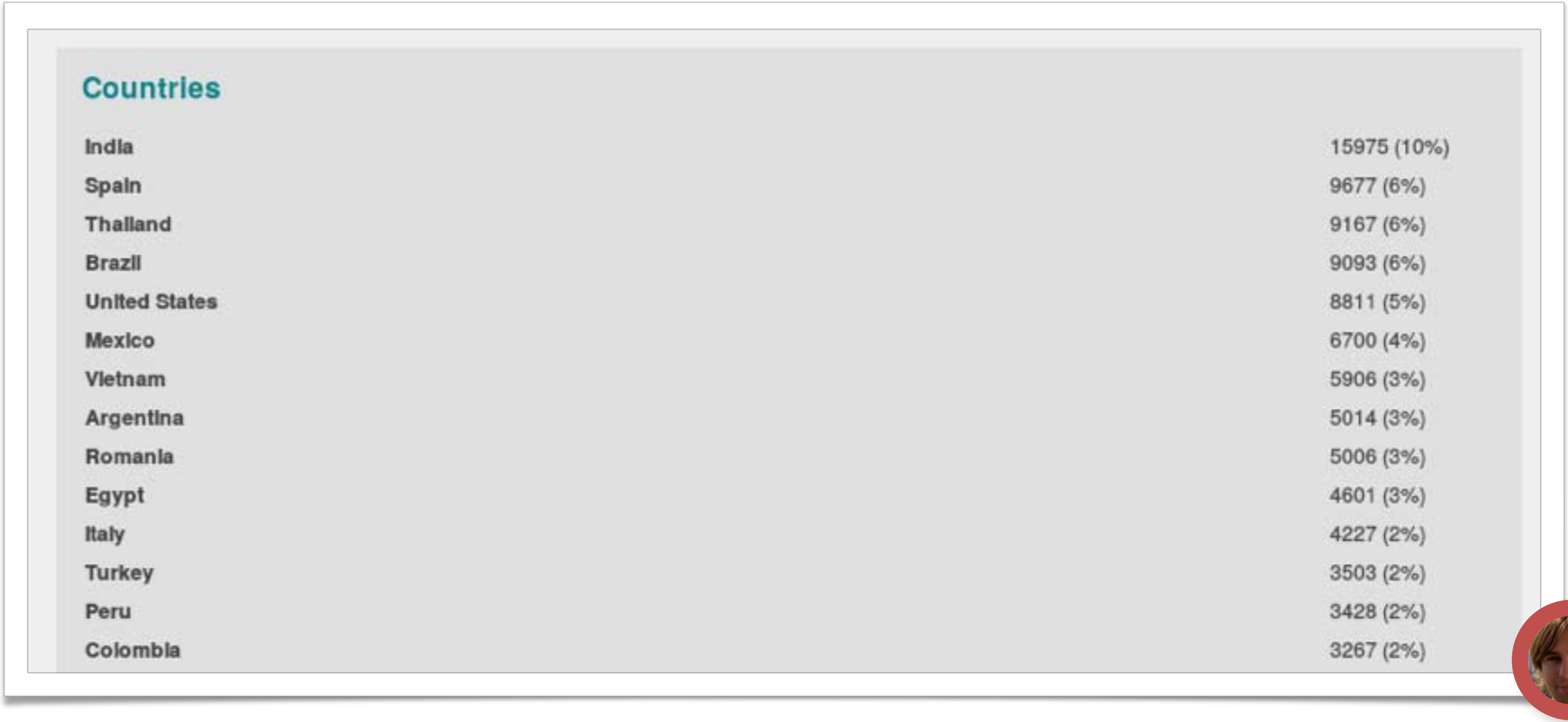


Statistic

Clients

total:	147679
Activity last Week:	119982 (81%)
Activity last 24 h:	71749 (48%)
Activily last 30 m:	20307 (13%)
Hash rate total:	344124.15
Average Hash rate:	2.33
Hash rate 24 hrs:	176008.80
Hash rate 30 min:	51362.38

CryptoCurrencies

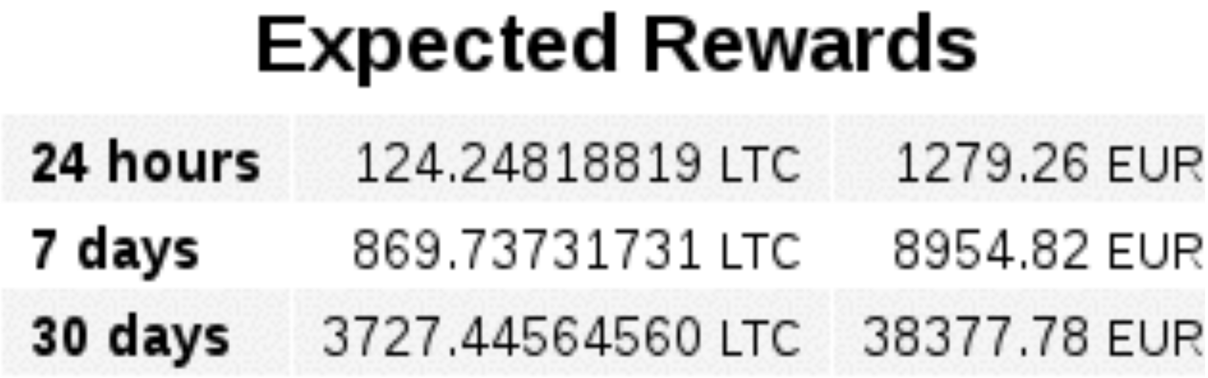


Countries

India	15975 (10%)
Spain	9677 (6%)
Thailand	9167 (6%)
Brazil	9093 (6%)
United States	8811 (5%)
Mexico	6700 (4%)
Vietnam	5906 (3%)
Argentina	5014 (3%)
Romania	5006 (3%)
Egypt	4601 (3%)
Italy	4227 (2%)
Turkey	3503 (2%)
Peru	3428 (2%)
Colombia	3267 (2%)

CryptoCurrencies

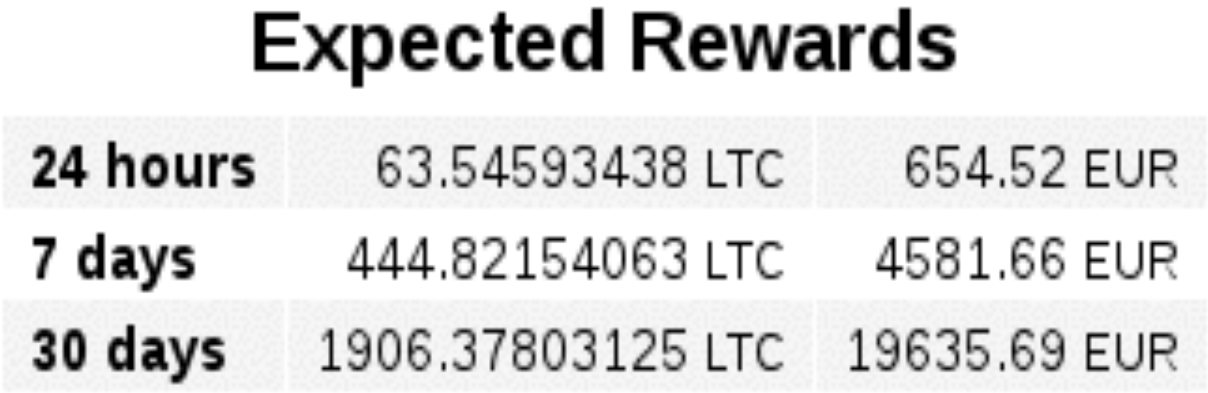
TOTAL HASH RATE



Expected Rewards

24 hours	124.24818819 LTC	1279.26 EUR
7 days	869.73731731 LTC	8954.82 EUR
30 days	3727.44564560 LTC	38377.78 EUR

24H HASH RATE



Expected Rewards

24 hours	63.54593438 LTC	654.52 EUR
7 days	444.82154063 LTC	4581.66 EUR
30 days	1906.37803125 LTC	19635.69 EUR

Hunting Malware Like a Sir

mlw.re

Examples! 🎯

Examples

Example

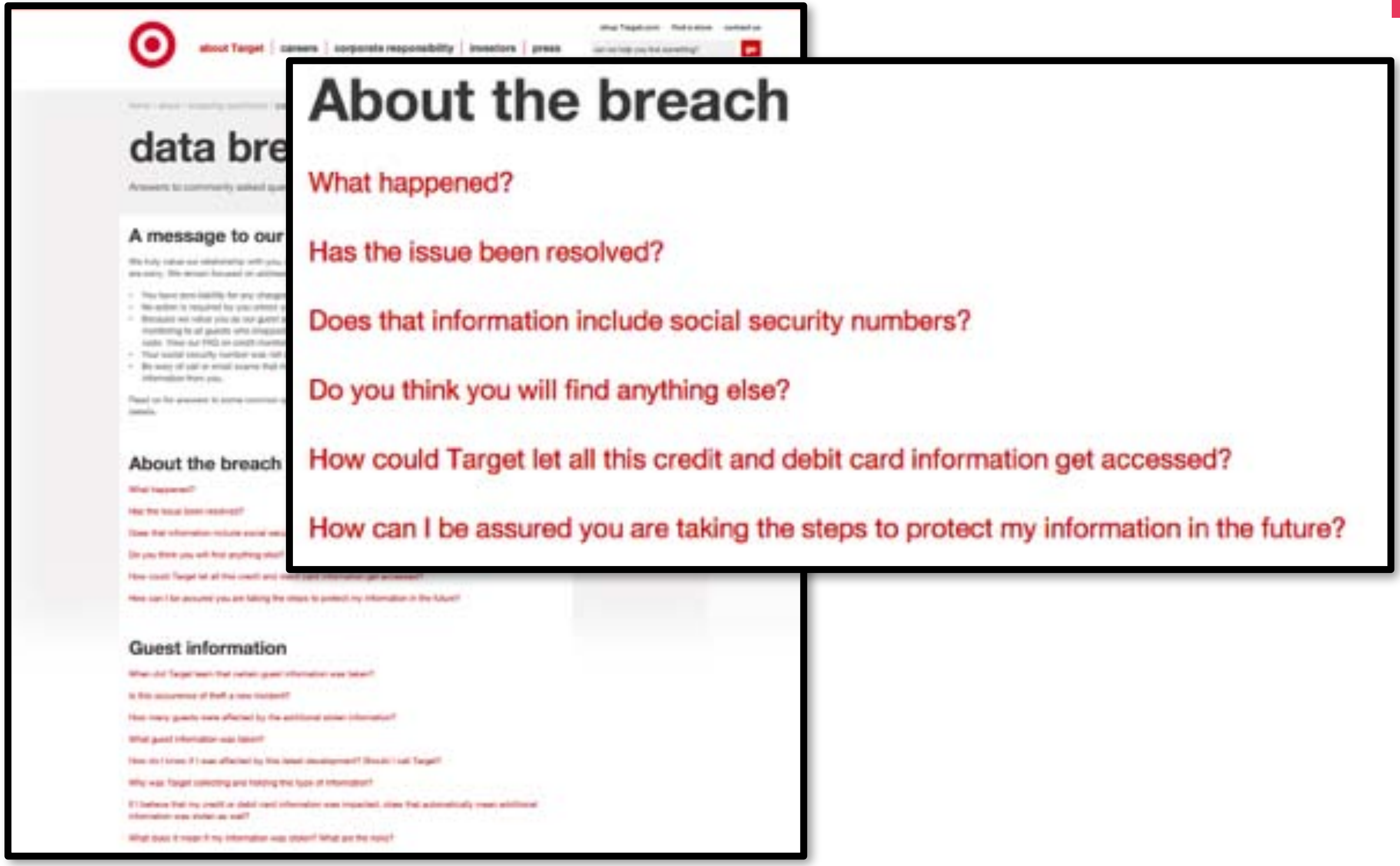
TimeLine

Brian Krebs
18/Dec/2013: Sources: Target Investigating Data Breach
20/Dec/2013: Cards Stolen in Target Breach Flood Underground Markets
22/Dec/2013: Non-US Cards Used At Target Fetch Premium
24/Dec/2013: Who’s Selling Credit Cards from Target?
10/Jan/2014: Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen
15/Jan/2014: A First Look at the Target Intrusion, Malware
16/Jan/2014: A Closer Look at the Target Malware, Part II
29/Jan/2014: New Clues in the Target Breach
04/Feb/2014: These Guys Battled BlackPOS at a Retailer
05/Feb/2014: Target Hackers Broke in Via HVAC Company
12/Feb/2014: Email Attack on Vendor Set Up Breach at Target
19/Feb/2014: Fire Sale on Cards Stolen in Target Breach
25/Feb/2014: Card Backlog Extends Pain from Target Breach

TARGET®

Examples

Example



about Target | careers | corporate responsibility | investors | press

data bre

A message to our

About the breach

Guest information

About the breach

What happened?

Has the issue been resolved?

Does that information include social security numbers?

Do you think you will find anything else?

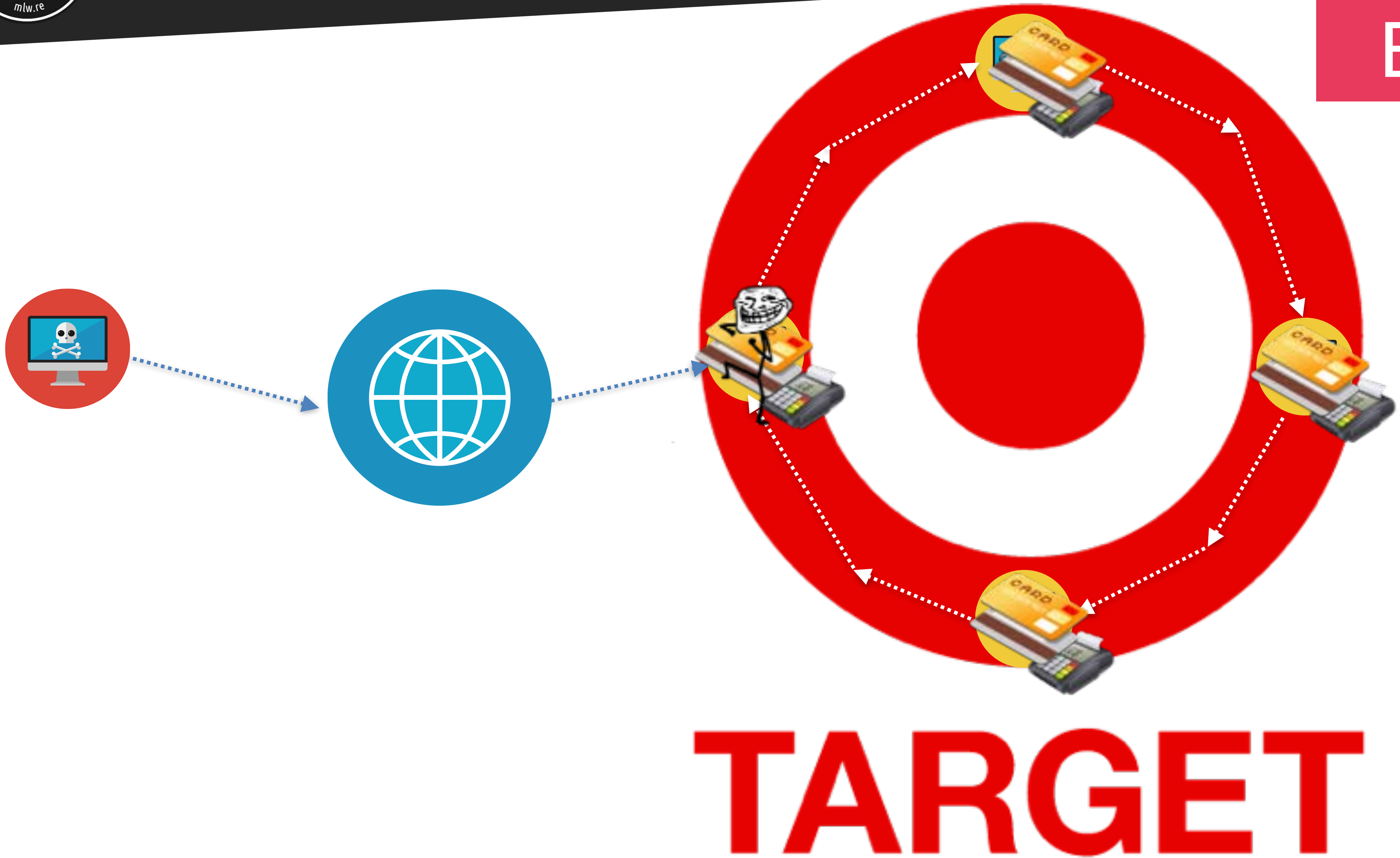
How could Target let all this credit and debit card information get accessed?

How can I be assured you are taking the steps to protect my information in the future?

TARGET®

Examples

Example



Hunting Malware Like a Sir

mlw.re

INTELLIGENCE

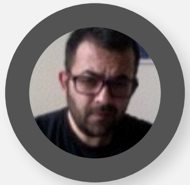
INTELLIGENCE

INTELLIGENCE

- Emerging threat research
- Strategic partnerships to share intelligence
- Tailored threat focus areas
- Live, dynamic intelligence feeds with advanced
- Actively tracking of cybercrime element
- Daily emerging threat reviews
- Awareness of the changing technology and business environment
- Metrics and rending data for multiple key threat indicators
- Recommendations on improved and refined processes

- Botnet monitoring and analysis
- Malware reverse engineering
- Social media monitor
- Reputation scans
- Deep web monitoring
- Social engineering threats
- Spoofed websites
- All Source Intelligence

- Emerging tech review
- Loss management
- Vendor management
- Executive identity monitoring



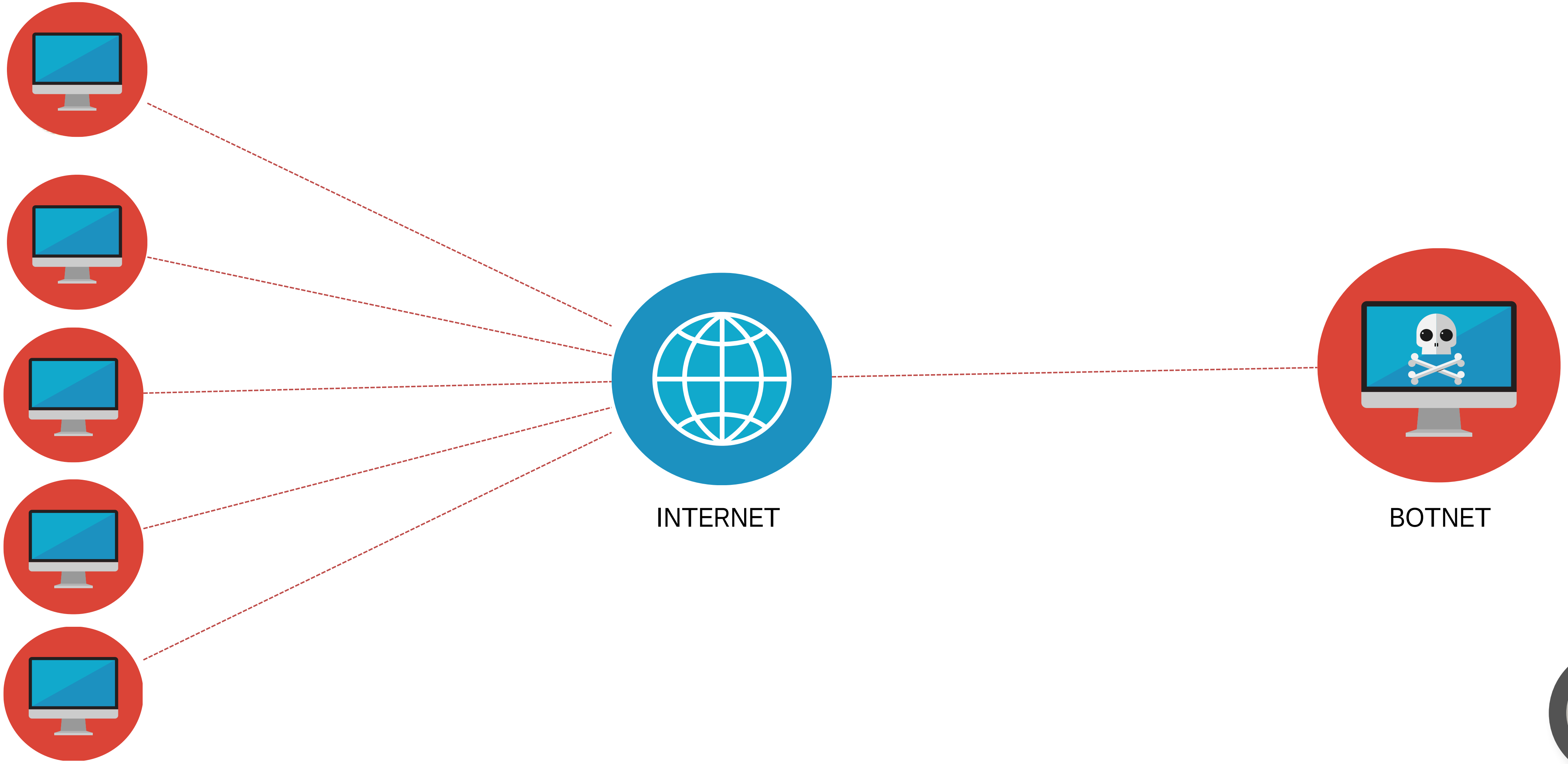
Hunting Malware Like a Sir

mlw.re

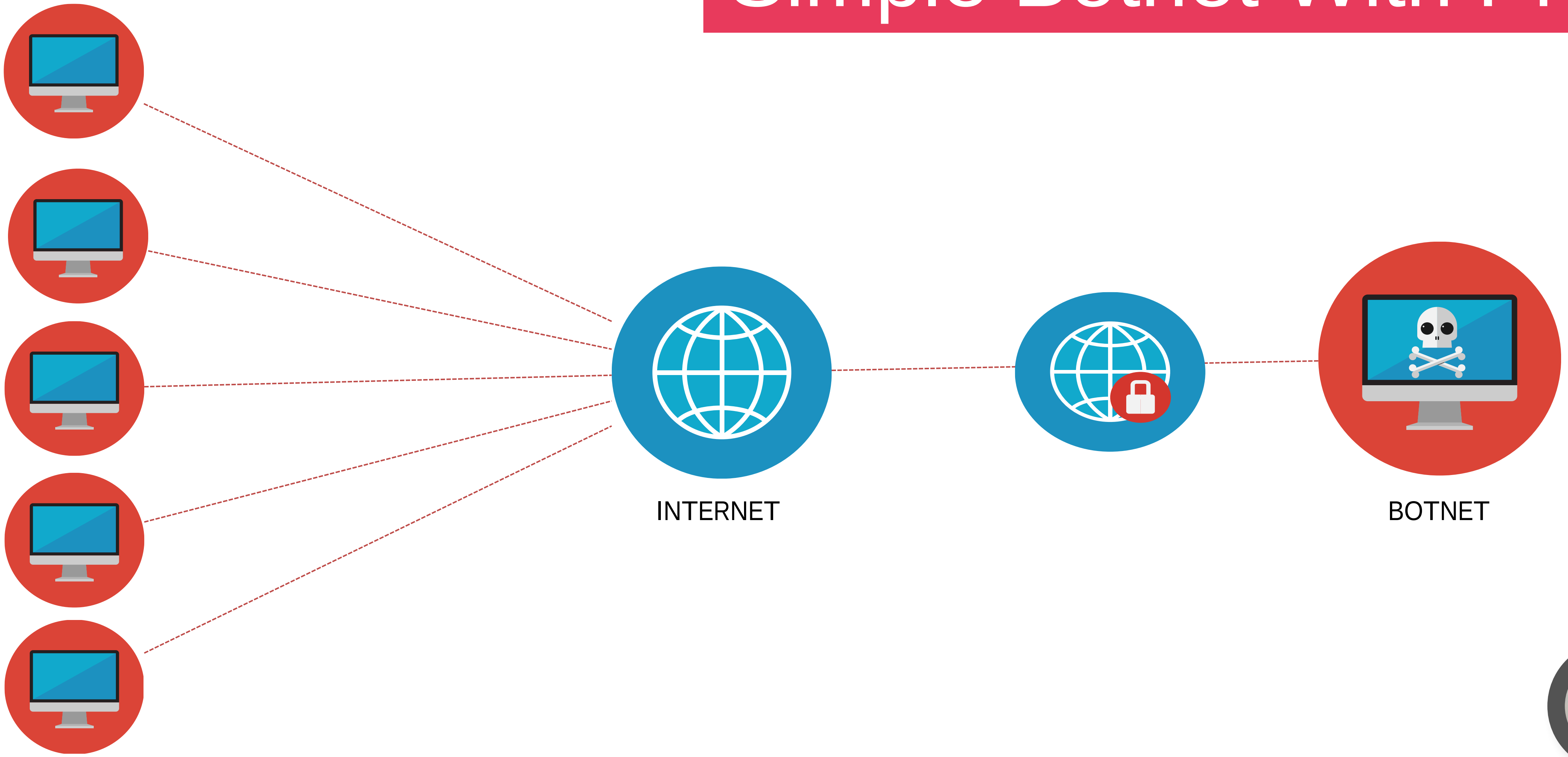
INFRASTRUCTURES

OUR SERVICES

Simple Botnet

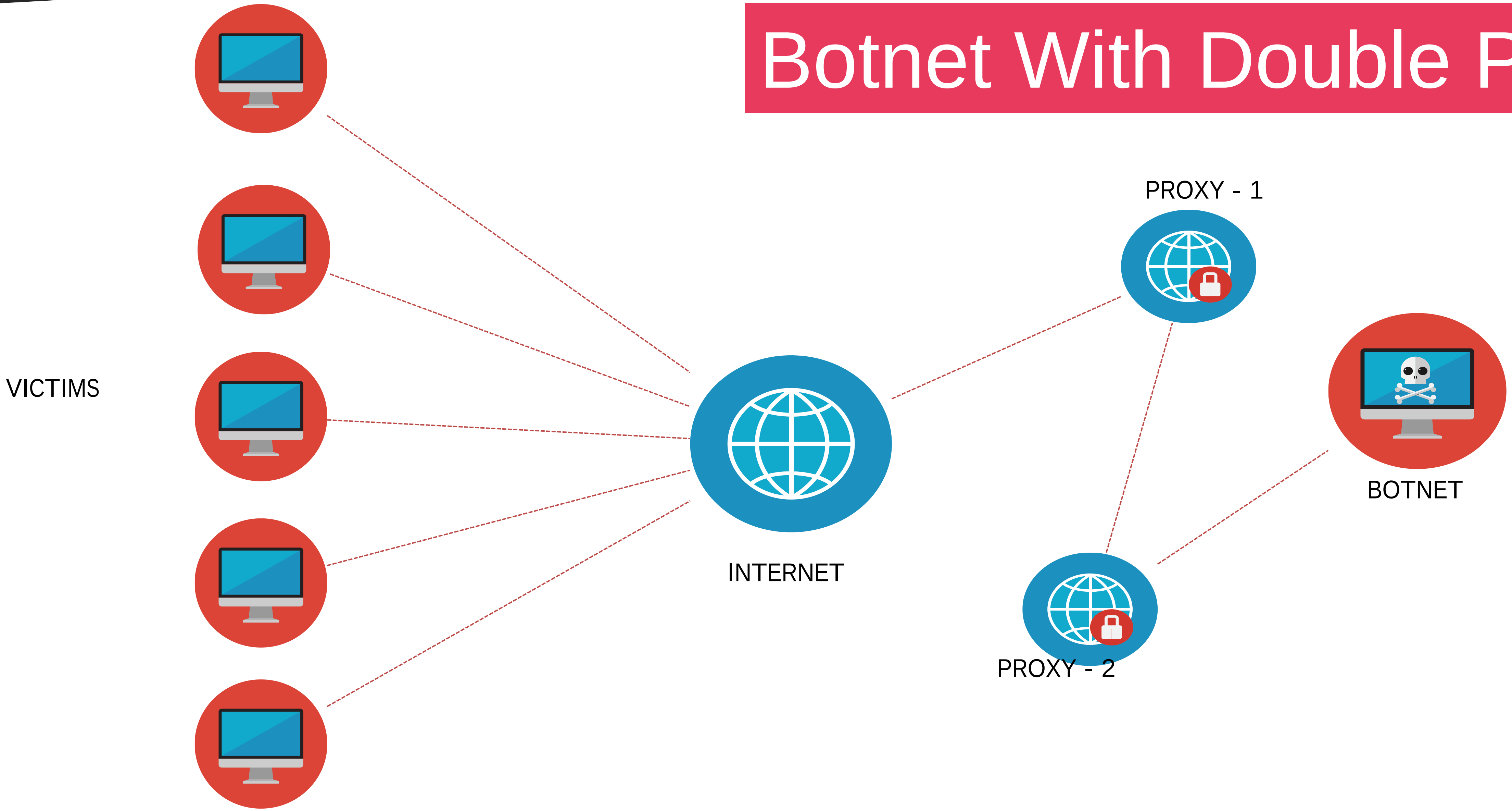


Simple Botnet With Proxy



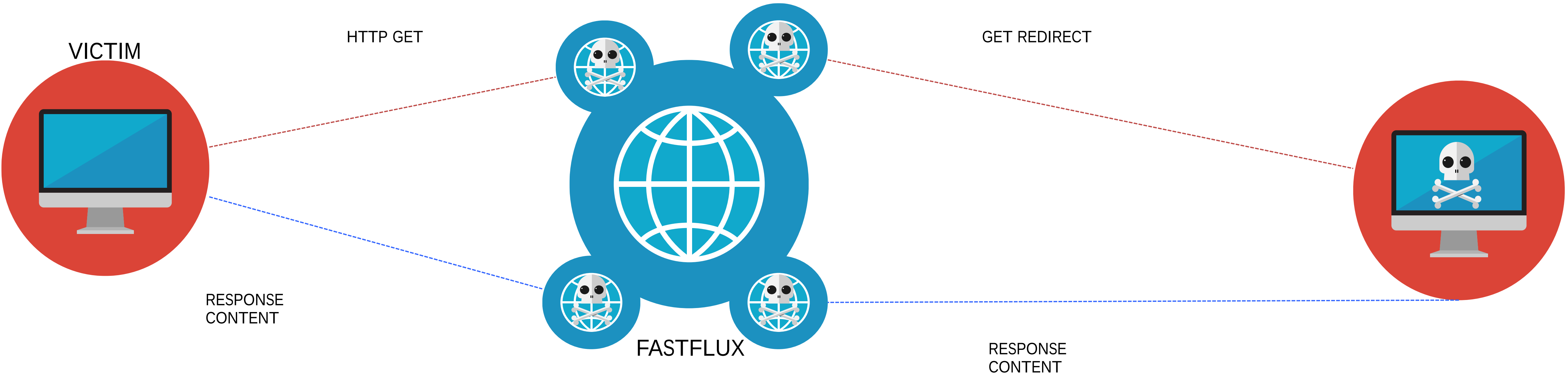
OUR SERVICES

Botnet With Double Proxy



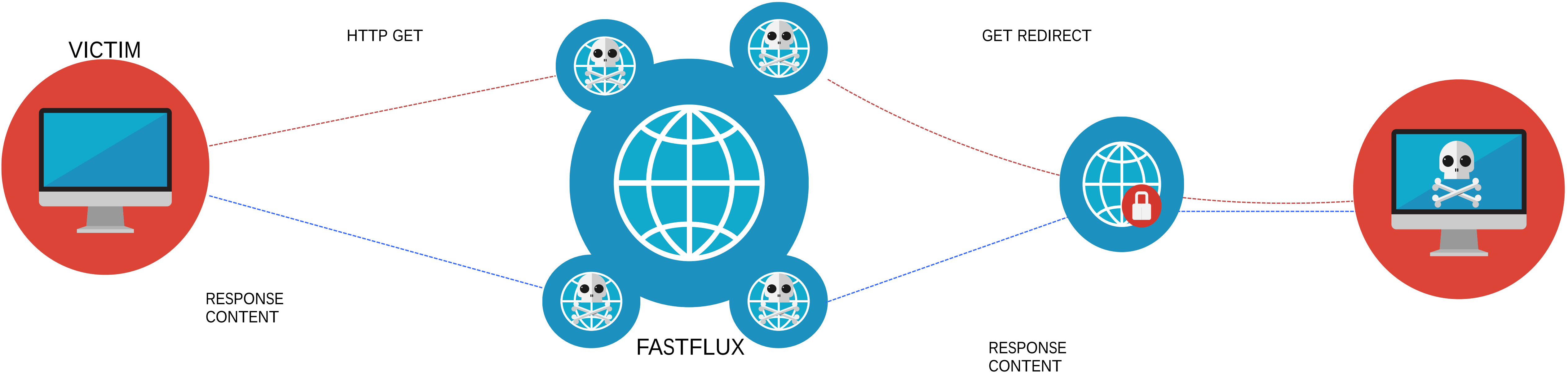
OUR SERVICES

FAST FLUX + C&C



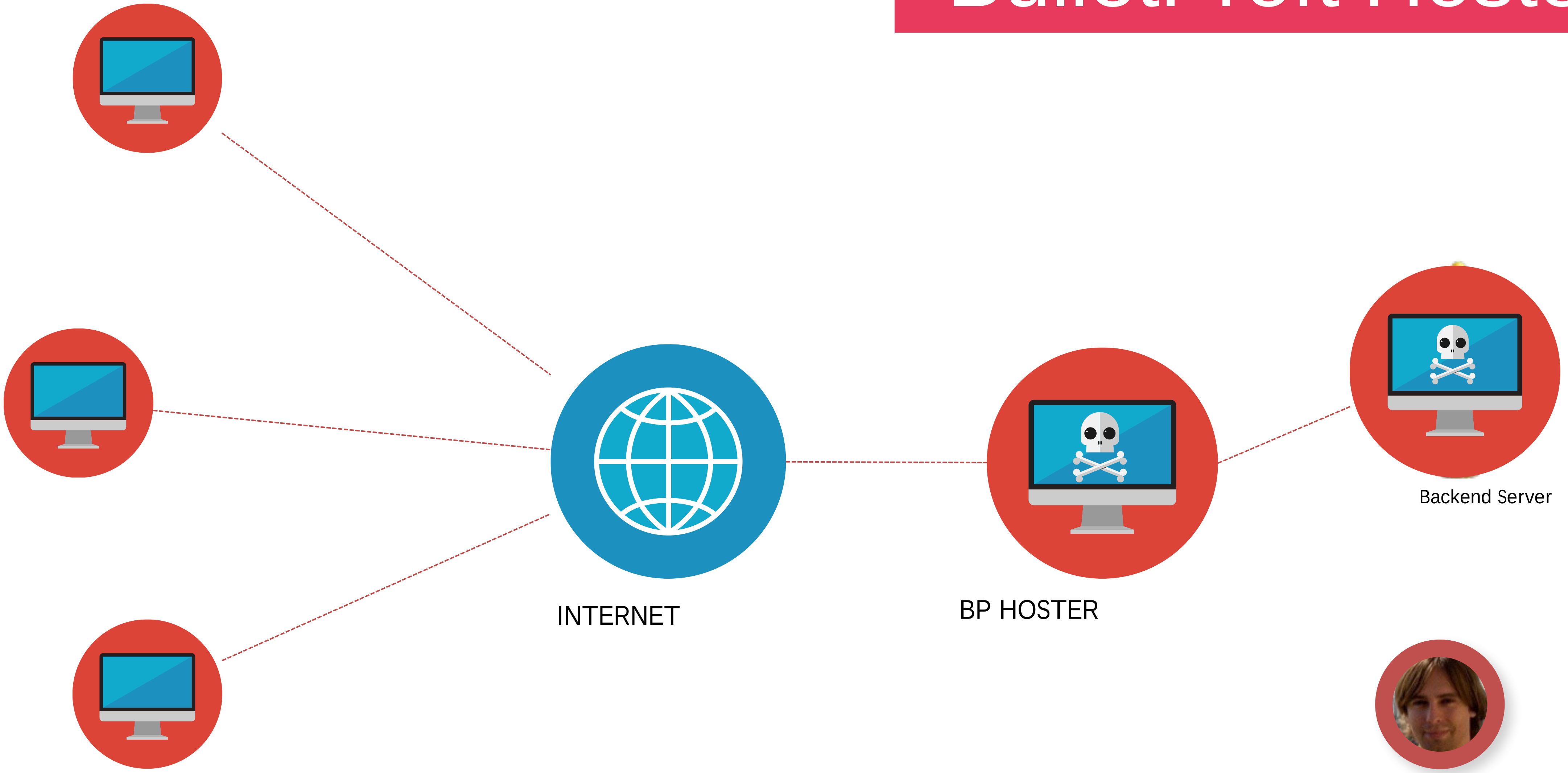
OUR SERVICES

FAST FLUX + PROXY+ C&C



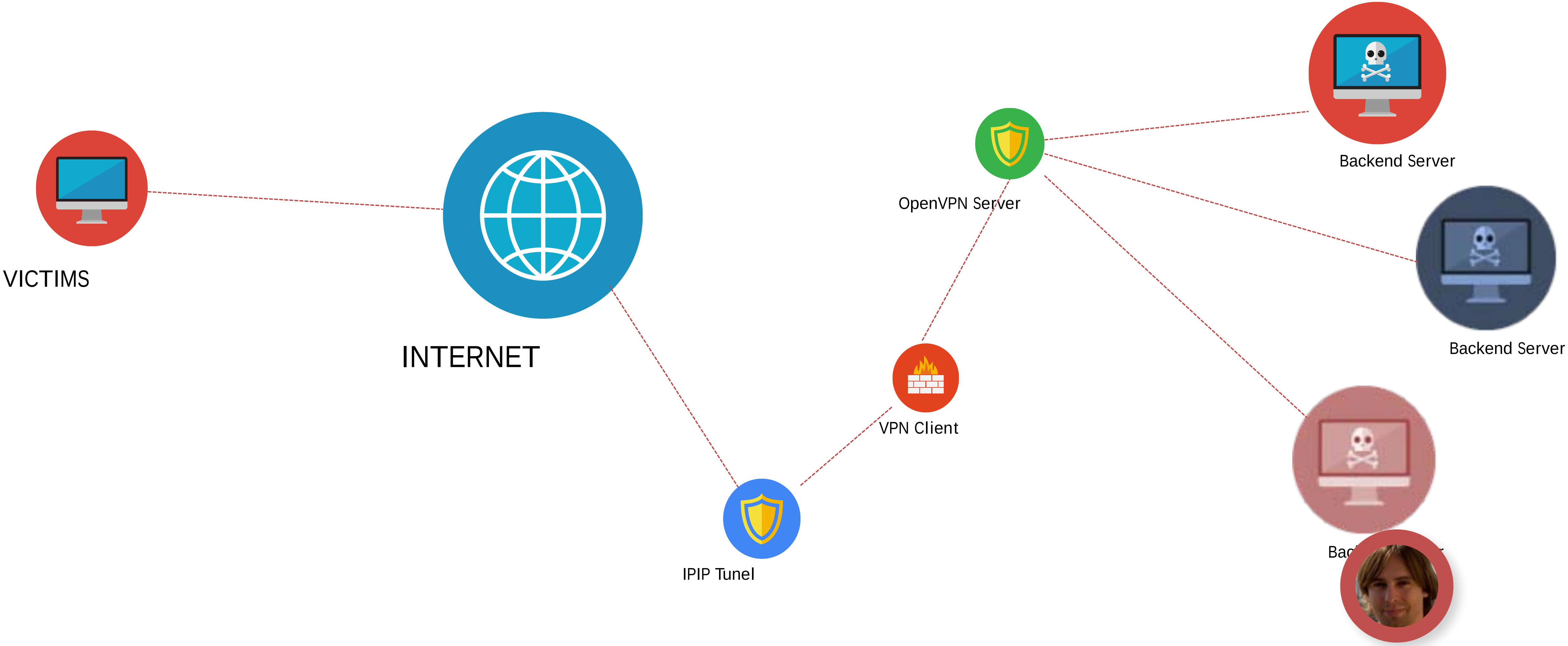
OUR SERVICES

BulletProft Hosters

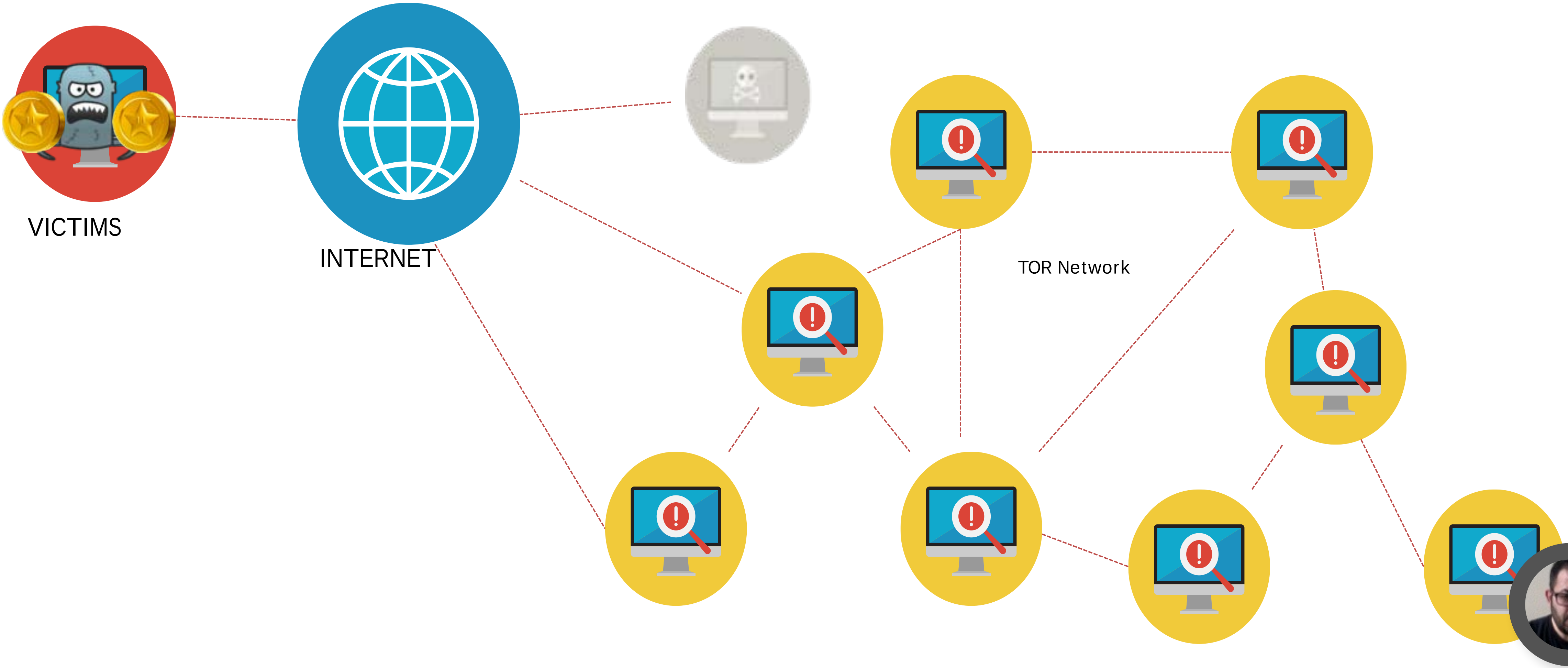


OUR SERVICES

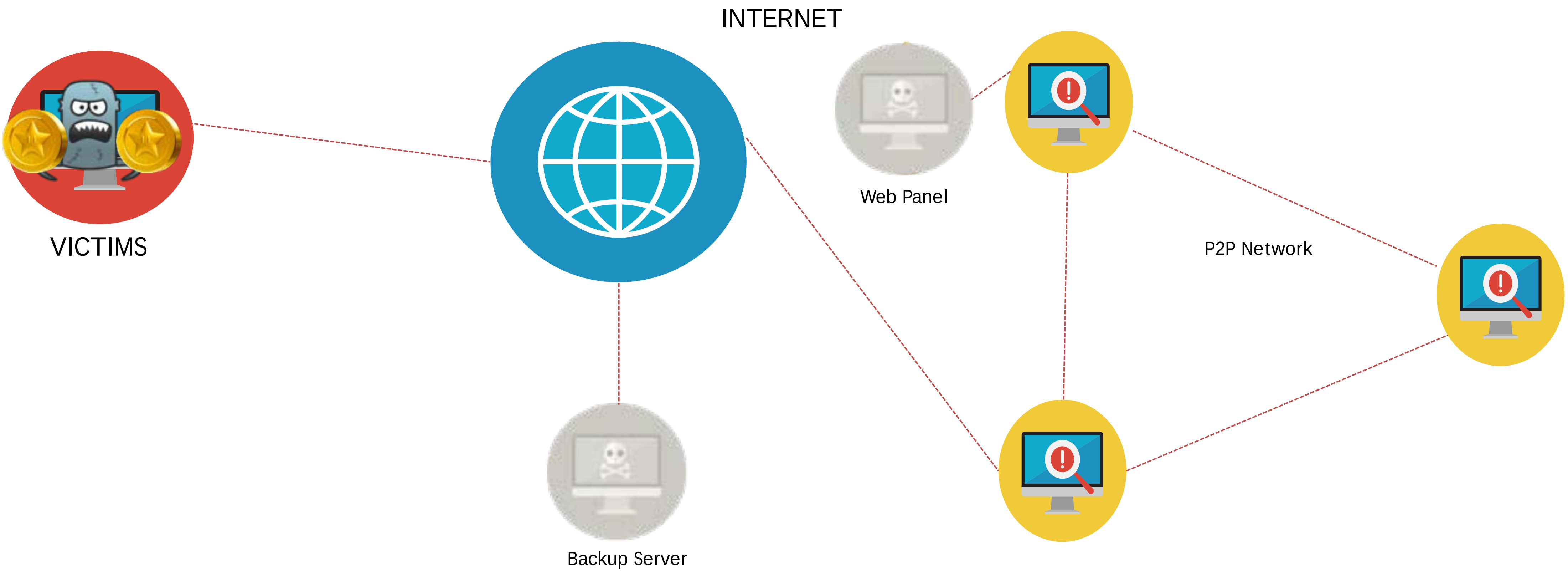
OWN INFRASTRUCTURES



TOR INFRASTRUCTURES



P2P INFRASTRUCTURE



Hunting Malware Like a Sir

mlw.re

DEMO TIME

DEMO Concept

BUILD POS ENVIROMENT

SWIPE OUR CREDIT CARD

BREATHE DEEPLY

INFECT OUR POS

CALM DOWN

PWN THE BOTNET AND GET OUR MONEY BACK!

DEMO RESULTS

Me robo mi tarjeta…

Yo quemé su botnet…

Deloitte.

FOX IT
FOR A MORE SECURE SOCIETY

®buguroo
offensive security

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

CUERPO NACIONAL DE POLICIA

GRUPO DE DELITOS TELEMATICOS

drainware

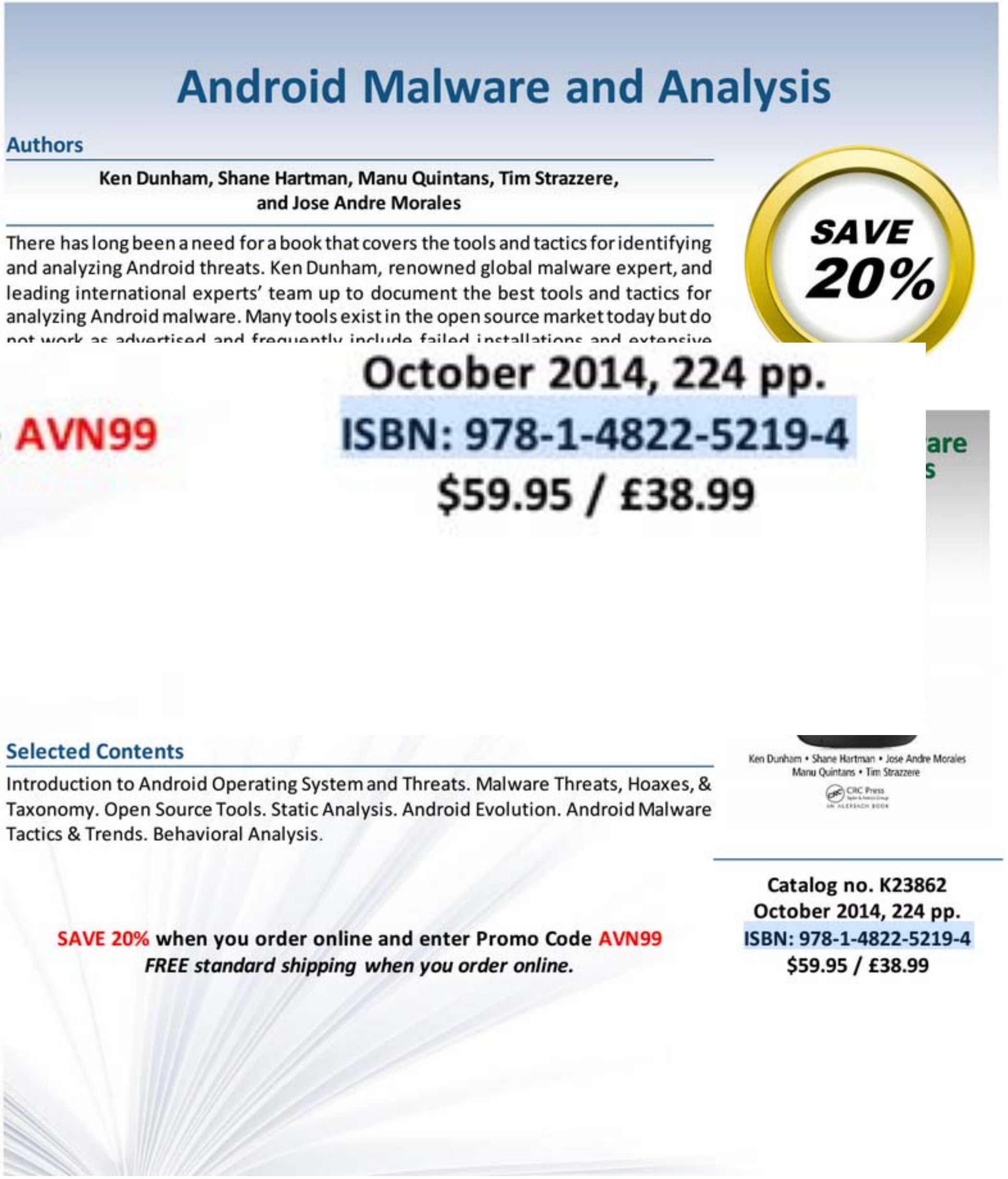
internet
security
auditors

laSalle
Universitat Ramon Llull

THANKS!

WARING!

COMING!



Android Malware and Analysis

Authors

Ken Dunham, Shane Hartman, Manu Quintans, Tim Strazzere,
and Jose Andre Morales

There has long been a need for a book that covers the tools and tactics for identifying and analyzing Android threats. Ken Dunham, renowned global malware expert, and leading international experts' team up to document the best tools and tactics for analyzing Android malware. Many tools exist in the open source market today but do not work as advertised and frequently include failed installations and extensive

Ken Dunham • Shane Hartman • Jose Andre Morales
Manu Quintans • Tim Strazzere
CRC Press

Selected Contents

Introduction to Android Operating System and Threats. Malware Threats, Hoaxes, & Taxonomy. Open Source Tools. Static Analysis. Android Evolution. Android Malware Tactics & Trends. Behavioral Analysis.

Catalog no. K23862
October 2014, 224 pp.
ISBN: 978-1-4822-5219-4
$59.95 / £38.99

SAVE 20% when you order online and enter Promo Code AVN99
FREE standard shipping when you order online.

SAVE 20% when you order online and enter Promo Code AVN99
FREE standard shipping when you order online.

October 2014, 224 pp.
ISBN: 978-1-4822-5219-4
$59.95 / £38.99

Hunting Malware Like a Sir

mlw.re

THANKS!!

Hunting Malware Like a Sir

mlw.re

Q/A