Ponmocup Hunter 2.0
The Sequel

Tom Ueltschi
@c_APT_ure

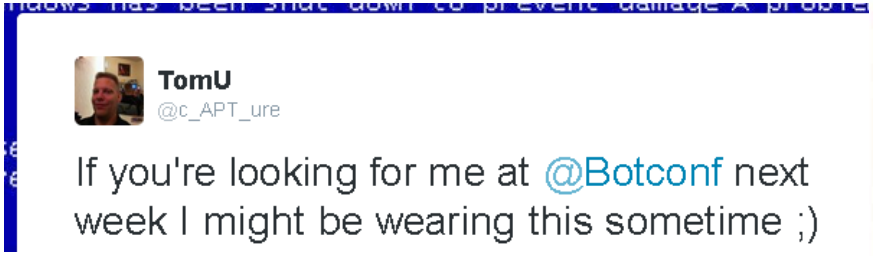
Disclaimer: No miscreants were killed for making this presentation


50 GREATEST
MOVIE SEQUELS
THE FOLLOW-UPS THAT ACHIEVE GREATNESS IN THEIR OWN RIGHT
I STILL KNOW...
WHAT YOU DID
LAST
botconf
First botnet fighting conference
2013

$ whoami / about.me

- Tom Ueltschi, SOC Analyst @ Swiss Post
- 1995 – 2001: B.S. & M.S. CSE @ UTA
- 2001 – 2007: Software Engineer (C++ / Java)
- 2007 – current: IT Security (SOC, CERT, CSIRT)
- SANS Courses, GIAC Certs (GCIH, GWAPT, GXPN, GCFA)
- Sharing and collaborating with public and trusted parties
- Member of several trusted / closed groups of Malware & APT Threat Intelligence sharing
- Founder of Ponmocup Botnet Working Group ☺

When I grow up I wanna be…



^^^ THIS ^^^

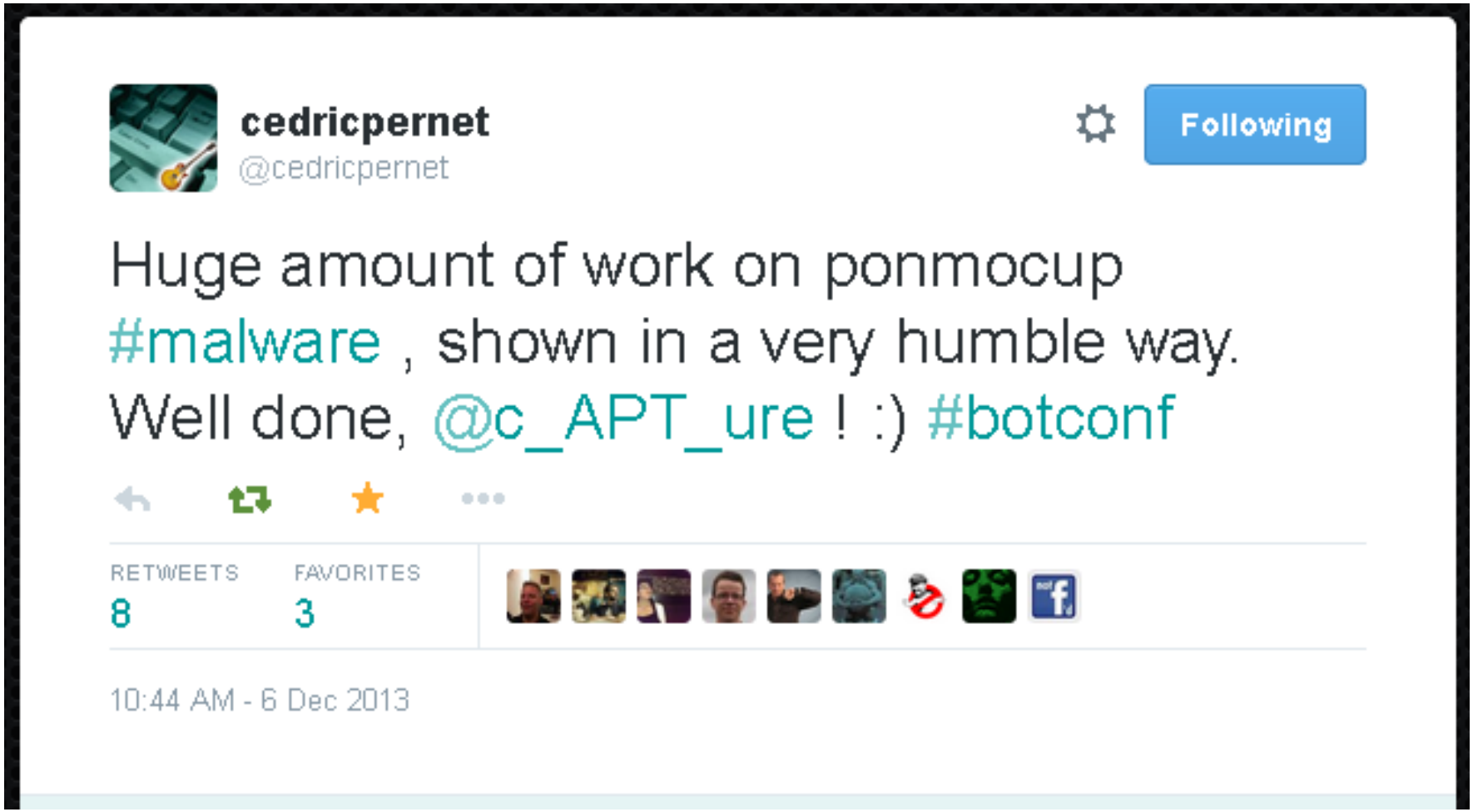
☺ ☺ ☺

What happened last year…

- SANS DFIR Summit (Austin TX), July 2013
  - 150 slides in 60 minutes *(I'm a slow talker ☺)*
- DeepSec (Vienna, Austria), November 2013
  - 130 slides in 50 minutes
- BotConf (Nantes, France), December 2013
  - 120 slides in 50 minutes
- Presentation slides and video linked from my blog

> http://c-apt-ure.blogspot.com/2013/12/ponmocup-hunter-is-re-tired.html

My favorite feedback



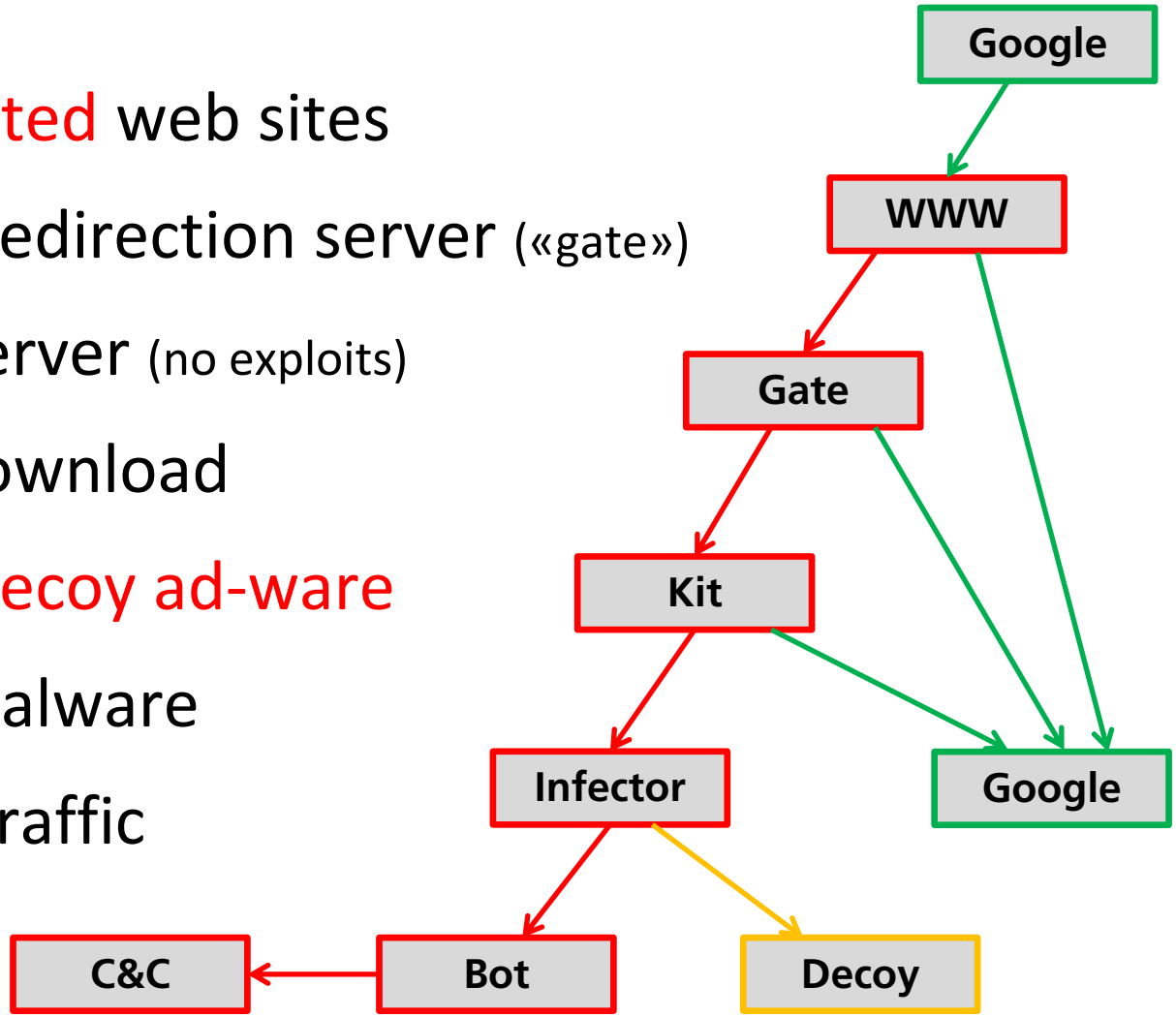
Outline

- Overview of malware infection steps
- Other publications about Zuponcic Kit
- Traffic delivery to Zuponcic Kit
- How to find infected web servers
- Ponmocup Finder for the Masses (Alexa top 1M scan)
- Botnet Anti-Sinkholing technique
- Finding Bot infections from DNS traffic
- Passive DNS on C2 domains

Overview of Malware infection steps

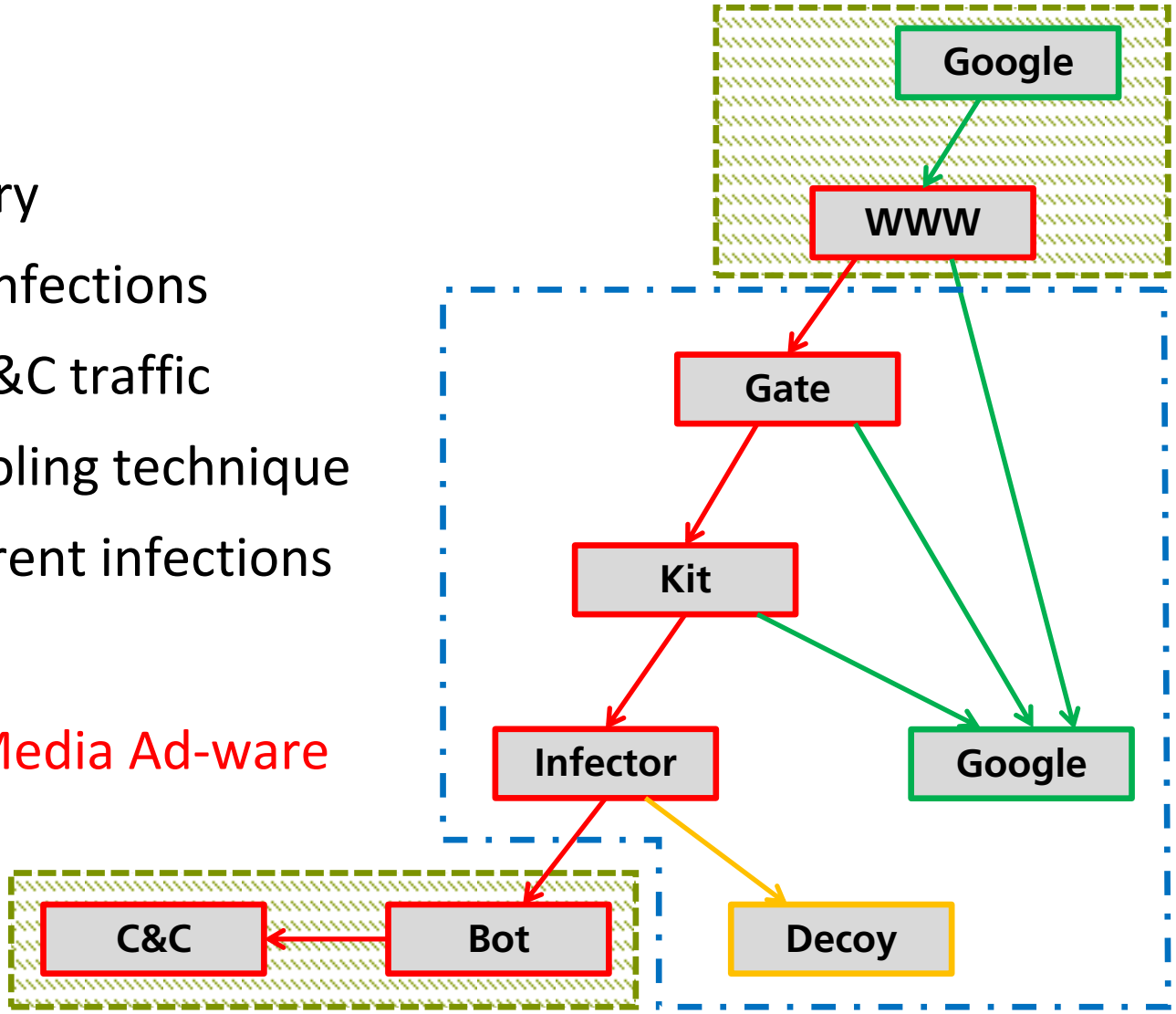
Overview: Bot infection steps

- .htaccess infected web sites
- Intermediate redirection server («gate»)
- Zuponcic Kit server (no exploits)
- Bot infector download
- Anti-analysis decoy ad-ware
- The real bot malware
- Stealthy C&C traffic
  (Anti-Sinkholing)



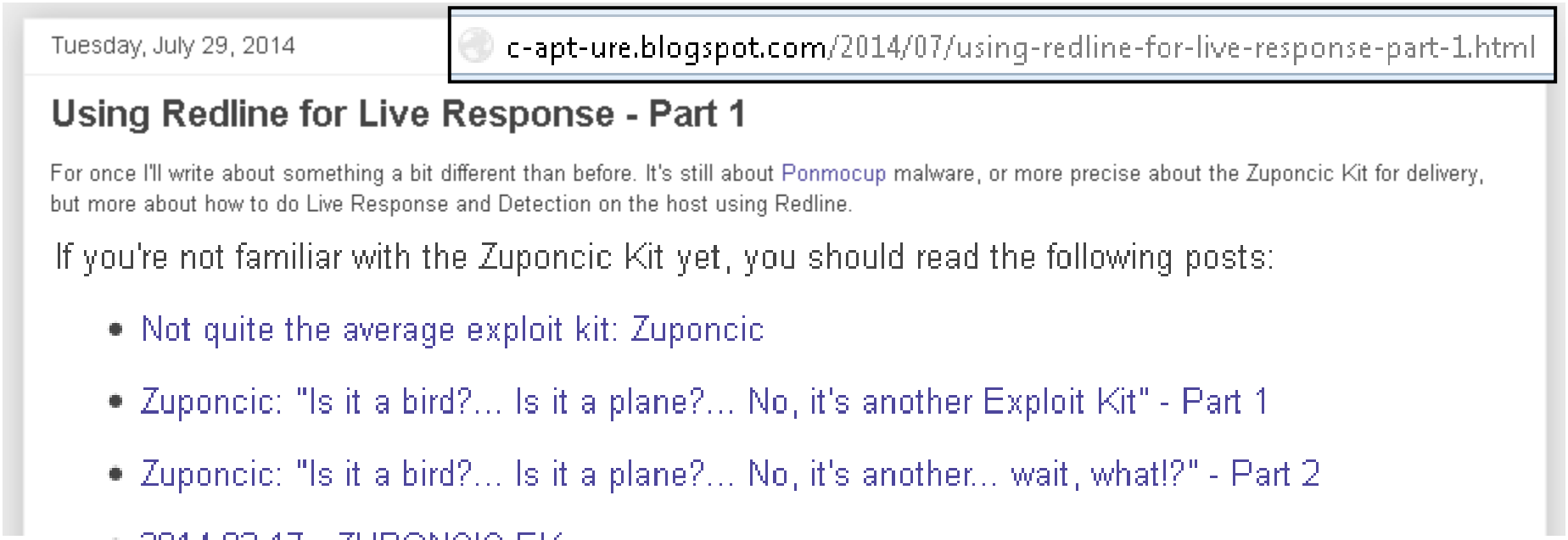
Overview: Focussing on…

- In focus
  - ➢ Traffic delivery
    - ✓ Stop new infections
  - ➢ Ponmocup C&C traffic
    - ✓ Anti-Sinkholing technique
    - ✓ Detect current infections
- Out of focus
  - ➢ Sanctioned Media Ad-ware
  - ➢ Zuponcic Kit

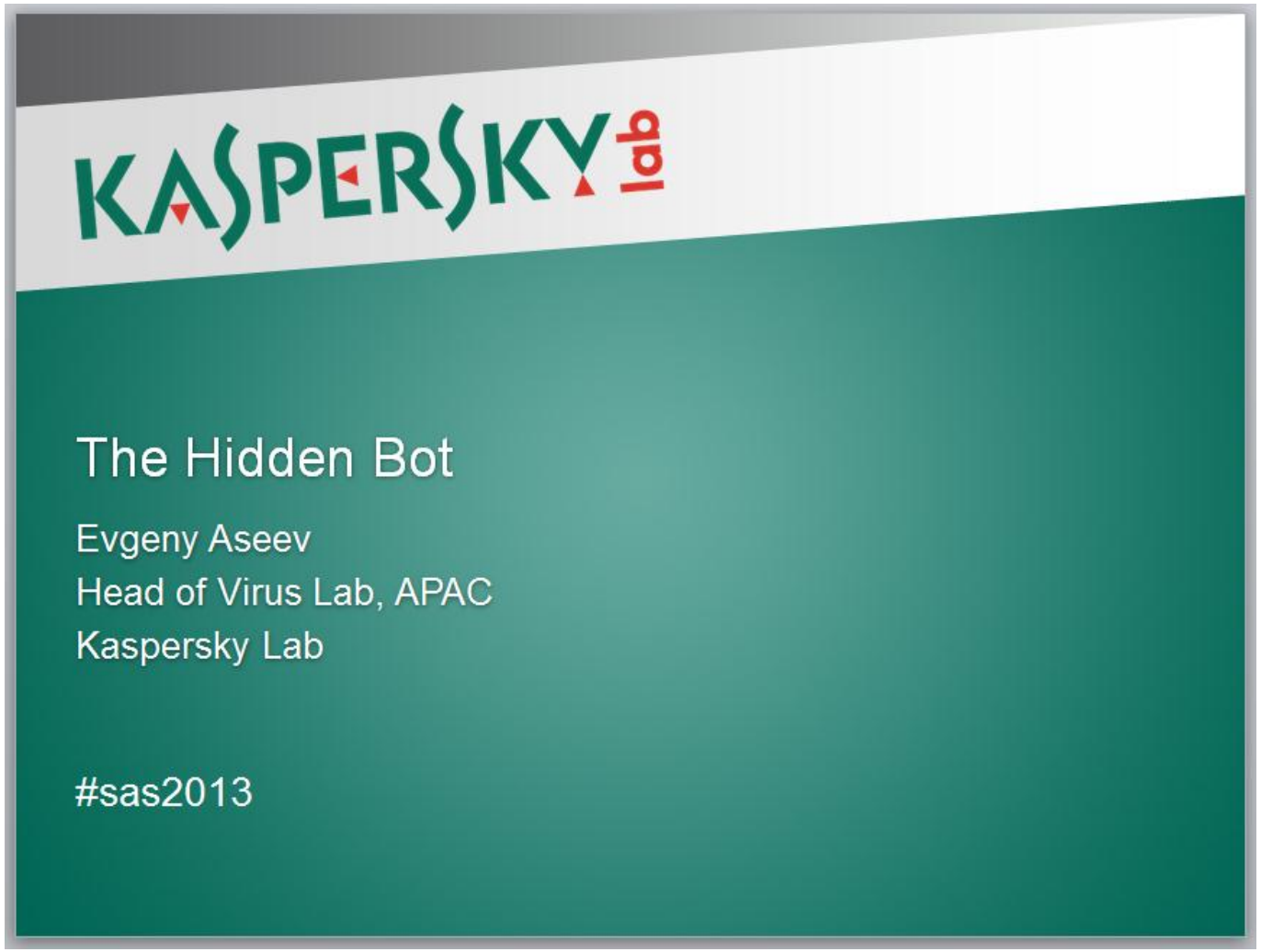


Other Publications about Zuponcic Kit

Other publications (Links on my Blog)



Kaspersky: «The Hidden Bot» SAS2013



http://media.kaspersky.com/en/Events/Presentations/Evgeny%20Aseev_The%20Hidden%20bot.pdf

Kaspersky: «The Hidden Bot» SAS2013

What is hidden needs to be unhidden

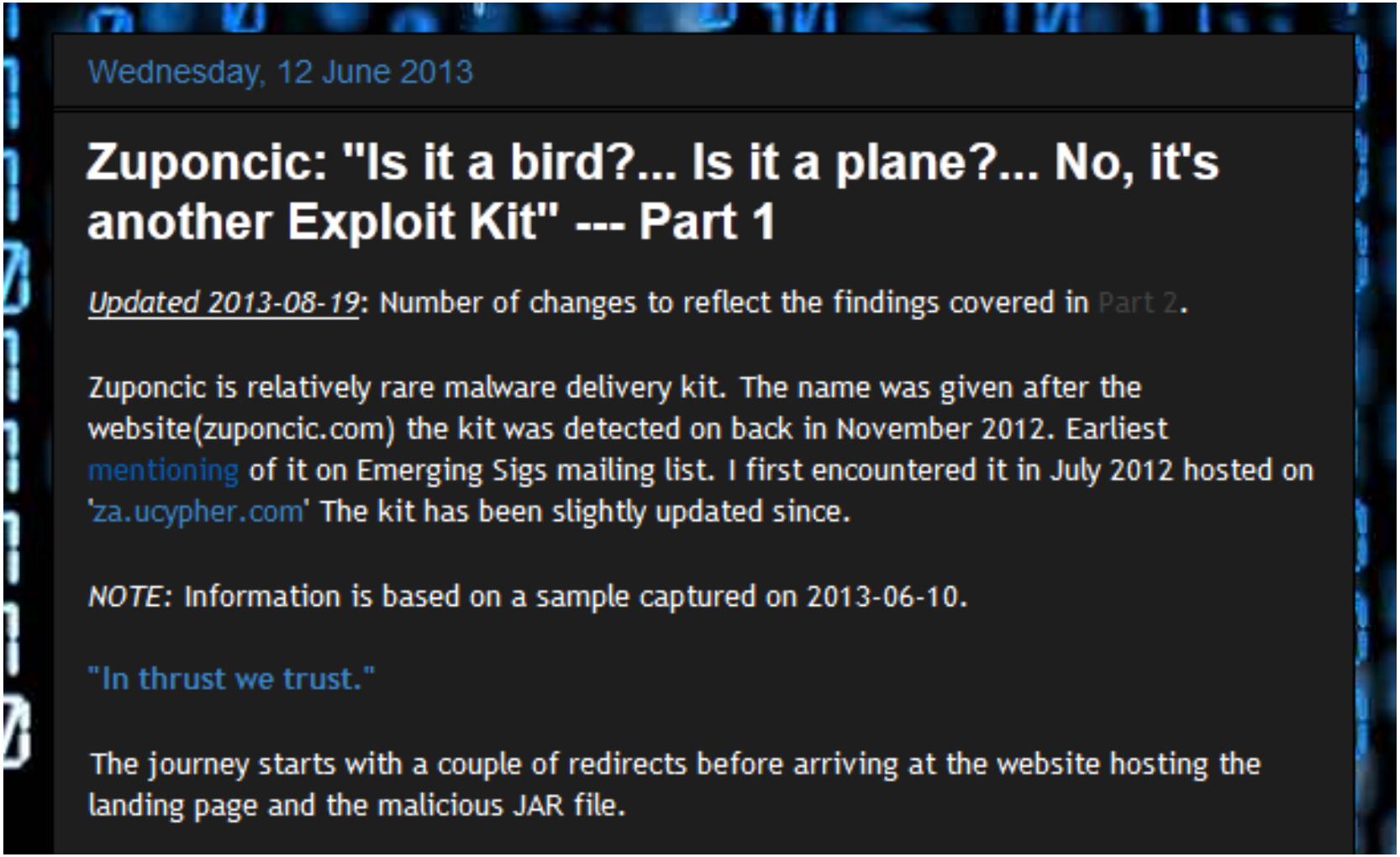
- What was unhidden
  - Very carefully crafted malicious campaign
  - Uses hacked websites, domains and dedicated servers for distribution, stolen digital certificates for infection
  - Robust protection from being analyzed/reversed
  - Target – install PUPs (PPI monetization model)
  - More than 3 years in the game, still roughly noticed by information security community and detected by AV vendors
- What needs to be unhidden
  - Current botnet size
  - Server-side code on dispatchers and infectors

PAGE 15 | 1 2 3 4

KASPERSKY

http://media.kaspersky.com/en/Events/Presentations/Evgeny%20Aseev_The%20Hidden%20bot.pdf

Malwageddon Blog: Zuponcic Kit



Wednesday, 12 June 2013

Zuponcic: "Is it a bird?... Is it a plane?... No, it's another Exploit Kit" --- Part 1

Updated 2013-08-19: Number of changes to reflect the findings covered in Part 2.

Zuponcic is relatively rare malware delivery kit. The name was given after the website(zuponcic.com) the kit was detected on back in November 2012. Earliest mentioning of it on Emerging Sigs mailing list. I first encountered it in July 2012 hosted on 'za.ucypher.com' The kit has been slightly updated since.

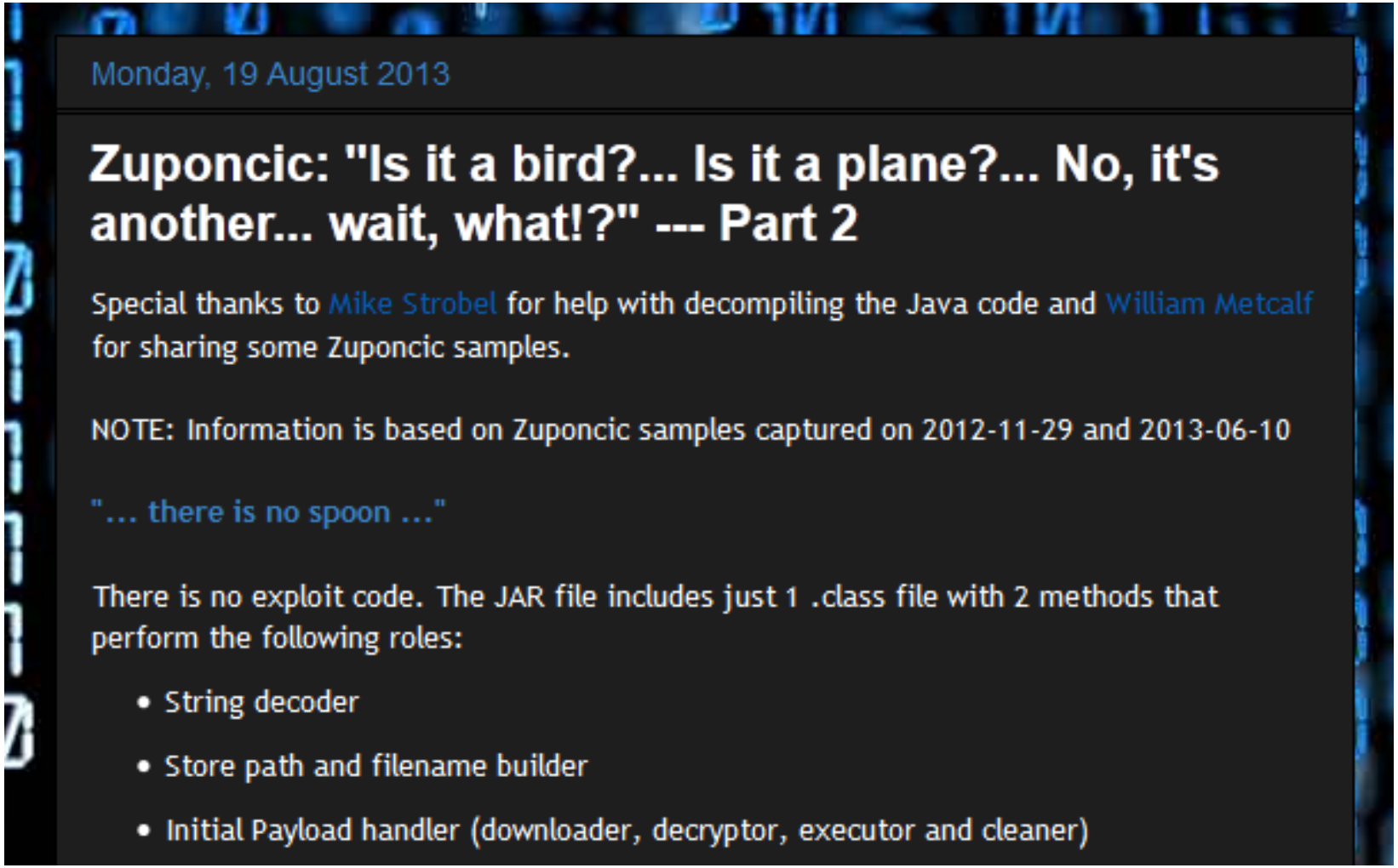
NOTE: Information is based on a sample captured on 2013-06-10.

"In thrust we trust."

The journey starts with a couple of redirects before arriving at the website hosting the landing page and the malicious JAR file.

http://malwageddon.blogspot.com/2013/06/zuponcic-is-it-bird-is-it-plane-no-its.html

Malwageddon Blog: Zuponcic Kit



Monday, 19 August 2013

Zuponcic: "Is it a bird?... Is it a plane?... No, it's another... wait, what!?" --- Part 2

Special thanks to Mike Strobel for help with decompiling the Java code and William Metcalf for sharing some Zuponcic samples.

NOTE: Information is based on Zuponcic samples captured on 2012-11-29 and 2013-06-10

"... there is no spoon ..."

There is no exploit code. The JAR file includes just 1 .class file with 2 methods that perform the following roles:

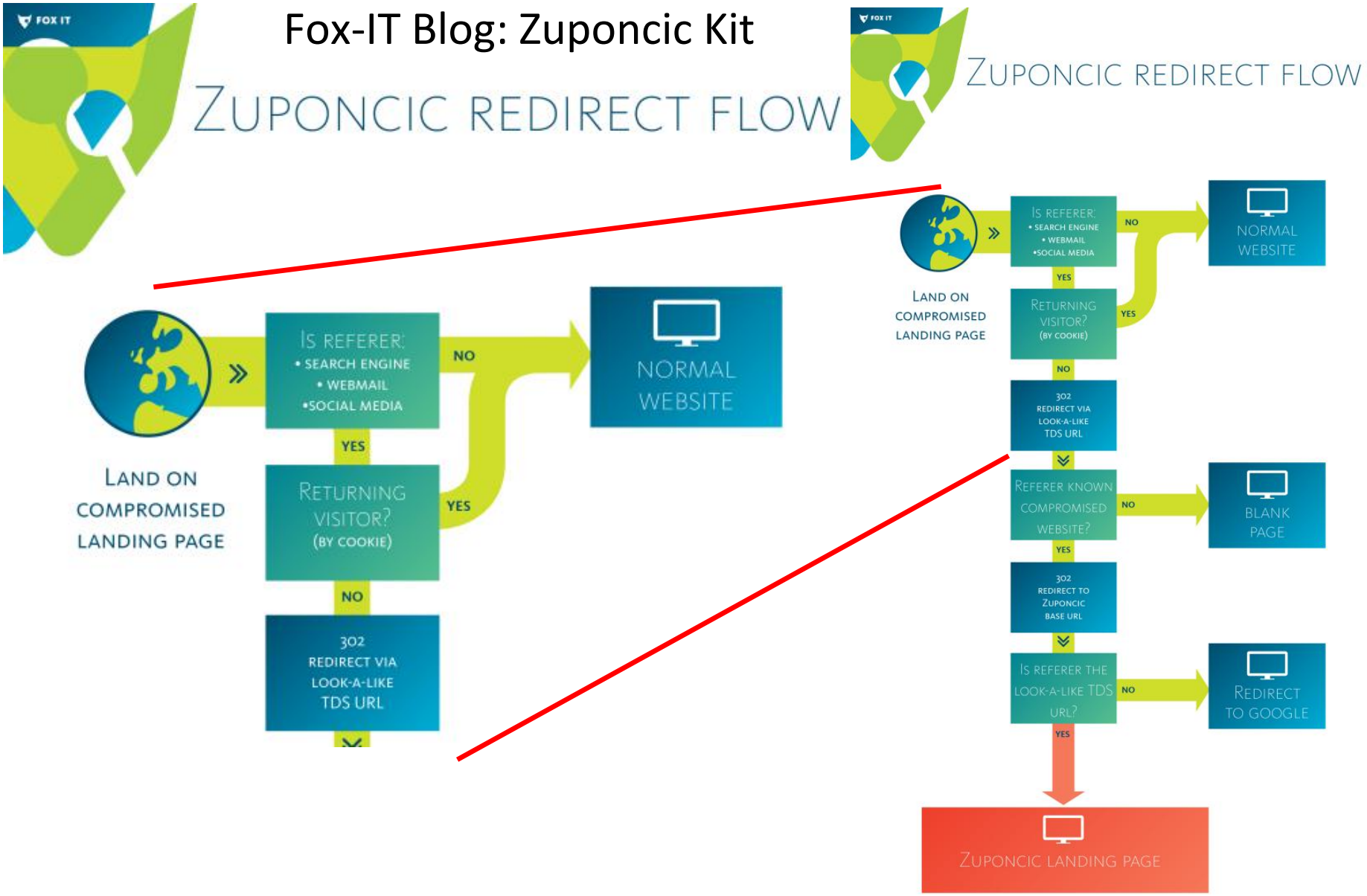
- String decoder
- Store path and filename builder
- Initial Payload handler (downloader, decryptor, executor and cleaner)

http://malwageddon.blogspot.com/2013/08/zuponcic-is-it-bird-is-it-plane-no-its.html

Fox-IT Blog: Zuponcic Kit

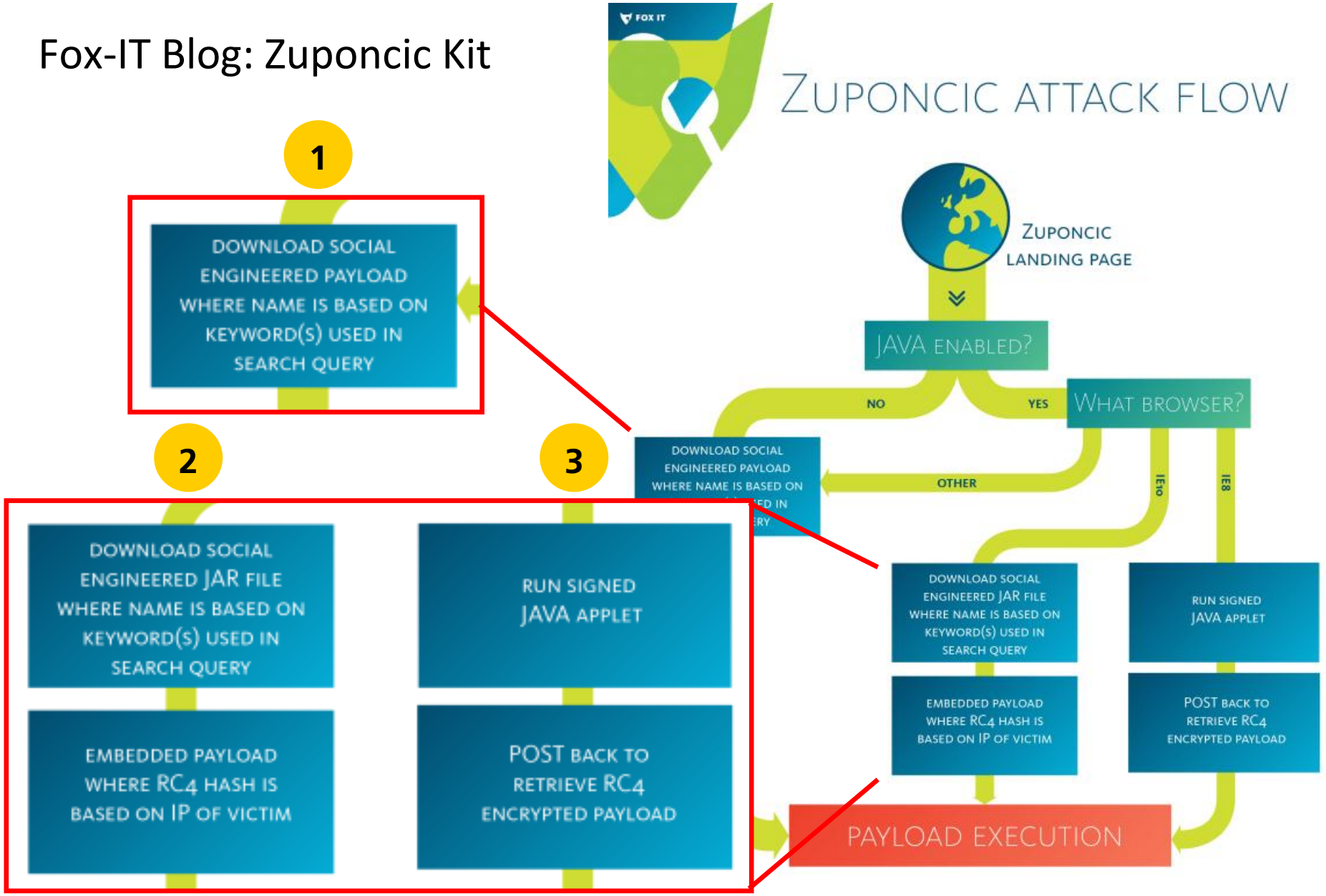
http://blog.fox-it.com/2013/12/19/not-quite-the-average-exploit-kit-zuponcic/

Fox-IT Blog: Zuponcic Kit



http://blog.fox-it.com/2013/12/19/not-quite-the-average-exploit-kit-zuponcic/

Fox-IT Blog: Zuponcic Kit



http://blog.fox-it.com/2013/12/19/not-quite-the-average-exploit-kit-zuponcic/

Other publications:

2014-03-17 - ZUPONCIC EK

PCAP AND MALWARE

- PCAP of the traffic: **2014-03-17-Zuponcic-EK-traffic.pcap**
- ZIP file of the malware: **2014-03-17-Zuponcic-EK-malware.zip**

NOTES

This is the first time I've run across Zuponcic. Here are some good blog posts about this exploit kit and the associated malware:

- **http://blog.fox-it.com/2013/12/19/not-quite-the-average-exploit-kit-zuponcic/**
- **http://malwageddon.blogspot.com/2013/08/zuponcic-is-it-bird-is-it-plane-no-its.html**
- **http://c-apt-ure.blogspot.com/2013/12/ponmocup-hunter-is-re-tired.html**

As the fox-it blog post states, the malware payload is encrypted using an RC4 hash, and I was unable to decrypted the malware payload disabled on the browser, the EK sends an archive for you to download. When I tried this, I was sent a 1.2 MB JAR file by the EK, which

PCAP and Malware in ZIP available for download

http://malware-traffic-analysis.net/2014/03/17/index.html

Other publications:

2014-03-17 - ZUPONCIC EK

PCAP AND MALWARE

CHAIN OF EVENTS

ASSOCIATED DOMAINS

- 217.76.156.117 - **www.silvergrey.es** - Compromised website
- 31.210.96.157 - **ambalanchery.drdekloet.com** - Redirect
- 178.33.192.35 - **ga.instylecuts.net** - Zuponcic EK
- 93.115.88.220 - **93.115.88.220** - First post-infection callback
- 66.254.123.33 - **www.sanctionedmedia.com** - Second post-infection callback

INFECTION CHAIN OF EVENTS

- 03:05:05 UTC - 192.168.204.188:49281 - 217.76.156.117:80 - www.silvergrey.es - GET /
- 03:05:06 UTC - 192.168.204.188:49282 - 31.210.96.157:80 - ambalanchery.drdekloet.com - GET /delivery/lg.php?bannerid=23350&campaignid=4402&zoneid=272&channel_ids=,&loc=http%3A%2F%2Fwww.silvergrey.es%2F&referer=http%3A%2F%2Fwww.silvergrey.es%2F&cb=bcaeb92e71
- 03:05:07 UTC - 192.168.204.188:49283 - 178.33.192.35:80 - ga.instylecuts.net - GET /
- 03:05:07 UTC - 192.168.204.188:49285 - 178.33.192.35:80 - ga.instylecuts.net - GET /js/java.js
- 03:05:07 UTC - 192.168.204.188:49286 - 178.33.192.35:80 - ga.instylecuts.net - GET /tr.gif
- 03:05:08 UTC - 192.168.204.188:49287 - 178.33.192.35:80 - ga.instylecuts.net - GET /favicon.ico
- 03:05:08 UTC - 192.168.204.188:49288 - 173.194.115.51:80 - www.google.com - GET /
- 03:05:18 UTC - 192.168.204.188:49289 - 178.33.192.35:80 - ga.instylecuts.net - GET /SnaorNJ.jar
- 03:05:24 UTC - 192.168.204.188:49290 - 178.33.192.35:80 - ga.instylecuts.net - POST /

http://malware-traffic-analysis.net/2014/03/17/index.html

Other publications:

MALWARE-TRAFFIC-ANALYSIS.NET

2014-03-17 - ZUPONCIC EK

PCAP AND MALWARE

CHAIN OF EVENTS

SNORT EVENTS

SNORT EVENTS FOR THE INFECTION TRAFFIC (from Sguil on **Security Onion**)

Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
2014-03-17 03:05:07	178.33.192.35	80	192.168.204.188	49283	6	ET CURRENT_EVENTS Unknown Java Exploit Version Check with hidden applet
2014-03-17 03:05:07	192.168.204.188	49285	178.33.192.35	80	6	ET CURRENT_EVENTS Zuponcic Hostile JavaScript
2014-03-17 03:05:07	178.33.192.35	80	192.168.204.188	49285	6	ET INFO JAVA - ClassID
2014-03-17 03:05:18	192.168.204.188	49289	178.33.192.35	80	6	ET POLICY Vulnerable Java Version 1.6.x Detected
2014-03-17 03:05:18	192.168.204.188	49289	178.33.192.35	80	6	ET CURRENT_EVENTS Zuponcic Hostile Jar
2014-03-17 03:05:18	178.33.192.35	80	192.168.204.188	49289	6	ET CURRENT_EVENTS Zuponcic EK Java Exploit Jar
2014-03-17 03:05:18	178.33.192.35	80	192.168.204.188	49289	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
2014-03-17 03:05:25	192.168.204.188	49290	178.33.192.35	80	6	ET CURRENT_EVENTS Zuponcic EK Payload Request

- 03:05:07 UTC - 192.168.204.188:49285 - 178.33.192.35:80 - ga.instylecuts.net - GET /js/java.js
- 03:05:07 UTC - 192.168.204.188:49286 - 178.33.192.35:80 - ga.instylecuts.net - GET /tr.gif
- 03:05:08 UTC - 192.168.204.188:49287 - 178.33.192.35:80 - ga.instylecuts.net - GET /favicon.ico
- 03:05:08 UTC - 192.168.204.188:49288 - 173.194.115.51:80 - www.google.com - GET /
- 03:05:18 UTC - 192.168.204.188:49289 - 178.33.192.35:80 - ga.instylecuts.net - GET /SnaorNJ.jar
- 03:05:24 UTC - 192.168.204.188:49290 - 178.33.192.35:80 - ga.instylecuts.net - POST /

http://malware-traffic-analysis.net/2014/03/17/index.html

Traffic Delivery to Zuponcic Kit Infection chain step 1

Malware Infection chain

- Traffic delivery through infected web servers
- Malicious .htaccess file
  - At least 3 major versions of .htaccess
- Commonly infected through stolen FTP creds

.htaccess – Hiding The Access

- .htaccess Kung-Fu checking for
  - Requested file type (web page, no pics etc.)
  - No cookie set (first visit)
  - User-Agent (regular browser / OS – no wget, crawler etc.)
  - Referer (coming from search engine, webmail, SNS)

```
RewriteCond %{REQUEST_FILENAME} !.*jpg$|.*gif$|.*png|.*jpeg|.*mpg|.*avi|.*zip|.*gz|.*t
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
RewriteCond %{HTTP_COOKIE}      !^.*MPR.*$ [NC]
RewriteCond %{HTTP_USER_AGENT}  .*(Windows|Macintosh|iPad|iPhone|iPod|Android).* [NC]
```

```
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
```

→ 2 x /16 blocked – hiding from who?

.htaccess – Hiding The Access

```
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
```

The following results may also be obtained via:
http://whois.arin.net/rest/nets;q=66.249.64.0?showDetails=true&showARIN=false&ext=netref2
#

NetRange:	66.249.64.0 - 66.249.95.255
CIDR:	66.249.64.0/19
NetName:	GOOGLE
NetHandle:	NET-66-249-64-0-1
Parent:	NET66 (NET-66-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	
Organization:	Google Inc. (GOGL)
RegDate:	2004-03-05
Updated:	2012-02-24
Ref:	http://whois.arin.net/rest/net/NET-66-249-64-0-1
OrgName:	Google Inc.
OrgId:	GOGL
Address:	1600 Amphitheatre Parkway
City:	Mountain View
StateProv:	CA

.htaccess – Hiding The Access

```
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
```

The following results may also be obtained via:
http://whois.arin.net/rest/nets;q=74.125.0.0?showDetails=true&showARIN=false&ext=netref2
#

NetRange:	74.125.0.0 - 74.125.255.255
CIDR:	74.125.0.0/16
NetName:	GOOGLE
NetHandle:	NET-74-125-0-0-1
Parent:	NET74 (NET-74-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	
Organization:	Google Inc. (GOGL)
RegDate:	2007-03-13
Updated:	2012-02-24
Ref:	http://whois.arin.net/rest/net/NET-74-125-0-0-1
OrgName:	Google Inc.
OrgId:	GOGL
Address:	1600 Amphitheatre Parkway
City:	Mountain View
StateProv:	CA

.htaccess – Hiding The Access

```
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
```

66.249.64.7	PTR	CRAWL-66-249-64-7.GOOGLEBOT.COM
66.249.64.56	PTR	CRAWL-66-249-64-56.GOOGLEBOT.COM
66.249.64.77	PTR	CRAWL-66-249-64-77.GOOGLEBOT.COM
66.249.64.139	A	CRAWL-66-249-64-139.GOOGLEBOT.COM
66.249.64.146	A	CRAWL-66-249-64-146.GOOGLEBOT.COM
66.249.64.158	PTR	CRAWL-66-249-64-158.GOOGLEBOT.COM
66.249.64.174	PTR	CRAWL-66-249-64-174.GOOGLEBOT.COM
66.249.64.205	A	CRAWL-66-249-64-205.GOOGLEBOT.COM
66.249.64.208	A	CRAWL-66-249-64-208.GOOGLEBOT.COM
66.249.64.209	A	CRAWL-66-249-64-209.GOOGLEBOT.COM
66.249.64.233	A	CRAWL-66-249-64-233.GOOGLEBOT.COM
66.249.64.236	PTR	CRAWL-66-249-64-236.GOOGLEBOT.COM
66.249.64.243	PTR	CRAWL-66-249-64-243.GOOGLEBOT.COM
66.249.65.9	A	CRAWL-66-249-65-9.GOOGLEBOT.COM
66.249.65.15	PTR	CRAWL-66-249-65-15.GOOGLEBOT.COM
66.249.65.22	A	CRAWL-66-249-65-22.GOOGLEBOT.COM

.htaccess – Hiding The Access

```
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
```

66.249.79.215	PTR	CRAWL-66-249-79-215.GOOGLEBOT.COM
66.249.79.252	PTR	CRAWL-66-249-79-252.GOOGLEBOT.COM
66.249.80.18	PTR	GOOGLE-PROXY-66-249-80-18.GOOGLE.COM
66.249.80.28	A	GOOGLE-PROXY-66-249-80-28.GOOGLE.COM
66.249.80.46	PTR	GOOGLE-PROXY-66-249-80-46.GOOGLE.COM
66.249.80.53	PTR	GOOGLE-PROXY-66-249-80-53.GOOGLE.COM
66.249.80.60	A	GOOGLE-PROXY-66-249-80-60.GOOGLE.COM
66.249.80.123	A	GOOGLE-PROXY-66-249-80-123.GOOGLE.COM
66.249.80.155	A	GOOGLE-PROXY-66-249-80-155.GOOGLE.COM
66.249.80.161	A+PTR	GOOGLE-PROXY-66-249-80-161.GOOGLE.COM
66.249.80.168	PTR	GOOGLE-PROXY-66-249-80-168.GOOGLE.COM
66.249.80.176	A	GOOGLE-PROXY-66-249-80-176.GOOGLE.COM
66.249.80.183	PTR	GOOGLE-PROXY-66-249-80-183.GOOGLE.COM
66.249.80.187	PTR	GOOGLE-PROXY-66-249-80-187.GOOGLE.COM
66.249.80.222	PTR	GOOGLE-PROXY-66-249-80-222.GOOGLE.COM
66.249.80.225	PTR	GOOGLE-PROXY-66-249-80-225.GOOGLE.COM

How to find infected web servers? Introducing Ponmocup Finder

c-APT-ure

Sunday, June 3, 2012

Introducing Ponmocup-Finder

Update 2013-06-01:
Please also read my newer blog posts about Ponmocup:

- "Ponmocup Hunter" SANS DFIR Summit 2013
- History of Ponmocup Malware / Botnet

Ponmocup-Finder has evolved in a little "workflow" :-)

1. add new infected domains to the list
2. daily cronjob to run Ponmocup-Finder
3. latest Ponmocup-Finder script
4. list of currently infected webservers
5. history of all previously infected webservers
6. notification lists for CH / LI and DE domains

If you can do notifications for any infected webservers, go ahead and feel free to let me know.

c-APT-ure

Tuesday, June 3, 2014

Two years later...

By chance I just noticed that I wrote the Introducing Ponmocup Finder blog post exactly two years ago.

So it's time to celebrate the second anniversary :-)

Well, I was wondering if anyone else is currently detecting the .htaccess infections that Ponmocup Finder (PF) reports. Let's see...

Let's just look at any of the almost 500 domains currently being detected by PF as infected.

http://security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-infected-domains-history-days-sort.txt

```
439 www.pino-travel.com
439 www.log-in-verlag.de
438 www.oople.com
438 www.franken-gmbh.de
438 www.brichzin.de
438 www.bad-saulgau.de
437 www.vitaminbude.de
```


```
438 www.bad-saulgau.de
437 www.vitaminbude.de
```


This German site has been seen infected since more than 430 days.

This German site has been seen infected since more than 430 days.

c-APT-ure

Tuesday, June 3, 2014

Two years later...

By chance I just noticed that I wrote the Introducing Ponmocup Finder blog post exactly two years ago.

So it's t

Well, I v

s. Let's see...

Let's jus

http://se

sort.txt

```
439 ww
439 ww
438 ww
438 ww
438 ww
438 ww
437 ww
```

This Ge

I haven't found any other detections. If you know of one, please let me know.

http://www.urlvoid.com/scan/bad-saulgau.de/

Website Information

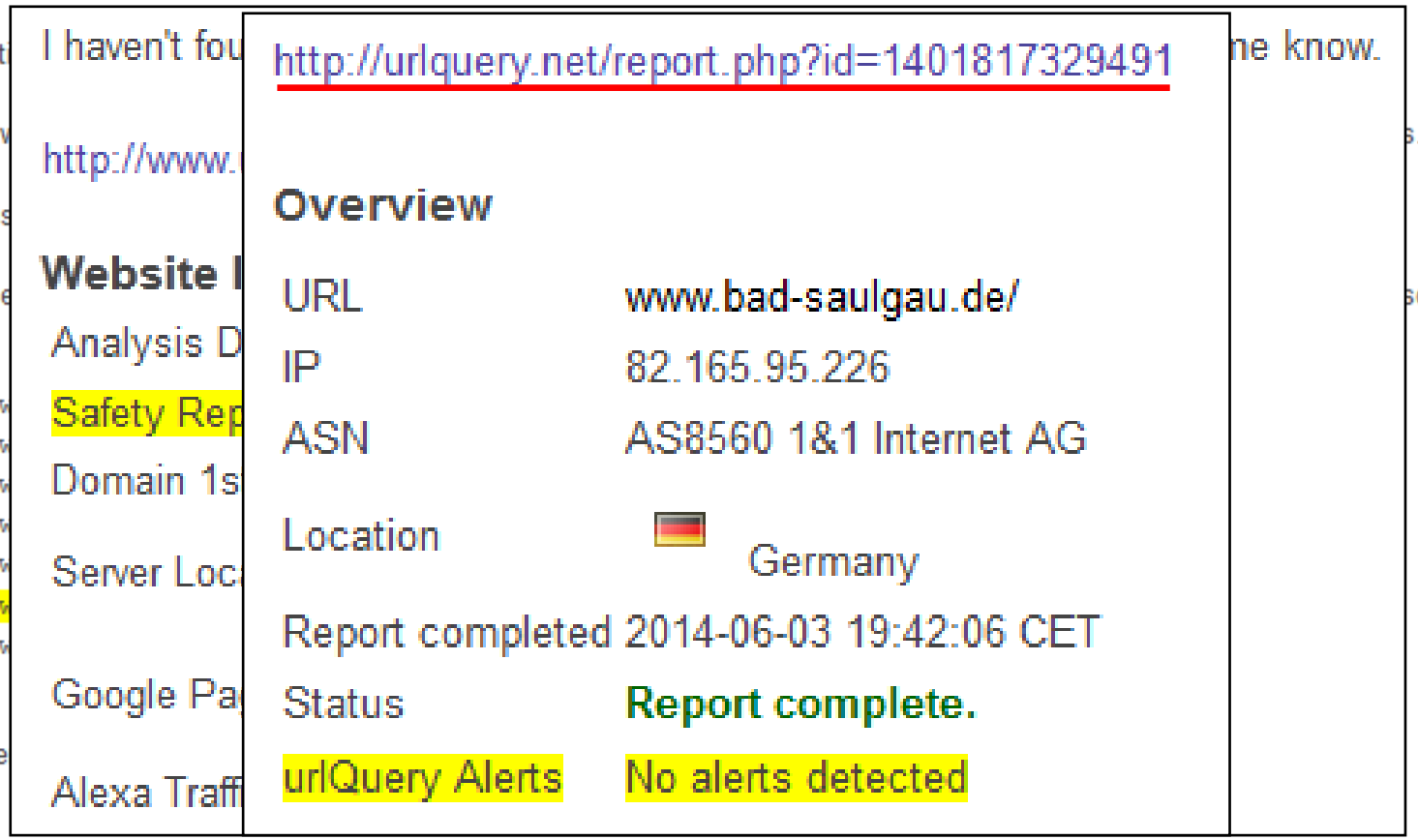
Analysis Date	8 seconds ago
Safety Reputation	0/28
Domain 1st Registered	Unknown
Server Location	(DE) Germany
Google Page Rank	PAGE RANK 4
Alexa Traffic Rank	1,751,096

c-APT-ure

Tuesday, June 3, 2014

Two years later...

By chance I just noticed that I wrote the Introducing Ponmocup Finder blog post exactly two years ago.



c-APT-ure

Tuesday, June 3, 2014

Two years later...

By chance I just noticed that I wrote the Introducing Ponmocup Finder blog post exactly two years ago.

So it's t

Well, I v

Let's jus

http://se

439 ww
439 ww
438 ww
438 ww
438 ww
438 ww
437 ww

This Ge

I haven't fou

http://www.

Website I

Analysis D

Safety Rep

Domain 1s

Server Loc

Google Pa

Alexa Traff

http://urlqu

Overview

URL

IP

ASN

Location

Report cor

Status

urlQuery A

Intrusion Detection Systems

Snort /w Sourcefire VRT	No alerts detected
Suricata /w Emerging Threats Pro	No alerts detected

Blacklists

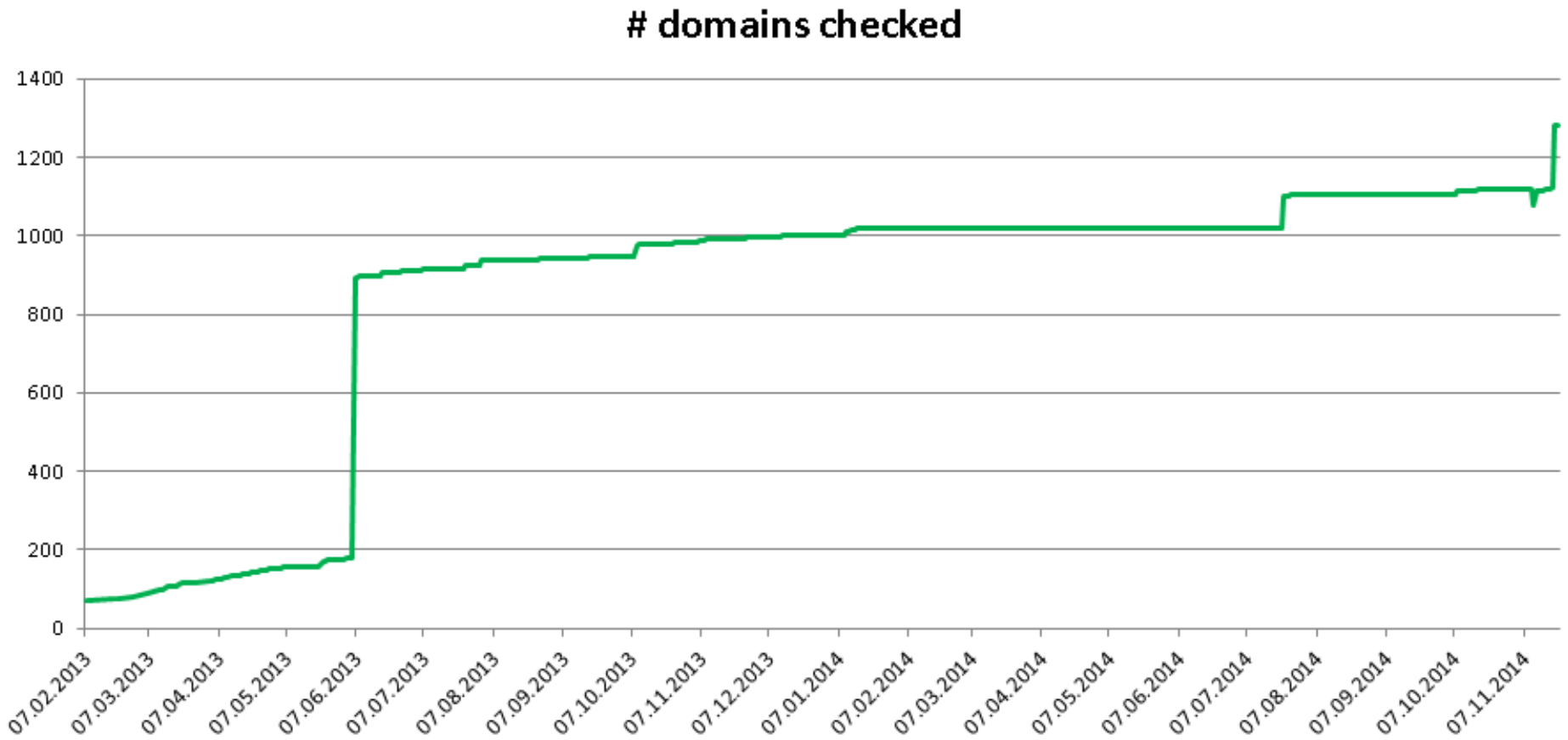
DNS-BH / malwaredomains.com	No alerts detected
PhishTank / phishtank.com	No alerts detected
Spamhaus DBL / spamhaus.org	No alerts detected

Files Captured

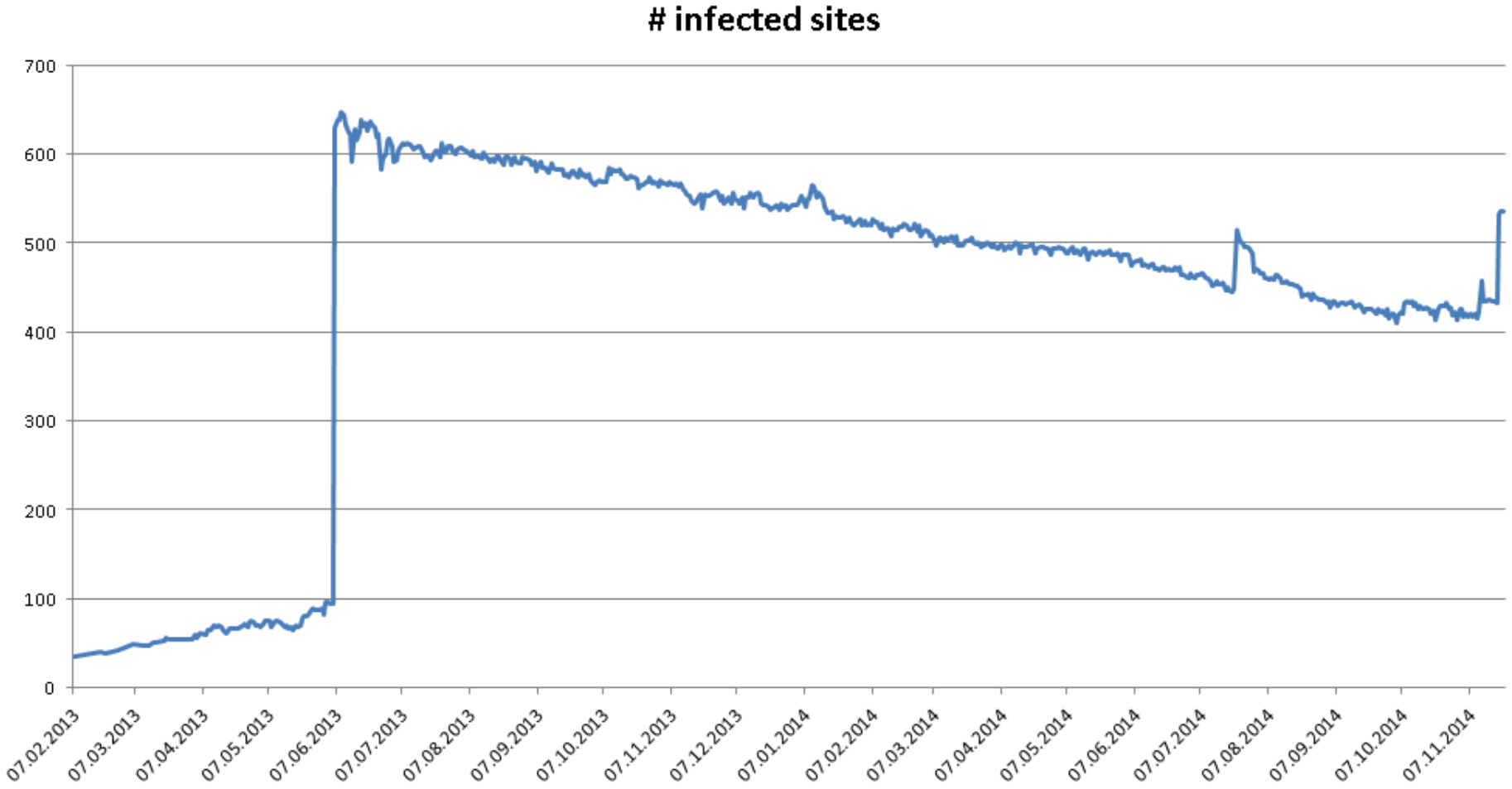
Suricata IDS No files captured

Thanks for mentioning ☺

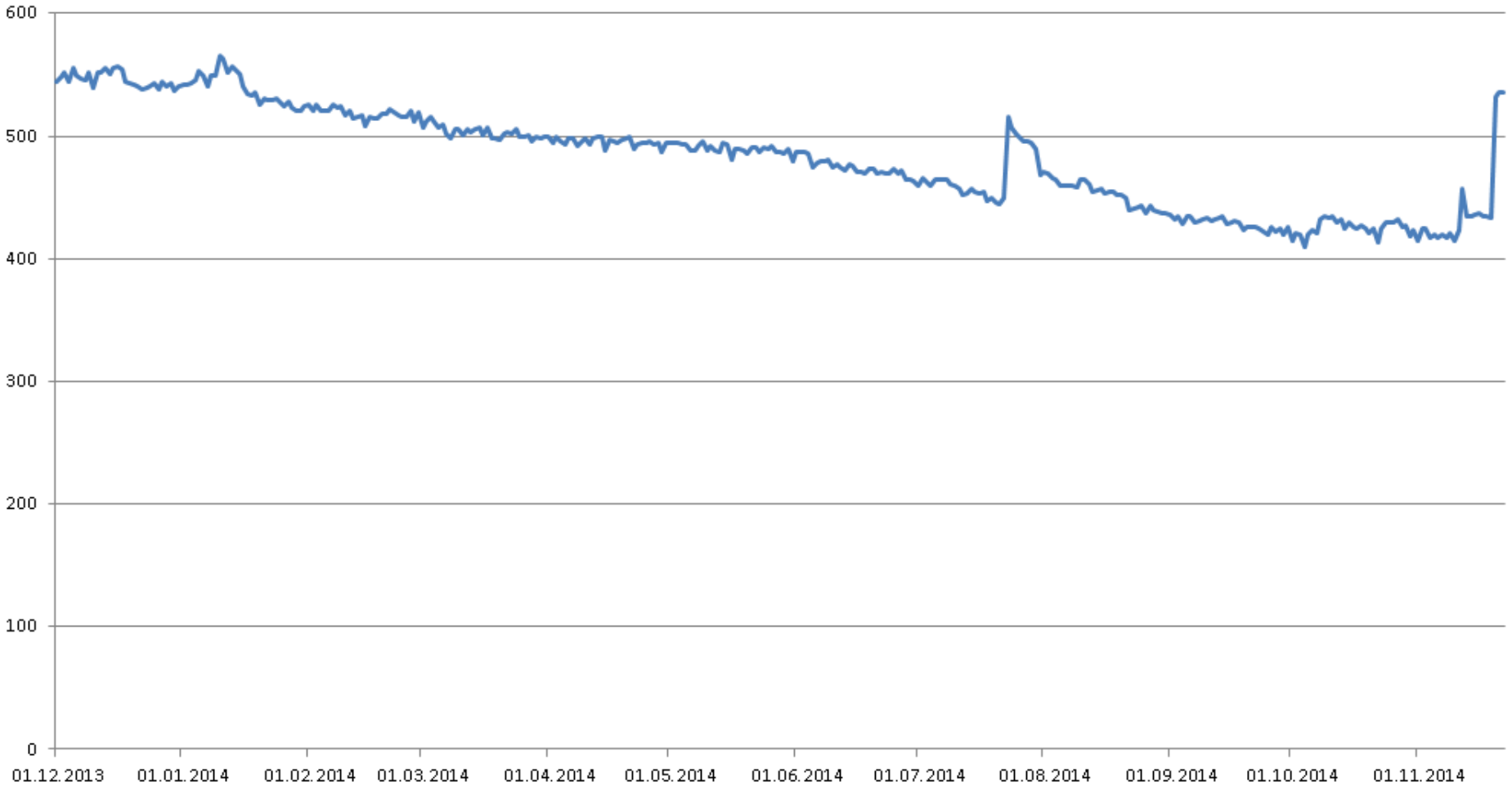
Tracking Infected Servers (21mo)



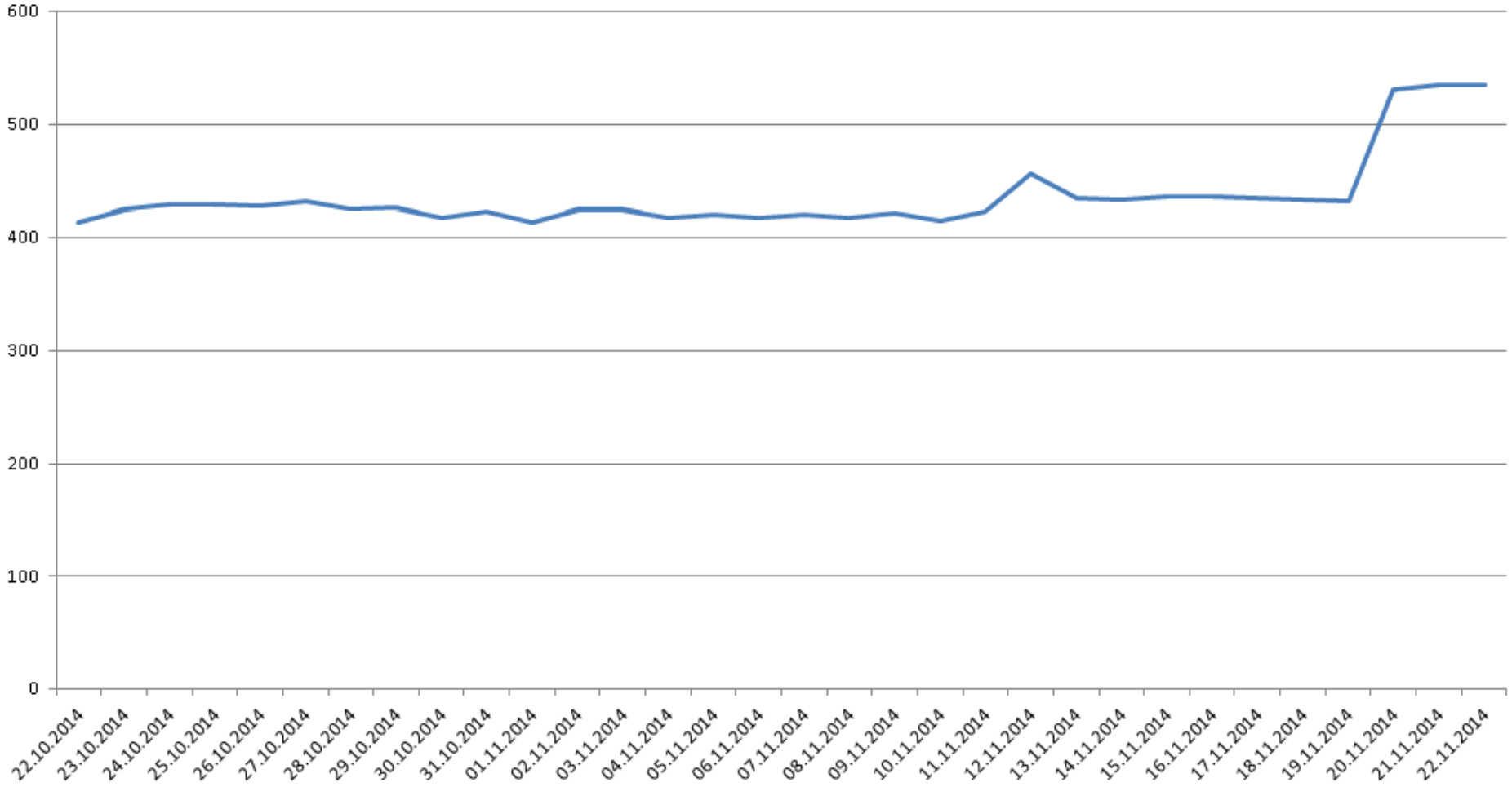
Tracking Infected Servers (21mo)



Tracking Infected Servers (12mo)



Tracking Infected Servers (1mo)



Tracking Infected Servers

last seen	first seen	domain	days
16.11.2014	07.02.2013	agroservis.rs	647
16.11.2014	07.02.2013	oople.com	647
16.11.2014	07.02.2013	www.asia-federblumen.de	647
16.11.2014	07.02.2013	www.bad-saulgau.de	647
16.11.2014	07.02.2013	www.greenfieldadvisorsltd.com	647
16.11.2014	07.02.2013	www.jordanbad.de	647
16.11.2014	07.02.2013	www.log-in-verlag.de	647
16.11.2014	07.02.2013	www.oople.com	647
16.11.2014	07.02.2013	www.pino-travel.com	647
16.11.2014	07.02.2013	www.vitaminbude.de	647
16.11.2014	19.02.2013	www.brichzin.de	635
16.11.2014	06.03.2013	www.foto-weller.de	620
16.11.2014	06.03.2013	www.golden-champion.com	620
16.11.2014	06.03.2013	www.mazus-art.com	620
16.11.2014	11.03.2013	www.niceshop.at	615
16.11.2014	13.03.2013	www.laufen-in-koeln.de	613
16.11.2014	15.03.2013	www.compta-geniale.com	611
16.11.2014	15.03.2013	www.xerox-drucker.de	611
16.11.2014	16.03.2013	www.recrutam.ro	610

Tracking Infected Servers

last seen	first seen	domain	days
06.03.2013	06.03.2013	www.lerchdesign.ch	0
23.07.2014	23.07.2014	blog.chlehmann.ch	0
23.07.2014	23.07.2014	www.bundesbaehnli.ch	0
23.07.2014	23.07.2014	www.lecubedeverre.ch	0
23.07.2014	23.07.2014	www.sanitaetshaus-brunner.ch	0
17.10.2014	17.10.2014	www.versoixathle.ch	0
16.11.2014	16.11.2014	www.weltkinderdoerfer.ch	0
28.11.2013	27.11.2013	cmsports.ch	1
11.01.2014	10.01.2014	www.elecar.ch	1
11.01.2014	10.01.2014	www.rigozzi.ch	1
24.07.2014	23.07.2014	www.bodenexpo.ch	1
24.07.2014	23.07.2014	www.holzsteiner.ch	1
24.07.2014	23.07.2014	www.terminkalender.ch	1
28.10.2013	26.10.2013	www.favremenuiserie.ch	2
09.11.2013	07.11.2013	promozionebenessere.ch	2
25.07.2014	23.07.2014	elevagedupetitroyaume.ch	2
25.07.2014	23.07.2014	saperiesaporidimarche.ch	2
25.07.2014	23.07.2014	www.carnatchaux.ch	2
25.07.2014	23.07.2014	www.delifranceshop.ch	2
25.07.2014	23.07.2014	www.eichhoernli-chueche.ch	2
25.07.2014	23.07.2014	www.hutchdesign.ch	2

~~Tracking~~ Clean-up Infected Servers

last seen	first seen	domain	days
06.03.2013	06.03.2013	www.lerchdesign.ch	0

security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-infected-domains-latest_CH-LI.txt

```
date started: Fri Nov 21 12:00:01 CET 2014
checking domain: www.weltkinderdoerfer.ch --> seems to be INFECTED: http://dekatey.cubpack910.com/url
date finished: Fri Nov 21 12:46:00 CET 2014
```

14	www.weltkinderdoerfer.ch	0
14	www.terminkalender.ch	1
13	www.favremenuiserie.ch	2
14	www.carnatchaux.ch	2
14	www.delifranceshop.ch	2
14	www.eichhoernli-chueche.ch	2
14	www.hutchdesign.ch	2

SWITCH

Thanks to SWITCH-CERT!

~~Tracking~~ Clean-up Infected Servers

security-research.dyndns.org/pub/malware-feeds/ponmocup-infected-domains-shadwoserver.csv

```
"timestamp","ip","http_host","url","port","application","tag","redirect_target"
"2014-11-30 12:00:01","85.13.131.32","b-my.de","/","80","http","htaccess-infected-webserver-leads-to
"2014-11-30 12:00:05","46.30.212.156","cioks.com","/","80","http","htaccess-infected-webserver-leads
"2014-11-30 12:00:09","193.104.37.193","www.toisondor.be","/","80","http","htaccess-infected-webserv
"2014-11-30 12:00:09","94.103.130.9","www.aca-uccle.be","/","80","http","htaccess-infected-webserver
"2014-11-30 12:00:10","188.165.238.48","www.lesscouts.be","/","80","http","htaccess-infected-webserv
"2014-11-30 12:00:11","109.72.85.37","www.centrumgregoriaans.be","/","80","http","htaccess-infected-
"2014-11-30 12:00:12","46.30.212.177","www.unetterbeek.be","/","80","http","htaccess-infected-webser
"2014-1                                                                                          webser
"2014-1                                                                                          bserv
"2014-1                                                                                          webser
"2014-1                                                                                          rver-l
"2014-1                                                                                          webser
"2014-1                                                                                          webser
"2014-1                                                                                          erver
"2014-1                                                                                          r-lea
"2014-1                                                                                          cted-
"2014-1                                                                                          cted-
"2014-11-30 12:00:46","200.234.196.139","agirazul.com.br","/","80","http","htaccess-infected-webserv
"2014-11-30 12:00:48","77.105.36.117","agroservis.rs","/","80","http","htaccess-infected-webserver-l
"2014-11-30 12:00:49","209.59.188.178","akhbaralyom.net","/","80","http","htaccess-infected-webserve
"2014-11-30 12:00:52","66.147.244.182","alastech.com","/","80","http","htaccess-infected-webserver-l
"2014-11-30 12:00:55","89.42.217.246","allandalla.ro","/","80","http","htaccess-infected-webserver-l
"2014-11-30 12:01:00","203.211.163.16","anzaisekizaiten.co.jp","/","80","http","htaccess-infected-we
"2014-11-30 12:01:06","199.16.128.51","apprendre-l-arabe.fr","/","80","http","htaccess-infected-webs
"2014-11-30 12:01:09","178.32.136.167","area-press.eu","/","80","http","htaccess-infected-webserver-
"2014-11-30 12:01:10","74.81.89.170","arlington.ph","/","80","http","htaccess-infected-webserver-lea
"2014-11-30 12:01:11","37.59.0.141","article-marketing.eu","/","80","http","htaccess-infected-webser
```

Ponmocup Finder for the masses

Idea: Find more Infected Servers

- Mass-Scan Ponmocup-Finder
- Rewrite Bash script in Python
- Use parallelization for more throughput
- Scan larger number of servers
- Use Alexa Top 1 million as PoC

«My crappy little Py script» [TM] ☺

```
#!/usr/bin/python

import sys
from grab import Grab

DOMAIN = sys.argv[1]
DOM_URL = ''.join(['http://', DOMAIN, '/'])

headers = {
           'User-Agent' : 'Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13)
           'Referer' : 'http://www.google.com/search?q=ponmocup+finder+check+pyGRAB'
           }

g = Grab(headers=headers)
g.setup(follow_location=False)
g.go(DOM_URL)

resp_code = g.response.code

if resp_code == 302:
    redir_loc = g.response.headers['Location']
    redir_url,redir_params = redir_loc.split("?")
    domain_found = redir_params.find(DOMAIN)
    if domain_found > 0:
        print "domain ", DOMAIN, " is INFECTED: ", redir_loc
        g.response.save(''.join([DOMAIN, '_infected.txt']))
    else:
        print "domain ", DOMAIN, " is clean (redir)"
else:
    print "domain ", DOMAIN, " is clean"
```

Idea: Find more Infected Servers

- Alexa Top 1M infected sites → 71 sites found
  - ➢ Top 16 and bottom 16

1	Alexa Rank	Infected Domain
2	7309	infobunda.com
3	26524	homeimprovement.com
4	50052	myomnistar.com
5	64445	d-math1.com
6	64537	mozicsillag.cc
7	97046	filmbirodalom.com
8	110536	ea3rf.com
9	138497	akhbaralyom.net
10	154791	ministerfortson.com
11	185226	cckorea.org
12	218318	hospitalesangeles.com
13	229974	dropshipthai.com
14	236924	espn-la.com
15	271997	desifucker.com
16	275080	tkne.net
17	279342	watch-movies-tv.info

1	Alexa Rank	Infected Domain
57	776810	badwapi.in
58	780345	sportstoursinternational.co.uk
59	781489	nicolaegabriel.info
60	790921	spitzer-onlinemarketing.de
61	800639	duikeninzutphen.nl
62	818311	healthnews8at8.com
63	821429	myyogasource.com
64	823227	intermundos.org
65	852531	radiogurbeti.com
66	864453	karavelle.com.br
67	879262	doggi-game.pl
68	899633	oople.com
69	899891	zarov.com.br
70	905825	munifrutillar.cl
71	979924	dialolinks.de
72	988485	webdesignfm.com

Higher Alexa rank != more secure

- Web site textpad.com infected in January 2014

  → Alexa Rank 134’291

www.urlvoid.com/scan/textpad.com/

Analyzed On	2014-01-10 16:19 GMT
Website Address	textpad.com
Blacklist Status	BLACKLISTED
Detection Ratio	1 / 27 (4 %)
Domain 1st Registered	1995-12-27 (18 years ago)
Google Page Rank	PAGE RANK 6
Alexa Rank	134,291

Website Blacklist Report

Engine	Status	Info
SCUMWARE	Alert DETECTED	Link

Higher Alexa rank != more secure

Follow TCP Stream

Stream Content

```
GET /products/textpad/features.html HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.google.com/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: www.textpad.com
Connection: Keep-Alive
Pragma: no-cache

HTTP/1.1 302 Found
Date: Fri, 10 Jan 2014 16:35:41 GMT
Server: Apache
Set-Cookie: kag=41; path=/; domain=www.textpad.com; expires=Sat, 18-Jan-2014 10:42:41 GMT
Location: http://reiseger.be3ne.com/pview?
event=pview&fpc=d96b1f4-137eaa87da1-3bf81330-7514&sessionID=1340974090144.21672&sourceURL=http%3A%2F%
2Fwww.textpad.com%2F&hostname=www.mangahere.com&location=/manga/anatolia_story/v02/
c004.1/11.html&publisher=e47efe7d-147b-4731-
ac42-9838ccdc52f2&shareHash=sthash.5HiSQv3v&incomingHash=&refDomain=www.mangahere.com&refQuery=manga/
anatolia_story/v02/c004.1/10.html&url=http%3A%2F%2Fwww.textpad.com%2F&sharURL=&source=share5x&title=Anatolia%
20Story%204.1%20-%20Read%20Anatolia%20Story%20Chapter%204.1%20Online%20-%20Page%2011&ts1340974090147.0=
Content-Length: 817
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://reiseger.be3ne.com/pview?
event=pview&amp;fpc=d96b1f4-137eaa87da1-3bf81330-7514&amp;sessionID=1340974090144.21672&amp;sourceURL=http%3A
%2F%2Fwww.textpad.com%2F&amp;hostname=www.mangahere.com&amp;location=/manga/anatolia_story/v02/
c004.1/11.html&amp;publisher=e47efe7d-147b-4731-
ac42-9838ccdc52f2&amp;shareHash=sthash.5HiSQv3v&amp;incomingHash=&amp;refDomain=www.mangahere.com&amp;refQuer
```

Higher Alexa rank != more secure

- 25% - 33% visitors from search engines ☹

Where do textpad.com's visitors come from?

www.alexa.com/siteinfo/textpad.com

Search Traffic

What percentage of visits to this site come from a search engine?

Search Visits

29.60% ▼ 2.00%

Top Keywords from Search Engines

Which search keywords send traffic to this site?

Keyword	Percent of Search Traffic
1. textpad	36.50%
2. text editor	18.20%
3. textpad download	15.57%
4. download textpad	2.97%
5. texteditor	2.32%

Upgrade to View

Prevent & Detect Bot Infections

- PRE-infection: Prevention
  - Block Malware IP-ranges (redirection / gate)
    - 178.211.33.202 – .206
    - 31.210.96.155 – .158
    - 81.92.219.60 – .62
- POST-infection: Detection (initial check-in only)
  - DNS Lookups for Domains:
    - intohave.com or fasternation.net
  - HTTP Connections to IP:
    - 88.216.164.117 or 5.199.175.164
    - 93.115.88.220

Find more infected Web Servers

- Search Proxy Logs for referrer URLs from requests to
  - Malware IP-ranges (redirection / gate)
    - 178.211.33.202 – .206
    - 31.210.96.155 – .158
    - 81.92.219.60 – .62

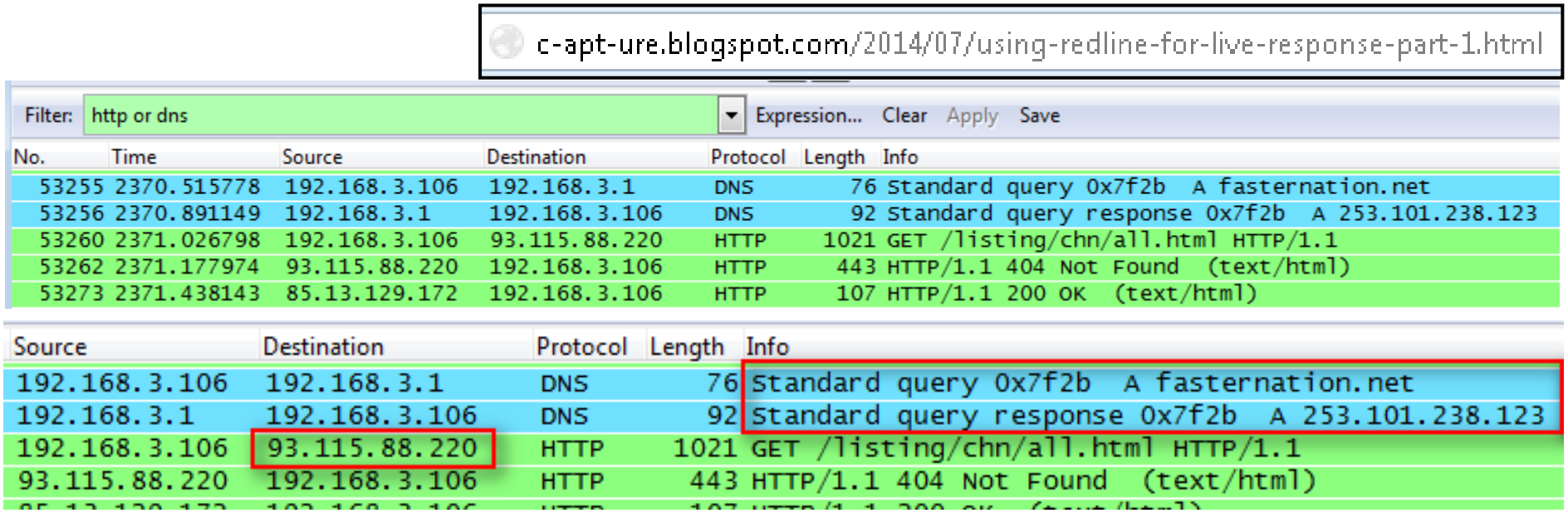
Sample Splunk & Bluecoat query:

```
index=bluecoat r_ip="178.211.33.202" OR r_ip="178.211.33.203" OR
r_ip="178.211.33.204" OR r_ip="178.211.33.205" OR
r_ip="178.211.33.206" OR r_ip="31.210.96.155" OR
r_ip="31.210.96.156" OR r_ip="31.210.96.157" OR
r_ip="31.210.96.158" OR r_ip="81.92.219.60" OR
r_ip="81.92.219.61" OR r_ip="81.92.219.62" | table _time, r_ip,
cs_host, cs_uri_path, cs_uri_query, cs_referer
```

Anti-Sinkholing technique of this botnet in detail

Anti-Sinkholing technique

- Resolving a C2-domain, but not using resolved IP?

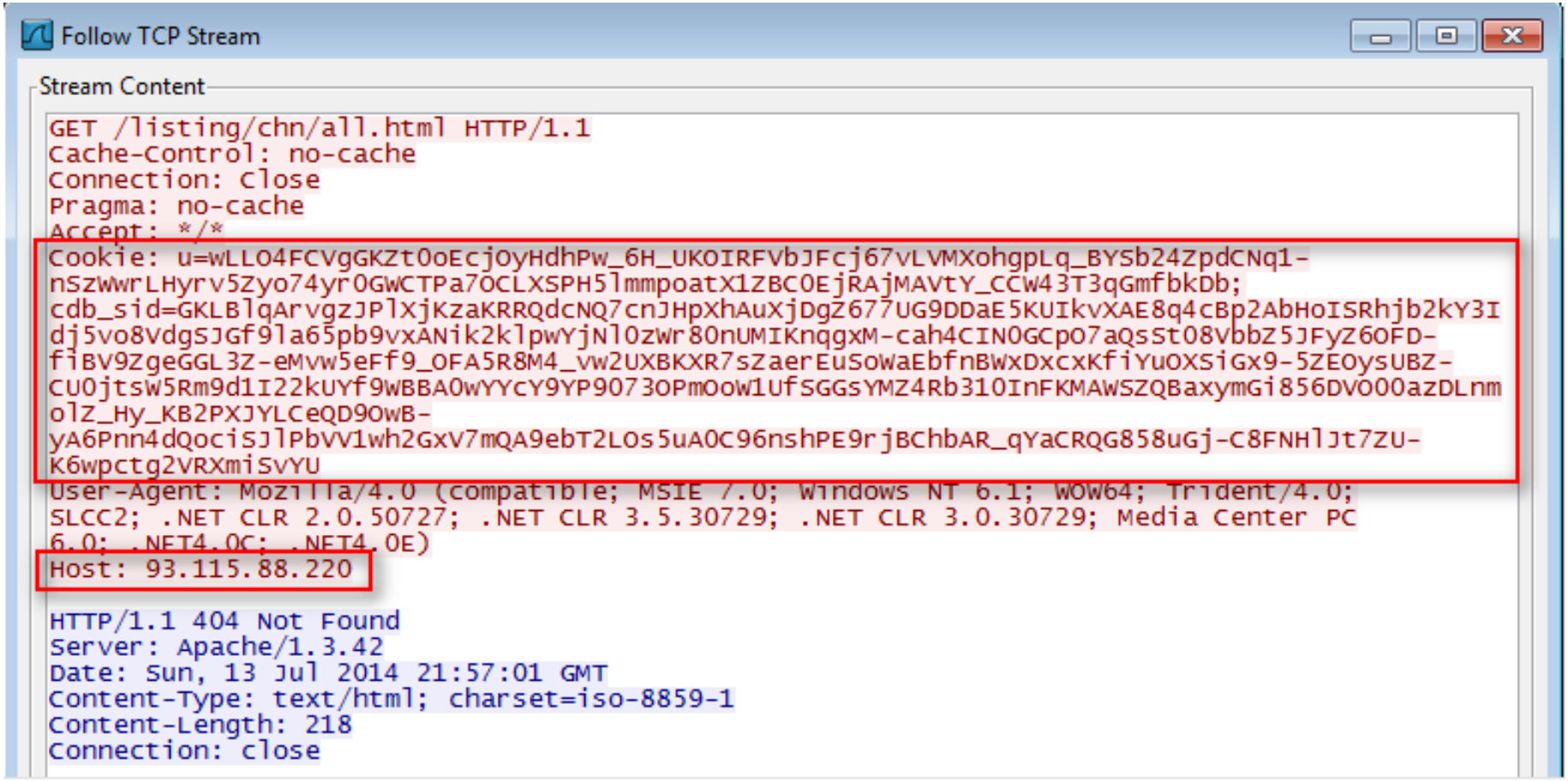


DNS(C2-domain) => IP1 → f() ? → C2(IP2)

- Unknown Anti-Sinkhole function f()

Anti-Sinkholing technique

- Data encrypted in Cookie value → C2(IP2)



Anti-Sinkholing technique

- Known variables
  - C2-domain = fasternation.net
  - DNS(fasternation.net) = 253.101.238.123
  - C2-IP = 93.115.88.220
- Unknown function
  - C2-IP = f(C2-domain, DNS(C2-domain))

→ Anyone wanna take a guess at f() ? ☺

Anti-Sinkholing technique

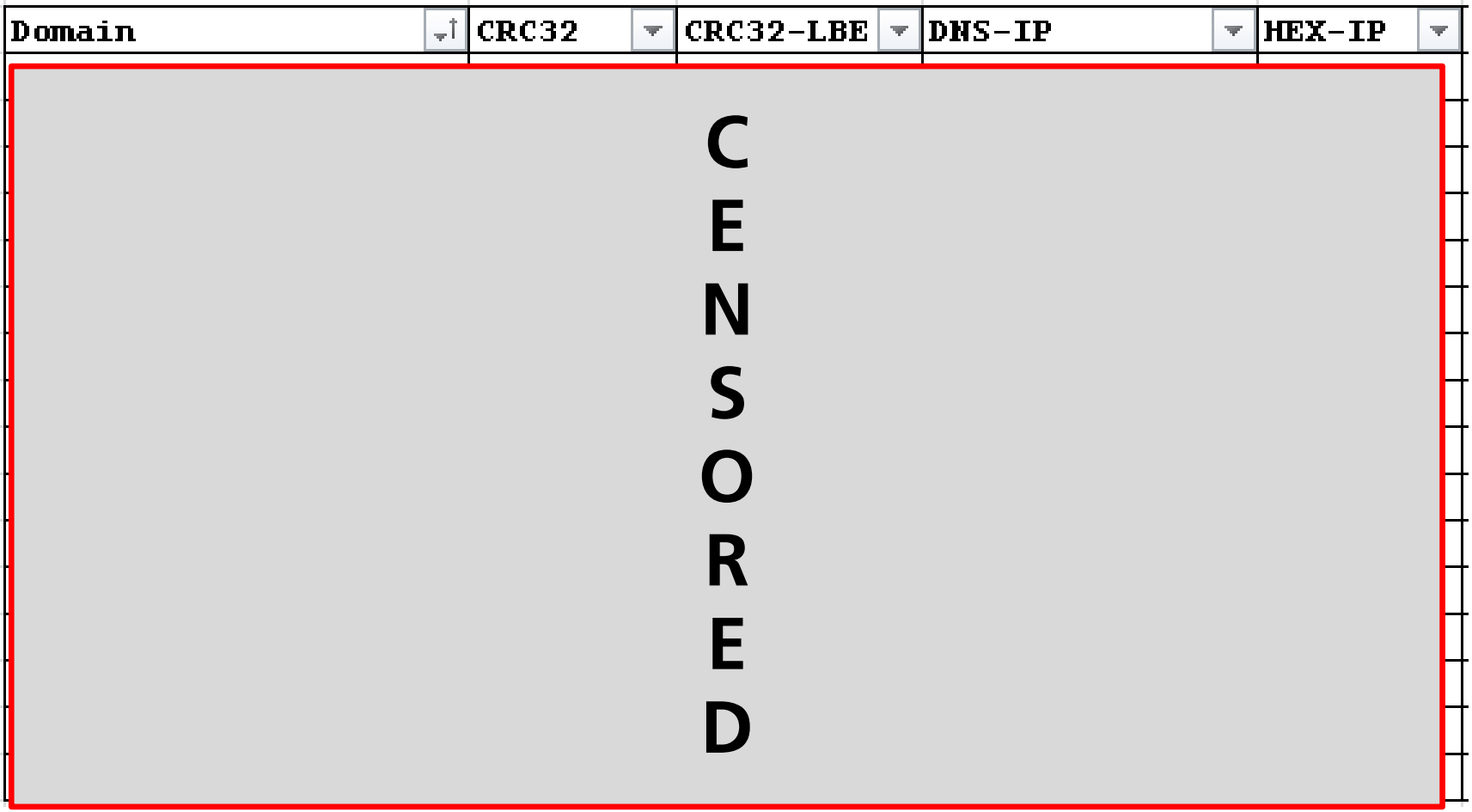
- Solving the unknown function
  - C2-domain = fasternation.net
  - DNS(fasternation.net) = 253.101.238.123
  - ip2hex(253.101.238.123) = **FD65EE7B**
  - CRC32(fasternation.net) = **A7B616A0**
  - little/big endian: **A7-B6-16-A0** → **A0-16-B6-A7**
  - **FD65EE7B** XOR **A016B6A7** = **5D7358DC**
  - hex2ip(**5D7358DC**) = 93.115.88.220

→ It's «trivial», right? ☺

→ Anti-Sinholing technique solved! *(with some help, thanks!)*

Anti-Sinkholing technique

- Here a few active C2 domains to practice ☺



Finding Bot infections from DNS traffic

Research on C2 domains

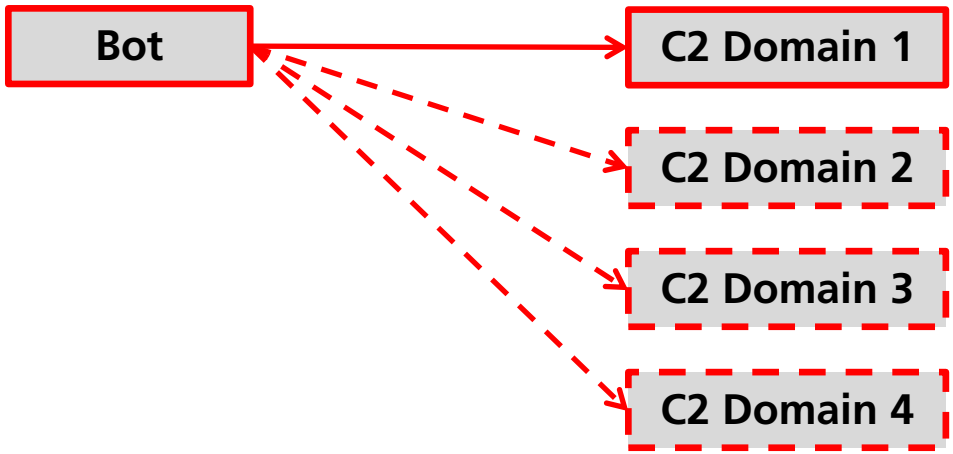
- Knowing some C2 domains and IPs
- Not having access to servers from IPs
- No sinkholing of C2 domains
  - How could we find infected bots?
  - How could we «guesstimate» botnet size?
  - What can we learn from Passive DNS?

Finding Bots w/out Sinkholing

- Starting with 5 known C2 domains
- Received DNS data from confidential source
  - Src-IP from C2 domain DNS requests
  - Total of 17 C2 domains (through correlation)
  - 27’404 requests in 6 days (10/29 – 11/04)
  - 6’814 unique Src-IPs
  - 2’177 unique ASN

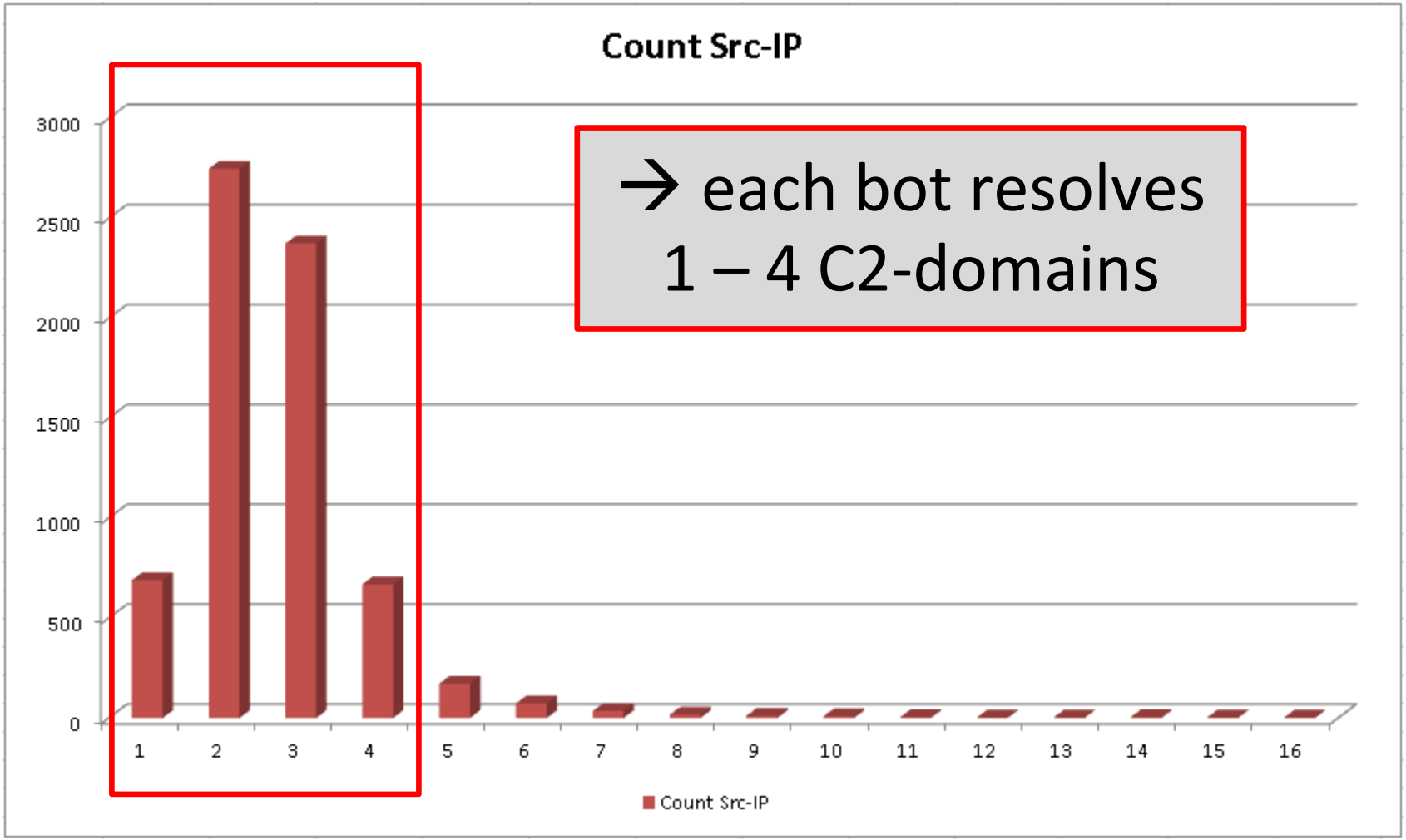
Finding Bots w/out Sinkholing

- Add some knowledge from a malware RE
- Malware has 4 C2 domains hardcoded
  - ➢ Possible 1 – 4 domains for C2 for each bot



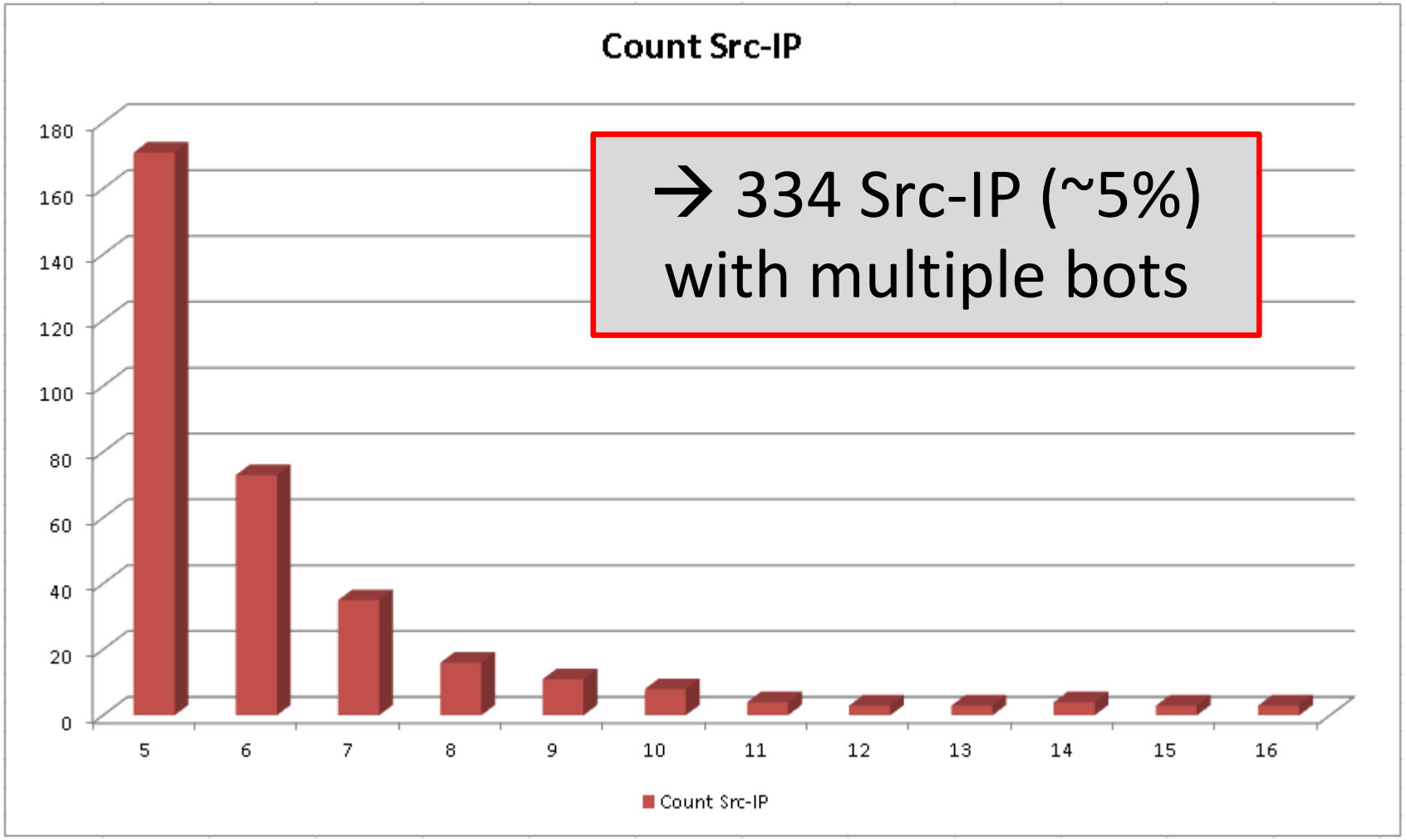
Finding Bots w/out Sinkholing

- How many C2-domains resolved per Src-IP (bot/bots)



Finding Bots w/out Sinkholing

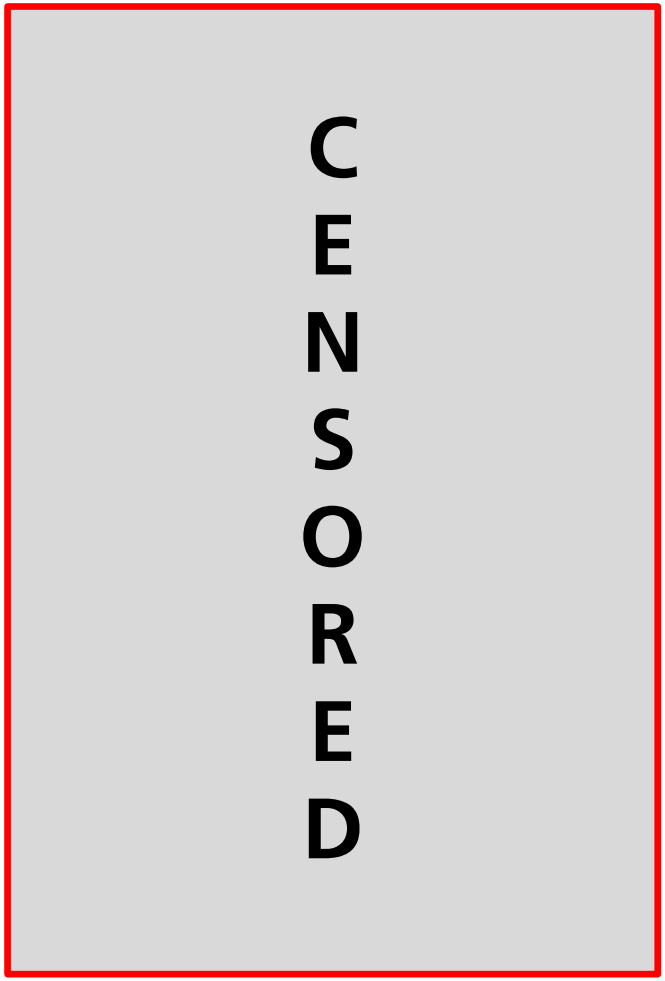
- How many Src-IP (bot/bots) with > 4 C2-domains



Finding Bots w/out Sinkholing

- # of DNS requests per C2 domain

2695
2664
2535
1941
1938
1794
1785
1757
1753
1710
1683
1648
996
991
798
670
45



Finding Bots w/out Sinkholing

- # of unique src-IP's per country (top 84)

#IPs	Country
1822	TR
910	US
465	BR
443	IN
228	VN
218	IT
168	DZ
164	GB
162	MX
148	AR
133	EG
130	CA
120	ID
107	TH
94	MY
92	DE
85	N/A
65	CO
62	SA
62	ES
60	PL

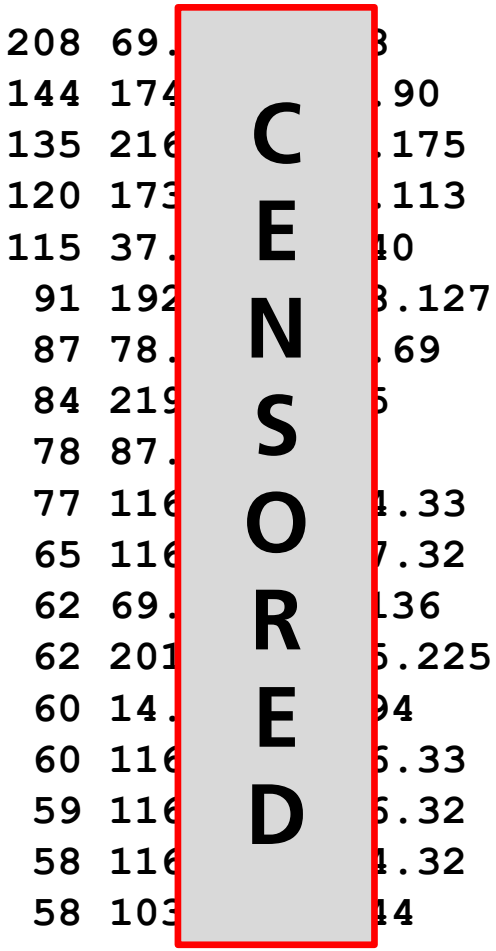
#IPs	Country
55	NL
50	PH
49	VE
47	EU
45	BE
41	AT
38	ZA
38	DK
36	PE
36	HU
35	CL
34	GR
32	PT
28	FR
26	AE
25	RO
24	IQ
18	BG
17	GT
16	RU
15	IR

#IPs	Country
14	HR
13	PR
13	DO
12	YE
12	SE
12	NG
12	IE
12	EC
12	CR
11	TN
11	BD
10	NO
10	BO
10	AU
9	UA
8	IL
7	QA
7	KE
7	BN
6	TT
6	SY

#IPs	Country
6	SG
6	PK
6	CY
6	CI
5	PS
5	KZ
5	JO
5	HK
5	CH
5	BA
4	UG
4	TW
4	RS
4	MK
4	LY
4	CZ
4	CN
4	AM
3	NI
3	LV
3	LU

Finding Bots w/out Sinkholing

- # of DNS requests per src-IP (top 18)



Finding Bots w/out Sinkholing

- ASN with most likely bot infections

```
AT   1853  STEIERMAERKISCHE KRANKENANSTALTEN GESMBH
DE  12312  STAEDTISCHE KLINIKEN FRANKFURT HOECHST
DE  20676  LANDESFINANZSCHULE BAYERN
DE   3320  BODENSEEWERK GERAETETECHNIK GMBH UEBERLINGEN
DE   3320  DEUTSCHE TELEKOM AG
DE   3320  LACK TISCHLER RECHTSANWAELTE PARTNERSCHAFT
BE   5432  BELGACOM S.A.
FR  51964  SITA-SOCIETE INTERNATIONALE DE TELECOMM. AERONAUTIQUES
GB  24958  THE BUNKER SECURE HOSTING LTD
GB    786  WELSH ASSEMBLY GOVERNMENT
IT   3269  FORD ITALIA S.P.A.
NL  42894  MINISTERIE VAN VERKEER EN WATERSTAAT/RIJKSWATERSTAAT
NO   5381  POWERTECH PTP NETWORK
US    100  THE ROYAL JORDANIAN AIRLINES PLC
US  16509  AMAZON TECHNOLOGIES INC.
US   1785  MECHANICAL DYNAMICS AND ANALYSIS
US  20115  AMERICAN CYBERSYSTEMS INC
US    209  AMERICARE SYSTEMS INC
US    209  COMMUNITY HOSPITAL
```

← not related to Regin ☺

Finding Bots w/out Sinkholing

- ASN with most likely bot infections

```
US    209  COMMUNITY HOSPITAL
US  20145  FLORIDA CANCER SPECIALISTS
US    209  FIELDS LAW
US  22803  NATIONAL OILWELL VARCO INC.
US  23148  JACKSON MEMORIAL HOSPITAL PUBLIC HEALTH
US  30437  GENERAL ELECTRIC COMPANY
US  30449  ARIZONA STATE GOVERNMENT
US  32291  ANNE ARUNDEL MEDICAL CENTER
US  33378  EASTERN BANK
US   3356  VERMONT ELECTRIC POWER COMPANY INC.
US   3356  ST MOBILE AEROSPACE ENGINEERING
US   3464  ALABAMA SUPERCOMPUTER NETWORK
US   4323  CINCINNATI TRANSPLANT INSTITUTE
US   4323  MEMORIAL HERMANN HEALTHCARE SYSTEM
US  46746  SECURE-24 LLC
US  53435  JACKSON ENERGY AUTHORITY
US   6128  ZUFALL HEALTH CENTER
US    714  APPLE INC. - 10G ASHBURN IDE
US   8075  MICROSOFT CORP
```

Passive DNS on C2 Domains
Data from Farsight's DNSDB

pDNS analysis (DNSDB by Farsight)

1	Domain	Count	First seen	Last seen	IP
2	CENSORED	314	29.01.2011 08:55	24.02.2011 18:33	CENSORED
13		24566	27.07.2012 13:48	26.02.2013 18:10	
15		24307	27.07.2012 13:48	26.02.2013 18:10	
19		42097	27.07.2012 13:49	08.02.2013 09:35	
21		29453	31.07.2012 15:38	26.02.2013 18:19	
22		32467	01.08.2012 02:03	26.02.2013 17:55	
25		48174	01.03.2013 19:26	21.09.2013 23:35	
29		35676	02.03.2013 08:21	24.11.2014 18:53	
30		27301	02.03.2013 09:25	24.11.2014 18:12	
33		14254	30.12.2013 19:55	27.11.2014 01:13	
35		15414	24.01.2014 03:51	27.11.2014 00:29	
37		15404	25.01.2014 04:27	27.11.2014 00:16	
40		25727	28.01.2014 03:17	27.11.2014 04:41	
41		16488	01.02.2014 04:38	27.11.2014 01:40	
43		14561	01.02.2014 05:55	27.11.2014 00:30	
44		28686	01.02.2014 08:00	26.11.2014 22:56	

pDNS analysis (DNSDB by Farsight)

	Domain	Count	First seen	Last seen	IP
19	CENSORED	35997	20.09.2013 16:08	26.11.2014 23:26	CENSORED
20		54773	20.09.2013 16:19	27.11.2014 01:49	
21		53987	20.09.2013 16:27	27.11.2014 05:56	
24		14254	30.12.2013 19:55	27.11.2014 01:13	
26		15414	24.01.2014 03:51	27.11.2014 00:29	
27		15404	25.01.2014 04:27	27.11.2014 00:16	
28		25727	28.01.2014 03:17	27.11.2014 04:41	
29		16488	01.02.2014 04:38	27.11.2014 01:40	
30		19693	01.02.2014 04:38	27.11.2014 04:53	
31		14561	01.02.2014 05:55	27.11.2014 00:30	
32		28686	01.02.2014 08:00	26.11.2014 22:56	
33		19712	01.02.2014 08:00	26.11.2014 23:31	
40		391	12.10.2014 04:30	27.11.2014 00:47	
41		43	24.11.2014 18:15	26.11.2014 23:04	
42		67	24.11.2014 18:40	27.11.2014 06:41	
43		63	24.11.2014 19:29	26.11.2014 23:46	
44		55	24.11.2014 19:35	26.11.2014 21:43	

1	Domain	Count	First seen	Last seen	IP
18	CENSORED	980	01.07.2013 18:34	16.10.2013 18:05	CENSORED
19		35997	**20.09.2013 16:08**	26.11.2014 23:26	
20		54773	**20.09.2013 16:19**	27.11.2014 01:49	
21		53987	**20.09.2013 16:27**	27.11.2014 05:56	
22		126	17.10.2013 16:32	06.11.2013 10:57	
23		650	06.11.2013 17:05	13.03.2014 06:41	
24		14254	30.12.2013 19:55	27.11.2014 01:13	
25		3	**24.01.2014 03:22**	26.01.2014 03:18	
26		15414	**24.01.2014 03:51**	27.11.2014 00:29	
27		15404	**25.01.2014 04:27**	27.11.2014 00:16	
28		25727	**28.01.2014 03:17**	27.11.2014 04:41	
29		16488	**01.02.2014 04:38**	27.11.2014 01:40	
30		19693	**01.02.2014 04:38**	27.11.2014 04:53	
31		14561	**01.02.2014 05:55**	27.11.2014 00:30	
32		28686	**01.02.2014 08:00**	26.11.2014 22:56	
33		19712	**01.02.2014 08:00**	26.11.2014 23:31	
34		266	08.02.2014 12:25	11.02.2014 10:26	
35		1596	13.03.2014 20:18	04.08.2014 21:08	
36		7	04.08.2014 23:32	05.08.2014 04:32	
37		223	05.08.2014 14:01	30.08.2014 08:32	
38		172	30.08.2014 17:32	12.09.2014 16:53	
39		411	13.09.2014 00:40	12.10.2014 00:40	
40		391	12.10.2014 04:30	27.11.2014 00:47	
41		43	**24.11.2014 18:15**	26.11.2014 23:04	
42		67	**24.11.2014 18:40**	27.11.2014 06:41	
43		63	**24.11.2014 19:29**	26.11.2014 23:46	
44		55	**24.11.2014 19:35**	26.11.2014 21:43	

How big was / is this Botnet?

http://www.abuse.ch/?p=3294 / How Big is Big? Some Botnet Statistics

abuse.ch

The Swiss Security Blog

Blog | Newsletter | ZeuS Tracker | Archives | SpyEye Tracker | Palevo Tracker | Contact

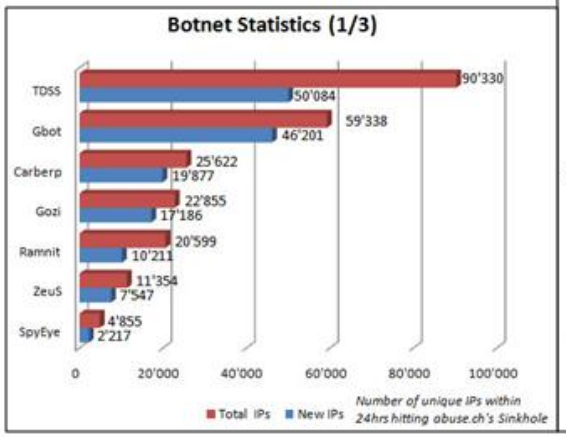
« Introducing: Palevo Tracker

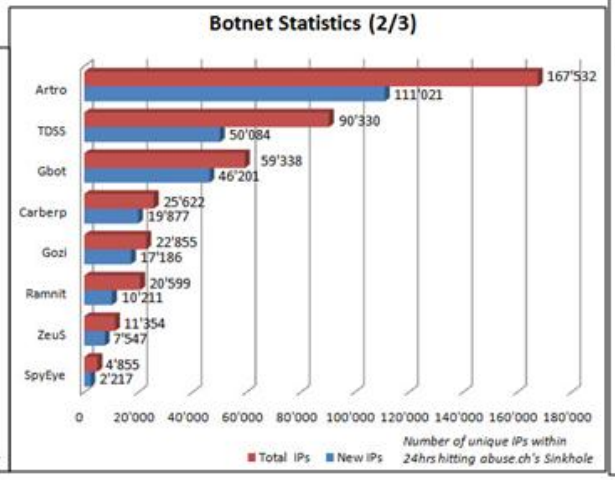
How Criminals Defend Their Rogue Networks »

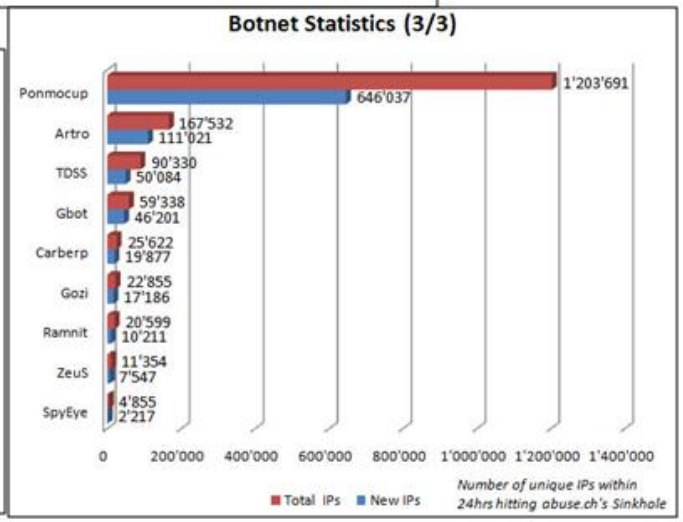
How Big is Big? Some Botnet Statistics

Published on May 23, 2011 in Malware & Virus Analysing and Monitoring & Reporting. 2 Comments

Tags: botnet, sinkhole, statistic



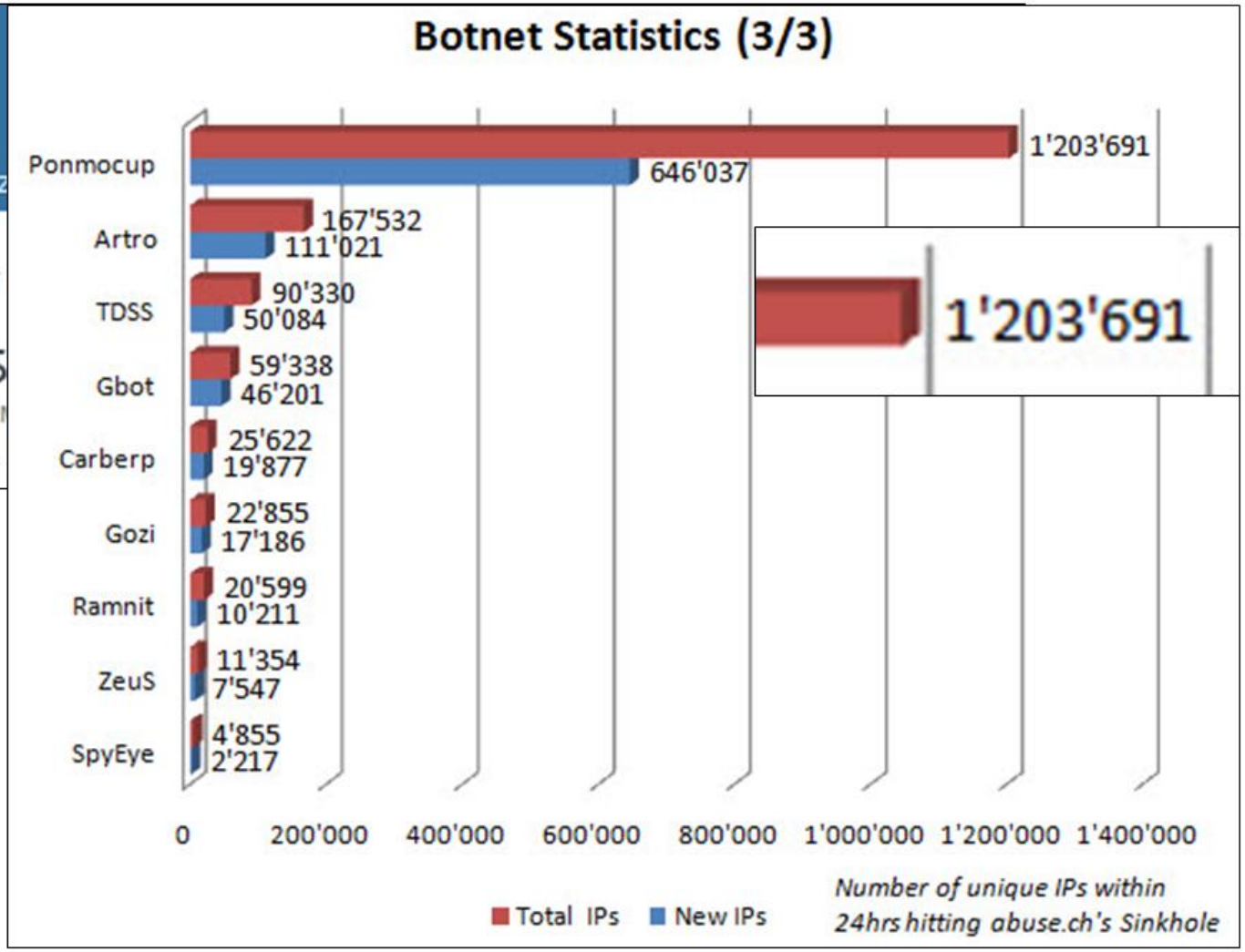


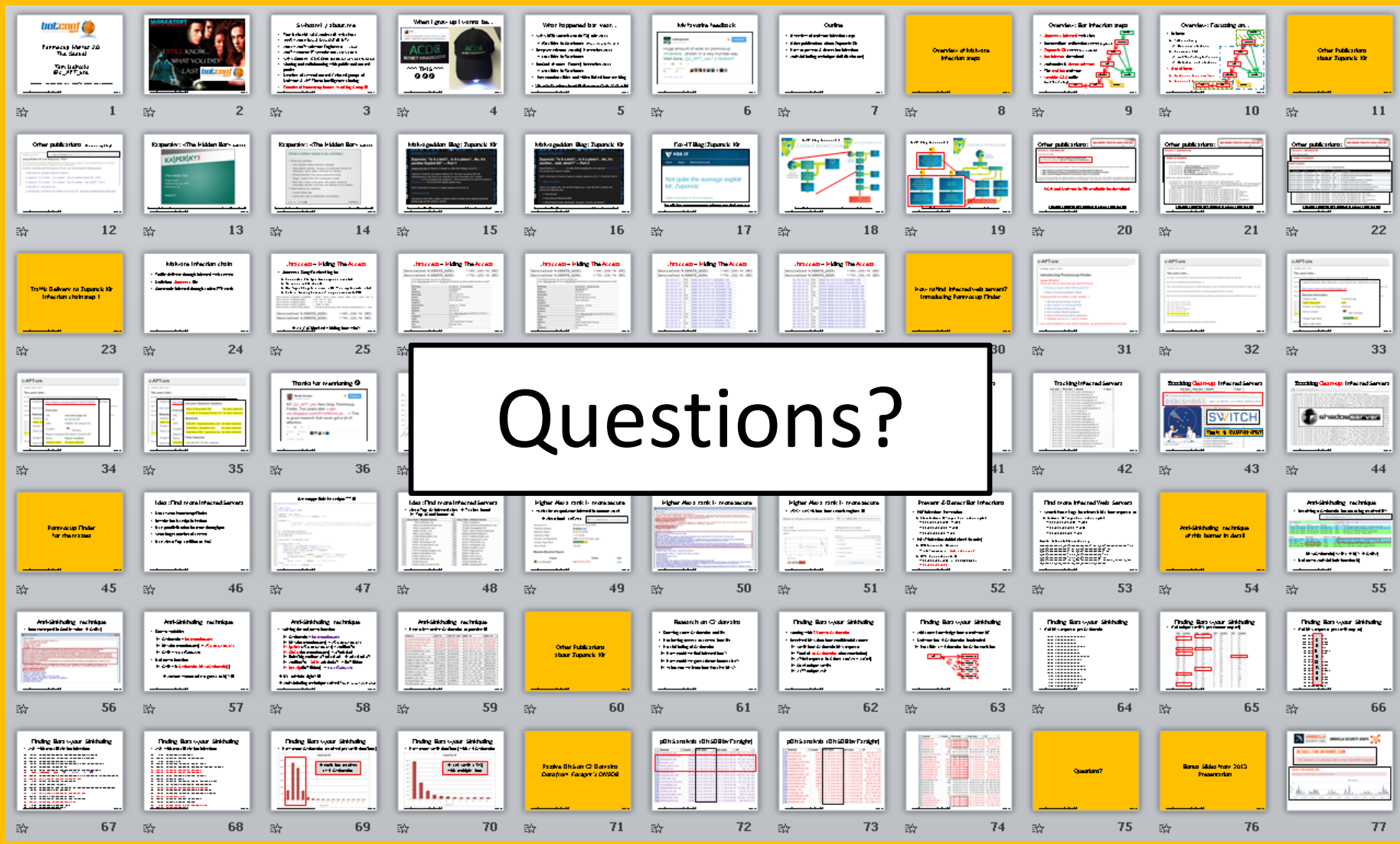


How big was / is this Botnet?

http://www.abuse.ch/?p=3294 / How Big is Big? Some Botnet Statistics

abuse.ch
The Swiss Security Blog
Blog Newsletter
« Introducing: Palevo Tracker
How Big is Big? S
Published on May 23, 2011 in
Tags: botnet, sinkhole, statistic




Questions?

References / Links

http://c-apt-ure.blogspot.com/2014/07/using-redline-for-live-response-part-1.html

http://media.kaspersky.com/en/Events/Presentations/Evgeny%20Aseev_The%20Hidden%20bot.pdf

http://malwageddon.blogspot.com/2013/06/zuponcic-is-it-bird-is-it-plane-no-its.html

http://malwageddon.blogspot.com/2013/08/zuponcic-is-it-bird-is-it-plane-no-its.html

http://malware-traffic-analysis.net/2014/03/17/index.html

http://blog.fox-it.com/2013/12/19/not-quite-the-average-exploit-kit-zuponcic/

Bonus Slides from 2013 Presentation

UMBRELLA SECURITY LABS

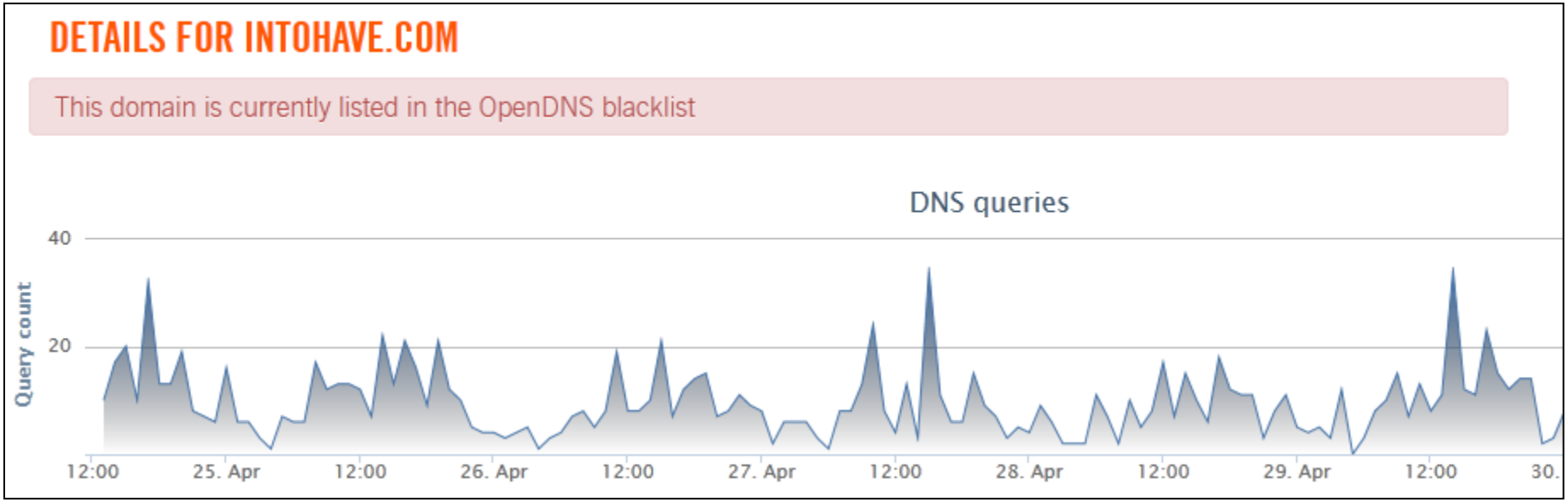
UMBRELLA SECURITY GRAPH

DETAILS FOR INTOHAVE.COM

This domain is currently listed in the OpenDNS blacklist

DETAILS FOR INTOHAVE.COM

This domain is currently listed in the OpenDNS blacklist



UMBRELLA SECURITY GRAPH

Requester geo distribution	TR (20.25 %) DZ (16.26 %) US (12.58 %) EG (5.83 %) [illegible] ID (1.84 %) VN (1.53 %) PL (1.53 %) FR (1.23 %) MX (1 ES (0.92 %) VE (0.61 %) CO (0.61 %) AZ (0.61 %) DK ([illegible] CW (0.31 %) MA (0.31 %) PY (0.31 %) HU (0.31 %) HK MY (0.31 %) SK (0.31 %) AU (0.31 %) CM (0.31 %) CR JM (0.31 %) NO (0.31 %)
Requester geo distribution (normalized)	AZ (10.74 %) PY (10.45 %) PE (7.38 %) CW (5.81 %) JM CM (2.70 %) EG (2.37 %) IR (2.27 %) NI (2.24 %) IL (1. VE (1.43 %) SK (1.26 %) TR (1.26 %) NG (1.20 %) CO ([illegible] PL (0.80 %) PK (0.79 %) ES (0.79 %) CL (0.77 %) BG ([illegible] IE (0.58 %) FR (0.55 %) BR (0.51 %) IT (0.50 %) CA (0. MY (0.21 %) GB (0.12 %)

UMBRELLA SECURITY LABS

UMBRELLA SECURITY GRAPH

DETAILS FOR CENSORED

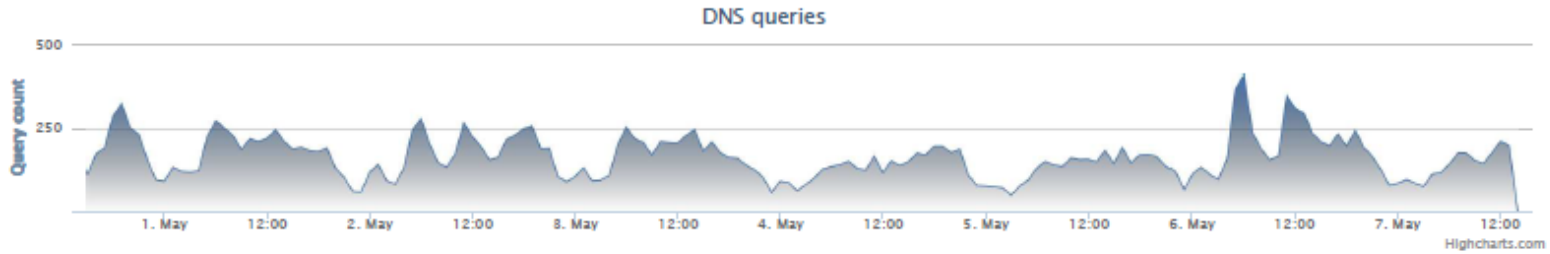
Search in Google

Classifier prediction: benign (confidence: 1)

Umbrella graph score: +100

This domain has a fairly good SecureRank 2

Download as CSV



DETAILS FOR CENSORED

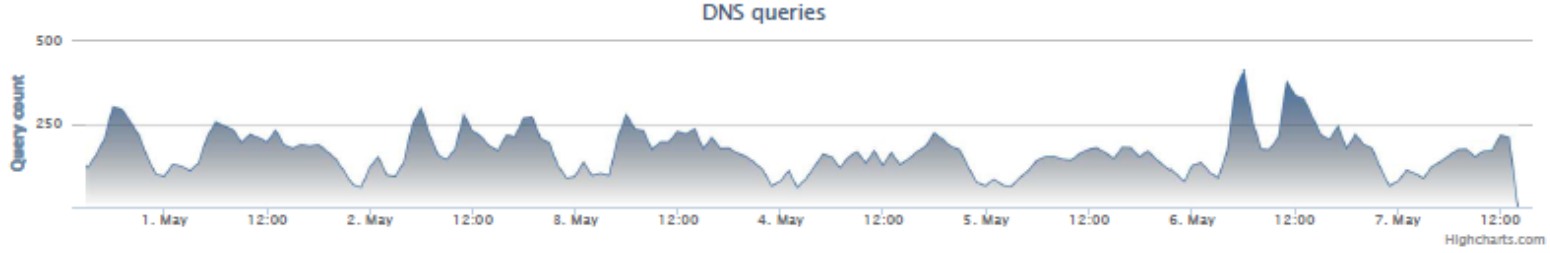
Search in Google

Classifier prediction: benign (confidence: 1)

Umbrella graph score: +100

This domain has a fairly good SecureRank 2

Download as CSV



UMBRELLA SECURITY LABS

UMBRELLA SECURITY GRAPH

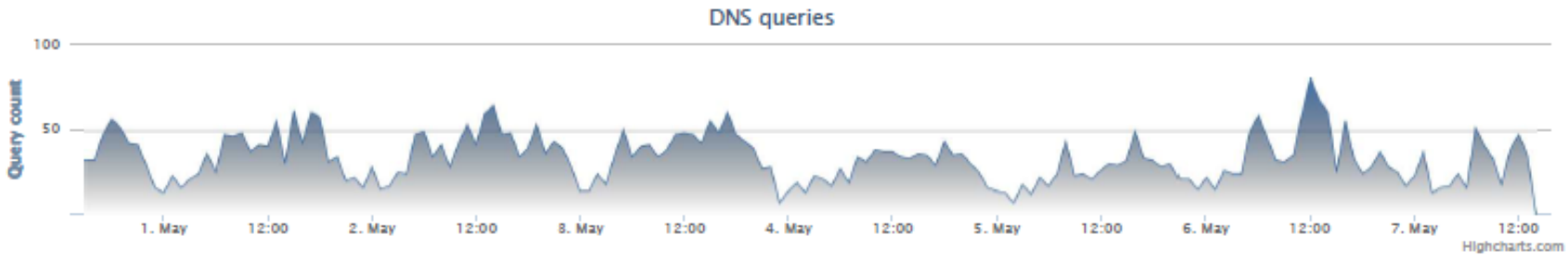
DETAILS FOR CENSORED

Search in Google

Classifier prediction: benign (confidence: 0.944)

Umbrella graph score: +89

Download as CSV



DETAILS FOR CENSORED

Search in Google

Geo distance between hosts serving this domain is fairly high

Classifier prediction: benign (confidence: 1)

Umbrella graph score: +100

Download as CSV