LAC
ともに、イキル

Lighting Talk

IoTバイナリ調査のツール紹介

(radare2 + α)

IoTSecJP 2019

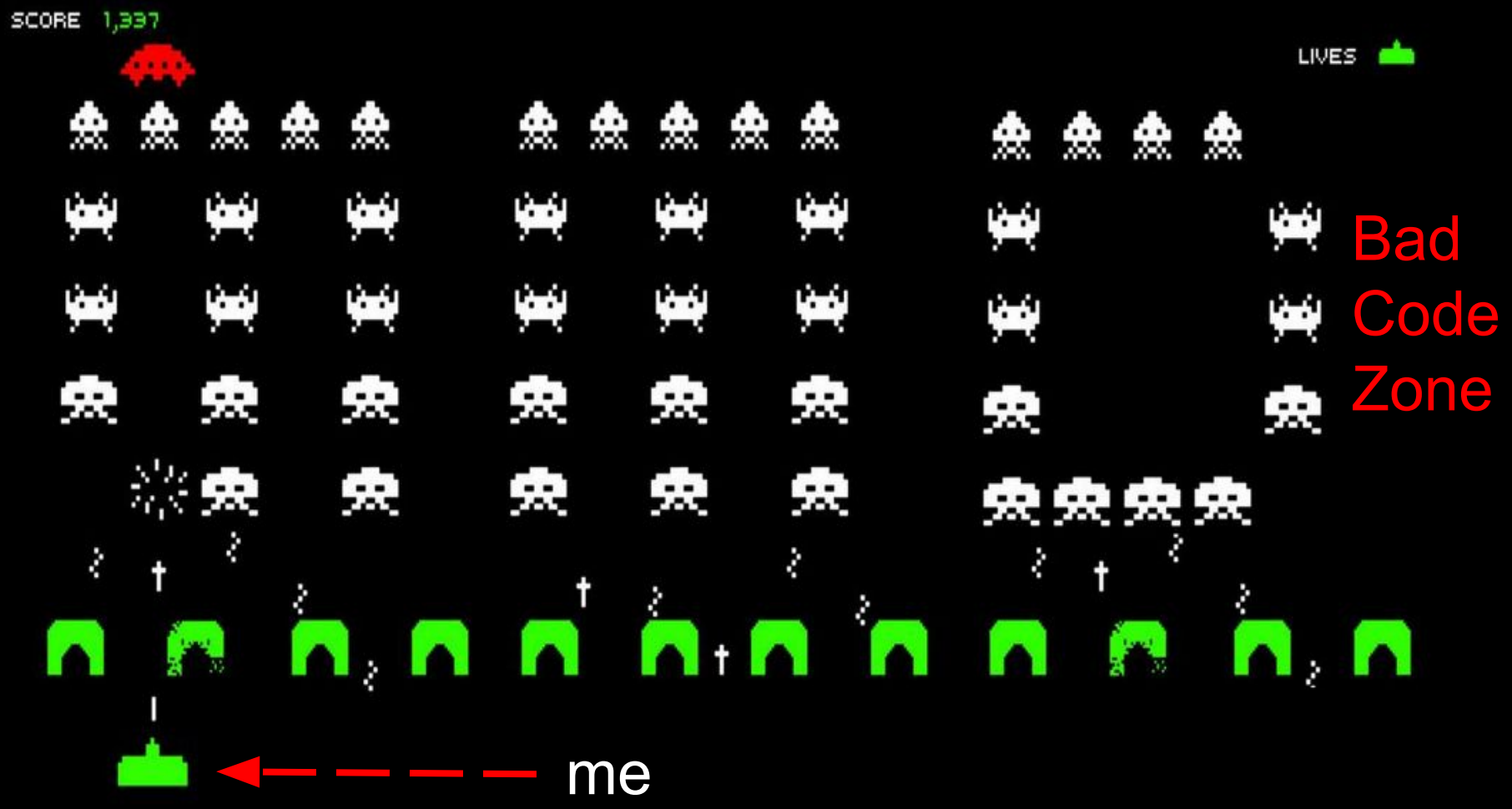
アドリアン・ヘンドリック - @unixfreaxjp
株式会社ラック サイバー救急センター
(C119/Cyber Emergency Center, LACERT)

Research material of malwaremustdie.org TLP WHITE

目次

- 自己紹介 (2分)
- ツールの説明 (5分)
- デモ (残りの時間)
- Ｑ＆Ａについて、木田さんに聞いてくださいね ｍｍ

毎日の仕事はこんな感じです



LAC
ともに、イキル

About me:

IoTバイナリ解析の教育実績について

講師の実績、IoT LinuxとRTOSマルウェアについて

- 2017年、2018年、2019年: 全国大会セキュリティキャンプ Zトラック
- 2017年、2018年、2019年: IPA ICSCoE CISO国際トレーニング(CyberCREST)
- 2018年、2019年: FIRST.ORGのICS SIGのCurator & Contributor
- 2016年、2017年、2018年、2019年: AVTokyo Linuxマルウェア解析ワークショップ（radare2, Tsurugi Linux, MISP for ICSとVirusTotal）
- 2018年 R2CONで IoT Binary Unpackingの発表
- 2019年 HACK.LUで Fileless infection: Linux Process Injection & Post Exploitation in Linux (incl IoT)の発表
- 2019年 MISPのICSTaxonomy作成（導入済み）

脆弱性の実績について

- CVE-2016-6564 Regentek Shanghai Android Mobile Phone backdoor on 2.8 million device (OEM to carriers)

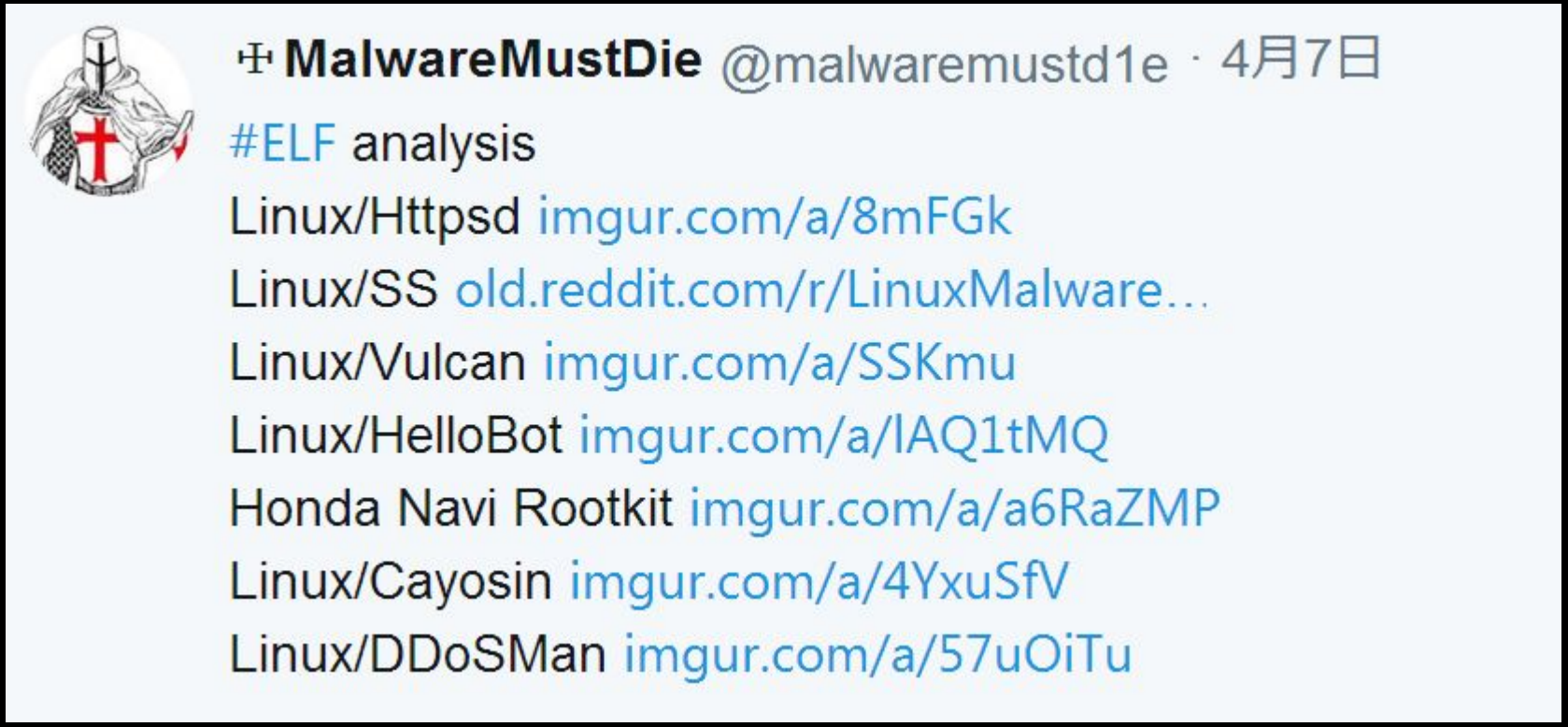
IoTバイナリ解析の教育実績について

IoTバイナリ解析の実績について

私が発見しましたIoTマルウェア

- 2014年5月18日: LightAidra (MIPSx, ARMx, x86)
- 2014年9月17日: Go言語 ArmBot (ARMx)
- 2014年9月25日: GayFgt/Bashdoor (aka lizkebab/torlus/bashlite) @ shellshock 0day脆弱性 (MIPSx, ARMx, x86)
- 2015年9月6日: Mr.Black (MIPSx, ARMx)
- 2016年8月28日: Mirai (MIPSx, ARMx,PPC,Sparc, SH)
- 2016年9月6日: Lua言語 Bot / “LuaBot” (MIPSx)
- 2016年10月14日: NyaDrop (MIPSx)
- 2016年10月29日: Ipv6に対応したNewAidra (MIPSx, ARMx,PPC,Sparc, SH)
- 2018年1月15日: ARC cpuマルウェアの発見
- :

IoTバイナリ解析の実績について



IoTバイナリ解析の実績について

Not logged in Talk Contributions Create account Log i

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

MalwareMustDie

From Wikipedia, the free encyclopedia

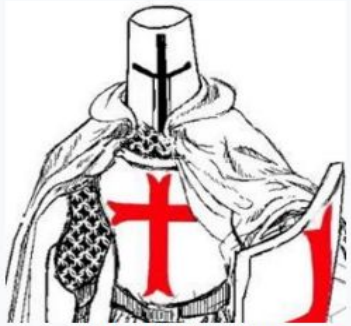
MalwareMustDie, NPO[1][2] as a whitehat security research workgroup, has been launched from August 2012. MalwareMustDie is a registered Nonprofit organization as a media for IT professionals and security researchers gathered to form a work flow to reduce malware infection in the internet. The group is known of their malware analysis blog.[3] They have a list[4] of Linux malware research and botnet analysis that they have completed. The team communicates information about malware in general and advocates for better detection for Linux malware.[5]

MalwareMustDie is also known for their efforts in original analysis for a new emerged malware or botnet, sharing of their found malware source code[6] to the law enforcement and security industry, operations to dismantle several malicious infrastructure,[7][8] technical analysis on specific malware's infection methods and reports for the cyber crime emerged toolkits.

Several notable internet threats that has been firstly discovered and announced by MalwareMustDie team are i.e.

- Prison Locker[9] (ransomware),
- Mayhem[10][11] (Linux botnet),
- Kelihos botnet v2[12][13]
- ZeusVM[14]
- Darkleech botnet analysis[15]
- KINS (Crime Toolkit)
- Cookie Bomb[16] (malicious PHP traffic redirection)
- Mirai[17][18][19][20]
- LuaBot[21][22]
- NyaDrop[23][24]

MalwareMustDie



MalwareMustDie logo

Abbreviation	MMD
Formation	August 28, 2012; 7 years ago
Type	Nonprofit organization & NGO
Purpose	Constructive research & awareness to reduce malware
Headquarters	Japan, Germany, France, United States
Region	Global
Membership	< 100
Website	malwaremustdie.org

IoTバイナリ解析の実績について

https://blog.malwaremustdie.org/2014/05/threat-analysis-zendran-elf-ddos-scheme.html

Malware Must Die!

The MalwareMustDie Blog (blog.malwaremustdie.org)

Sunday, May 18, 2014

MMD-0022-2014 - Zendran, Multi-Arc ELF DDoS (lightaidra ircd base) - Part 1: background, installation, reversing & CnC access

The background

There are a lot of DDoS attacks performed each day. Our systems are also being abused by these, and maybe some of you have the same shares too. MalwareMustDie analysis is focusing on malware, and recently we are raising priority to analysis aiming the UNIX or Linux platform. And, luckily one of the sample dropped this time is the multi-CPU architecture DDoS ELF tool, which is a nice topic to disclose, and we plan to disclosing this threat down to its threat root.

This is the analysis of the DDoS tool that was made based from the C code of IRCd program called Lightaidra, and aiming infection on Linux OS in x86, x64, PPC, MIPS, MIPSEL, ARM, and SuperH architectures, meaning, not only aiming servers but also linux workstations, routers and any related devices that is connecting to the global internet, to be badly utilized as a cyber attack tool to perform DDoS attack. The case is complicated and various in analysis skill set + volume, so to save time, myself and @wirehack7 are on the case to split the writing into 2 (two) parts, I, in this post do the first part contains the background, installation & reversing materials, with aiming the

IoTバイナリ解析の実績について

LINUX/GOARM.BOT

15 posts | 1 | 2 | Next

Linux/GoARM.Bot

by **unixfreaxjp**
Wed Sep 17, 2014 6:55 am

I was reported this GOARM Binary: https://www.virustotal.com/en/file/81c9 ... 410603481/ Many downloads:

文件名 .扩展名	大小(类型)	修改时间↓	点击量
cr	3.21 MB	2014-9-5 18:15:58	6190

uploaded date　　downloaded times

Username	unixfreaxjp
Posts	501
Joined	Thu Apr 12, 2012 4:53 pm

It's an ARM architecture bot, based on Go programming compiled for Armv6 with Cypto and Encoding libs. Go projects PoC:

CODE: SELECT ALL

```
// go runtime..
0x29B39C   runtime.selectgo
0x2AB1EC   runtime.gogo
(etc)
// go project..
0x31A3D1   /Users/fc/GoProjects/armv6/src/server2/server.go
0x31A403   /Users/fc/GoProjects/armv6/src/server2/message.pb.go
0x31A439   /Users/fc/GoProjects/armv6/src/server2/client.go
0x31BDE1   /Users/fc/GoProjects/armv6/src/main.go
0x31A3D1   /Users/fc/GoProjects/armv6/src/server2/server.go
0x31A403   /Users/fc/GoProjects/armv6/src/server2/message.pb.go
0x31A439   /Users/fc/GoProjects/armv6/src/server2/client.go
```

HTTP send template:

CODE: SELECT ALL

```
%s %s HTTP/1.1
User-Agent: %s
; Domain=%s
; Path=%s
; Expires=%s
; Max-Age=%d
```

IoTバイナリ解析の実績について

LINUX/BASH0DAY ALIAS SHELLSHOCK ALIAS BASHDOOR

43 posts | 1 | 2 | 3 | 4 | 5 | Next

Linux/Bash0day alias Shellshock alias Bashdoor

by **unixfreaxjp**
Thu Sep 25, 2014 12:10 pm

I am not feeling well, but this is important. It's the first 0day bash injected ELF malware spotted in ITW attack of CVE-2014-6271.
ThIs sample was found via @Yinettesys's (credit) IDS sigs: https://gist.github.com/anonymous/929d622f3b36b00c0be1
The sample is up and alive, my analysis I posted in VT (see the comment tab): https://www.virustotal.com/en/file/73b0 ... 411634118/
Announced was 6h ago here: https://twitter.com/yinettesys/status/5 ... 6268604416
And detection ratio is still ZERO.. :twisted:

> /* THIS is what I am afraid of for the ELF malware...sigh.. now you know why I yell ELF a lot!! The AV scanning performance for new ELF itself is ANOTHER 0day actually..*/

Anyway, the malware is new, spotted and saved/designed (firstly found) for a #0day , so I named it as Linux/Bash0day < (if you have better name..pls feel free to change.. :))
Basically the malware is backdoors to a CNC and remotely control (bot) with the busybox rooter attack. CNC info is in the analysis.
It scans for logins + tries to exploit via SCANNER (telnet?) on IPs & gained shell with an "overdue" busybox skids exec_code.. :lol: (often sighted in telnet flaw ref is here: https://isc.sans.edu/diary/Busybox+Hone ... nner/18055) and gain privilege of the admin/root (if possible).
The main course is : It does DDoS in TCP and UDP so does other attacks (JUNK, HOLD), with backdoor to its CNC.
So it is the "another" DDoS botnet story..

The binary wasn't clearly stripped, yet using silly decrypter, it looks like a "quicky" codings job in some parts, yet well-designed/crypted in many others, I think they prepared it a bit (for this kind of occassion) BEFORE 0day was publicly announced (still < 24day), since the 0day was found in about a week before and mostly is leaked to bad guys faster than good guys.
Answering twitter comments:

> Q: So, not a worm at least, though that's no consolation for public-facing systems

A: That SCANNER part is aiming IPs+sent "that" BusyBox codes to exploit (should be telnet..other protocol just doesnt work)..Maybe not a worm, but a morons who wanna build #botnet #DDoS'er upon #0day #bash

Username	unixfreaxjp
Posts	501
Joined	Thu Apr 12, 2012 4:53 pm

IoTバイナリ解析の実績について

Malware Must Die!

The MalwareMustDie Blog (blog.malwaremustdie.org)

Sunday, September 6, 2015

MMD-0042-2015 - Hunting Mr. Black IDs via Zegost cracking

This is a short writing, Please bear the straight forward detail w/very few of explanation.
During investigating *ELF malware* I met this Windows PE binary, it contains an important infrastructure information used by Mr. Black actor (the one who loves attacking our MIPS routers), so I decided to check and post a bit here.

Win32/Zegost.rfn [link] (according to Microsoft)

The malware is sitting in the panel waiting to be distributed by the time I spotted:

Name .extension	Size	Timestamp	Hits
hr.exe	204.48 KB	2015-9-2 23:26:37	0

The actor who put the PE binary in the picture was attacking my "router" with the other ELF binary one, a MIPS architecture of **Linux/Mr.Black**, a family of *Linux/AES.DDoS*, a China ELF backdoor and DDoS'er variant, with the source IP of attacker and CNC lead to that panel's address.

IoTバイナリ解析の実績について

Malware Must Die!

The MalwareMustDie Blog (blog.malwaremustdie.org)

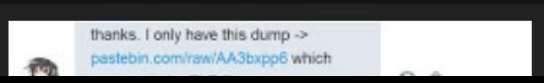
Friday, October 14, 2016

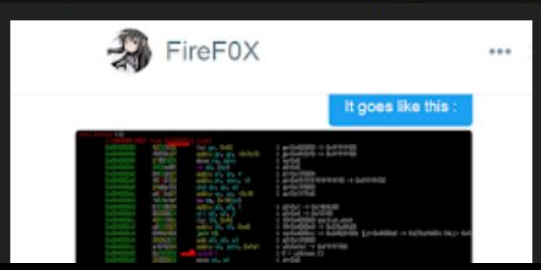
MMD-0058-2016 - Linux/NyaDrop - a linux MIPS IoT bad news

Background

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

This is not the "really" first time we're seeing this threat actually, in this year, some small events was detected on having these attacks which I ignored for some reasons, and on May 22th, me and hFiref0x of KernelMode was in a convo regarding to the threat which was detected. It was obviously the same threat (proof is as per picture below, thanks to hFiref0x for the ping that time).





IoTバイナリ解析の実績について

Malware Must Die!

The MalwareMustDie Blog (blog.malwaremustdie.org)

Thursday, September 1, 2016

MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled..

Background

From August 4th 2016 several sysadmin friends were helping us by uploading this malware files to our dropbox. The samples of this particular ELF malware ware not easy to retrieve, there are good ones and also some broken ones, I listed in this post for the good ones only. This threat is made by a new ELF trojan backdoor which is now in on-going stage aiming IoT, the name of the binary is **"mirai.*"** and is having telnet attack as main functionality to other boxes.

As I see these samples as something new, it would be good to start to write analysis for the purpose to raise awareness of this threat widely, since the attacks are actively spotted in the wild on plenty of infected IoT networks. During the checks I discussed about the threat to the engineer friends in ETLabs,[links] who also detecting the same attack phenomena, and then having dialogue with our supporters who reported this threat directly too.

ELF Linux/Mirai is currently having a very low ELF/Linux antivirus detection ratio, even in the architecture of x86. The detection in VT for the collected multiplatform samples can be viewed in the several links below:
Linux/Mirai ITW samples: [link] [link] [link] [link] [link] [link] [link] [link] [link]

The reason for the lack of detection is because of the lack of samples, which are difficult to fetch from the infected IoT devices, routers, DVR or WebIP Camera, the Linux with Busybox binary in embedded platform, which what this threat is aiming.

IoTバイナリ解析の実績について

The MalwareMustDie Blog (blog.malwaremustdie.org)

Tuesday, September 6, 2016

MMD-0057-2016 - Linux/LuaBot - IoT botnet as service

Background

On Mon, Aug 29, 2016 at 5:07 PM I received this ELF malware sample from a person (thank you!). There wasn't any detail or comment what so ever just one cute little ARM ELF stripped binary file with following data:

```
arm_lsb: ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV), statically l
hash: a220940db4be6878e47b74403a8079a1
```

This is a cleanly GCC: (GNU) 5.3.x compiled ARM arch ELF binary:

```
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           ARM
  Version:                           0x1
  Entry point address:               0x11940
  Start of program headers:          52 (bytes into file)
  Start of section headers:          995912 (bytes into file)
  Flags:                             0x5000202, has entry point, Version5 EABI
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         4
  Size of section headers:           40 (bytes)
  Number of section headers:         15
  Section header string table index: 14
</unknown>
```

All of the sections and headers are all there:

IoTバイナリ解析の実績について

The MalwareMustDie Blog (blog.malwaremustdie.org)

Saturday, October 29, 2016

MMD-0059-2016 - Linux/IRCTelnet (new Aidra) - A DDoS botnet aims IoT w/ IPv6 ready

It's a Kaiten/Tsunami? No.. STD?? No! It's a GayFgt/Torlus/Qbot? No!! Is it Mirai?? NO!!
*It's a **Linux/IRCTelnet (new Aidra)**! ..a new coded IoT DDoS botnet's Linux malware..*

Summary

This post is a report of what it seems to be a new IRC botnet ELF malware, that is obviously used for performing DDoS attack via IRC botnet. It was coded with partially is having specification as per Tsunami/Kaiten protocol, but it is a re-coded one with the different way, with adding some more features in messaging and malicious/attack vectors used. The malware (the bot client) is designed to aim IoT device via telnet protocol, by using its originally coded telnet scanner function, which is brute-forcing the known vulnerable credential of the Linux IoT boxes, via command sent from a CNC malicious IRC server.

The way this new malware was composed is interesting, as a combination concept of kaiten (for some same IRC protocol used), the GayFgt/Torlus/Lizkebab/Bashdoor/Bashlite (for the telnet scanner and infection's injection code) and using the Mirai's botnet's leaked IoT's credential list. Furthermore, it is having an encoded CNC info for avoiding a plain text sight view. And having some hard-coded Italian language messages in the user's communication interface. The botnet is having DoS attack mechanism like UDP flood, TCP flood, along with other series of attack methods, in both IPv4 and IPv6 protocol, with extra IP spoof option in IPv4 or IPv6 too.

I use name **Linux/IRCTelnet (new Aidra)** as codename for this ELF malware. Some friends are advising to name as per language that spotted, but I personally don't think it is ethic to use other country's or language's or culture's into naming of malware..

[EDIT] After further analysis comparing the overall done reversed code to the historically known / detected ELF malware botnet libraries that I can find, I found a very good match, that confirms the source code used to build this botnet malware is based on the root codes of **Aidra botnet**.

IoTバイナリ解析の実績について

The Hacker News

Click to Subscribe

Home | Data Breaches | Cyber Attacks | Vulnerabilities | Malware | Deals | Contact

TESOL Special seminars

Open to the public. First three hours are free. Temple University, Japan Campus

TEMPLE UNIVERSITY Japan Campus TUJ

New Mirai Okiru Botnet targets devices running widely-used ARC Processors

January 15, 2018 Mohit Kumar

IoTバイナリ解析の実績について

Ragentek's binary also runs as root, a level of access that gives it complete control over the device.

Spotted Before

In January, the nonprofit research group MalwareMustDie published a post on Pastebin that came essentially to the same conclusion as AnubisNetworks. It's unclear why it took so long for the issue to be resolved, especially for such a serious vulnerability.

But researchers often have trouble flagging the interest of manufacturers and software developers, some of whom aren't terribly responsive to security reports. The lack of alarm often becomes more common down the software food chain where vendors compete largely on costs rather than other merits, such as security.

Last week, attention was focused on BLU Products after Kryptowire, an enterprise mobile security company, found one of its devices transmitted call logs and text messages every 72 hours to a server in Shanghai (see *Why Did Chinese Spyware Linger in U.S. Phones?*).

紹介するツールの内容

Radareとは?

- 12年間開発されているオープンソースプロジェクト(無料)
- リバースエンジニアリングのフレームワークとツールセットで構成
- オリジナル(初期)は私(pancake)が開発
- コミュニティとコントリビューターのコーダーが参加
- 個人による開発スタイルから、プロジェクトリーダー、メンテナーのスタイルに移行

- 現状は6週間ごとにマイナーバージョンアップをリリース
- +1.0となるメージャーバージョンアップは毎年r2conの後にリリース
- r2conはバルセロナで開催(2017年はおよそ230人の参加者)
- r2conの全セッションはYouTubeにて公開

紹介するツールの内容

radare2の機能

- プログラムを解析して動作を理解する
- 様々なエンコード文字列の認識 (中国語, 韓国語, キリルなど)
- いくつかの異なるテクニックを用いて文字列を検索
- メモリダンプやファームウェアなどのフォレンジック調査
- ファイルシステムのマウントとパーティションテーブルの解析
- その他のデバッガーとの連携機能(gdb, r2, frida, windbg,など)
- プログラムの一部をエミュレートしてブロックを復号
- 外部デコンパイラまたはグラフ作成ツールを使用
- 2つのバイナリの違いを確認できるdiff機能
- 2048やr2warsのようなゲームもプレイできる！

IOTに関してのメリット、デメリットについて

- (+) FreeBSDとLinux Debianベースでテストを行っています、Debianで問題がなさそうで、Debianみ対応してるcpu/archも問題がないはず
- (+) RTOSのTopperssファームウェアバイナリ、何件IoTとAndroidカーネルの解析実績があります
- (+) 無料ナDECOMPILERがあります、今年から R2GHIDRAの追加！
- (+) その側FRIDA経由の解析も可能！
- (+) 日本にコミュニティーがあります

- (-) CLI環境が嫌い人に向いていないかも、すみません m m
- (-) KNOW HOWが分かりにくいかも

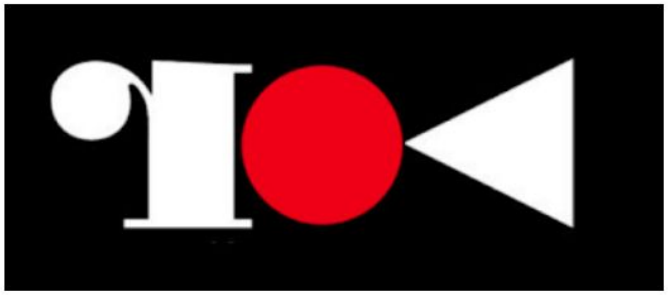
参考情報

r2jp = Japanese Community of radare2

repo/ホームページURL

```
https://github.com/radareorg/r2jp
```

ロゴ



r2jpは日本国内のradare2コミュニティで、ここでradare2に対しての日本国内ユーザのサポート、イベントと技術交換などのやり取りを行っております。目的は下記の内容をフォローが出来るように強い国内コミュニティを作る前提ですので、ターゲットは例えば下記の対応が出来る迄と考えております。

```
- 質問/ Q&A（質問があれば新規Issuesのチケットで対応、日本語で書いてください）
- 開発(プラグイン、追加機能、アイデア)
- 日本語ドキュメンテーション
- ワークショップ、トレーニング、プレゼンテーションなど
```

現在対応方法について

```
内容によって、radare2ベテランのユーザーが便利な使い方、質問の回答、howto手順などをWikiで書きます。
```

参考情報

radare2全般の重要なリンク情報

- site https://www.radare.org/ or http://rada.re/
- releases https://github.com/radare/radare2/releases
- dev/source: https://github.com/radare/radare2
- doc http://rada.re/vdoc/
- book https://radare.gitbooks.io/radare2book/content/
- wiki https://r2wiki.readthedocs.io/en/latest/
- etc documentaton http://radare.today/posts/radare2-is-documented/
- blog http://radare.today
- installers http://radare.mikelloc.com/list
- r2con conference https://rada.re/con/ or https://github.com/radareorg/r2con
- web demo http://cloud.rada.re (今メインテナンス中)
- ctf tips http://radare.today/posts/using-radare2/
- devcode CLang checks (Jenkins) http://ci.radare.org/job/radare2-scan-build/
- twitter @radareorg https://twitter.com/radareorg

イベントの情報

```
1. 2017年11月02日「radare2」ワークショップ AVTokyo 2017 (by pancake)
2. 2018年08月31日 radare2JP/r2jpのOB会イベント
3. 2018年09月07日 r2jpチームからR2CON 2018コンファレンスでのプレゼンテーション (unixfreaxjp/Unpacking the Non-Unpackable
4. 2018年12月23日 SECCON 2018 CTF YOROZUワークショップでr2con 2018のレポートとv3.1.2でソフトウエア解析入門
5. 2019年のワークショップ予定(tba)
```

サイトのメインテナー

```
@trufae @tessy_jp @unixfreaxjp @luffykuroneko (r2jp)
```

オブザーバー

```
@sonodam (r2jp)
```

参考情報

Repositories
Code 0
Commits
Issues 37
Packages
Marketplace
Topics 582K
Wikis
Users 0

States
Closed 33
Open 4

Languages
C 29
Ruby 2

Advanced search Cheat sheet

37 issues

Sort: **Best match**

radareorg/radare2 #15085
ctype.c:14: error: redefinition of typedef 'RParseCType' - previous declaration of 'RParseCType' was in libr/include/r_parse.h:80
Work environment | Questions | Answers | | --- | --- | | OS/arch/bits (mandatory) | FreeBSD | | Architecture/bits of the file (mandatory) | x86/32 | | Error log | https://github.com/unixfreaxjp/dev/blob/master/FreeBSD-2019-057.md ...
unixfreaxjp opened Sep 20, 2019 8 comments

radareorg/radare2 #15079
Ragg rop chain (R_SYS_ASM_START_ROP) doesn't check unsupported "r_sys_run_rop" FreeBSD kernel, need ifdef to check for unsupported version.
Work environment | Questions | Answers | | --- | --- | | OS/arch/bits (mandatory) | FreeBSD9 base (custom, patched, supported, development machine) | | Error log | https://github.com/radareorg/radare2/issues /10440#issuecomment-533181103 ...
unixfreaxjp opened Sep 19, 2019 5 comments

radareorg/radare2 #12334
ARM5 x32 | Err: Selected processor does not support ARM mode `bkpt $0
Work environment | Questions | Answers | | --- | --- | | OS/arch/bits (mandatory) | Debian arm5 | | File format of the file you reverse (mandatory) | -. | | Architecture/bits of the file (mandatory) | ...
unixfreaxjp opened Nov 27, 2018 10 comments

radareorg/radare2 #11834
HAS_CLOCK_NANOSLEEP crash the build (radare2 v 3.0 in #FreeBSD 10.4 RELEASED and Legacy Linux C compilers)
Work environment | Questions | Answers | | --- | --- | | OS/arch/bits (mandatory) | FREEBSD 10.4-RELEASED - AMD 64, Debian Wheezy, additional MIPS, ARM5 IoT SDK | | File format of the file you reverse ...
unixfreaxjp opened Oct 16, 2018 10 comments

radare/r2hate #16
TL;DR | issue/report handling expected:
In every open source community, response from users are gold, users are kings, they are the power. I would rant

参考情報

radare released this Dec 3, 2018 · 3027 commits to master since this release

Release Notes

Version: 3.1.2
Previous: 3.1.1
Commits: 12
Contributors: 4

Description

This is a bug-fix release, fixing crashes in the x86, arm64 assemblers and the macho parser.
But also improving the xrefs visual navigation experience and panels.

This is the 2nd minor-release after 3.1.0, which also fixed a lot of portability issues. Thanks **@unixfreaxjp** for all the testing on freebsd, powerpc, sparc, mips, armv5 spotting out some issues with inline assembly it. Also say thanks to **@revskills** and **@HongxuChen** for fuzzing and spotting some crashes fixed by **@trufae** . Thanks to **@ret2libc** for all the refactoring in RBin, which are most of the WIP but setting the base for future directions and code cleanups.

Some users will notice some more warning at runtime. Don't worry, they are debugging messages for things that were happening before already, some can be ignored and others are expected, but they are useful for the users too in order to understand better some behaviours or bugs in the analysis.

The 3.1.0 release (compared to 3.0.0) introduced the following important changes:

デモ