



2018 and IoT Linux Malware

@unixfreaxjp

HaCk3r's PArTy .JP - 2018

Before..

1. Read blog.malwaremustdie.org

20. *) SSHV [1]
21. *) DDOS.TF [1]
22. Torte [1]
23. *) Tiny backdoor2 [1]
24. *) KillFile (unixfreaxjp/MMD) [1]
25. *) Dtool (unixfreaxjp/MMD) [1]
26. BossaBot (found by Malekal) [1] [2] [3] [4] [5] [6]
27. *) Mubot [1] [2]
28. Skiddies VARIOUS DDOS'ers [1]
29. STDBot [1] [2] [3] [4]
30. PnScan [1]
31. *) Mirai [1]
32. *) Luabot [1]
33. *) NyaDrop (Tiny backdoor3) & s_malware [1]
34. *) IRCtelnet (New Aidra) [1]
35. *) UDPfker [1]
36. Linux Website Ransomware - Reversing (in Japanese) [1]
37. OverkillMod / "EnergyMech 2.8 overkill mod" [1]

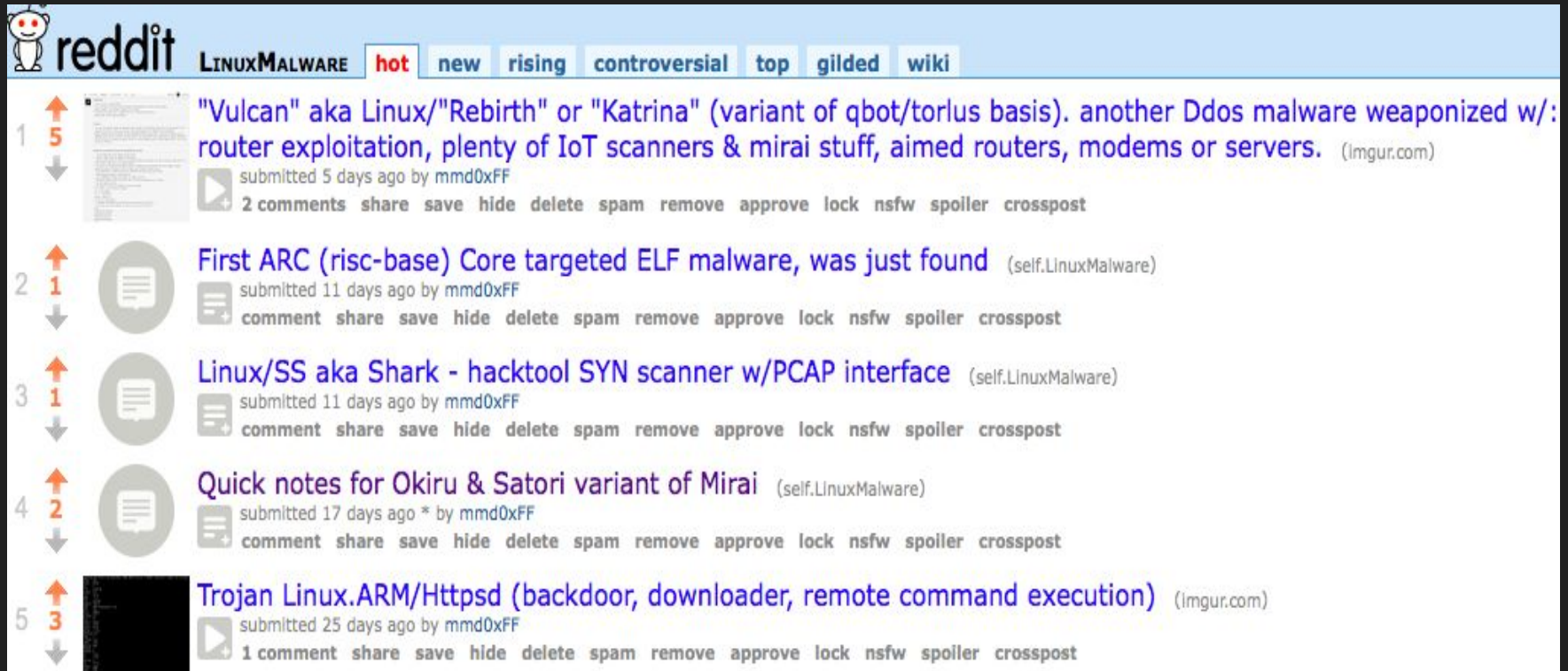
1. Tsunami/Kaiten [1]
2. *) DNSAmp [1]
3. *) LightAidra (Mod Zendran) [1]
4. Elknot [1]
5. Darkleech [1] [2] [3]
6. *) Mayhem [1] [2]
7. *) pscan & sshscan [1]
8.) *lptabLex and lptabLes [1] [2]
9. *) AES.DDoS [1] [2]
10. *) GayFgt/Bashdoor & Tiny backdoor1 [1] [2] [3] [4] [5]
11. *) XOR.DDoS [1] [2] [3]
12. *) ChinaZ [1] [2] [3] [4]
13. *) DES.Downloader [1]
14. *) Linux/BillGates.Lite [1] [2] [3] [4] [5]
15. Mr. Black [1] [2] [3]
16. *) BangSYN (unixfreaxjp/MMD) [1]
17. *) Golang ARMBot (unixfreaxjp/MMD) [1] [2] [3]
18. *) Yangji (unixfreaxjp/MMD) [1]
19. *) KDefend [1]

What now?






- Combination malicious functionalities in binaries
- Evolution (Scripting to Binary Executables)
- Inspired and motivated (by...)
- Aggressive (target vulns, aim specific device in services/network)
- Faster
- They watch us as we watch them

So.. get ready!

Snapshot of new Linux Malware in 2018



The screenshot shows the Reddit interface for the **LINUXMALWARE** subreddit. The top navigation bar includes the subreddit name and sorting options: **hot**, **new**, **rising**, **controversial**, **top**, **gilded**, and **wiki**. The main content area displays a list of five posts, each with a rank, a score, a thumbnail, a title, a submission time, a username, and a set of interaction buttons.

Rank	Score	Thumbnail	Title	Submitted	By	Source
1	5		"Vulcan" aka Linux/"Rebirth" or "Katrina" (variant of qbot/torlus basis). another Ddos malware weaponized w/: router exploitation, plenty of IoT scanners & mirai stuff, aimed routers, modems or servers. (imgur.com)	5 days ago	mmd0xFF	(imgur.com)
2	1		First ARC (risc-base) Core targeted ELF malware, was just found (self.LinuxMalware)	11 days ago	mmd0xFF	(self.LinuxMalware)
3	1		Linux/SS aka Shark - hacktool SYN scanner w/PCAP interface (self.LinuxMalware)	11 days ago	mmd0xFF	(self.LinuxMalware)
4	2		Quick notes for Okiru & Satori variant of Mirai (self.LinuxMalware)	17 days ago	mmd0xFF	(self.LinuxMalware)
5	3		Trojan Linux.ARM/Https (backdoor, downloader, remote command execution) (imgur.com)	25 days ago	mmd0xFF	(imgur.com)

New kids on the block

For r2 preview:

- HttpsD
- Vulcan
- SS
- Mirai Okiru & ARC version <===== this

What's the strategy?

- Use RE to try to understand how it works than reading reports
↓ ↓ ↓
- Use better signature to “Boost Detection” part..
↓ ↓ ↓
- Use IOC for the awareness, use MISIP for making sure we all aware
↓ ↓ ↓
- Help law enforcement, help us!

Linux and Vulnerability...

If we see it, blackhats sees it too..

Patches is coming...

Malware is also coming...

Incomiiiiing....!!!

```
>> Unauthenticated LAN remote code execution in AsusWRT
>> Discovered by Pedro Ribeiro (pedrib@gmail.com), Agile Information Security
```

```
=====
Disclosure: 22/01/2018 / Last updated: 25/01/2018
```

>> Background and summary

AsusWRT is the operating system used in mid range and high end Asus routers. It is based on Linux but with a sleek web UI and a slimmed down profile suitable for running on resource constrained routers.

Thankfully ASUS is a responsible company, and not only they publish the full source code as required by the GPL, but they also give users full root access to their router via SSH. Overall the security of their operating system is pretty good, especially when compared to other router manufacturers.

However due to a number of coding errors, it is possible for an unauthenticated attacker in the LAN to achieve remote code execution in the router as the root user.

A special thanks to Beyond Security SecuriTeam Secure Disclosure (SSD) programme for disclosing these vulnerabilities to the manufacturer, speeding the resolution of the issues discovered (see [1] for their advisory).

>> Technical details:

#1

Vulnerability: HTTP server authentication bypass

CVE-2018-5999

Attack Vector: Remote

Constraints: None; exploitable by an unauthenticated attacker

Affected versions: confirmed on v3.0.0.4.380.7743; possibly affects every version before

v3.0.0.4.384.10007

<https://raw.githubusercontent.com/pedrib/PoC/master/advisories/asuswrt-lan-rce.txt>

Boost detection, help filtration!

Mastering your signature skillset now!

- Snort rules (filter the traffic)
- ClamAV and YARA rule (filter the payload)
- IOC, STIX, TAXII (spread the detection indicators)
- Re-process the all rules for further OSINT

TLP RED Threat actors list & Demo



Name:

DOB:

Nationality:

Proof:

Signature: