MIPS ROUTER TARGETED WORM BOTNET WITH OPENWRT SDK TOOLCHAINS

Rizal rasmalian
https://github.com/rasmalian
Rizal.rasmalian@gmail.com

\x4D\x45

IT enthusiast ,
self-taught programmer,

Morris Worm

2 November 1988
Robert Tappan Morris Jr , merilis apa yang di yakini banyak ahli computer sebagai worm internet pertama.

Attack Vectors:
- Finger – Buffer OverFlow/OverRun bug
- Sendmail debug – RCE Vuln
- Rexec/Rsh – Bruteforce login

Results:
- 6.000 of 60.000 connected computers infected
- Arpanet network shutdown
- CERT (Computer Emergency Response Team)

Notable Worms

Code Red – Exploit IIS Webserver .ida file

ADMWorm – Exploit BIND DNS Hole

Sadmind – Exploit IIS & Sun Microsystems' Solaris

Blaster– Exploit Microsoft Windows RPC DCOM

SQLammer(Slammer) – Exploit Microsoft SQL Server

Conficker – Exploit Windows Netbios hole & Bruteforce ADMIN$ share

Stuxnet – Memakai 4 Exploit Zero-day termasuk Cpllink Bug (Shortcut icon). Salah satu worm yang di yakini sebagai senjata digital.

Mirai Botnet

未来

21 Oktober 2016

Mirai botnet memecahkan rekor serangan DDOS sebesar 1.2 terabits per detik. Utamanya pada dyndns ,OVH dan web krebsonsecurity.com , web seorang peneliti keamanan yang akhirnya dapat mengungkap pembuat mirai botnet.

Attack Vectors:

- Telnet Bruteforce pada Smart CCTV & Router

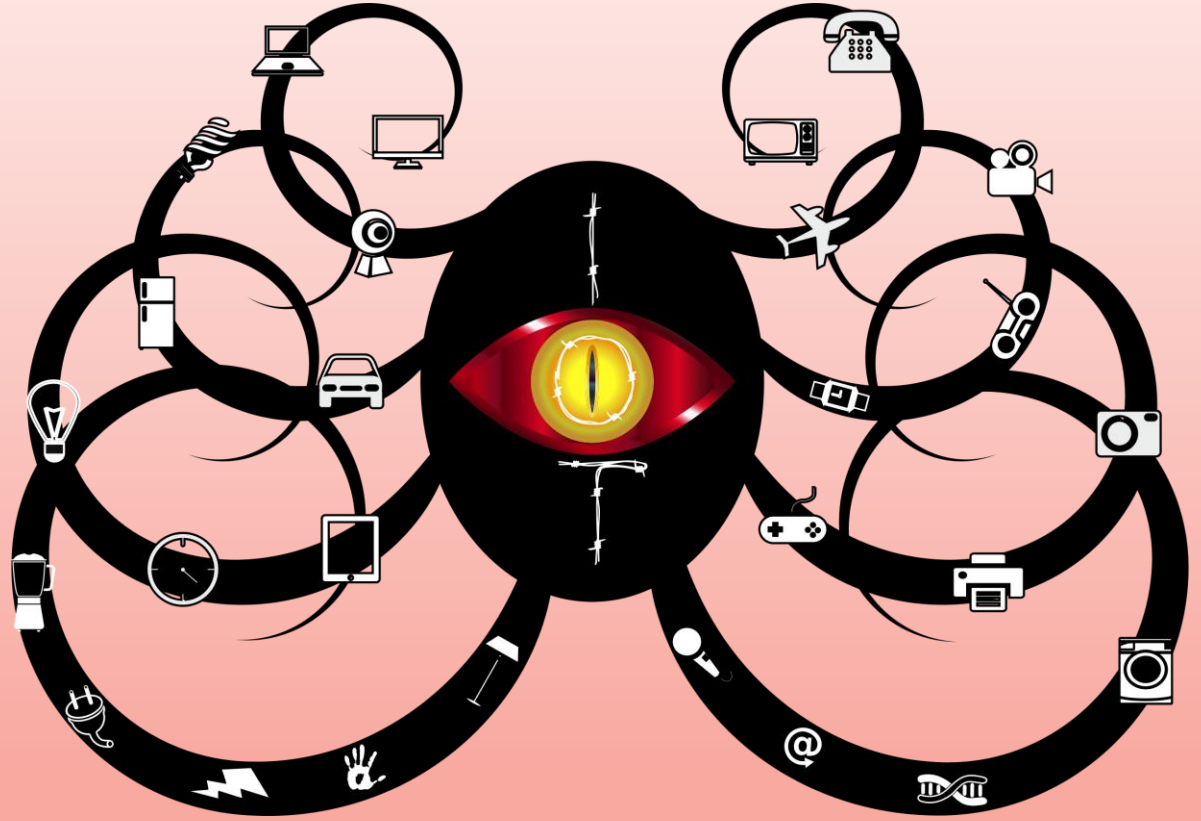
Results:

- Estimated : 1 Juta device terinfeksi Mirai original

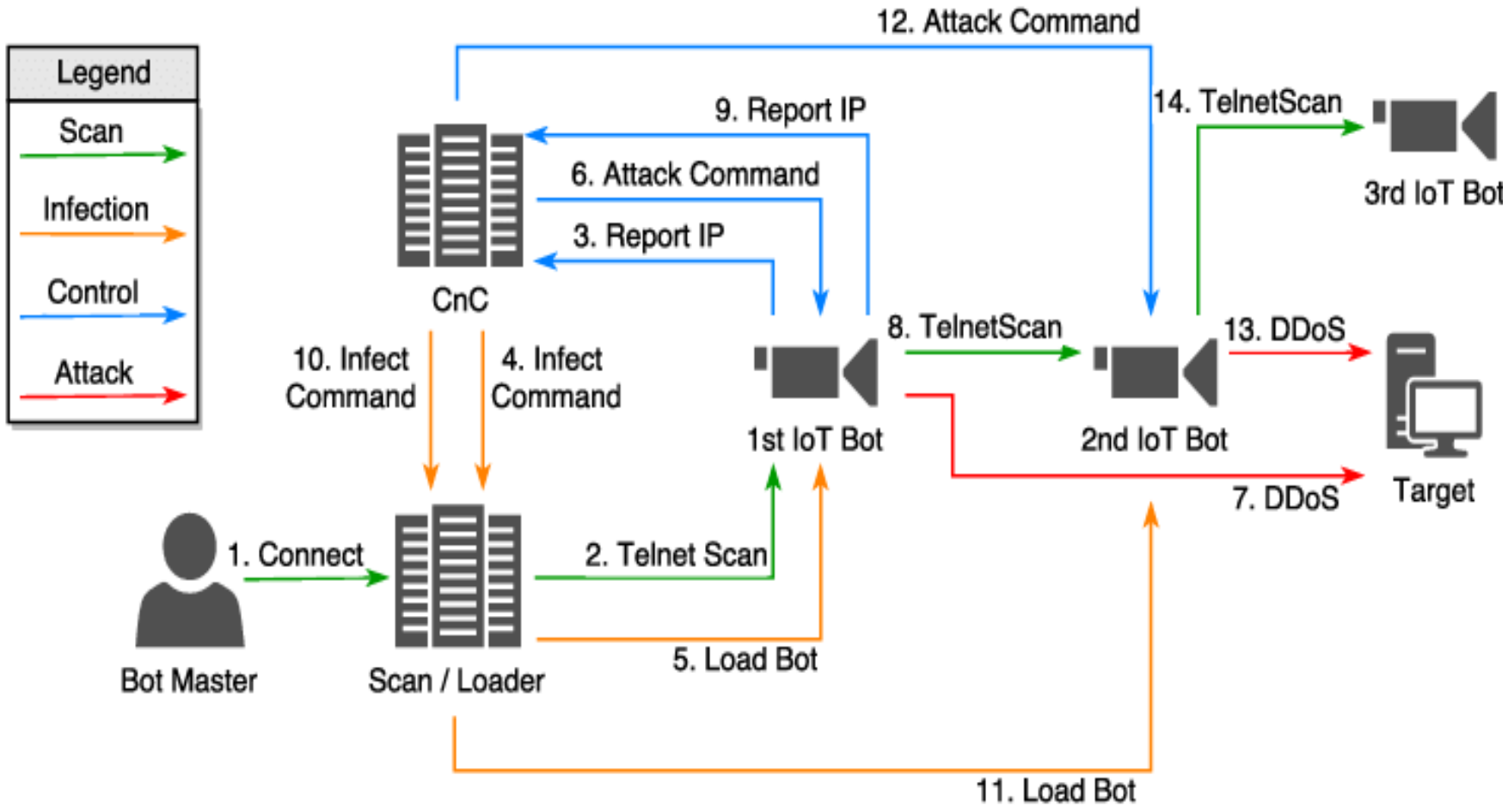
Mirai Botnet

Actors?

Paras Jha
Josiah White
Dalton Norman



Mirai Botnet



Botnet 2020

New Ttint IoT botnet caught exploiting two zero-days in Tenda routers

Ttint is a new form of IoT botnet that also includes remote access tools-like (RAT) features, rarely seen in these botnets before.

Several Botnets Using Zero-Day Vulnerability to Target Fiber Routers

By Ionut Arghire on April 17, 2020

Multiple botnets are targeting a zero-day vulnerability in fiber routers in an attempt to ensnare them and leverage their power for malicious purposes, security researchers warn.

The security bug impacts Netlink Gigabit Passive Optical Networks (GPON) routers and could
ution. Proof-of-concept (PoC) code targeting the
e for nearly a month.

Netlab have **observed** multiple attempts to target the
hed, starting with the Moobot botnet that successfully
n February.

g the 0day in March, they contacted the vendor, but was
targeted device should not be impacted. The

past several weeks, and multiple botnets are targeting
ne vendors appear to be affected, likely because they

were observed leveraging the PoC exploit, albeit failing
because the PoC needs to be chained with another
the security researchers say.

threatpost

Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Podcasts

13 new exploits have been added to the malware's bag of tricks.

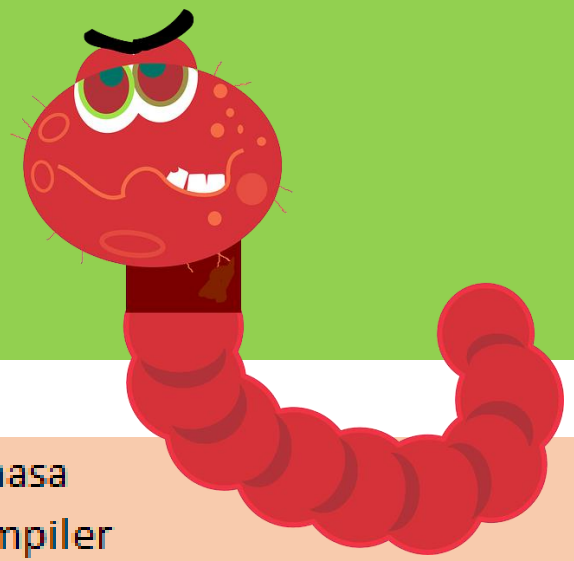
A variant of the Mirai Internet of Things (IoT) botnet known as "Echobot" has added 13 more vulnerability exploits to its bag of infiltration tricks, according to researchers. These target a range of devices, including routers, firewalls, IP cameras, server management utilities, a programmable logic controller used in industrial environments, an online payment system and even a Yachtcontrol web application.

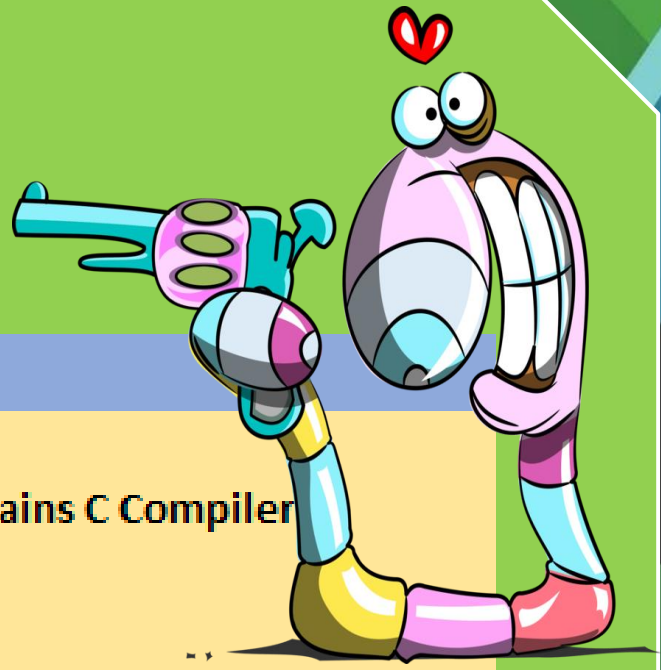
The new additions range from old CVEs (one from 2006 is for Barracuda spam firewalls) to a bug that was disclosed just in early December. They bring the latest version of the malicious code to having a total of 71 unique exploits.

IoT botnets are bent on infecting connected devices in order to marshal their resources to carry out various nefarious activities, such as carrying out distributed denial-of-service (DDoS) attacks. As such, casting a wide net is a savvy strategy to scale the botnet.

JellyFish

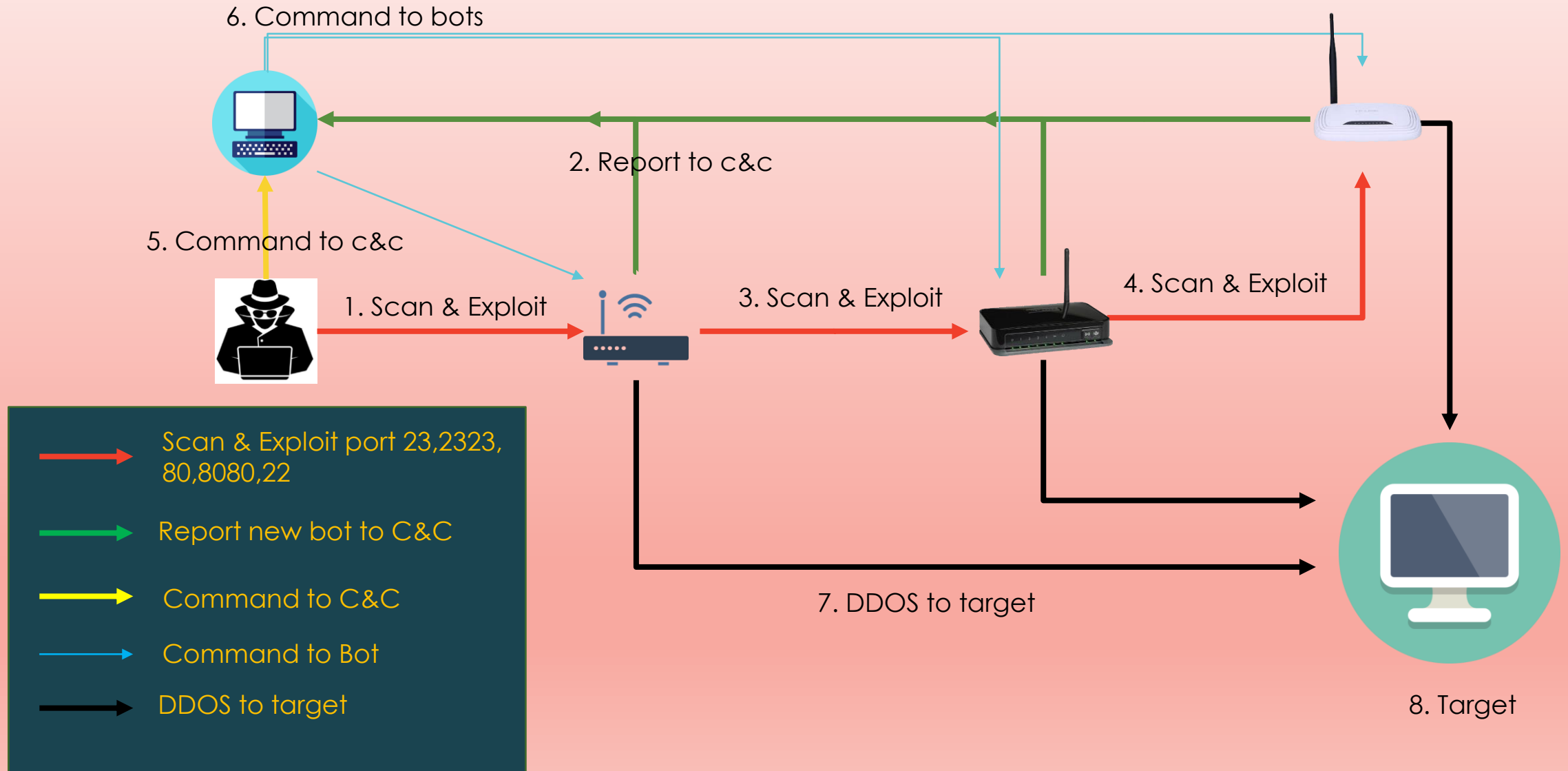
Komparasi

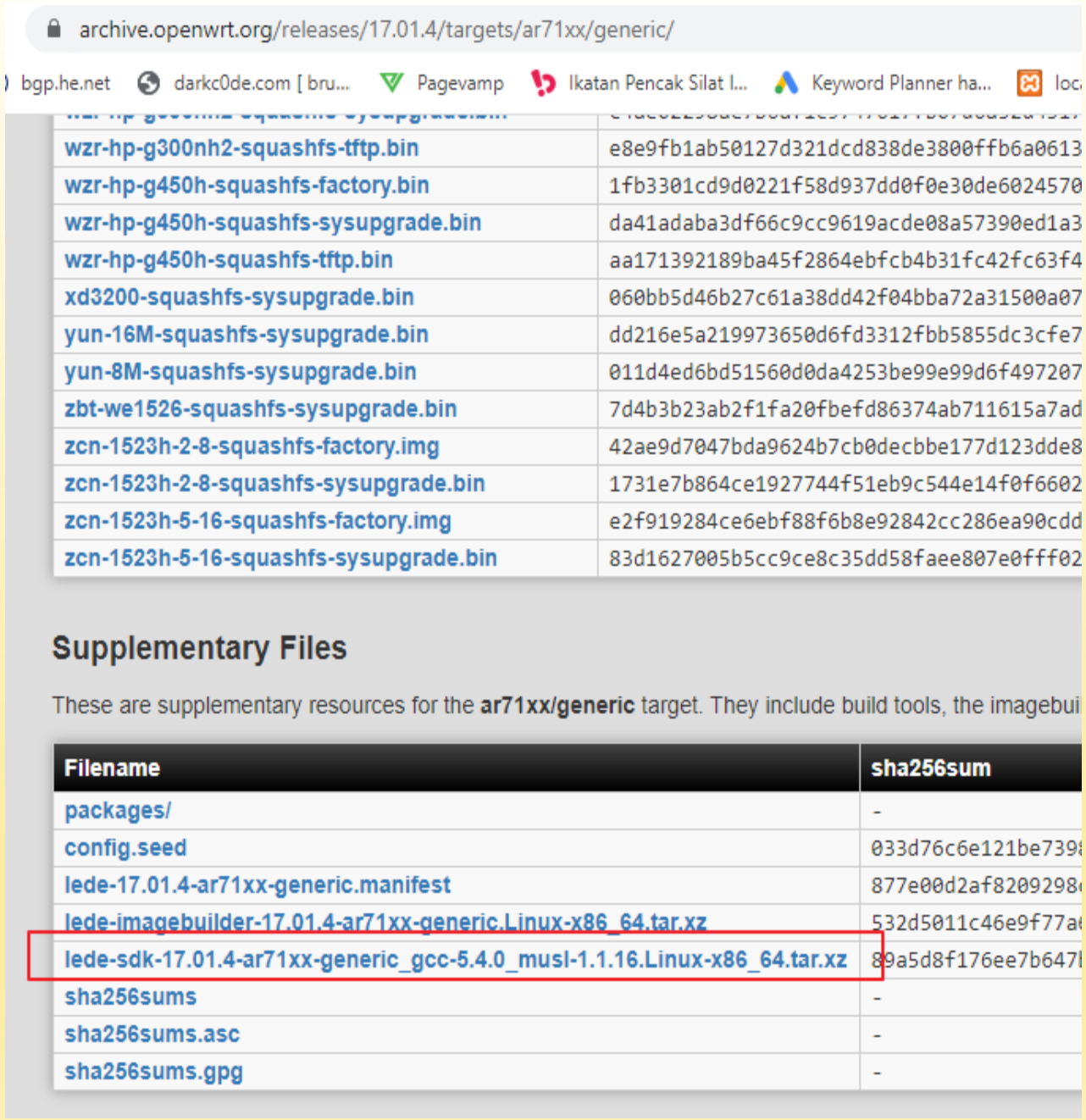




	Mirai Botnet	JellyFish
Bahasa	C	C
Compiler	Cross-Compiler	OpenWrt ToolChains C Compiler
Arsitektur target	Arm,Mipsel,Mipsbe,Sparc,dll	Mipsel/Mipsbe
Loader	Loader Server	-
Vektor serangan	Telnet Bruteforce	Telnet bruteforce
		SSH Bruteforce
		HTTPAuth Bruteforce
		Netgear DGN1000/2200 Exploit (4 Exploit)
Target Scan	Synscan	Synscan
Port scan	23,2323	23,2323,80,8080,22
Comunication to C&C	Binary (xor encryption)	Binary (xor encryption)
Network Tamper	-	Yes

Jellyfish workflow





Openwrt sdk

Compiler yang di pakai adalah **mips-openwrt-linux-gcc** yang di sertakan dalam paket OpenWrt SDK. Hasilnya adalah binary untuk arsitektur Mips (Mipsel dan/atau Mipsbe).

Karna awalnya coding untuk device **TL-MR3020** yang sudah saya install Lede, saya memakai Lede SDK.

Url:
https://archive.openwrt.org/releases/17.01.4/targets/ar71xx/generic/

JellyFish Attack vectors

1. Telnet bruteforce
2. SSH Bruteforce
3. HttpAuth Bruteforce
4. EDB-25978
5. Netgear Telnetable
6. CVE-2017-6077
7. CVE-2017-6334

*CVE-2019-20215 (D-Link ssdpcgi Unauthenticated Remote Command Execution)

Exploit yang di pakai

1. EDB-25978
2. Netgear Telnetable
3. CVE-2017-6077
4. CVE-2017-6334

My Lab Devices

Tidak semua Teknik serangan JellyFish di uji coba, yang sudah di uji coba terbatas pada device yang saya miliki dan gunakan sebagai simulasi jaringan. Berikut beberapa device yang saya pakai untuk percobaan worm/botnet ini.

1. Laptop system operasi windows sebagai CNC server menggunakan python, xampp (apache + mysql)
2. Laptop system operasi Ubuntu untuk compile menggunakan OpenWrt SDK toolchain .
3. TL-WR3020 , hadiah om Lirva32 dengan Lede terinstall di dalamnya.
4. TL-WR741ND, terinstall OpenWrt.
5. Netgear DGN1000, sebagai penghubung antar device tersebut. Selain sebagai simulasi jaringan internet, juga akan menjadi target untuk serangan worm botnet menggunakan bug pada device NETGEAR.

Compile & Test

Selesai

Terima Kasih

Title Lorem Ipsum

LOREM IPSUM DOLOR SIT AMET, CONSECTETUER ADIPISCING ELIT.

NUNC VIVERRA IMPERDIET ENIM. FUSCE EST. VIVAMUS A TELLUS.

PELLENTESQUE HABITANT MORBI TRISTIQUE SENECTUS ET NETUS.