



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

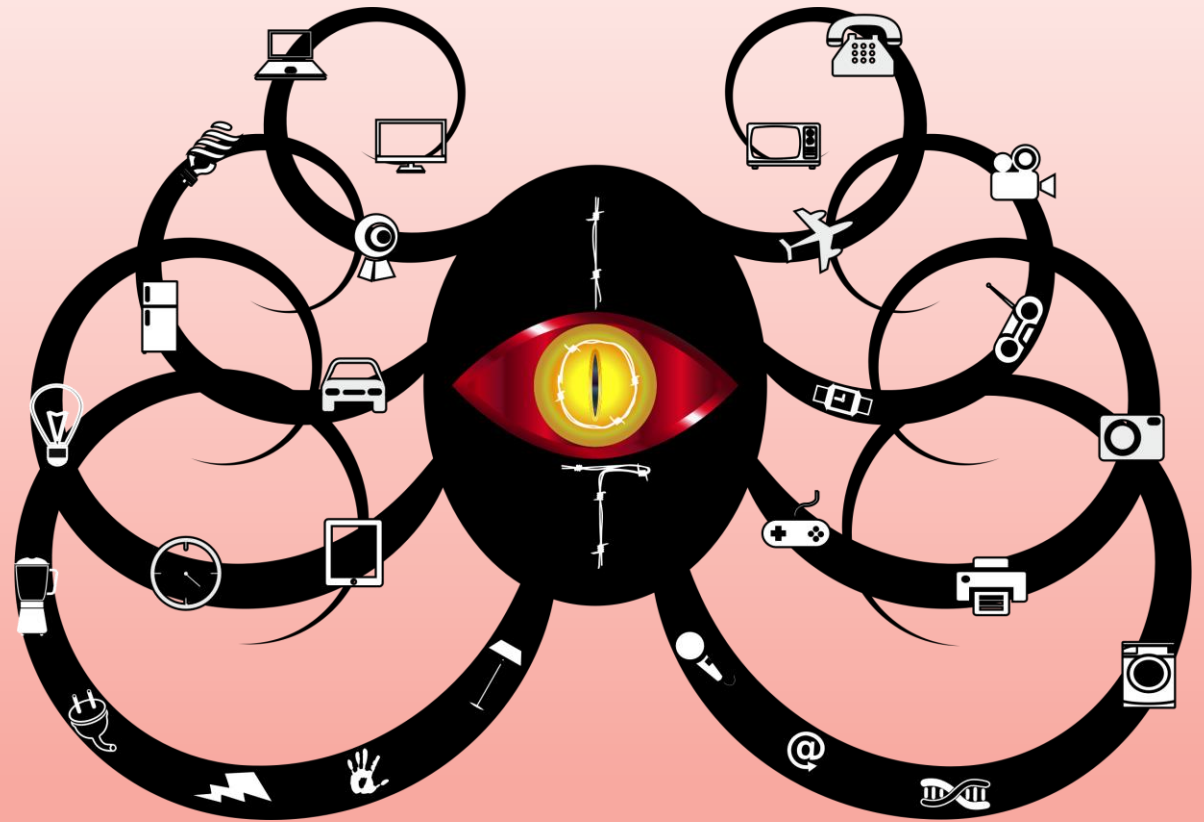


Actors?

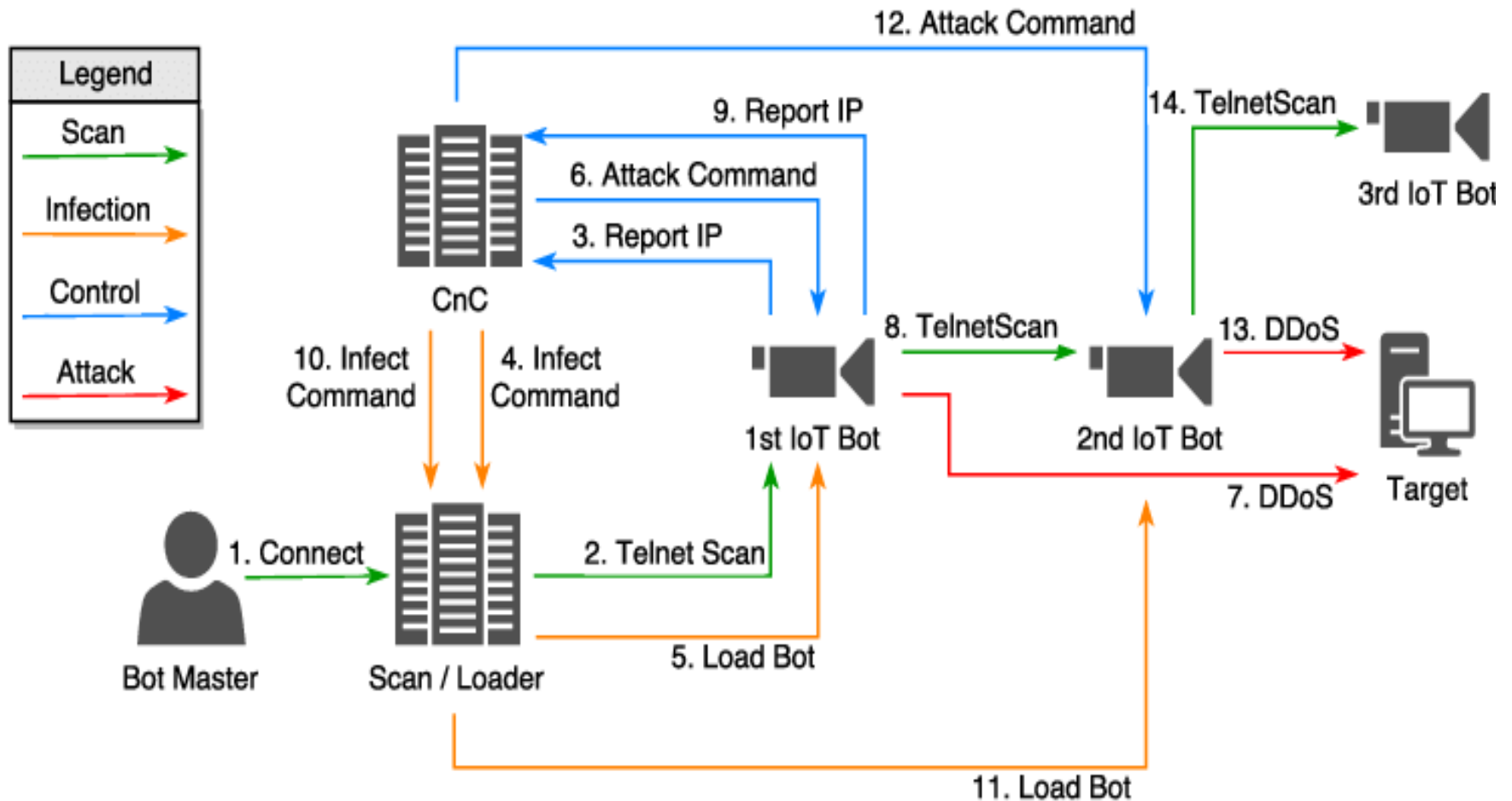
Paras Jha

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.

Who is Micro Focus?
High Tech. Low Drama.

Find out why >



By Catalin Cimpenaru for Zero Day | October 4, 2019
(22:06 SGT) | Topic: Security



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.



Several Botnets Using Zero-Day Vulnerability to Target Fiber Routers

By Ionut Arghire on April 17, 2020



Share



Tweet



Recommend

13



RSS

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 be used to launch a denial-of-service attack. Proof-of-concept (PoC) code targeting the vulnerability was released for nearly a month.

Netlab have observed multiple attempts to target the vulnerability, starting with the Moobot botnet that successfully exploited the bug in February.

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

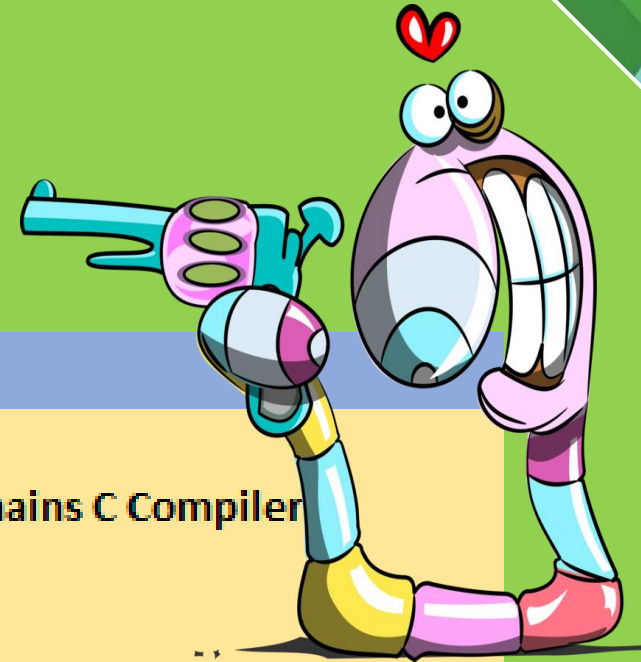
Over the past several weeks, and multiple botnets are targeting the vulnerability. The vendors appear to be affected, likely because they

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

JellyFish

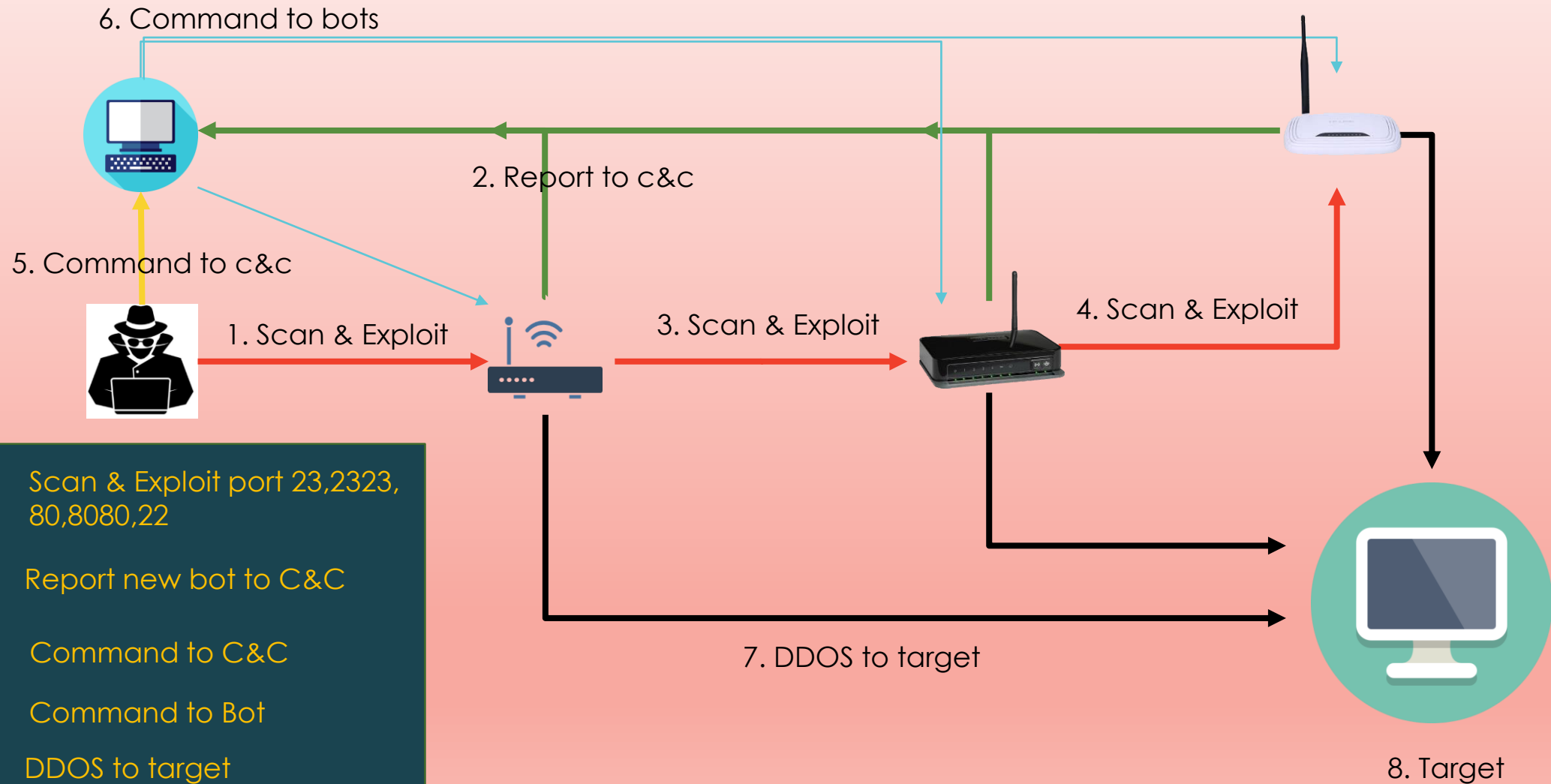


Komparasi



	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



archive.openwrt.org/releases/17.01.4/targets/ar71xx/generic/

bgp.he.net darkc0de.com [bru... Pagevamp Ikatan Pencak Silat L... Keyword Planner ha... loc

wzr-hp-g300nh2-squashfs-tftp.bin	e8e9fb1ab50127d321dcd838de3800ffb6a0613
wzr-hp-g450h-squashfs-factory.bin	1fb3301cd9d0221f58d937dd0f0e30de6024570
wzr-hp-g450h-squashfs-sysupgrade.bin	da41adaba3df66c9cc9619acde08a57390ed1a3
wzr-hp-g450h-squashfs-tftp.bin	aa171392189ba45f2864ebfcb4b31fc42fc63f4
xd3200-squashfs-sysupgrade.bin	060bb5d46b27c61a38dd42f04bba72a31500a07
yun-16M-squashfs-sysupgrade.bin	dd216e5a219973650d6fd3312fbb5855dc3cfe7
yun-8M-squashfs-sysupgrade.bin	011d4ed6bd51560d0da4253be99e99d6f497207
zbt-we1526-squashfs-sysupgrade.bin	7d4b3b23ab2f1fa20fbefd86374ab711615a7ad
zcn-1523h-2-8-squashfs-factory.img	42ae9d7047bda9624b7cb0decbbbe177d123dde8
zcn-1523h-2-8-squashfs-sysupgrade.bin	1731e7b864ce1927744f51eb9c544e14f0f6602
zcn-1523h-5-16-squashfs-factory.img	e2f919284ce6ebf88f6b8e92842cc286ea90cdd
zcn-1523h-5-16-squashfs-sysupgrade.bin	83d1627005b5cc9ce8c35dd58faee807e0ffff02

Supplementary Files

These are supplementary resources for the **ar71xx/generic** target. They include build tools, the imagebuilder

Filename	sha256sum
packages/	-
config.seed	033d76c6e121be7398
lede-17.01.4-ar71xx-generic.manifest	877e00d2af8209298
lede-imagebuilder-17.01.4-ar71xx-generic.Linux-x86_64.tar.xz	532d5011c46e9f77a
lede-sdk-17.01.4-ar71xx-generic_gcc-5.4.0_musl-1.1.16.Linux-x86_64.tar.xz	89a5d8f176ee7b6471
sha256sums	-
sha256sums.asc	-
sha256sums.gpg	-

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.