Enemybot: A Look into Keksec's Latest DDoS Botnet

fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet

April 12, 2022

In mid-March, FortiGuard Labs observed a new DDoS botnet calling itself “Enemybot” and attributing itself to Keksec, a threat group that specializes in cryptomining and DDoS attacks.

This botnet is mainly derived from Gafgyt’s source code but has been observed to borrow several modules from Mirai’s original source code.

It uses several methods of obfuscation for its strings to hinder analysis and hide itself from other botnets. Furthermore, it connects to a command-and-control (C2) server that is hidden in the Tor network, making its takedown more complicated.

Enemybot has been seen targeting routers from Seowon Intech, D-Link, and exploits a recently reported iRZ router vulnerability to infect more devices.

This blog details how this malware leverages these vulnerabilities and the commands it can execute once inside an infected device.

Affected Platforms: Linux
Impacted Users: Any organization
Impact: Remote attackers gain control of the vulnerable systems
Severity Level: Critical

Enemybot by Keksec

One of the first things Enemybot does is to drop a file in */tmp/.pwned*, containing a message that attributes itself to Keksec. In earlier samples, this message was stored as cleartext. Only a few days after, a new sample was released with the message encoded with an XOR operation using a multiple-byte key. This suggests that this malware is being actively developed.

A sample,
SHA256: fec09b614d67e8933e2c09671e042ce74b40048b5f0feed49ba81a2c18d4f473, captured on March 24, 2022 has the message in cleartext:

"ENEMEYBOT V3.1-ALCAPONE hail KEKSEC"

A sample from March 28, 2022 SHA256:
93706966361922b493d816fa6ee1347c90de49b6d59fc01c033abdd6549ac8b9, encoded the message with an XOR operation using a multi-byte key.

Upon decoding, the message has also been changed to:

"ENEMEYBOT V3.1-ALCAPONE - hail KEKSEC, ALSO U GOT haCkED MY [REDACTED] (Your device literally has the security of a [shitty device] / [smart doorbell])"

Figure 1: Code snippet from decoding .pwned message

Subsequently, FortiGuard Labs researchers discovered newer samples that reverted to the cleartext versions of the */tmp/.pwned* message, which might suggest the possibility of multiple developers working with different versions of the codebase or having different programming habits.

Keksec is known for operating multiple botnets, some of which are based on Gafgyt (a.k.a. Bashlite). Gafgyt is a DDoS botnet whose source code was leaked way back in 2015.

In the case of Enemybot, although it is mainly based on Gafgyt, it was observed that some of its modules are clearly borrowed from Mirai's source code. One of these is Enemybot's scanner module as shown in the screenshots below.

Figure 2: Obvious code similarities between Mirai and Enemybot's scanner modules

Another module shared with Mirai is the bot killer module where it searches for any running processes started from certain file paths or with specific keywords in its process memory. It then terminates these processes. Enemybot enhances the original Mirai code with over sixty keywords to identify and kill off any competitors running on the same devices.

While researching this botnet, FortiGuard Labs observed that Enemybot shares several similarities with Gafgyt_tor previously reported by other researchers, and assessed that Enemybot is likely an updated and "rebranded" variant of Gafgyt_tor.

Technical Details

Infects Multiple Architectures

Like most botnets, this malware infects multiple architectures to increase its chances of infecting more devices. In addition to IoT devices, Enemybot also targets desktop/server architectures such as BSD, including Darwin (macOS), and x64.

Enemybot targets the following architectures:

- arm
- arm5
- arm64
- arm7
- bsd
- darwin
- i586
- i686
- m68k
- mips
- mpsl
- ppc
- ppc-440fp
- sh4
- spc
- x64
- x86

Enemybot's download server was previously misconfigured and displayed a list of ELF binaries for different architectures (Figure 3). Threat actors have fixed this at the time of writing.

Figure 3: Open directory of Enemybot's download server

Obfuscation

Enemybot obfuscates strings in a variety of ways:

- C2 domain uses XOR encoding with a multi-byte key
- Credentials for SSH brute-forcing and bot killer keywords use Mirai-style encoding, i.e., single byte XOR encoding with 0x22
- Commands are encrypted with a substitution cipher, i.e,, swapping one character for another
- Some strings are encoded by just adding three to the numeric value of each character

While these obfuscation techniques are simplistic, they are sufficient to hide tell-tale indicators of its presence from casual analysis and other botnets. Most IoT botnets including Enemybot are known for searching for such indicators to terminate other botnets running on the same device.

Infecting More Devices

In terms of spreading, Enemybot uses several methods that have also been observed in other IoT botnet campaigns.

One way is using a list of hardcoded username/password combinations to login into devices configured with weak or default credentials. This is another module that was copied from Mirai's source code.

This malware also tries to run shell commands to infect misconfigured Android devices that expose Android Debug Bridge port (5555).

The last method is to target devices with specific vulnerabilities as listed below:

CVE-2020-17456 is a vulnerability that targets SEOWON INTECH SLC-130 and SLR-120S routers. Malicious commands can be injected into the *pingIPAddr* parameter (Figure 4)

Figure 4: CVE-2020-17456 exploit request

Another vulnerability (no CVE assigned) targets the Seowon SLC-130 router. This is similar to the previous exploit, only this time the command could be injected in the vulnerable *queriesCnt* parameter. The implementation was likely based on publicly available exploit code.

Figure 5: Another exploit targeting Seowon SLC-130 router

CVE-2018-10823 is an older D-Link router vulnerability that allows an authenticated user to execute a malicious command into the *Sip* parameter of the *chkisg.htm* page (Figure 6). The following devices are affected by this vulnerability.

- DWR-116 through 1.06
- DWR-512 through 2.02
- DWR-712 through 2.02
- DWR-912 through 2.02
- DWR-921 through 2.02
- DWR-111 through 1.01

D-Link provided updated firmware for some of the above-mentioned devices. It's recommended to check and update these devices if they still have vulnerable versions.

Figure 6: CVE-2018-10823 exploit request

CVE-2022-27226 is a recent vulnerability on iRZ mobile routers that was exploited by Enemybot shortly after it was published on March 19, 2022. In fact, this is the first botnet observed by FortiGuard Labs to target devices from this vendor.

This vulnerability allows an attacker to execute a command by adding a crontab entry in the infected device via the */api/crontab* (Figure 7).

Figure 7: CVE-2022-27226 exploit request

During the past few weeks, FortiGuard Labs researchers also observed different samples adding and removing exploits. A list of these exploits seen in use by Enemybot for propagation are as follows:

- CVE-2022-25075 to 25084: Targets TOTOLINK routers, previously exploited by the Beastmode botnet
- CVE-2021-44228/2021-45046: Better known as Log4j, more details are available on our Fortinet PSIRT blog
- CVE-2021-41773/CVE-2021-42013: Targets Apache HTTP servers
- CVE-2018-20062: Targets ThinkPHP CMS
- CVE-2017-18368: Targets Zyxel P660HN routers
- CVE-2016-6277: Targets NETGEAR routers
- CVE-2015-2051: Targets D-Link routers
- CVE-2014-9118: Targets Zhone routers
- NETGEAR DGN1000 exploit (No CVE assigned): Targets NETGEAR routers

This mix of exploits targeting web servers and applications beyond the usual IoT devices, coupled with the wide range of supported architectures, might be a sign of Keksec testing the viability of expanding the botnet beyond low-resource IoT devices for more than just DDoS attacks. Based on their previous botnet operations, using them for cryptomining is a big possibility.

After a successful exploit, a shell command is executed to download another shell script from a URL. In most cases, particularly in Mirai-based botnets, this URL is hardcoded. In the case of Enemybot however, this URL is dynamically updated by the C2 server via the command *LDSERVER*. The clear advantage of this method is that when the download server is down for whatever reason, the botnet operators can just update the bot clients with a new URL.

The shell script *update.sh* then downloads the actual Enemybot binaries compiled for every architecture it targets and executes them.

Figure 8: Code snippet from update.sh

Commands and DDoS capabilities

Once the bot gets installed on a victim's device, it connects to its C2 server and waits for further commands. The C2 server hides in the Tor network and the bot tries to access the serverusing a hardcoded list of SOCKS proxy IPs.

This bot supports several commands listed in the following table.

Conclusion

Based on the analysis of FortiGuard Labs, Enemybot is Keksec's latest tool for performing DDoS attacks.

To protect itself, it uses simple obfuscation techniques on its strings as well as hosting its C2 server in the Tor network, taking advantage of the network's anonymity. It uses several techniques commonly found in other DDoS botnet malware to infect other devices.

Seeing how this malware has undergone changes during the research for this article, we expect that more updated versions will be distributed in the wild soon.

FortiGuard Labs will keep monitoring this botnet.

Fortinet Protections

Fortinet customers are protected by the following:

- The FortiGuard Antivirus service detects and blocks this threat as ELF/Gafgyt, Linux/Gafgyt, and Linux/Mirai

- FortiGuard Labs provides IPS signatures against attacks exploiting the following vulnerabilities:
    - CVE-2022-27226 - iRZ.Mobile.Router.API.crontab.AUTH.Remote.Code.Execution
    - CVE-2021-44228/2021-45046 - Apache.Log4j.Error.Log.Remote.Code.Execution
    - CVE-2021-41773/CVE-2021-42013 - Apache.HTTP.Server.cgi-bin.Path.Traversal
    - CVE-2020-17456 - Seowon.Intech.Routers.system_log.CGI.Command.Injection
    - Seowon SLC-130Vulnerability RCE (vulnerable “queriesCnt” parameter) - Seowon.Intech.Routers.Unauthenticated.Remote.Code.Execution
    - CVE-2018-20062 - ThinkPHP.Controller.Parameter.Remote.Code.Execution
    - CVE-2018-10823 - D-Link.DWR.CVE-2018-10823.Remote.Code.Execution
    - CVE-2017-18368 - TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection
    - CVE-2016-6277 - NETGEAR.WebServer.Module.Command.Injection
    - CVE-2015-2051 - D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
    - Netgear DGN1000 exploit (No CVE) - NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution
- The FortiGuard Web Filtering Service blocks downloaded URLs.

FortiGuard IP Reputation & Anti-Botnet Security Service proactively blocks these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

FortiGuard Application Control Service provides organizations the capability to monitor or block access to malicious, risky, or unwanted applications. Customers without specific business requirements for Tor can refer to these Fortinet Technical Tips for blocking inbound and outbound Tor traffic using the Application Control Service.

IOCs

Files

5260b9a859d936c5b8e0dd81c0238de136d1159e41f0b148f86e2555cf4a4e38
Download
URLsb025a17de0ba05e3821444da8f8fc3d529707d6b311102db90d9f04c11577573
bf2f2eb08489552d46b8f50fb07073433f4af94e1215865c48d45f795f96342f
adb51a8d112590a6fdd02ac8d812b837bbe0fcdd762dba6bbba0bd0b538f9aef
373b43345a7e4a6b1d5a6d568a8f6a38906760ea761eacd51a11c164393e4bad
b56655c3c9eed7cd4bce98eeebdcead8daa75a33498ad4f287c753ecc9554aca
cebd50b3a72a314c935b426c0e6b30ec08e0e0cb53e474efffb66f0907309243
73e929575afc04758a23c027ebe4f60ab5c4ba0ab7fa8756b27ed71548302009

33d282c6bccf608d4fbf3a211879759019741c1b822c6cea56c6f479be598367
80f264d7b45a52bd000165f3f3b0fdc0e405f3f128a60a9ec6f085bfba114971
9acf649b74f4aae43a2db90b8d39a7cd39bf6b82c995da7a1ffa6f23c3549b14
a7213ae906a008ad06020436db120a14568c41eae4335d6c76f2bbc33ee9fbcc
2ea62957b9dd8e95052d64a48626c0fa137f0fa9ca4fa53f7f1d8fe35aa38dc0
2ec8016e5fb8375d0cc66bc81f21c2d3f22b785eb4f8e2a02b0b5254159696f5
06f9083e8109685aecb2c35441932d757184f7749096c9e23aa7d8b7a6c080f8
fec09b614d67e8933e2c09671e042ce74b40048b5f0feed49ba81a2c18d4f473
c01156693d1d75481dc96265b41e661301102f3da4edae89338ee9c64dc57d32
820703b9a28d4b46692b7bf61431dc81186a970c243182740d623817910051d1
9790f79da34a70e7fb2e07896a5ada662978473457ca5e2701bd1d1df0b9f10f
a799be50ad82e6338c9e0b33d38612e6ad171872407d5d7de36022adf9b8bf63
4b2b4876ecc7d466eceb30ecbd79001af142b629200bbe61ebd45f4e63cd62ef
d14df997bdf1e3fd3d18edf771376a666dd791dcac550c7dd8de0323823e1037
32faf178c5929510234f2d02aea39ca67ab893e18f60c1593f0c043153625e9d
cc5a743b458bb098998693a73b6a13b9946d375c7c01ac6d37937871d6539102
980fb4731a70a472699fcbee1a16e76c78c1b36ab6430b94dbe2169f8ac21340
93706966361922b493d816fa6ee1347c90de49b6d59fc01c033abdd6549ac8b9
f805f22f668bd0414497ddc061e021c5b80b80c9702053d72fc809f19307073b
2e6305521d4ac770fc661658da6736d658eef384a9aa68bc49613d2be2d23a0d
e8c9452581830668941b3dca59896d339eb65cd8f21875b0e36261e5c093f7fe

Download URLs

http://198[.]12[.]116[.]254/folder/dnsamp.txt
http://198[.]12[.]116[.]254/folder/enemybotarm
http://198[.]12[.]116[.]254/folder/enemybotarm5
http://198[.]12[.]116[.]254/folder/enemybotarm64
http://198[.]12[.]116[.]254/folder/enemybotarm7
http://198[.]12[.]116[.]254/folder/enemybotbsd
http://198[.]12[.]116[.]254/folder/enemybotdarwin
http://198[.]12[.]116[.]254/folder/enemybotі586
http://198[.]12[.]116[.]254/folder/enemybotі686
http://198[.]12[.]116[.]254/folder/enemybotm68k
http://198[.]12[.]116[.]254/folder/enemybotmips
http://198[.]12[.]116[.]254/folder/enemybotmpsl
http://198[.]12[.]116[.]254/folder/enemybotppc
http://198[.]12[.]116[.]254/folder/enemybotppc-440fp
http://198[.]12[.]116[.]254/folder/enemybotsh4
http://198[.]12[.]116[.]254/folder/enemybotspc
http://198[.]12[.]116[.]254/folder/enemybotx64

http://198[.]12[.]116[.]254/folder/enemybotx86
http://198[.]12[.]116[.]254/folder/enemybotx64
http://198[.]12[.]116[.]254/update.sh

C2

xfrvkmokgfb2pajafphw3upl6gq2uurde7de7iexw4aajvslnsmev5id[.]onion (Tor network)

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.