Miori IoT Botnet Delivered via ThinkPH Exploit

blog.trendmicro.com/trendlabs-security-intelligence/with-mirai-comes-miori-iot-botnet-delivered-via-thinkphp-remote-code-execution-exploit/

December 20, 2018

Malware

We analyzed another Mirai variant called "Miori," which is being spread through a Remote Code Execution (RCE) vulnerability in the PHP framework, ThinkPHP.

By: Augusto Remillano II, Mark Vicente December 20, 2018 Read time: (words)

Content added to Folio

SHA-256	
ee9c7a5b9f7059bdd0649eaaa0adb762683c79fbda91746048332813b44fa1e2	Backdoor.Linux.MIRAI.AR
0d3a8933735a8d19c234db8a5ba1a0c2de390ae59b7298494a4e3bf139851d5f	Backdoor.Linux.MIRAI.AR
a6956f98deec26bdaed948cd36ef6bfe954dbba227fd66ad3babd3a7fa4b4d96	Backdoor.Linux.MIRAI.AR
239c9aeec6e17a2739c12b7a4821b99be53375b085210a14d2f4f3e362dd3b7c	Backdoor.Linux.MIRAI.AR
adb8271ed2342f50fd602353251574504672992db45fdde7e1e9a223cbd9a10a	Backdoor.Linux.MIRAI.AR
868a582cd87418faac09859527b1b9405b287799429c424552551a5a3ddfe1b3	Backdoor.Linux.MIRAI.AR
25a5415a04ff746d0cfa4f5e82b00d7aaac60e92424dd94bb8cf9626e6b724ef	Backdoor.Linux.MIRAI.AR
f271d7a3290581f552376cf00006b961fcf54b0d9aa1365c4550113a1132f32d	Backdoor.Linux.MIRAI.AR
bd188c69264362b8a09d14af6196b83a6c3da5d6d3b6dc95b97fe87108500c91	Backdoor.Linux.MIRAI.AR
c5e79ceb1878ad4aebf3e8a33a66aeed535aecc1e5ebca0dd0122a6ecfbfe207	Backdoor.Linux.MIRAI.AS
e51c2675430ebb1e49b4187508eae926fdfc52560074a23f937fe50c72c3d56d	Backdoor.Linux.MIRAI.AS

76049e93887525e097c9fd06bdc31dad6a118082f5b2fc581020ae11ad80be95	Backdoor.Linux.MIRAI.AS
119c33956bb26fdb697b2e042cde106c98cb1562fdbd5bb2acb2d8e7e603a303	Backdoor.Linux.MIRAI.AS
4825e628d3d6442870821823c14bac5bcab93658e3dbf426b8e6c479320077a9	Backdoor.Linux.MIRAI.AS
4dfab085dcc8d1a4ea6be2f6ca08970d238ffcd4b9ee0728d1f38070750e5f7b	Backdoor.Linux.MIRAI.AS
937df675fba3e58e41514ec1881bd9298043533ca9e113b91240d916761fa704	Backdoor.Linux.MIRAI.AS
d6cf67dea7f89d87636f80eba76d4bfcdd6a5fc6540967c446c33522e95f156e	Backdoor.Linux.MIRAI.AS
1b20bedd8a69695ba30a4284c19fe84e5926ed8de4f9074b4137ee07e6674d77	Backdoor.Linux.MIRAI.AS
37b6a3b2ca8681abfcaa79868963046aeaab8a46e123d5311d432bd9d11fcc80	Backdoor.Linux.MIRAI.AS
19eb54eea5dfd71d5753ed94e1845fa81b88545f47c14a2c90960da8e06e6c1b	Backdoor.Linux.MIRAI.AS
ec77dcab385c31bbbf228df92dcaecc947279c3143afc478807184395b06a6e6	Backdoor.Linux.MIRAI.AS
83619527ba2e4c20d1eb5206f058ca55358b4b3ac032ee8d22616a020c8853d0	Backdoor.Linux.MIRAI.AS
27f6c7ce88d874a270d197bb91d419783bf5e08e16fa43ced57607748f2fc5b2	Backdoor.Linux.MIRAI.AS
404ea2a77693b0ab4c76da65aae7451d83d621a75b8eb8d2736998bf1c23ecf3	Backdoor.Linux.MIRAI.AS
64e1f581d42f2c9e0c1f13b4f814d4a4b0cad2e3ac1c8a754f6a912ab07b4bc1	Backdoor.Linux.MIRAI.AS
231d0913bba4b8c02f93fca2a917762eb94013d31f0ac4c9703b498b6ab9a87f	Backdoor.Linux.MIRAI.AS
bf3190c7746775a7756d76d0c4bbeedeb1b4bc2a14fb3465da0bd49dfae14503	Backdoor.Linux.MIRAI.AS
eba3e81fcedaaa9661c5faa41b98c1d7906fdad7f960530f936ac2ad0b921ac3	Backdoor.Linux.MIRAI.AS
ad463ae6c08a085a1c45fc8da32c736bb1ced083d0cc0619a7d0a919c43a3717	Backdoor.Linux.MIRAI.AS
eefa90ebde0d5d16c71315f292f86a72735e62af686a7872d1d153694582404d	Backdoor.Linux.MIRAI.AS
7408a894f4c278155b5ab28ebd48269075ee73ad24dc877cecd7b41a97b6d975	Backdoor.Linux.MIRAI.AS
282836e3d6649d9f97cdbf6b373329386a4fd290b87599f84f1d84ecfe5586eb	Backdoor.Linux.MIRAI.AS
73036a31742e52cca9cfb02883cef62efb7f9129c14e2e2fd3064d2b4b8ec6e0	Backdoor.Linux.MIRAI.AS

The exploitation of vulnerabilities in smart devices has been a persistent problem for many internet of things (IoT) users. Perhaps the most infamous IoT threat is the constantly evolving Mirai malware, which has been used in many past campaigns that compromised devices with default or weak credentials. Different Mirai variants and derivatives have cropped up since its source code was leaked in 2016.

We analyzed another Mirai variant called “Miori,” which is being spread through a Remote Code Execution (RCE) vulnerability in the PHP framework, ThinkPHP. The exploit related to the vulnerability is relatively new — details about it have only surfaced on December 11. For its arrival method, the IoT botnet uses the said exploit that affects ThinkPHP versions prior to 5.0.23 and 5.1.31. Interestingly, our Smart Protection Network also showed a recent increase on events related to the ThinkPHP RCE. We expect malicious actors to abuse the ThinkPHP exploit for their respective gains.

Aside from Miori, several known Mirai variants like IZ1H9 and APEP were also spotted using the same RCE exploit for their arrival method. The aforementioned variants all use factory default credentials via Telnet to log in and spread to other devices. Once any of these Mirai variants infects a Linux machine, it will become part of a botnet that facilitates distributed denial-of-service (DDoS) attacks.

Looking into the Mirai Variant, Miori

Miori is just one of the many Mirai offshoots. Fortinet once described its striking resemblance to another variant called Shinoa. Our own analysis revealed that the cybercriminals behind Miori used the ThinkPHP RCE to make vulnerable machines download and execute their malware from *hxxp://144[.]202[.]49[.]126/php*:

Figure 1. RCE downloads and executes Miori malware

Figure 1. RCE downloads and executes Miori malware

Upon execution, Miori malware will generate this in the console:

Figure 2. Miori infects device

Figure 2. Miori infects device

It will start Telnet to contactother IP addresses. It also listens on port 42352 (TCP/UDP) for commands from its C&C server. It then sends the command “/bin/busybox MIORI” to verify infection of targeted system.

Figure 3. Miori sends command

Figure 3. Miori sends command

We were able to decrypt Miori malware’s configuration table embedded in its binary and found the following notable strings. We also listed the usernames and passwords used by the malware, some of which are default and easy-to-guess.

Mirai variant: **Miori**

XOR key: 0x62

Username/Password	Notable strings

1001chin	/bin/busybox kill -9
adm	/bin/busybox MIORI **(infection verification)**
admin123	/bin/busybox ps **(kills parameters)**
admintelecom	/dev/FTWDT101\ watchdog
aquario	/dev/FTWDT101_watchdog
default	/dev/misc/watchdog
e8ehome	/dev/watchdog
e8telnet	/dev/watchdog0
GM8182	/etc/default/watchdog
gpon	/exe
oh	/maps
root	/proc/
support	/proc/net/route
taZz@23495859	/proc/net/tcp
telecomadmin	/sbin/watchdog
telnetadmin	/status
tsgoingon	account
ttnet	enable
vizxv	enter
zte	incorrect
	login
	lolistresser[.]com **(C&C server)**
	MIORI: applet not found **(infection verification)**
	password
	shell
	system
	TSource Engine Query
	username
	your device just got infected to a bootnoot

Table 1. Related Miori credentials and strings

A closer look also uncovered two URLs used by two other variants of Mirai: **IZ1H9** and **APEP**. We then looked into the binaries (x86 versions) located in the two URLs. Both variants use the same string deobfuscation technique as Mirai and Miori, and we were likewise able to decrypt their configuration table.

hxxp://94[.]177[.]226[.]227/bins/

Mirai variant: **IZ1H9**

XOR key: 0xE0

Username/Password	Notable strings
00000000	/bin/busybox IZ1H9 **(infection verification)**
12345	/bin/watchdog /dev/FTWDT101\ watchdog **(watchdog disabling)**
54321	/dev/FTWDT101_watchdog
123456	/dev/misc/watchdog
1111111	/dev/watchdog
20080826	/dev/watchdog0
20150602	/dev/watchdog1
88888888	/etc/default/watchdog
1234567890	/etc/resolv.conf
/ADMIN/	/proc/
admin1	/proc/net/tcp
admin123	/sbin/watchdog
admin1234	assword
antslq	enable
changeme	enter
D13hh[	IZ1H9: applet not found
default	j.#0388 **(printed out in console after execution)**
ezdvr	linuxsh
GM8182	linuxshell
guest	nameserver
hi3518	ncorrect
ipc71a	system
IPCam@sw	TSource Engine Query
ipcam_rt5350	
juantech	

jvbzd

klv123

klv1234

nimda

password

qwerty

QwestM0dem

root123

service

smcadmin

support

svgodie

system

telnet

tl789

vizxv

vstarcam2015

xc3511

xmhdpic

zlxx.

zsun1188

Zte521

Table 2. Related IZ1H9 credentials and strings

hxxp://cnc[.]arm7plz[.]xyz/bins/

Mirai variant: **APEP**

XOR key: 0x04

Username/Password	C&C server	Notable strings

123456	*cnc[.]arm7plz[.]xyz*	%4'%-\F
888888	*scan[.]arm7plz[.]xyz*	/bin/busybox APEP **(infection verification)**
20150602		/bin/watchdog **(watchdog disabling)**
1q2w3e4r5		/dev/FTWDT101/watchdog
2011vsta		/dev/FTWDT101_watchdog
3ep5w2u		/dev/misc/watchdog
admintelecom		/dev/watchdog
bcpb+serial#		/dev/watchdog0
default		/etc/default/watchdog
e8ehome		/etc/watchdog /maps/
e8telnet		/proc/
fliruser		/proc/net/tcp
guest		/sbin/watchdog /status
huigu309		CIA NIGGER
juniper123		enable
klv1234		enter
linux		incorrect
maintainer		linuxshell
Maxitaxi01		password
super		shell
support		start
taZz@01		system
taZz@23495859		terryadavis
telecomadmin		
telnetadmin		
tsgoingon		
vstarcam2015		
Zte521		
ZXDSL		

Table 3. Related APEP credentials, C&C servers, and strings

It should be noted that aside from dictionary attacks via Telnet, APEP also spreads by taking advantage of CVE-2017-17215, which involves another RCE vulnerability and affects Huawei HG532 router devices, for its attacks. The vulnerability was also reported to be involved in Satori and Brickerbot variants. Huawei has since released a security notice and outlined measures to circumvent possible exploitation.

Figure 4. Exploit related to CVE-2017-17215

Figure 4. Exploit related to CVE-2017-17215

Conclusion and Recommendations

Telnet default password login attempts to connected devices aren't new. Factory default passwords, which many users may ignore or forget to change, are commonly used to access vulnerable devices. Mirai has since spawned other botnets that use default credentials and vulnerabilities in their attacks. Users are advised to change the default settings and credentials of their devices to deter hackers from hijacking them. As a general rule, smart device users should regularly update their devices to the latest versions. This will address vulnerabilities that serve as potential entry points for threats and will also improve the functionality of the devices. Finally, enable the auto-update feature if the device allows it.

Users can also adopt IoT security solutions that are designed to combat these kinds of threats. Trend Micro Smart Home Network™ protects users from this threat via this intrusion prevention rule:

> 1135215 WEB ThinkPHP Remote Code Execution

Indicators of Compromise (IoCs)

Related malicious URLs:

hxxp://144[.]202[.]49[.]126/miori[.]mips

hxxp://144[.]202[.]49[.]126/miori[.]mpsl

hxxp://144[.]202[.]49[.]126/miori[.]arm

hxxp://144[.]202[.]49[.]126/miori[.]arm5

hxxp://144[.]202[.]49[.]126/miori[.]arm6

hxxp://144[.]202[.]49[.]126/miori[.]arm7

hxxp://144[.]202[.]49[.]126/miori[.]sh4

hxxp://144[.]202[.]49[.]126/miori[.]ppc

hxxp://144[.]202[.]49[.]126/miori[.]x86

hxxp://144[.]202[.]49[.]126/miori[.]arc

hxxp://144[.]202[.]49[.]126/php

hxxp://94[.]177[.]226[.]227/bins/

hxxp://cnc[.]arm7plz[.]xyz/bins/

hxxp://scan[.]arm7plz[.]xyz