Mirai, RAR1Ransom, and GuardMiner – Multiple Malware Campaigns Target VMware Vulnerability

fortinet.com/blog/threat-research/multiple-malware-campaigns-target-vmware-vulnerability

October 20, 2022

In April, VMware patched a vulnerability CVE-2022-22954. It causes server-side template injection because of the lack of sanitization on parameters “deviceUdid” and “devicetype”. It allows attackers to inject a payload and achieve remote code execution on VMware Workspace ONE Access and Identity Manager. FortiGuard Labs published Threat Signal Report about it and also developed IPS signature in April.

We observed attacks in the wild since then. Most of the payloads focus on probing a victim’s sensitive data, for example, passwords, hosts file, etc. But in August, there were a few particular payloads, which got our interest. They had the intention of deploying Mirai targeting exposed networking devices running Linux, RAR1ransom that leverages legitimate WinRaR to deploy encryption, and GuardMiner that is a variant of xmrig used to “mine” Monero.

In this blog, we will elaborate on how these malware leveraged the VMware vulnerability and the behavior after exploitation in more detail.

Affected platforms: VMware Workspace ONE Access and Identity Manager
Impacted parties: VMware users
Impact: Attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands
Severity level: Critical

Figure 1 CVE-2022-22954 Activity

Mirai Variant

The complete payload from Mirai is shown in Figure 2, it enters temp directory and downloads Mirai variant from http[:]//107[.]189[.]8[.]21/pedalcheta/cutie[.]x86_64, then executes with parameter “VMware”.

Figure 2 Attacking traffic capture

Figure 3 Decoded command

Like most Mirai botnets, this variant’s main jobs include deploying DoS and launching a brute force attack. We can decode part of the configuration after we XOR the data with 0x54 and get C2 server is “cnc[.]goodpackets[.]cc”. Following is the decoded strings:

Figure 4 Decoded configuration string

We also identify the brute force function with encoded account and password strings:

Figure 5 Functions for brute force attack

The decoded passwords are listed below, they are commonly used passwords and also some default credentials for well-known IoT devices:

hikvision	1234	win1dows	S2fGqNFs
root	tsgoingon	newsheen	12345
default	solokey	neworange88888888	guest
bin	user	neworang	system
059AnkJ	telnetadmin	tlJwpbo6	iwkb
141388	123456	20150602	00000000
adaptec	20080826	vstarcam2015	v2mprt
Administrator	1001chin	vhd1206	support
NULL	xc3511	QwestM0dem	7ujMko0admin
bbsd-client	vizxv	fidel123	dvr2580222
par0t	hg2x0	samsung	t0talc0ntr0l4!
cablecom	hunt5759	epicrouter	zlxx
pointofsale	nflection	admin@mimifi	xmhdipc
icatch99	password	daemon	netopia
3com	DOCSIS_APP	hagpolm1	klv123
OxhlwSG8			

After being executed, the variant shows hardcoded string “InfectedNight did its job”, and sends heartbeat along with parameter “VMware”, then it will wait for further commands from C2 server. Below is the traffic session from heartbeat and brute force attack.

Figure 6 Heartbeat traffic capture

Figure 7 Brute force attack session

Initialization Script for RAR1Ransom and GuardMiner

Another noticeable payload is from 67[.]205[.]145[.]142. It contains two sessions, each has different commands depending on the victim’s operation system. One leveraged PowerShell to download “init.ps1”, the other uses curl, wget, and urlopen in Python library to download “init.sh”.

Figure 8 Attack traffic capture for Windows

Figure 9 Attack traffic capture for Linux

From the PowerShell script file “init.ps1”, it includes a few links to cloudflare-ipfs[.]com for further attack and each file has its own backup link to crustwebsites[.]net.

Figure 10 Download links in init.ps1

There are 7 files for initialization:

- phpupdate.exe: Xmrig Monero mining software
- config.json: Configuration file for mining pools
- networkmanager.exe: Executable used to scan and spread infection
- phpguard.exe: Executable used for guardian Xmrig miner to keep running
- init.ps1: Script file itself to sustain persistance via creating scheduled task
- clean.bat: Script file to remove other cryptominers on the compromised host
- encrypt.exe: RAR1 ransomware

Figure 11 "start encrypt" section in init.ps1

In the “start encrypt” section shown in Figure 11, it first checks “flag_encrypt.flag” before launching RAR1ransom, if the flag file existed and the “encrypt.exe” was also download before, it will delete “encrypt.exe” and go to the next stage. Otherwise, it checks the file size to determine if the file path should be updated or not. Finally, it executes the ransomware after checking process. The detail of RAR1 ransomware will be elaborated in the next section.

Then, the script starts the GuardMiner attack. GuardMiner is a cross-platform mining Trojan, which has been active since 2020. And FortiGuard Labs has a detailed report covering it. In this version, it also drops the script file “init.sh” for Linux system.

Figure 12 “init.sh” for Linux

We also noticed that GuardMiner updates “networkmanager.exe” with the more recently vulnerability. From the name of each exploit module, it might collect the exploit list from Chaitin Tech Github which is for security testing purposes.

Figure 13 rdata section contains vulnerability list in networkmanager.exe

We extract the complete vulnerability list below:

eyou-email-system-rce	maccms-rce
thinkphp5-controller-rce	seacms-rce
terramaster-tos-rce-cve-2020-28188	spon-ip-intercom-ping-rce
thinkphp5023-method-rce	yonyou-grp-u8-sqli-to-rce

yccms-rce	gitlist-rce-cve-2018-1000533
phpunit-cve-2017-9841-rce	pandorafms-cve-2019-20224-rce
yonyou-nc-bsh-servlet-bshservlet-rce	CVE-2022-22947-spring-clond-Gateway-RCE
CVE-2022-22954-VMware-RCE	amtt-hiboss-server-ping-rce
inspur-tscev4-cve-2020-21224-rce	dlink-dsl-2888a-rce
phpstudy-backdoor-rce	Confluence-CVE-2022-26134
seacms-before-v992-rce	apache-flink-upload-rce
dedecms-cve-2018-7700-rce	solr-velocity-template-rce
webmin-cve-2019-15107-rce	jumpserver-unauth-rce
Hotel-Internet-Manage-RCE	drupal-cve-2018-7600-rce
seacms-v654-rce	S2-045-rce
tamronos-iptv-rce	ecshop-rce
satellian-cve-2020-7980-rce	opentsdb-cve-2020-35476-rce
zeroshell-cve-2019-12725-rce	struts2-062-cve-2021-31805-rce
dlink-cve-2019-16920-rce	h3c-imc-rce

RAR1Ransom

RAR1ransom drops “rar.exe” in C:/Windows/Temp folder which is legitimate WinRaR software to compress a victim’s files with a password. It uses several default options in WinRaR to complete the encryption for efficiency, we can locate these processes from Process Explorer in Figure 14.

Figure 14 Processes while RAR1Ransom encrypted files

The whole command is below, options “df” and “m0” mean delete files after adding files to archive without compression, “mt10” means it will use ten threads, and “ep” means exclude path from name. The “hp” is to encrypt both file data and headers with password.

C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQqYpzrkjwvuNSjsnQlicOxNPi0iKzKeQO1Besbpbx1iKWNeOfFQDEw8qaoAGmN1Nx9i0vbUcr "C:/Python27/Lib/json/MVXGG33EMVZC44DZ.rar1" "C:/Python27/Lib/json/MVXGG33EMVZC44DZ"

RAR1Ransom targets a compromised victim’s file with particular extensions as in Figure 15.

Figure 15 Target file extension

All the encrypted files will have an unique filename and “.rar1” extension, and it drops a text file “READ_TO_DECRYPT.txt” in the same folder with message in Figure 17.

Figure 16 Encrypted files

Figure 17 Ransom note

From the wallet string in the ransom note, which is identical with the one in the miner's configuration shown in Figure 17. We can tell the attacker intends to utilize a victim's resources as much as possible, not only to install RAR1Ransom for extortion, but also to spread GuardMiner to collect cryptocurrency.

Figure 18 Configuration"config.json" for GuardMiner

Conclusion

Although the critical vulnerability CVE-2022-22954 is already patched in April, there are still multiple malware campaigns trying to exploit it. Users should always keep systems updated and patched and be aware of any suspicious process in environment. These Mirai variants, RAR1Ransom, and GuardMiner are not extremely complicated samples, but their methods are always changing and evolving. FortiGuard Labs will continue to monitor and provide the latest updates.

Fortinet Protections

Fortinet released IPS signature VMware.Workspace.ONE.Access.Catalog.Remote.Code.Execution for CVE-2022-22954 to proactively protect our customers. The signature is officially released in IPS definition version 20.297.

The scripts and malwares are detected and blocked by FortiGuard Antivirus, and FortiEDR services:

Adware/Miner
W32/PossibleThreat
Riskware/Agent
BASH/CoinMiner.RZ!tr
PowerShell/CoinMiner.BW!tr
ELF/GuardMiner.A!tr
W64/GuardMiner.A!tr
BAT/Cleaner.CC41!tr

IOCs

SHA256:

66db83136c463441ea56fb1b5901c505bcd1ed52a73e23d7298f7055db2108d1
4761e5d9bd3ebe647fbd7840b7d2d9c1334bde63d5f6b05a4ed89af7aa3a6eab
9c00823295f393358762542418bb767b44cfe285c4ab33e7e57902c6e1c2dacb
23270d23f8485e3060f6ea8c9879177781098b1ed1b5117579d2f4d309aeffd2
4b3578ee9e81f356a89ff2e1aff6bbee8441472869b0c6c4792fc9fd486a0df5
0212b447c25e9db55f7270e1e2a45846e22614454748459 97a314cb1ddeea4f7
a372e07a691f8759e482615fd7624bfca2a2bc2cd8652a47ff9951ff035759a5
f2a6827ea5f60cefc2f6528269b2d1557a7cc1e68f84edca4029e819dd0509cb
4b4c0d3cb708612b1fdb0394e029e507e4c0f6136fc44e415200694624ed5b68
7fc7c242ad1fa439e515725561a9e304b3d94e40ba91f61df77471a4c2ff2b39

Learn more about Fortinet's FortiGuard Labs threat research and global intelligence organization and Fortinet's FortiGuard AI-powered Security Services portfolio. Sign up to receive our threat research blogs.