KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lockbit3.0 associate abuses Windows Defender loads Cobalt Strike

Tracker ID: TN0802 **Date:** 05/Aug/2022 **Category:** Threat Actor **Industry:** All **Region**: All

Background

A threat actor associated with the LockBit3.0 ransomware operation was observed exploiting the Windows Defender command-line tool in a recent campaign. To evade detection by security tools, it encrypts and loads Cobalt Strike payloads onto infected devices using the Windows Defender command line tool "MpCmdRun.exe." Threat actors are actively employing Cobalt Strike, a legitimate penetration testing tool with numerous features, to conduct covert network reconnaissance and lateral movement before stealing and encrypting data.

The initial network intrusion was accomplished by leveraging an unpatched Log4j bug on vulnerable VMware Horizon Servers, followed by the execution of PowerShell code. The attacker added a web shell to the application's Blast Secure Gateway component using PowerShell code. After gaining initial access, threat actors attempt to execute a myriad of post-exploitation tools, including Meterpreter, PowerShell Empire, and a new technique of side-loading Cobalt Strike.

After gaining access to a target system and obtaining the requisite user privileges, threat actors utilize PowerShell to execute commands and exfiltrate the command output via a POST base64 encoded request to an IP address. From their controlled C2, the threat actor downloads a malicious DLL, the encrypted payload, and the legitimate utility. The threat actor decrypts and loads Cobalt Strike payloads via the legitimate Windows Defender command line utility MpCmdRun.exe. Soon after downloading Cobalt Strike, a correlation was discovered between the IP address used to download the payload and the IP address utilized for reconnaissance. The threat actor attempted to execute the program and transmit the output to the IP address starting with 139. The threat actor then downloads three files from their controlled C2: a malicious DLL file, a clean copy of a Windows CL tool, and the encrypted payload as a LOG file.

MpCmdRun.exe is a command-line utility that is used to perform Microsoft Defender activities. It allows instructions to search for malware, collect data, recover items, perform diagnostic tracing, and more. When MpCmdRun.exe is executed, the legitimate DLL "mpclient.dll," which is required for the software to operate normally, is loaded. The threat actors have modified mpclient.dll to be used as a weapon and positioned it in a location where loading the malicious version of the DLL file takes precedence over the normal version of the DLL file. A "c0000015.log" file dumped with the other two files from the earlier stage of the assault contained an encrypted Cobalt Strike payload that was loaded and decoded by the malware that was being executed.

Previous techniques of evasion included the removal of EDR/userland EPP hooks, Event Tracing for Windows, and Antimalware Scan Interface. LockBit has observed Cobalt Strike beacons being side-loaded onto compromised systems; in fact, analogous infection chains have been observed via utility usage. Defenders should be aware that LockBit ransomware operators and affiliates are exploring and exploiting unique "living off the land" methods to assist them in loading Cobalt Strike beacons and evading detection by several standard EDR and traditional AV tools.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lockbit3.0 associate abuses Windows Defender loads Cobalt Strike

Tracker ID: TN0802 **Date:** 05/Aug/2022 **Category:** Threat Actor **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Persistence, Defense Evasion, Command and Control, Exfiltration

Indicators of Compromise

Please refer to the attached sheet for IOCs

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Validate the IOCs attached and implement the detection & prevention accordingly.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Perform regular data backup procedures and maintain up-to-date incident response and recovery procedures.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart ransomware threats.
- Monitor the beacon on the network level to prevent data exfiltration by malware or threat actors.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.

References

- Julio Dantas, James Haughom and Julien Reisdorffer, Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool, 28th July 2022, Sentinel One, External Link (sentinelone.com)
- Bill Toulas, LockBit ransomware abuses Windows Defender to load Cobalt Strike, 29th July 2022, Bleeping Computer, External Link (bleepingcomputer.com)
- Ravie Lakshmanan, LockBit Ransomware Abuses Windows Defender to Deploy Cobalt Strike Payload, 02nd August 2022, TheHackerNews External Link (thehackernews.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lockbit3.0 associate abuses Windows Defender loads Cobalt Strike

Tracker ID: TN0802 **Date:** 05/Aug/2022 **Category:** Threat Actor **Industry:** All **Region**: All

SHA1 Hash	IP	Domain
a512215a000d1b21f92dbef5d8d57a420197d262	45.32.108[.]54	info.openjdklab[.]xyz
729eb505c36c08860c4408db7be85d707bdcbf1b	149.28.137[.]7	
10039d5e5ee5710a067c58e76cd8200451e54b55	139.180.184[.]147	
ff01473073c5460d1e544f5b17cd25dadf9da513		
e35a702db47cb11337f523933acd3bce2f60346d		
82bd4273fa76f20d51ca514e1070a3369a89313b		
091b490500b5f827cc8cde41c9a7f68174d11302		
0815277e12d206c5bbb18fd1ade99bf225ede5db		
eed31d16d3673199b34b48fb74278df8ec15ae33		