BLACKSWAN CYBERSECURITY

THREAT ADVISORY

May 30, 2023

Lazarus Group attacking Windows IIS Web Servers

SUMMARY

The North Korean APT group Lazarus is targeting Microsoft IIS servers in attacks that include dropping webshells and malware and harvesting credentials to propagate across the network. Attack vectors include Log4Shell and the 3CX supply chain attack.

TECHNICAL DETAILS

The AhnLab Security Response Center (ASEC) reported that the latest round of espionage attacks used the Lazarus Group's signature DLL side-loading technique during the initial web server compromise. DLL side-loading refers to the proxy execution of a rogue DLL via a benign binary that is planted in the same directory.

Attackers place a malicious DLL (e.g., msvcr100.dll) in the same folder path as a normal application, like Wordconv.exe, by using the Windows IIS web server process w3wp.exe. Attackers then execute the normal application to initiate the execution of the malicious DLL. The malicious msvcr100.dll library is designed to decrypt an encoded payload that is then executed in memory.

The attack chain also includes the exploitation of a discontinued open source Notepad++ plugin called Quick Color Picker to deliver additional malware that then facilitates the credential harvesting and lateral movement.

INDICATORS OF COMPROMISE (IoCs)

DLL Side-loading File Path:
C:\ProgramData\USOShared\Wordconv.exe
C:\ProgramData\USOShared\msvcr100.dll

MD5:
diagn.dll : e501bb6762c14baafadbde8b0c04bbd6
msvcr100.dll : 228732b45ed1ca3cda2b2721f5f5667c
? (Variant malware of msvcr100.dll): 47d380dd587db977bf6458ec767fee3d
cylvc.dll (Variant malware of msvcr100.dll): 4d91cd34a9aae8f2d88e0f77e812cef7

RECOMMENDATIONS

- If running IIS servers, review your environment for evidence of these IOCs.
- Ensure that systems and applications are updated and hardened to the extent possible, especially Internet-facing systems.
- Monitor systems for abnormal process execution 24x7, ideally with a UEBA tool that can detect deviations from a baseline.
- Include hash values in manifest files to help prevent side-loading of malicious libraries.

REFERENCES

- https://asec.ahnlab.com/en/53132/
- https://duo.com/decipher/lazarus-group-targets-iis-servers
- https://www.darkreading.com/cloud/lazarus-group-striking-vulnerable-windows-iis-web-servers
- https://attack.mitre.org/techniques/T1574/002/
- https://www.mandiant.com/sites/default/files/2021-09/rpt-dll-sideloading.pdf
- https://attack.mitre.org/datasources/DS0011/#Module%20Lo