Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

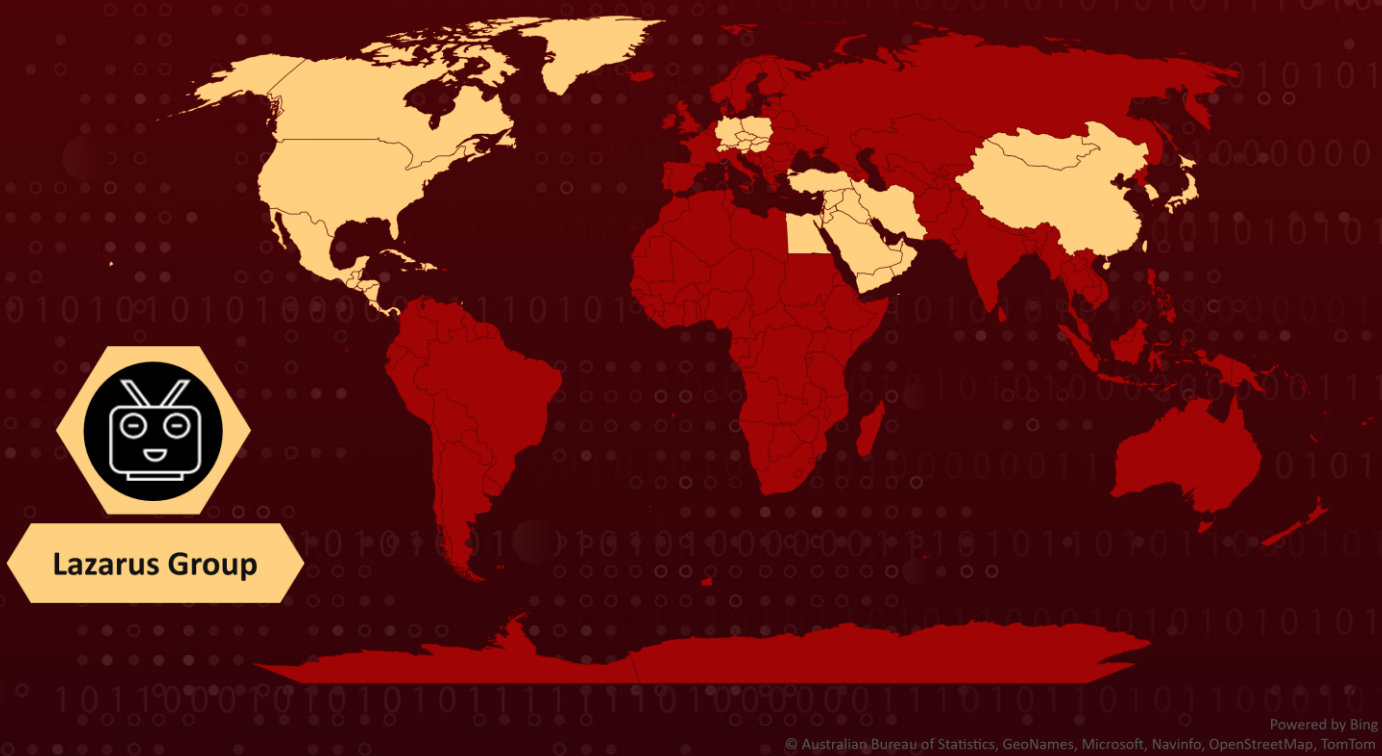
Lazarus Strikes with WinorDLL64 Backdoor Discovered in Wslink Malware loader

Date of Publication	Admiralty Code	TA Number
February 24, 2023	A3	TA2023102

Summary

Attack began: 2021
Threat Actor: Lazarus Group
Attack Region: Central Europe, North America, East Asia, and the Middle East.
Attack Sector: Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology, and BitCoin exchanges.
Attack: A newly discovered backdoor named WinorDLL64 seems to be associated with the malware downloader Wslink. This revelation suggests that Lazarus, the notorious North Korea-aligned group, may have employed this tool. WinorDLL64 enables the manipulation of various files, such as exfiltration, and deletion, as well as executing further commands.

Attack Regions



Attack Details

#1

In October 2021, Wslink was initially documented as a payload designed to facilitate file manipulation, code execution, and system information gathering, potentially for lateral movement. This payload has a particular interest in network sessions. The Wslink loader, which listens on a port specified in the configuration, can serve other connecting clients and even load different payloads. Recently, a new backdoor called WinorDLL64 has been found, which is linked to the Wslink malware downloader. Experts suggest that the Lazarus Group, a notorious North Korea-aligned organization, is likely behind this tool.

#2

The backdoor is a DLL that features a single unnamed export, which accepts one parameter. Messages communicated through WinorDLL64 are encrypted with 256-bit AES-CBC to ensure secure data exchange between the operator and the tool over an already-established connection. Furthermore, WinorDLL64 shares similarities in development environment, behavior, and code with various Lazarus samples found in Operation GhostSecret and the Bankshot implant.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0040 Impact	T1587 Develop Capabilities	T1587.001 Malware
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1106 Native API	T1134 Access Token Manipulation
T1134.002 Create Process with Token	T1070 Indicator Removal	T1070.004 File Deletion	T1087 Account Discovery
T1087.001 Local Account	T1087.002 Domain Account	T1083 File and Directory Discovery	T1135 Network Share Discovery
T1057 Process Discovery	T1012 Query Registry	T1082 System Information Discovery	T1614 System Location Discovery
T1614.001 System Language Discovery	T1016 System Network Configuration Discovery	T1049 System Network Connections Discovery	T1033 System Owner/User Discovery
T1560 Archive Collected Data	T1560.002 Archive via Library	T1005 Data from Local System	T1531 Account Access Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	13a44e5599c225d88d20398b4bec842a
SHA1	1BA443FDE984CEE85EBD4D4FA7EB1263A6F1257F
SHA-256	3bc8bbf4a1b3596e54e20609c398eab877c581ea369f6e1ef0ab0f9afe330d12

References

https://www.welivesecurity.com/2023/02/23/winordll64-backdoor-vast-lazarus-arsenal/

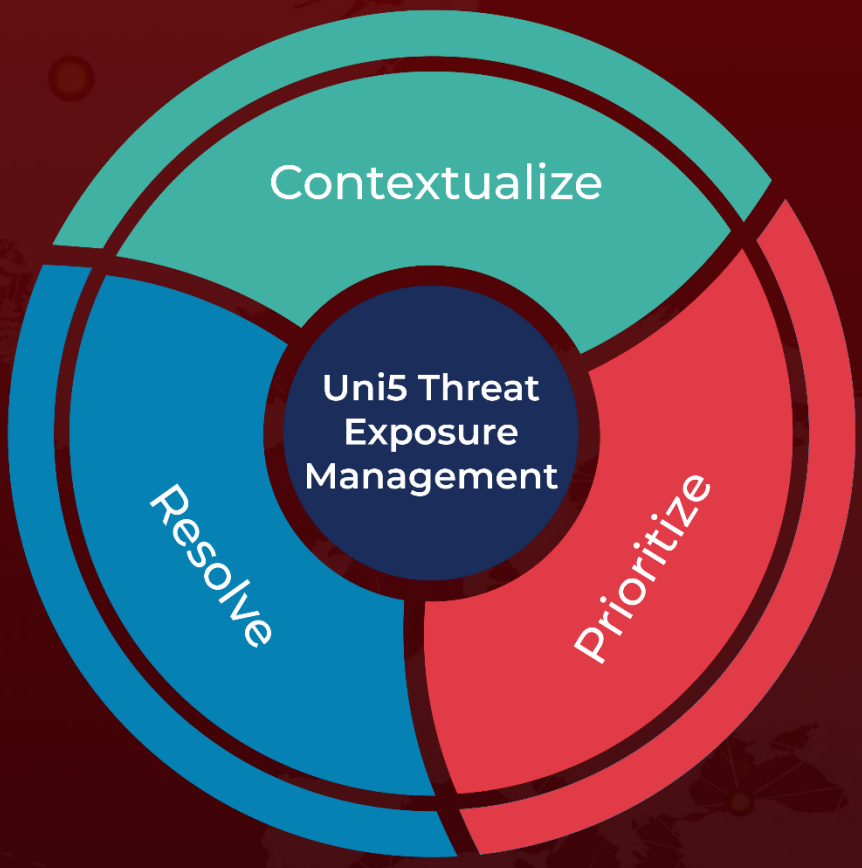
https://thehackernews.com/2023/02/lazarus-group-using-new-winordll64.html

https://attack.mitre.org/groups/G0032/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 24, 2023 • 2:00 AM

More at www.hivepro.com