

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

Lazarus Group's New Comebacker Variant Targets Aerospace & Defense

Date of Publication

November 14, 2025

Admiralty Code

A1

TA Number

TA2025348

Summary

First Seen: March 2025

Targeted Countries: Worldwide

Targeted Platform: Windows

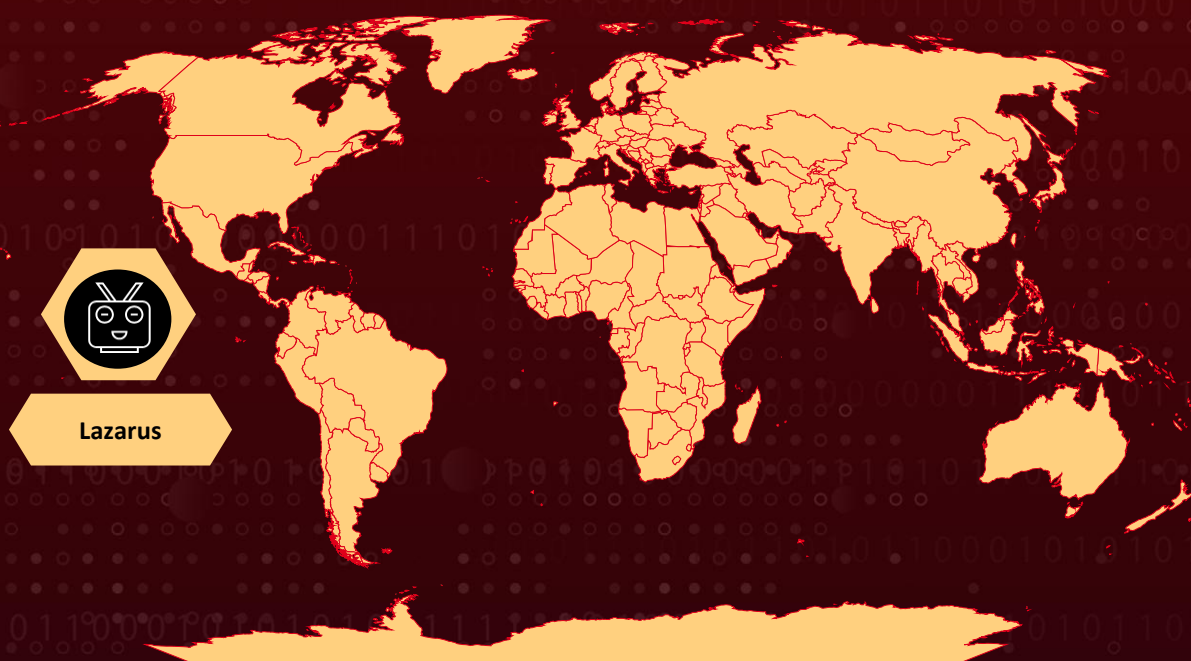
Targeted Industries: Aerospace, Defense, and Research

Threat Actor: Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces, G0032)

Malware: Comebacker

Attack: The latest Lazarus Group campaign targets aerospace and defense organizations using a malicious macro-enabled Word document that delivers an updated variant of the Comebacker backdoor. The attack employs a multi-stage infection chain, strong encryption, memory-resident payloads, and stealthy persistence techniques to evade detection. Command-and-control communication is routed through attacker-controlled domains disguised as legitimate services, reinforcing its espionage focus. This operation reflects continued technical refinement by Lazarus and poses a significant threat to organizations handling sensitive research, engineering data, and strategic information.

Attack Regions



Attack Details

#1

The Lazarus Group, a well-known advanced persistent threat (APT) actor linked to North Korea, has a long history of carrying out cyber-espionage and financially motivated attacks across multiple sectors. Over the years, the group has repeatedly targeted defense, aerospace, and high-technology organizations to obtain sensitive intellectual property and strategic intelligence. Their campaigns typically rely on well-crafted phishing lures, custom malware families, and layered evasion techniques, traits that also characterize the latest attack.

#2

In this newly identified operation, Lazarus deployed an updated variant of its longstanding Comebacker backdoor. The intrusion begins with a malicious Word document disguised as legitimate content related to aerospace and defense companies. When the victim enables macros, the embedded VBA code decrypts and deploys two additional components: a loader DLL and a decoy document that helps maintain the appearance of legitimacy. This marks the start of a multi-stage infection chain that is consistent with Lazarus's preference for stealthy, modular delivery.

#3

The loader places itself within a seemingly benign directory and establishes persistence using a shortcut in the Windows Startup folder. It then decrypts the final Comebacker payload using strong encryption algorithms such as ChaCha20 and executes it directly from memory to reduce forensic visibility. Once active, the backdoor communicates with attacker-controlled servers over HTTPS, encrypting all traffic with AES before transmission. These measures help conceal command-and-control activity from standard network monitoring tools.

#4

The upgraded Comebacker backdoor provides attackers with capabilities typical of an espionage-focused toolset: system reconnaissance, execution of remote commands, and the ability to download or upload additional files. The infrastructure supporting the operation includes multiple domains designed to mimic legitimate services, further complicating detection. The overall toolset and delivery method align closely with [Lazarus's](#) prior campaigns but demonstrate incremental improvements in obfuscation and operational security. This campaign underscores the persistent and evolving threat that the Lazarus Group poses to aerospace and defense organizations worldwide.

Recommendations



Strengthen Email & Document Security: Block or quarantine macro-enabled Office documents from external senders. Enable Microsoft Office's "Block macros from the internet" policy across all endpoints. Use advanced email security filters to detect spoofed domains, malicious attachments, and targeted phishing content.



Harden Endpoint Protection: Deploy an EDR/XDR platform capable of detecting rundll32-based execution, in-memory payload loading, and other DLL side-loading behavior used by the Comebacker loader. Enable AMSI (Antimalware Scan Interface) and real-time scanning for suspicious macro activity. Restrict write permissions to sensitive directories like ProgramData and require admin privileges for DLL deployments.



Improve Network Monitoring & Threat Detection: Monitor outbound HTTPS connections for unusual destinations, especially to newly registered or low-reputation domains. Use TLS inspection (where appropriate) to analyze encrypted traffic patterns; watch for consistent beaconing intervals or abnormal authentication failures. Implement DNS filtering to block access to known malicious domains and prevent communication with attacker-controlled C2 servers.



Enhance System Hardening & Access Controls: Apply the principle of least privilege: limit the ability of users to install or execute unsigned software. Enforce strong endpoint isolation for sensitive roles, such as defense engineering teams. Enable Windows Exploit Guard policies to block suspicious script execution and DLL run behaviors.



Potential **MITRE ATT&CK** TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control
TA0003 Persistence	TA0005 Defense Evasion	T1071 Application Layer Protocol	T1071.001 Web Protocols



<u>T1574</u> Hijack Execution Flow	<u>T1574.002</u> DLL	<u>T1573</u> Encrypted Channel	<u>T1573.001</u> Symmetric Cryptography
<u>T1583</u> Acquire Infrastructure	<u>T1583.001</u> Domains	<u>T1566.001</u> Spearphishing Attachment	<u>T1566</u> Phishing
<u>T1204</u> User Execution	<u>T1204.005</u> Malicious Library	<u>T1059.001</u> PowerShell	<u>T1059</u> Command and Scripting Interpreter
<u>T1204.002</u> Malicious File	<u>T1059.003</u> Windows Command Shell	<u>T1059.005</u> Visual Basic	<u>T1547.001</u> Registry Run Keys / Startup Folder
<u>T1547</u> Boot or Logon Autostart Execution	<u>T1547.009</u> Shortcut Modification	<u>T1140</u> Deobfuscate/Decode Files or Information	<u>T1027</u> Obfuscated Files or Information
<u>T1027.013</u> Encrypted/Encoded File	<u>T1027.015</u> Compression	<u>T1218.011</u> Rundll32	<u>T1132</u> Data Encoding
<u>T1218</u> System Binary Proxy Execution	<u>T1620</u> Reflective Code Loading	<u>T1102</u> Web Service	<u>T1132.001</u> Standard Encoding

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	126961b8c9a7a0e78899943f6c2a7ce9, c014a2ac8c89abc3799a520da331caf5, d90aeea054ae8cfbd6fca2bd1588a852, e4541d91fca9df943b6e119dc1c6cd7f, f5475608c0126582081e29927424f338
SHA1	1bfc157677167c4d5498a0821f3d40691f1e137, 6c6419ee544e78448d0641f88ebd3ea2279f4f66, 701296f6ff0daf3264dd8814c469b2c7f56df1ec, 8e88fd82378794a17a4211fbf2ee2506b9636b02, a0e0a94417e9c594c5c68a6c815160c8b6a980ae

TYPE	VALUE
SHA256	046caa2db6cd14509741890e971ddc8c64ef4cc0e369bd5ba039c40c907d1a1f, 14213c013d79ea4bc8309f730e26d52ff23c10654197b8d2d10c82bbbcd88382, 7e61c884ce5207839e0df7a22f08f0ab7d483bfa1828090aa260a2f14a0c942c, 96b973e577458e5b912715171070c0a0171a3e02154eff487a2dcea4da9fb149, a75886b016d84c3eaacaf01a3c61e04953a7a3adf38acf77a4a2e3a8f544f855, ad9c5aca9977d04c73be579199a827049b6dd9840091ffe8e23acc05e1d4a657, b357b3882cf8107b1cb59015c4be3e0b8b4de80fd7b80ce3cd05081cd3f6a8ff, b7d625679fbcc86510119920ffdd6d21005427bf49c015697c69ae1ee27e6bab, c4a5179a42d9ff2774f7f1f937086c88c4bc7c098963b82cc28a2d41c4449f9e, f2b3867aa06fb38d1505b3c2b9e523d83f906995dcdd1bb384a1087b385bfc50
URLs	hxxp[:]//birancearea[.]com/adminv2, hxxp[:]//hiremployee[.]com,
Domains	birancearea[.]com, hiremployee[.]com, office-theme[.]com

References

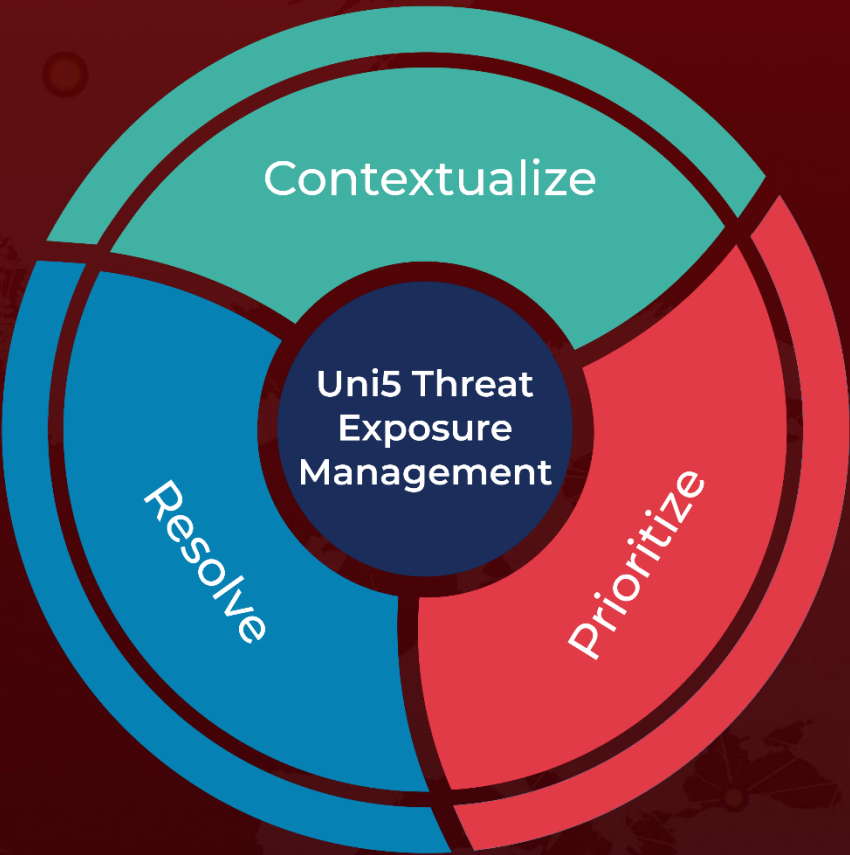
<https://www.enki.co.kr/en/media-center/blog/lazarus-group-targets-aerospace-and-defense-with-new-comebacker-variant>

<https://hivepro.com/threat-advisory/lazarus-targets-europes-uav-innovation/>

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

November 14, 2025 • 9:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com