Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

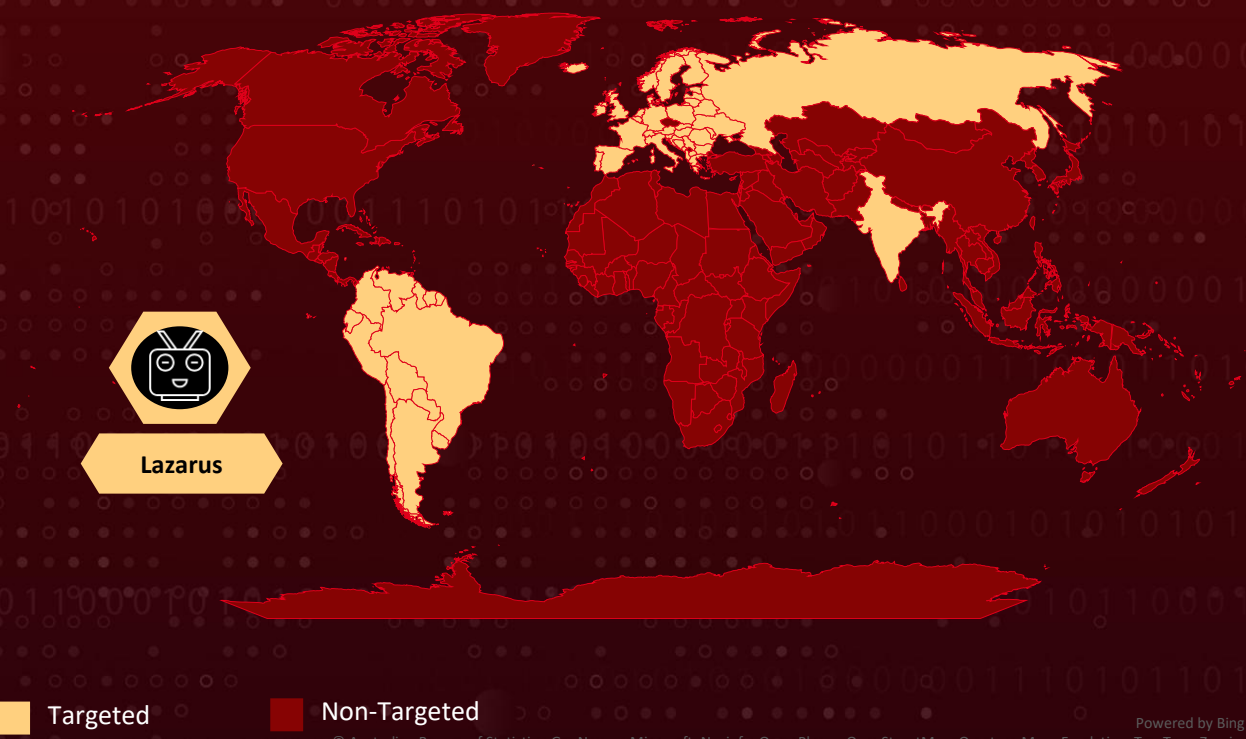
Operation Dream Job: Lazarus Exploits a Windows Zero-Day to Deploy Backdoor

Date of Publication	Admiralty Code	TA Number
August 13, 2026	A1	TA2026231

Summary

First Seen: Early July 2026
Campaign: Operation Dream Job
Targeted Regions: Europe (France, Germany), India, and South America (Brazil)
Targeted Products: Microsoft Windows, Roundcube Webmail
Targeted Industries: Defense, Aerospace, and Aviation
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: Troy, FudModule, RelayShell, MISTPEN, ForestTiger
Attack: Lazarus revived its long-running Operation Dream Job campaign, luring defense and aerospace staff with fake recruiter job offers that delivered malicious PDFs or a trojanized PDF viewer. The intrusions chained an in-memory downloader (MISTPEN), a new backdoor (Troy), and an implant (ForestTiger) with a Windows zero-day, CVE-2026-68820 in AFD.sys, to gain SYSTEM privileges and load the FudModule 3.1 kernel rootkit. To stay hidden, the group routed command-and-control through legitimate cloud services and compromised WordPress, SharePoint, and Roundcube servers, exploiting the older CVE-2025-49113 to plant the RelayShell web shell.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-68820	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-49113	RoundCube Webmail Deserialization of Untrusted Data Vulnerability	Roundcube Webmail	✗	✓	✓

Attack Details

#1

Lazarus has been exploiting a Windows zero-day vulnerability (CVE-2026-68820) as part of its long-running Operation Dream Job campaign, and each intrusion opened with a recruitment lure. Posing as recruiters for well-known defense and technology firms, the group approached targets, most likely over LinkedIn or messaging apps, and steered them toward downloading malicious files. Two delivery paths ran in parallel. In the first, the victim received an encrypted ZIP holding a legitimately signed PDF viewer, a malicious DLL, and an encrypted payload disguised as a PDF; launching the viewer side-loaded the rogue libmupdf.dll, which showed a convincing decoy job description while quietly unpacking and running code in memory. In the second, victims were told to install "SecurityPDF," a trojanized open-source PDF viewer offered through at least three fake Enveil websites that ranked highly in search results, and opening a specially prepared PDF through it triggered a hidden payload.

#2

Once running, the first chain loaded MISTPEN, an in-memory downloader that profiled the machine and pulled additional modules for host and process reconnaissance, screenshot capture, and privilege escalation. MISTPEN reached its operators through legitimate cloud services, using the Microsoft Graph API and OneDrive to blend in with normal traffic. Its privilege-escalation loader negotiated a session key using the ML-KEM post-quantum algorithm, then used that key to decrypt and run FudModule 3.1, Lazarus's kernel-mode rootkit. The second chain instead decrypted and loaded the Troy backdoor directly into memory, handing operators remote control through 17 commands covering reconnaissance, file upload and download, archiving and exfiltration, hidden shell execution, process termination, in-memory DLL injection, and changes to beacon timing.

#3

To gain SYSTEM privileges, the attackers exploited CVE-2026-68820, a use-after-free flaw in the Windows AFD.sys WinSock driver that had not yet been patched when the campaign began in early July. With SYSTEM access, FudModule 3.1 worked to blind defenders by disabling EDR telemetry, interfering with security products, and, in a new twist, tampering with Windows Smart App Control by resetting its policy state and forcing an in-place reload of the code-integrity policy from within a SYSTEM-level msiexec.exe process. The rootkit also injected a fresh copy of MISTPEN into a SYSTEM process so the implant could run with elevated rights and out of sight of monitoring tools.

#4

Rather than build its own servers, Lazarus hid inside trusted infrastructure. The group hijacked legitimate but compromised WordPress and SharePoint sites and Roundcube webmail servers to relay command-and-control traffic for ForestTiger, its remote-access implant. Many of those Roundcube servers still ran versions vulnerable to CVE-2025-49113, so the attackers likely authenticated with stolen credentials and then exploited the PHP object-deserialization flaw to plant RelayShell, a previously undocumented web shell that exchanges commands and results as text files. In at least one case a compromised France-based organization was used to send spear-phishing to fresh targets, letting the messages slip past reputation-based filters. Data collected on victim hosts was staged, archived, and exfiltrated over these blended channels.

Recommendations

Patch the Windows AFD.sys Zero-Day (CVE-2026-68820): Apply Microsoft's August Patch Tuesday update across all Windows 10, Windows 11 (including builds 26100 and 26200), and Windows Server systems without delay, prioritizing internet-exposed and privileged hosts.

Update Roundcube Webmail (CVE-2025-49113): Upgrade any Roundcube instance to version 1.5.10 or 1.6.11 or later, and audit self-hosted webmail for the RelayShell web shell and unexpected text-file command artifacts.

Hunt for the Trojanized PDF Viewer: Search endpoints for the SecurityPDF application and for PDF documents containing the marker string "This document is encrypted with sumatrapdf reader!!!!!!!!!!!", which triggers execution of the embedded payload.

Watch Cloud Services Used as C2: Monitor for anomalous Microsoft Graph API and OneDrive activity from endpoints that have no business reason to call them, a technique MISTPEN uses to hide command-and-control.

Verify Software Through Official Channels: Instruct staff to install applications only from vendor-verified sources rather than search-result links, since the attackers deliberately rank fake vendor sites highly to appear legitimate.

Strengthen Recruitment-Themed Phishing Awareness: Train employees in sensitive roles to treat unsolicited recruiter outreach and job-offer attachments with caution, especially requests to download a viewer or open an "encrypted" document.

Rotate Credentials and Enforce MFA on Webmail: Reset credentials for any exposed Roundcube or webmail accounts and require phishing-resistant MFA to counter the stolen-credential access observed in this campaign.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.004: Server
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.006: SEO Poisoning
	T1586: Compromise Accounts	T1586.002: Email Accounts
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
		T1566.001: Spearphishing Attachment
	T1190: Exploit Public-Facing Application	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1505: Server Software Component	T1505.003: Web Shell
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1014: Rootkit	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection

Tactic	Technique	Sub-technique
Defense Evasion	T1684: Social Engineering	T1684.001: Impersonation
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1070: Indicator Removal	T1070.004: File Deletion
Credential Access	T1078: Valid Accounts	
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
Collection	T1113: Screen Capture	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2b4987c07a3d9a9a5d1a9bf4efa3d1903e775090b611710edafdc92874265ca8, 3a02d0d798e8d35555776886d92b20ff38a101c9ef7e0eebc8ce5d259516525a, 92106b0c62a0a42678232f8273f030b2d3c8e92efce81b98b9eec70cfe98afa1, 396192d92d17ace1a521f1351eeeba2825e60badd0d799cc5c338e4934b3c82c, f7e620134ca935067797ab957317b346ce0df84a4e9b9ca54a6acc9b75afda4d, 75b93a7103b0562f6497d30052c0c5cf7aa58c1bf0e9297022b74469a7f096f1, a45144d22cac70a45d71cf4dffa4efbc373658779a56cf1300d6ac863d6cc7e2, 1de949c71efcfb0ffc41f33d38833dbc4b082075b1a540fc68c18c535d7ad86c, 4c9b804d6155b29f1e27a9ffe531e10bc42a7bdab42f905b50146bf2026768d9, 29e24c007549e51319ff3aee011da6f9f93568e8c85a5ad69c9e53bd3f4533a2, 4ebdce2f47c23ff8c9e8e80c8b5239c7a5764da31cd3ab8f0505926890adc105, c2aa28bb5e2a749c693712008276f311edd912f689371ef9e8a1ee5fb4167461, 2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87bd7232e141eb, 5278ee922838352f1480a73e971161017d643a80b7ec22bf725897dfd088696d, b4082d21070d9ddf53fde4ea22524d09e41ec9826ce63cef3c6235e458d21afb, fb3fc5626f68677fb1269a2fefbe70e719211b4065e836ab92e06a8210139a2d, ea7056f2bf36c66a61ff787ff5be975a85f534c3c5ca178791dac2504db2c619, 13d10bc99f7f7abe7ee0902be87920b73b2ea41bd9683dbfcad340dacbcdef79, 4fd32432341dfcf54d0517a6bbc38e5d265be70933493e4183c2a340cdde9a2d, 4dd792c9f672bbdcc8d363d745994efe90f4ffc5fdc2c059c8e379a48ad6a68a, ba96c603e44046de703c67b2c3b7e4ca974afef7b437a0244418bc4edc781bb7,

TYPE	VALUE
SHA256	72dccae85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289, 231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858, 6da9b1e6f3315ceb77dd14a937a26cc3602bf6a7e2c2ecafb3c65ce5319837be, a0578a2b7821d7e2c573530648f26d7a0d98b373ab24fb7f0c792736761e542d, 82268052f94df6f4870d02e57b18d4c54136cc7a8c8d80ad162631f99462c943, 3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8347b2637c245d, a673ae661593c0de9bbb815593b816a6853dad6d55ad5042d2ef1875cd13d6e7, 8ce6c29f92dc45b1474417cbdff4ed0c18e58fa63e3a071ee9f85aa9d2aac07c, acb97cec84e08b89f41967a24e965d1fd2c51751cef158f7aa35bb4306b87b97, 3601060c62edeeaa49def6a13be6e126e1024ce011faad4e2d9f585ccf6bd5a6, fecf1208884380121589844 2bd1ff3e266f29d14e29a94780e857f69c4915d6b, d578c28c9afe7457a0d81f6701332ef8197e8f7468de654935fb29a50ea66459, 743172aab606974b054a64561534ae66baa3a840657f79d7c6fa18350e8d45d1, db3d69b7eeda2e35e23006bf4b7e206281fce809584207214fc213f9bc30376d, 590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6d115e1615d6, 68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac933030a68faac0bb, a738059ce07c951c31ab2da3d93d8f69bff32f9b7d933dbf5943441b9cc99075, 21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21eb47c9e22762, Cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e132963d2e222
Domains	envell[.]xyz, enveil[.]online, uxtramine[.]org
IPv4	135[.]181[.]67[.]203, 135[.]181[.]185[.]158

Patch Links

CVE-2026-68820
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

CVE-2025-49113
https://github.com/roundcube/roundcubemail/releases

References

https://research.checkpoint.com/2026/shattering-the-dream-when-a-job-offer-becomes-a-zero-day-attack/

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

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 Demo of **HivePro**.

REPORT GENERATED ON

August 13, 2026 • 08:30 AM

More at www.hivepro.com