Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

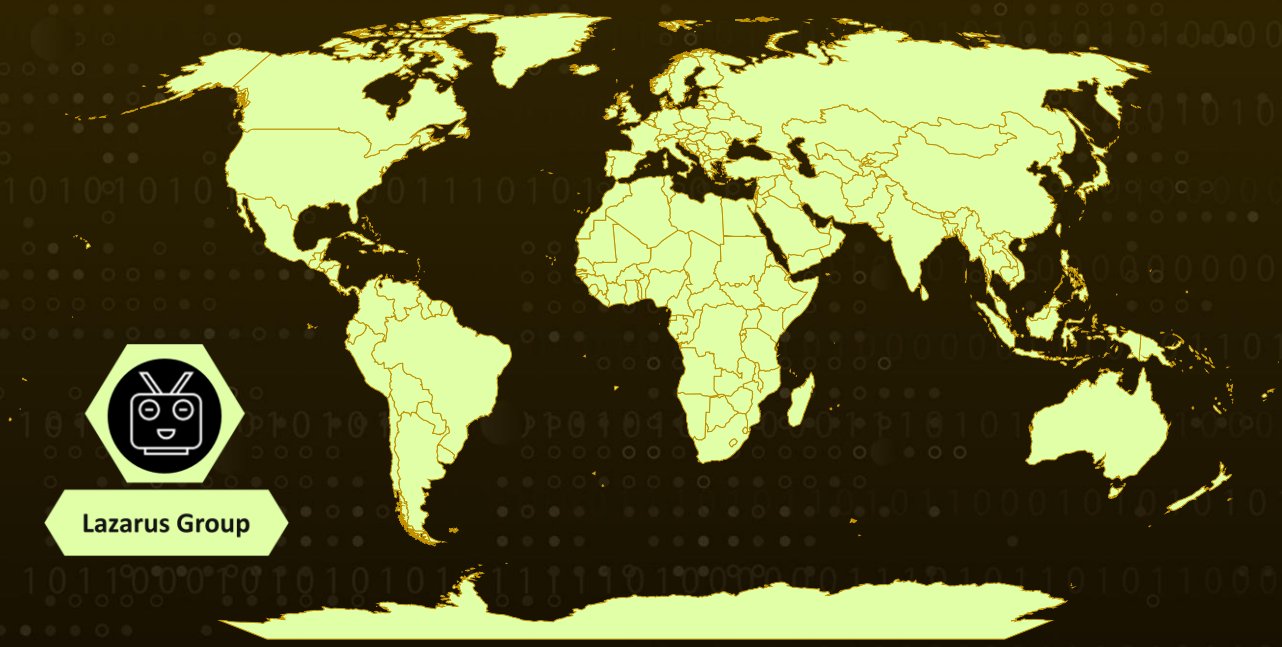
ClickFake Interview: Lazarus Group's New Crypto Heist via Fake Job Offers

Date of Publication	Admiralty Code	TA Number
April 4, 2025	A1	TA2025101

Summary

Attack Discovered: February 2025
Targeted Countries: Worldwide
Targeted Industry: Cryptocurrency, centralized finance (CeFi)
Affected Platforms: Windows, macOS
Malware: GolangGhost, FrostyFerret
Actor: Lazarus Group (aka UNC2970, 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, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)
Campaign: ClickFake Interview
Attack: The Lazarus Group has launched ClickFake Interview, a new campaign targeting job seekers in the cryptocurrency sector, particularly centralized finance (CeFi). Using fake job interview websites, attackers deploy malware through a deceptive technique called ClickFix, tricking victims into installing backdoors on Windows and macOS. The GolangGhost backdoor serves as the final implant, granting remote access and enabling attackers to steal browser data, credentials, and cryptocurrency wallets.

Attack Regions



Attack Details

#1 The Lazarus Group, a North Korean state-sponsored hacking collective, has been conducting cyberattacks for espionage and financial gain since 2009. Initially targeting the defense and government sectors, its tactics have evolved to focus on cryptocurrency firms, generating illicit revenue for the regime. Its latest operation, ClickFake Interview, underscores its ability to adapt and refine deception strategies.

#2 Uncovered in February 2025, ClickFake Interview has targeted software developers through fake job interviews. Since November 2023, Lazarus has expanded its operations to macOS, using a new technique called ClickFix, which tricks victims into manually executing malicious commands disguised as system fixes.

#3 In ClickFake Interview, the attack begins with fraudulent job invitations on social media, leading victims to a fake interview website built with ReactJS. The process appears legitimate, requiring candidates to answer questions and submit an introductory video. However, in the final stage, victims are prompted to enable their camera, triggering an error message that instructs them to download a driver an elaborate trap.

#4 Windows users unknowingly execute a VBS script, while macOS users run a Bash script, both resulting in the installation of GolangGhost, a stealthy Go-based backdoor that steals credentials, browser data, and cryptocurrency wallets. Notably, on macOS, a stealer dubbed FrostyFerret is executed to retrieve the user's system password. Despite platform-specific variations, both attack paths ultimately lead to the persistent installation of a Go-based implant on the compromised host.

#5 A detailed analysis of 184 fake job websites suggests that Lazarus is shifting its focus from decentralized finance (DeFi) platforms to centralized finance (CeFi) platforms, which act as intermediaries managing large cryptocurrency reserves, making them prime targets. Unlike previous Lazarus campaign, **Contagious Interview**, primarily targeted software developers by luring victims into downloading a malicious project embedded with BeaverTail, an infostealer that delivers a secondary payload, InvisibleFerret, to establish remote access, this operation is aimed at business managers, asset managers, and product developers.

#6 This shift indicates a tactical move toward less technical victims who may be less vigilant against security threats. The ClickFake Interview campaign builds on previous operations like Contagious Interview, introducing advanced evasion strategies and a broader victim profile. It is evident that Lazarus remains highly active, using social engineering to infiltrate the cryptocurrency sector and finance North Korea’s cyber warfare efforts.

Recommendations

- **Be Careful with Job Offers and Recruiters:** Always verify job offers by checking the company's official website or contacting them directly. If you get a job offer from someone you don't know, especially on social media, be cautious it could be a scam.
- **Watch Out for Suspicious Interview Requests:** If you're asked to download unknown software or "drivers" during an interview, it's a red flag. Legitimate companies won't ask you to install special tools just to join a video call.
- **Boost Your Device Security and Monitor Your Network:** On macOS, disable Terminal auto-execution and avoid running unverified scripts. On Windows, enable script-blocking policies to prevent harmful VBS files from running. Keep an eye on network activity watch for unusual connections, especially those linked to cryptocurrency transactions. Use network segmentation to limit the spread of threats if an attacker gains access.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1204 User Execution	T1204.001 Malicious Link
T1555 Credentials from Password Stores	T1555.001 Keychain	T1059 Command and Scripting Interpreter	T1059.007 JavaScript

T1059.005 Visual Basic	**T1059.004** Unix Shell	**T1059.003** Windows Command Shell	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1217** Browser Information Discovery	**T1071** Application Layer Protocol	**T1036** Masquerading
T1027 Obfuscated Files or Information	**T1560** Archive Collected Data	**T1041** Exfiltration Over C2 Channel	**T1567** Exfiltration Over Web Service
T1567.002 Exfiltration to Cloud Storage	**T1082** System Information Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	vid-crypto-assess[.]com, assessiohq[.]com, blockassess[.]com, blockchainjobassessment[.]com, blockchainjobhub[.]com, candidateinsightinfo[.]com, coinbase-walet[.]biz, coinbase-walet[.]me, competency-core[.]com, devchallengehq[.]com, evalassesso[.]com, evalswift[.]com, quickskill-review[.]com, jobinterview360[.]com, livehirehub[.]com, talenthiring360[.]com, quickassessio[.]com, quickhire360[.]com, quickinterview360[.]com, eskillprof[.]com, evalvidz[.]com, intervwolf[.]com, vidcruiterinterview[.]com, vidcruitermaster[.]com, vidintermaster[.]com, skillhiretrack[.]com, skillprooflab[.]com,

TYPE	VALUE
Domains	talentcheck[.]pro, talentsnaptest[.]com, talentview360[.]com, test-wolf[.]com, toptalentassess[.]com, ugethired360[.]com, vidassess360[.]com, vidassesspro[.]com, videorecruitpro[.]com, vidhirehub[.]com, zenspiretech[.]com
Hostname	api[.]camdriverhub[.]cloud, api[.]camdrivers[.]cloud, api[.]camdriverstore[.]cloud, api[.]drivercamhub[.]cloud, api[.]driversnap[.]cloud, api[.]driverstream[.]cloud, api[.]provideodrivers[.]cloud, api[.]smartdriverfix[.]cloud, api[.]vcamdriverupdate[.]cloud, api[.]videocarddrivers[.]cloud, api[.]videodriverzone[.]cloud, api[.]videotechdrivers[.]cloud, api[.]vidtechhub[.]cloud, api[.]webcamdrivers[.]cloud, api[.]webcamwizard[.]cloud, api[.]camdriversupport[.]com, api[.]camera-drive[.]org, api[.]camtechdrivers[.]com, api[.]drivercams[.]cloud, api[.]drive-release[.]cloud, api[.]nvidia-drive[.]cloud, api[.]nvidia-release[.]org, api[.]nvidia-release[.]us, api[.]smartdriverfix[.]cloud, api[.]web-cam[.]cloud
URLs	hxxp[:]//38[.]134[.]148[.]218[:]8080, hxxp[:]//154[.]62[.]226[.]22[:]8080, hxxp[:]//72[.]5[.]42[.]93[:]8080

TYPE	VALUE
SHA256	e88700d069a856e1a16c0da317a6f18fa626dd2d46dcbee1a7403d2e2d9ed097, bfac94bfb53b4c0ac346706b06296353462a26fa3bb09fbfc99e3ca090ec127e, 887189269c3594e1a851eb22f7c174a7c28618114b7dbaab6b645f34bd809f5a, e88700d069a856e1a16c0da317a6f18fa626dd2d46dcbee1a7403d2e2d9ed097, 6289ef57b1772d78da0e54ba4730b6fc79f5ec1620ff63c3abaebea70190eba9, 0cbbf7b2b15b561d47e927c37f6e9339fe418badf49fa5f6fc5c49f0dc981100, ef9f49f14149bed09ca9f590d33e07f3a749e1971a31cb19a035da8d84f97aa0, 3fec701b5e8486081c7062590f4ff947fcf51246cb067f951e90eb43dad930b4, f4b4411e403dd5094eef9c8946522fc9a99cf1676c8de5926b3c343264b126e6, d00ca82a32b5e8063492f27dfec225b0888cd6135db3e2af65be3782bbfa16e5, 6e186ada6371f5b970b25c78f38511af8d10faaeaed61042271892a327099925, ba81429101a558418c80857781099e299c351b09c8c8ad47df2494634a5332dc, b7b9e7637a42b5db746f1876a2ecb19330403ecb4ec6f5575db4d94df8ec79e8, a803c043e12a5dac467fae092b75aa08b461b8e9dd4c769cea375ff87287a361, e52118fc7fc9b14e5a8d9f61dfae8b140488ae6ec6f01f41d9e16782febad5f2

References

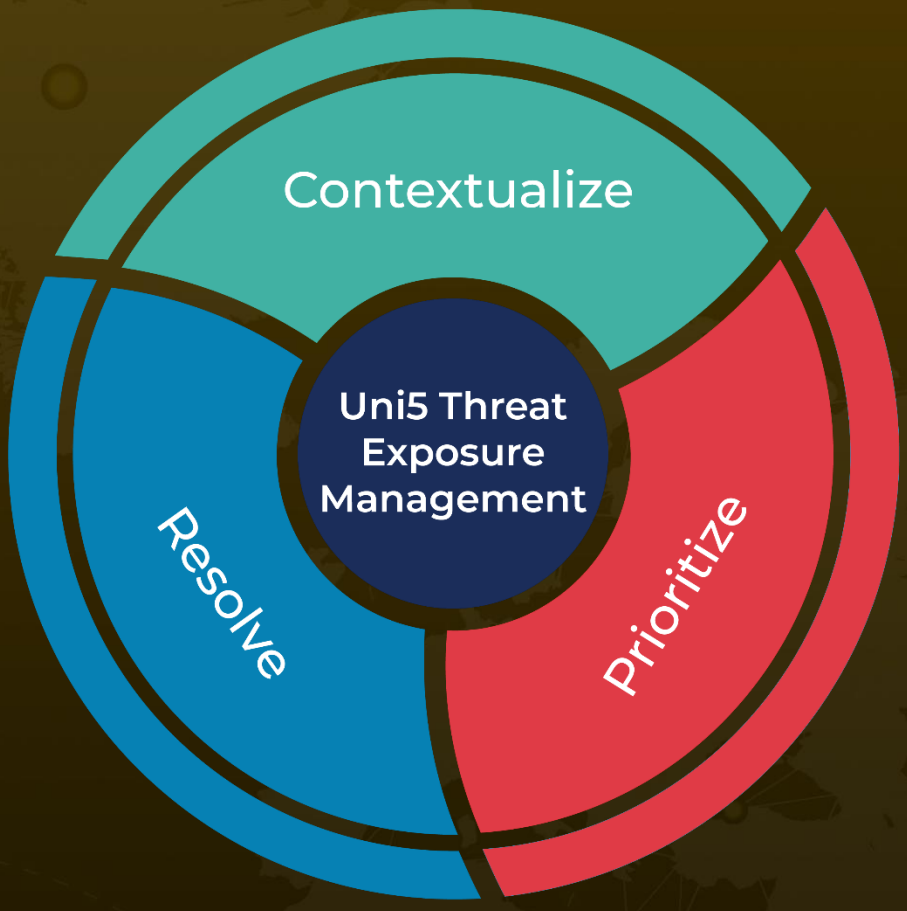
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/

https://hivepro.com/threat-advisory/contagious-interview-targets-macos-with-flexibleferret-malware/

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

April 4, 2025 • 5:10 AM

More at www.hivepro.com