Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

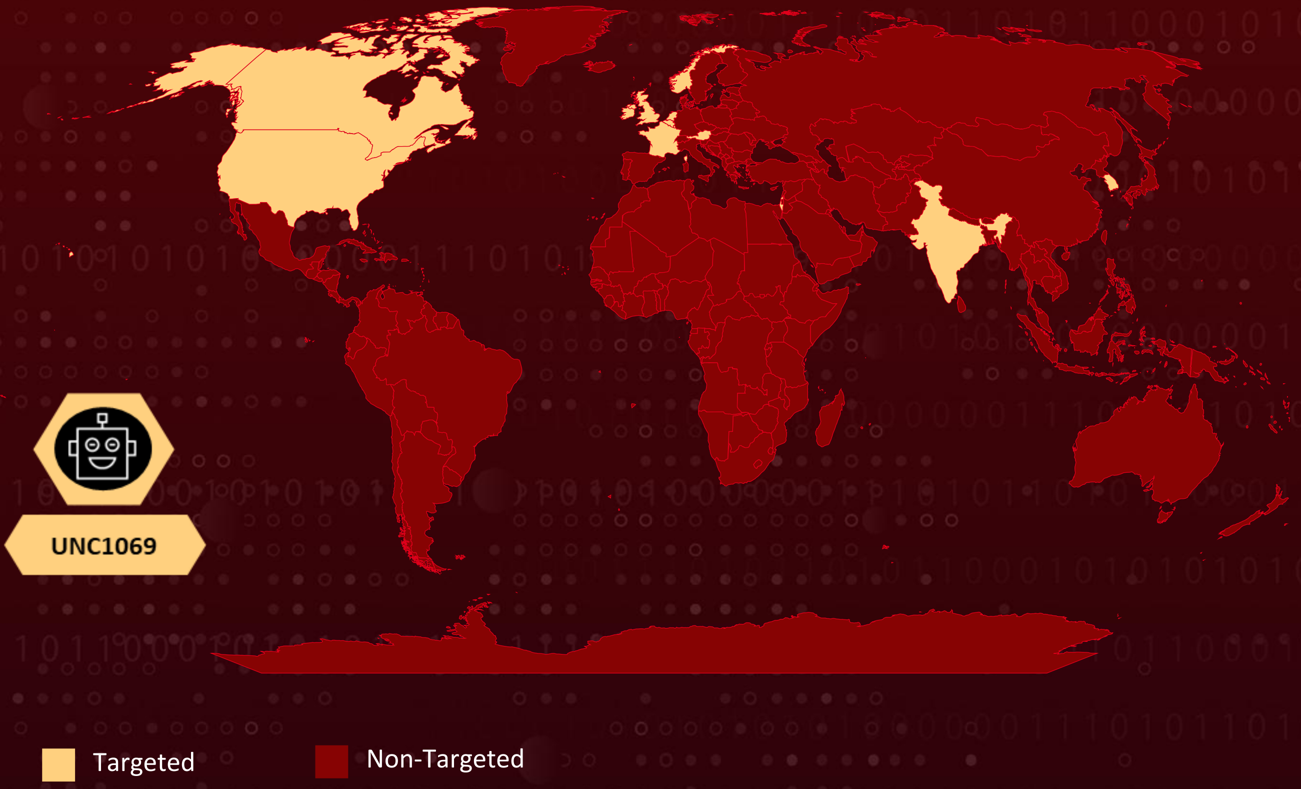
UNC1069's Social Engineering Operations Focused on Crypto Sector

Date of Publication	Admiralty Code	TA Number
February 17, 2026	A1	TA2026046

Summary

First Seen: 2018
Threat Actor: UNC1069 (alias CryptoCore, MASAN)
Targeted Regions: United States, Canada, Norway, Austria, Netherlands, United Kingdom, France, Belgium, Ireland, Luxembourg, Monaco, South Korea, India, Israel, Hong Kong
Targeted Products: macOS, Windows, Telegram, Chromium-Based Browsers (Google Chrome, Brave, Microsoft Edge), Zoom
Targeted Industries: Cryptocurrency, FinTech, Financial Services, High Tech, Manufacturing, Transportation
Malware: WAVESHAPER, SUGARLOADER, SILENCELIFT, HYPERCALL, DEEPBREATH, CHROMEPUSH
Attack: UNC1069, a financially motivated North Korea-linked threat actor, conducted a targeted intrusion against a financial technology (FinTech) entity in the cryptocurrency sector. The attack leveraged a compromised Telegram account, a spoofed Zoom meeting featuring AI-generated deepfake video, and a ClickFix infection vector to trick the victim into executing malicious commands. The intrusion resulted in the deployment of seven distinct malware families designed to harvest credentials, browser data, messaging content, and session tokens, facilitating cryptocurrency theft.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1

The North Korea-linked actor UNC1069 targeted cryptocurrency employees to obtain system access and steal funds. Contact began through Telegram using a hijacked executive account. After a brief rapport, the victim received a scheduling link from Calendly that led to a counterfeit Zoom meeting page hosted by the attacker. A fabricated video of a cryptocurrency CEO reinforced legitimacy. The group relied on generative-AI tools to prepare scripts, visuals, and operational research for the deception.

#2

During the call, the attacker staged audio problems and guided the victim through troubleshooting commands. These commands executed malicious instructions: macOS fetched a payload through shell piping, while Windows used mshta to run the same file. An immediate AppleScript event marked the infection chain and deployed WAVESHAPER, a macOS C++ backdoor. It collected host identifiers, hardware details, and running processes, and transmitted them to command servers.

#3

WAVESHAPER installed HYPERCALL, a Go downloader that retrieved additional malware. Three components followed. HIDDENCALL enabled direct remote control. SUGARLOADER established persistence through a launch daemon. SILENCELIFT transmitted system status and could disrupt Telegram communications when run with root privileges.

#4

Data theft relied on two miners. DEEPBREATH bypassed macOS privacy controls by abusing full disk permissions from Apple Finder access. It extracted Keychain credentials, browser data from Google Chrome, Brave Software Brave, and Microsoft Edge, plus Telegram files and Apple Notes databases. The data was compressed and exfiltrated to a remote server.

#5

CHROMEPUSH, delivered by SUGARLOADER, posed as a Google Docs offline extension and persisted as a browser messaging host. It logged keystrokes, captured credentials, extracted cookies, and uploaded the information to the attacker's infrastructure.

Recommendations

Restrict Unsigned Script Execution on macOS: Configure macOS systems to prevent unauthorized AppleScript and shell script execution. Enforce Gatekeeper policies and restrict curl-to-shell piping through endpoint security policies.

Audit macOS Launch Daemons and Agents: Regularly inspect /Library/LaunchDaemons/ and /Library/LaunchAgents/ directories for unauthorized plist files, particularly those mimicking Apple naming conventions such as com.apple.system.updater.plist.

Monitor TCC Database Integrity: Implement monitoring for unauthorized modifications to the macOS TCC database (TCC.db). Alert on any process that stages, copies, or modifies the TCC folder or database outside of normal user consent workflows.

Inspect Chrome Native Messaging Hosts: Audit NativeMessagingHosts directories under Google Chrome, Brave, and other Chromium-based browser application support paths for unauthorized extensions or manifest files, such as com.google.docs.offline.json.

Enforce Meeting Link Verification Policies: Educate employees to verify meeting links received via messaging platforms, particularly Telegram. Establish organizational procedures to confirm meeting invitations through secondary communication channels before clicking links.

Monitor for Anomalous Curl and WebSocket Activity: Implement detection rules for curl commands with suspicious user agents (e.g., "audio"), curl-to-shell piping, and WebSocket connections to unknown domains on TCP port 443.

Reset Credentials and Session Tokens Post-Incident: If compromise is suspected, immediately reset all iCloud Keychain credentials, browser-stored passwords, Telegram session data, and Apple Notes data on affected systems. Revoke and rotate all cryptocurrency wallet keys and API tokens.

Enable XProtect Behavioral Service Monitoring: Leverage macOS XProtect Behavioral Service (XBS) detections by monitoring the XPdb SQLite database at /var/protected/xprotect/XPdb for behavioral violations that may indicate malware execution.

Restrict mshta Execution on Windows: Block or monitor mshta.exe execution through application control policies, as UNC1069 uses this Living-off-the-Land Binary (LOLBin) as part of the Windows infection chain.

Strengthen Anti-Deepfake Awareness Training: Conduct targeted security awareness training focused on AI-generated deepfake video and audio used in social engineering attacks, particularly for employees in cryptocurrency, finance, and venture capital roles.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
		T1566.004: Spearphishing Voice
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.002: AppleScript
	T1218: System Binary Proxy Execution	T1218.005: Mshta
Persistence	T1543: Create or Modify System Process	T1543.004: Launch Daemon
	T1176: Browser Extensions	
Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
	T1620: Reflective Code Loading	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Credential Access	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1056: Input Capture	T1056.001: Keylogging
Collection	T1005: Data from Local System	
	T1185: Browser Session Hijacking	
	T1074: Data Staged	T1074.001: Local Data Staging
Exfiltration	T1041: Exfiltration Over C2 Channel	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1102: Web Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	mylingocoin[.]com, zoom[.]uswe05[.]us, breakdream[.]com, dreamdie[.]com, support-zoom[.]us, supportzm[.]com, zmsupport[.]com, cmailer[.]pro
URLs	hxxp[:]//mylingocoin[.]com/audio/fix/6454694440, hxxp[:]//cmailer[.]pro[:]80/upload
SHA256	b452C2da7c012eda25a1403b3313444b5eb7C2c3e25eee489f1bd256f8434735, 1a30d6cdb0b98feed62563be8050db55ae0156ed437701d36a7b46aabf086ede, b525837273dde06b86b5f93f9aeC2C29665324105b0b66f6df81884754f8080d, c8f7608d4e19f6cb03680941bbd09fe969668bcb09c7ca985048a22e014dffcd, 603848f37ab932dccef98ee27e3c5af9221d3b6ccfe457ccf93cb572495ac325, c3e5d878a30a6c46e22d1dd2089b32086c91f13f8b9c413aa84e1dbaa03b9375, 03f00a143b8929585c122d490b6a3895d639c17d92C2223917e3a9ca1b8d30f9
File Path	/Library/Caches/System Settings, /Library/OSRecovery/SystemUpdater, /Library/Caches/com.apple.mond, /Library/SystemSettings/com.apple.system.settings, /Library/Fonts/com.apple.logd, /Library/SystemSettings/.CacheLogs.db, /Library/LaunchDaemons/com.apple.system.updater.plist, /Library/OSRecovery/com.apple.os.config, /Library/Caches/.Logs.db

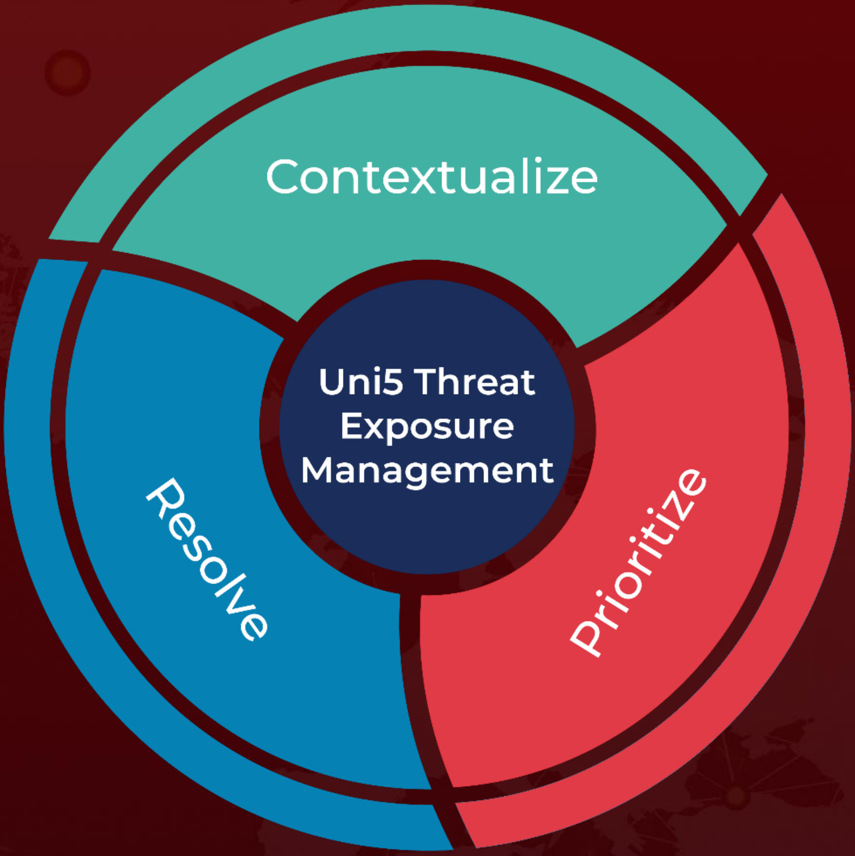
References

https://cloud.google.com/blog/topics/threat-intelligence/unc1069-targets-cryptocurrency-ai-social-engineering

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 17, 2026 • 05:00 AM

More at www.hivepro.com