INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 06:51 UTC

BlueNoroff Weaponizes Victims as Lures: AI-Augmented Zoom Fraud Targets Crypto Executives

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0235
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cryptocurrency industry executives (targeted sector); Zoom platform (abused as lure vector); macOS endpoints (confirmed compromise platform per Microsoft/Sapphire Sleet reporting)
Published	2026-04-28T17:38:39
Discovery Source	Rss

Executive Summary

BlueNoroff, a North Korean state-sponsored group targeting cryptocurrency firms for regime revenue, has escalated its attack tradecraft by combining AI-generated deepfake avatars with stolen victim video footage to impersonate trusted contacts in fraudulent Zoom meetings. Targeted cryptocurrency executives are tricked into executing malicious commands through a technique called ClickFix, resulting in macOS compromise. Organizations in the crypto sector face direct risk of significant financial theft and secondary reputational harm as compromised personnel are recycled as lures against their own networks and peers.

Technical Analysis

BlueNoroff (Microsoft tracking designation: Sapphire Sleet; parent cluster: Lazarus Group) is conducting targeted social engineering intrusions against cryptocurrency sector executives. The infection chain begins with spearphishing lures delivered via fraudulent Zoom meeting invitations, augmented with AI-generated deepfake avatars and video sourced from previously compromised victims (T1656, Impersonation; T1566, Phishing; T1566.004; T1598). Lure delivery exploits Zoom's legitimate meeting infrastructure to bypass sender-based trust signals. Victims are directed to execute the ClickFix payload, a social engineering technique that presents a fabricated UI prompt causing the user to manually run a malicious command (T1204, User Execution; T1204.002). Post-execution, the chain achieves macOS compromise, with kill-chain details including command-line patterns, file hashes, and persistence mechanisms documented in Microsoft's April 2026 Sapphire Sleet macOS analysis. Observed post-compromise behaviors include screen capture (T1113), data

archiving (T1560), code execution (T1059), account abuse (T1078), and masquerading (T1036). No CVE applies; exploitation relies entirely on user execution rather than technical vulnerability. Relevant CWEs: CWE-1021 (UI Redressing), CWE-693 (Protection Mechanism Failure), CWE-184 (Incomplete List of Disallowed Inputs). AI-generated avatars materially degrade visual identity verification as a trust control. Primary source: Microsoft Security Blog, April 16 2026, Dissecting Sapphire Sleet's macOS intrusion from lure to compromise (https://www.microsoft.com/en-us/security/blog/2026/04/16/dissecting-sapphire-sleets-macos-intrusion-from-lure-to-compromise/).

Action Checklist

1. Step 1: Containment, Identify all cryptocurrency sector personnel who conduct external Zoom meetings with counterparties in the crypto/investment space. Alert this population immediately with campaign-specific guidance: do not execute any command presented in or following a Zoom meeting, regardless of the apparent identity of the requester. Suspend unvetted inbound Zoom meeting requests from unknown or newly introduced contacts pending review.
2. Step 2: Detection, Review macOS endpoint telemetry for the following indicators: unexpected Terminal or shell process spawns coinciding with active Zoom sessions; clipboard modification events during or shortly after Zoom calls; outbound connections to new or unrecognized infrastructure from macOS hosts following Zoom activity; Zoom remote-control feature grant events not initiated by your organization. Query EDR for process lineage where Zoom.app is a parent or grandparent of shell interpreters (bash, zsh, osascript). Cross-reference against IOCs published in the Microsoft April 2026 Sapphire Sleet report.
3. Step 3: Eradication, For any host showing ClickFix execution indicators: isolate immediately, preserve forensic image before remediation. Remove persistence mechanisms identified in the Microsoft kill-chain analysis. Revoke and rotate all credentials accessible from the compromised host, including crypto wallet keys, exchange API keys, and any SSO sessions active during the compromise window. Disable or remove any unauthorized Zoom integrations or remote-control grants.
4. Step 4: Recovery, Before returning any remediated host to production, confirm: all persistence artifacts removed per the Microsoft Sapphire Sleet IOC set; credential rotation completed and verified across all downstream systems; macOS endpoint enrolled in EDR with behavioral monitoring active; Zoom remote-control feature disabled at the organizational policy level unless operationally required. Monitor restored hosts for 30 days with elevated alert sensitivity.
5. Step 5: Post-Incident, This campaign exposes three specific control gaps: (1) visual identity verification via video is no longer a reliable trust signal, implement out-of-band verbal confirmation (pre-shared code words or callback to a known number) before granting trust to any video-based identity; (2) user execution is the sole exploitation mechanism, reinforce security awareness training specific to ClickFix-style UI prompts with crypto sector personnel; (3) compromised individuals become propagation vectors, establish a protocol to notify peer organizations when a compromise is confirmed, to disrupt the victim-reuse chain.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and FS-ISAC immediately if: any ClickFix execution is confirmed on a host with access to cryptocurrency wallets, exchange API keys, or custodied assets; if a compromised identity is identified as having been reused by BlueNoroff to target peer organizations; or if forensic evidence suggests active exfiltration or unauthorized cryptocurrency transactions are in progress, which may trigger FinCEN SAR filing obligations and state-level breach notification requirements.
Recovery Notes	Restored macOS hosts must not be returned to production until all three verifications are complete: (1) forensic confirmation that all LaunchAgent, LaunchDaemon, and Login Item persistence artifacts match the pre-incident clean baseline and no Sapphire Sleet IOC hashes are present; (2) downstream confirmation from each crypto exchange and wallet provider that rotated API keys are active and prior keys are fully invalidated with no pending transactions; (3) EDR enrollment verified with at least 24 hours of clean behavioral telemetry showing no Zoom.app-to-shell-interpreter process lineage. Maintain elevated monitoring — specifically alerting on any bash, zsh, or osascript process with Zoom.app in the parent chain — for a minimum of 30 days post-restoration given BlueNoroff's documented use of delayed-activation persistence mechanisms on macOS.
Forensic Artifacts	macOS Unified Log archive (/private/var/db/diagnostics/) — primary source for reconstructing the ClickFix execution chain: process launch events will show Terminal, bash, zsh, or osascript spawned from Zoom.app with timestamps correlating to the fraudulent meeting window | Zoom application logs (~/Library/Logs/zoom.us/) — capture meeting join/leave events, remote-control grant/revoke events, and in-meeting chat content where BlueNoroff delivered the ClickFix paste instruction to the victim | macOS TCC database (/Library/Application Support/com.apple.TCC/TCC.db and ~/Library/Application Support/com.apple.TCC/TCC.db) — records accessibility and automation permission grants that ClickFix payloads require to execute osascript or control system UI elements post-execution | LaunchAgent and LaunchDaemon plist files (~/Library/LaunchAgents/, /Library/LaunchAgents/, /Library/LaunchDaemons/) with SHA-256 hashes — BlueNoroff macOS payloads establish persistence via these mechanisms; cross-reference hashes against the Microsoft April 2026 Sapphire Sleet IOC set | macOS Keychain artifacts (~/Library/Keychains/) and any browser-stored credential databases — ClickFix payloads targeting crypto executives are specifically designed to harvest stored wallet seeds, exchange API keys, and browser-saved passwords; these must be preserved as evidence of credential exposure scope before the host is wiped

Per-Action IR Details

Step 1: Containment — Identify all cryptocurrency sector personnel who conduct external Zoom meetings with counterparties in the crypto/investment space. Alert this population immediately with campaign-specific guidance: do not execute any command presented in or following a Zoom meeting, regardless of the apparent identity of the requester. Suspend unvetted inbound Zoom meeting requests from unknown or newly introduced contacts pending review.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: prioritize actions that prevent further damage while preserving evidence; coordinate communication to affected personnel as part of the incident response plan execution.

Controls: NIST IR-4 (Incident Handling) — implement containment as part of the incident handling capability, NIST IR-6 (Incident Reporting) — require personnel to report suspected ClickFix prompt encounters immediately, NIST IR-8 (Incident Response Plan) — execute the IR plan communications component to notify at-risk crypto sector staff, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce identity verification controls on Zoom access as a containment-layer compensating measure, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — ensure crypto-sector executives are not operating with elevated privileges that would amplify ClickFix

execution impact

Compensating: For teams without enterprise communication tooling: distribute a templated alert via email to all identified crypto/investment-facing personnel listing the exact ClickFix UI characteristics observed in the BlueNoroff campaign (e.g., a Zoom dialog requesting the user open Terminal and paste a command to 'fix audio/video'). Publish a shared block-list of known BlueNoroff-associated Zoom display names or email domains from the Microsoft April 2026 Sapphire Sleet IOC set to your email gateway manually. Use a free Zoom admin policy export (zoom.us admin portal > Account Management > Account Settings) to audit and disable the Remote Control feature org-wide at no cost.

Evidence: Before alerting personnel, preserve: Zoom meeting invite metadata (sender email, Zoom meeting ID, display name used) for any suspicious inbound meeting requests received in the prior 30 days; email gateway logs showing inbound Zoom invite delivery including originating IP and envelope-from address; Zoom administrative audit logs (zoom.us > Account Management > Reports > Audit Logs) capturing remote-control grant events and meeting join events for crypto-sector accounts. Do not purge calendar or email artifacts — BlueNoroff leverages stolen victim identities, and these records establish the impersonation chain.

Step 2: Detection — Review macOS endpoint telemetry for the following indicators: unexpected Terminal or shell process spawns coinciding with active Zoom sessions; clipboard modification events during or shortly after Zoom calls; outbound connections to new or unrecognized infrastructure from macOS hosts following Zoom activity; Zoom remote-control feature grant events not initiated by your organization. Query EDR for process lineage where Zoom.app is a parent or grandparent of shell interpreters (bash, zsh, osascript). Cross-reference against IOCs published in the Microsoft April 2026 Sapphire Sleet report.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate endpoint telemetry and network indicators to identify ClickFix execution events; use process lineage analysis to distinguish legitimate Zoom subprocess activity from attacker-induced shell spawns.

Controls: NIST SI-4 (System Monitoring) — monitor macOS endpoints for anomalous process creation events associated with Zoom.app parent processes, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review macOS Unified Log and EDR telemetry for ClickFix execution artifacts at defined frequency, NIST AU-3 (Content of Audit Records) — ensure audit records capture process lineage, parent-child relationships, and command-line arguments needed to identify bash/zsh spawned from Zoom.app, NIST IR-5 (Incident Monitoring) — track and document all identified ClickFix execution indicators and correlate to affected host inventory, CIS 8.2 (Collect Audit Logs) — ensure macOS endpoint logging (Unified Log, audit framework) is enabled and forwarded before querying for indicators

Compensating: Without EDR, run the following on each macOS host under review: (1) Query Unified Log for Zoom-adjacent shell spawns: 'log show --predicate "processImagePath contains \'Terminal\' OR processImagePath contains \'bash\' OR processImagePath contains \'zsh\'" --last 7d | grep -i zoom' — flag any entries where Zoom activity timestamps overlap. (2) Use osquery with the 'processes' and 'process_events' tables: 'SELECT pid, parent, name, cmdline, start_time FROM processes WHERE parent IN (SELECT pid FROM processes WHERE name = \'zoom.us\');' (3) Deploy the free Sigma rule mapped to ClickFix macOS execution (search the SigmaHQ repository for 'ClickFix' or 'Zoom lure' rules; convert to osquery or auditd format using sigmac). (4) Check for BlueNoroff C2 IOC hits in macOS /private/var/log/system.log and Little Snitch or pfctl connection logs if available.

Evidence: Capture before analysis: macOS Unified Log archive from /private/var/db/diagnostics/ covering the suspected compromise window — this records process launches with parent-child relationships and is the primary source for detecting Terminal/bash/zsh spawned from Zoom.app; macOS TCC (Transparency Consent and Control) database at /Library/Application Support/com.apple.TCC/TCC.db — ClickFix payloads frequently require or abuse accessibility/automation permissions granted during or after the Zoom session; Zoom application logs at ~/Library/Logs/zoom.us/ — these capture meeting join/leave events, remote-control grant events, and in-meeting chat (where ClickFix paste instructions may have been delivered); macOS clipboard history (if a clipboard manager is installed) or pbpaste output captured immediately on the suspect host to recover the exact command the user was instructed to paste; network flow logs or pfctl/Little Snitch logs showing outbound connections from the Zoom.app process or any child process within 10 minutes of meeting end.

Step 3: Eradication — For any host showing ClickFix execution indicators: isolate immediately, preserve forensic image before remediation. Remove persistence mechanisms identified in the Microsoft kill-chain analysis. Revoke and rotate all credentials accessible from the compromised host, including crypto wallet keys, exchange API keys, and any SSO sessions active during the compromise window. Disable or remove any unauthorized Zoom integrations or remote-control grants.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove malicious artifacts and persistence mechanisms from all affected hosts; credential revocation is a required eradication action when attacker access to authenticated sessions is confirmed or suspected.

Controls: NIST IR-4 (Incident Handling) — execute eradication phase of incident handling capability including persistence removal and credential revocation, NIST SI-2 (Flaw Remediation) — while no CVE applies, treat ClickFix execution as a system compromise requiring verified clean-state restoration, NIST SI-7 (Software, Firmware, and Information Integrity) — employ integrity verification to confirm persistence mechanisms have been fully removed post-eradication, NIST AC (Access Control) — revoke and rotate all credentials and API keys accessible from the compromised macOS host, including crypto exchange API keys and SSO tokens, CIS 5.2 (Use Unique Passwords) — enforce credential rotation with unique values for all accounts accessible from the compromised host, CIS 6.2 (Establish an Access Revoking Process) — execute the documented access revoking process for all sessions and credentials confirmed or suspected active during compromise

Compensating: For teams without enterprise forensic tooling: (1) Acquire a forensic image using the free 'dc3dd' or 'ddrescue' tool before any remediation — on macOS, boot to Recovery Mode or use a Thunderbolt target disk mode connection to a forensic workstation. (2) To identify BlueNoroff persistence mechanisms on macOS, check these locations manually via Terminal before wiping: LaunchAgents (~/.config/LaunchAgents/, ~/Library/LaunchAgents/, /Library/LaunchAgents/), LaunchDaemons (/Library/LaunchDaemons/), Login Items (System Settings > General > Login Items), and cron jobs ('crontab -l' for each user). (3) For credential revocation without a PAM/IAM platform: manually invalidate all active sessions in each crypto exchange admin portal, rotate all API key pairs, and force re-authentication on any SSO provider (Okta, Azure AD) by terminating active sessions from the admin console. (4) Use the free 'KnockKnock' tool from Objective-See to enumerate all persistent items on the macOS host and cross-reference against the Microsoft Sapphire Sleet IOC list.

Evidence: Preserve before eradication: full forensic disk image of the compromised macOS host (APFS volume); memory dump using the free 'osxpmem' tool — BlueNoroff macOS payloads may stage in-memory components that will not survive a reboot; complete list of LaunchAgent and LaunchDaemon plist files with SHA-256 hashes for comparison against the Microsoft Sapphire Sleet IOC set; Keychain access logs and contents (~/Library/Keychains/) — ClickFix payloads targeting crypto executives frequently harvest macOS Keychain to extract stored wallet seeds and exchange API credentials; list of all active Zoom remote-control grants and integrations exported from the Zoom admin portal before they are revoked, to document the scope of unauthorized access.

Step 4: Recovery — Before returning any compromised host to production, confirm: all persistence artifacts removed per the Microsoft Sapphire Sleet IOC set; credential rotation completed and verified across all downstream systems; macOS endpoint enrolled in EDR with behavioral monitoring active; Zoom remote-control feature disabled at the organizational policy level unless operationally required. Monitor restored hosts for 30 days with elevated alert sensitivity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify system integrity before restoration to production; implement enhanced monitoring on recovered systems for a defined period to detect re-compromise or residual attacker persistence.

Controls: NIST IR-4 (Incident Handling) — execute recovery phase including verification of eradication completeness before production restoration, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of restored macOS system and Zoom application installation before returning to production, NIST SI-4 (System Monitoring) — implement elevated behavioral monitoring on recovered hosts for the 30-day post-recovery window, specifically watching for Zoom.app spawning shell interpreters, NIST CM (Configuration Management) — enforce organizational Zoom policy disabling remote-control feature as a hardened configuration baseline, CIS 4.6 (Securely Manage

Enterprise Assets and Software) — manage Zoom configuration through documented policy, disabling remote-control unless explicitly required and approved, CIS 7.3 (Perform Automated Operating System Patch Management) — confirm macOS is fully patched before returning to production to eliminate any secondary exploitation surface, CIS 7.4 (Perform Automated Application Patch Management) — confirm Zoom client is updated to the latest version before re-enrollment

Compensating: Without enterprise EDR, implement the following free monitoring stack on recovered hosts for the 30-day window: (1) Deploy Objective-See's free 'BlockBlock' tool to alert on any new persistence mechanism installation in real time. (2) Enable macOS built-in audit framework: 'sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist' and configure /etc/security/audit_control to log exec and file events. (3) Create a cron job to run daily: 'find ~/Library/LaunchAgents /Library/LaunchAgents /Library/LaunchDaemons -newer /var/db/receipts -type f | sha256sum' and diff output against the clean baseline captured at imaging time. (4) Enforce Zoom remote-control policy by deploying a free MDM profile via Apple Configurator 2 that sets the Zoom configuration key 'disable_remote_control' to true.

Evidence: Before returning to production, document and retain: integrity verification report comparing restored host file hashes against a known-good macOS baseline (use 'sudo /usr/bin/openssl dgst -sha256' on critical system binaries); Zoom admin portal export confirming remote-control is disabled at the account policy level with a timestamp; completed credential rotation verification checklist documenting each crypto exchange API key, wallet access credential, and SSO account rotated, with confirmation tokens or audit log entries from each downstream system; enrollment confirmation from EDR console showing the recovered host is reporting telemetry before production re-authorization.

Step 5: Post-Incident — This campaign exposes three specific control gaps: (1) visual identity verification via video is no longer a reliable trust signal — implement out-of-band verbal confirmation (pre-shared code words or callback to a known number) before granting trust to any video-based identity; (2) user execution is the sole exploitation mechanism — reinforce security awareness training specific to ClickFix-style UI prompts with crypto sector personnel; (3) compromised individuals become propagation vectors — establish a protocol to notify peer organizations when a compromise is confirmed, to disrupt the victim-reuse chain.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review to address the three control gaps exposed by this BlueNoroff campaign; update detection capabilities and training to address deepfake-augmented social engineering and ClickFix UI lure techniques specifically.

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to incorporate out-of-band identity verification requirements for video-based communications with external counterparties, NIST IR-2 (Incident Response Training) — deliver BlueNoroff/ClickFix-specific awareness training to crypto sector personnel, including simulated ClickFix prompt exercises, NIST IR-3 (Incident Response Testing) — test updated procedures including out-of-band verification protocols with tabletop exercises simulating a deepfake Zoom lure scenario, NIST IR-8 (Incident Response Plan) — update the IR plan to include a victim-reuse notification protocol for peer organization disclosure when BlueNoroff compromise is confirmed, NIST SI-5 (Security Alerts, Advisories, and Directives) — disseminate the Microsoft April 2026 Sapphire Sleet advisory and BlueNoroff campaign IOCs to peer organizations via ISACs (FS-ISAC for crypto/financial sector), CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate deepfake/social engineering lure campaigns as a tracked threat category in the vulnerability and threat management process, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — audit all external-facing accounts used by crypto sector personnel for evidence of BlueNoroff reconnaissance or prior contact attempts

Compensating: For teams without a formal awareness training platform: (1) Conduct a 30-minute tabletop exercise with crypto-sector personnel using a free slide deck that walks through the BlueNoroff Zoom lure scenario step by step — include a screenshot of a representative ClickFix dialog so personnel can recognize the exact UI pattern. (2) Distribute a one-page quick-reference card listing the out-of-band verification protocol: pre-shared code words, callback numbers, and the rule that no command execution request from a Zoom meeting is ever legitimate. (3) Submit confirmed IOCs (C2 domains, payload hashes from the Microsoft Sapphire Sleet report) to FS-ISAC's free threat intelligence sharing portal and to CISA's voluntary reporting form at cisa.gov/report to contribute to the victim-reuse disruption chain. (4) Create a free YARA rule based on the ClickFix payload characteristics published in the Microsoft report and deploy via ClamAV on all macOS endpoints.

Evidence: Retain for post-incident review and potential regulatory reporting: complete incident timeline documenting first contact through confirmed compromise, including all Zoom meeting metadata, impersonated identity details, and ClickFix execution timestamp — this supports FinCEN Suspicious Activity Report (SAR) filing obligations if cryptocurrency assets were accessed or transferred; all IOC artifacts collected during detection and eradication phases preserved in a chain-of-custody log; written record of the three identified control gaps with assigned owners and remediation deadlines for the lessons-learned report; copies of all peer notification communications sent to disrupt the BlueNoroff victim-reuse chain, retained for legal and regulatory purposes.

Detection Guidance

Detection centers on macOS endpoint behavioral analysis and Zoom session correlation. Key signals: (1) Shell interpreter processes (bash, zsh, osascript, python3) spawned with Zoom.app or ZoomOpener as a parent or ancestor process, this is the primary ClickFix execution indicator. (2) Clipboard write events containing encoded strings or command syntax during active Zoom sessions. (3) Zoom remote-control feature activation events, query Zoom admin logs for 'remote control granted' events, particularly for sessions with external participants. (4) Outbound DNS and network connections from macOS hosts to uncategorized or newly registered domains within 10 minutes of Zoom session termination. (5) New LaunchAgent or LaunchDaemon plist files created outside of standard software installation windows, common macOS persistence mechanism. (6) Screen capture activity (screencapture binary or equivalent API calls) from processes without a documented business use. Hunt: correlate Zoom meeting participant lists against known BlueNoroff infrastructure and the victim identity reuse pattern, participants presenting video that does not match calendar invitations or prior verified interactions warrant out-of-band identity confirmation. Reference the Microsoft April 2026 Sapphire Sleet report for specific file hashes, domains, and command-line patterns associated with this campaign.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.microsoft.com/en-us/security/blog/2026/04/16/dissecting-sapphire-sleets-macos-intrusion-from-lure-to-compromise/`	Microsoft primary source — Sapphire Sleet macOS kill-chain analysis; contains campaign-specific IOCs including file hashes, domains, and command-line indicators	HIGH

Framework Mappings

MITRE-ATTACK

- **T1560** — Archive Collected Data
- **T1656** — Impersonation
- **T1204** — User Execution
- **T1598** — Phishing for Information
- **T1566** — Phishing
- **T1585** — Establish Accounts
- **T1113** — Screen Capture

- **T1566.004** — Spearphishing Voice
- **T1204.002** — Malicious File
- **T1036** — Masquerading
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1560	Archive Collected Data	Collection
T1656	Impersonation	Defense-Evasion
T1204	User Execution	Execution
T1598	Phishing for Information	Reconnaissance
T1566	Phishing	Initial-Access
T1585	Establish Accounts	Resource-Development
T1113	Screen Capture	Collection

Technique ID	Technique Name	Tactic
T1566.004	Spearphishing Voice	Initial-Access
T1204.002	Malicious File	Execution
T1036	Masquerading	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/bluenoroff-t...	T3
North Korean Hackers Target Crypto Firms with ClickFix and Zoom ...	https://www.infosecurity-magazine.com/news/bluenoroff-dprk-hackers-...	T3
Hackers Exploit Zoom's Remote Control Feature in Cryptocurrency ...	https://www.secureworld.io/industry-news/zoom-remote-control-crypto...	T3
Dissecting Sapphire Sleet's macOS intrusion from lure to compromise	https://www.microsoft.com/en-us/security/blog/2026/04/16/dissecting...	T1
North Korean hackers targeted crypto exec with fake Zoom meeting ...	https://therecord.media/north-korean-hackers-targeted-crypto-exec-c...	T3

Generated 2026-04-29 06:51 UTC by TJS Security Command Center