Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

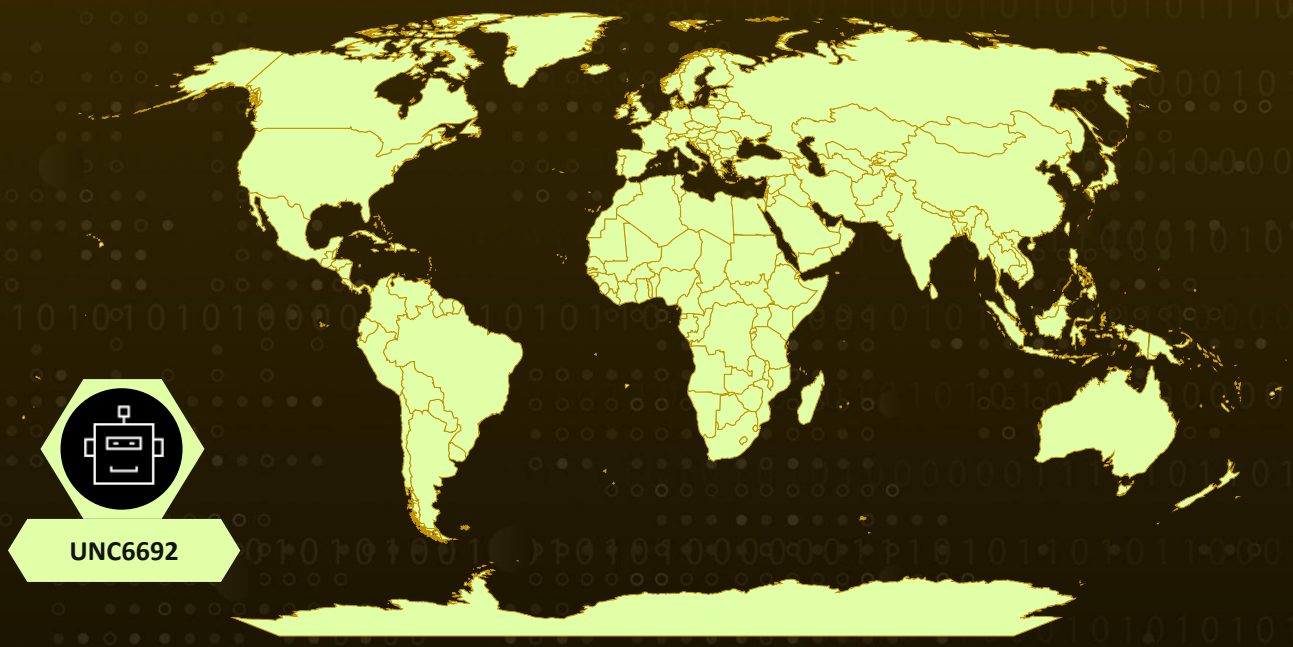
# UNC6692 Social Engineering Campaign Deploying SNOW Malware Suite


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| April 24, 2026 | A1 | TA2026112 |

# Summary

**First Seen:** Late December 2025
**Targeted Regions:** Worldwide
**Targeted Platforms:** Windows, Linux
**Threat Actor:** UNC6692
**Malware:** SNOWBELT, SNOWGLAZE, SNOWBASIN
**Attack:** UNC6692 conducted a multistage intrusion leveraging persistent social engineering, impersonating IT helpdesk personnel via Microsoft Teams to lure victims into installing a custom modular malware suite. The campaign employed email bombing to create urgency, followed by a phishing page hosted on an attacker-controlled AWS S3 bucket that harvested credentials and deployed a trio of malware components, SNOWBELT (browser extension backdoor), SNOWGLAZE (Python tunneler), and SNOWBASIN (Python bindshell), ultimately achieving deep network penetration, credential theft, lateral movement via Pass-The-Hash, and data exfiltration through LimeWire and attacker-controlled cloud infrastructure.

## Attack Regions






Targeted  Non-Targeted

# Attack Details

**#1**

What began as a simple flood of emails quickly unfolded into a carefully staged intrusion, blending psychological pressure with technical precision. In late December 2025, UNC6692 launched a large-scale email bombing campaign, overwhelming targets with a surge of messages to induce urgency and confusion. Capitalizing on this chaos, the attacker followed up via Microsoft Teams, impersonating helpdesk personnel and offering assistance. Victims were guided to install a so-called “local patch” to mitigate the spam, which in reality redirected them to a malicious HTML page hosted on an attacker-controlled AWS S3 bucket. Disguised as a “Mailbox Repair and Sync Utility,” the page enforced specific conditions, such as requiring Microsoft Edge and validating URL parameters, to enhance its credibility. A cleverly designed credential harvesting prompt used a “double-entry” trick, rejecting initial password attempts to simulate user error while ensuring accurate credential capture. Meanwhile, stolen data was quietly exfiltrated via asynchronous PUT requests, masked behind a deceptive progress bar.

**#2**

Once initial access was secured, the operation shifted into a more technical phase. Victims unknowingly downloaded a renamed AutoHotKey binary along with a malicious script, which executed reconnaissance commands and deployed SNOWBELT, a rogue Chromium-based browser extension posing as “MS Heartbeat” or “System Heartbeat.” Persistence was methodically established through startup folder shortcuts and scheduled tasks that ensured the extension ran silently in the background. SNOWBELT acted as a command relay, bridging communication between the attacker and SNOWBASIN, a Python-based backdoor operating locally. Leveraging techniques such as time-based domain generation algorithms (DGA), AES-GCM encryption, and browser push notifications, the malware maintained resilient and covert command-and-control (C2) communication.

**#3**

Building on this foothold, UNC6692 expanded its toolkit by deploying additional payloads, including SNOWGLAZE, SNOWBASIN, and supplementary AutoHotKey scripts, along with a portable Python environment. Internal reconnaissance followed, with scripts scanning for commonly exposed ports such as 135, 445, and 3389. Using SNOWGLAZE, a cross-platform tunneling utility, the attacker established a secure WebSocket-based channel to a cloud-hosted C2 infrastructure, effectively transforming the compromised system into a SOCKS proxy. This allowed arbitrary TCP traffic to be routed discreetly, with data encapsulated in JSON and Base64-encoded to blend in with normal encrypted web traffic.

**#4**

With internal access deepening, UNC6692 moved laterally across the network. Through the SNOWGLAZE tunnel, the attacker initiated remote sessions using Sysinternals PsExec to enumerate administrative accounts and extend control. Access to a backup server via RDP marked a critical escalation point, where LSASS process memory was dumped using Windows Task Manager and exfiltrated via LimeWire. Credential material extracted offline enabled Pass-the-Hash attacks, granting access to domain controllers. From there, the attacker deployed FTK Imager to extract high-value assets, including the Active Directory database (NTDS.dit) and critical registry hives such as SAM, SYSTEM, and SECURITY. These were also exfiltrated through LimeWire, while telemetry indicated targeted screen captures of sensitive operations, suggesting deliberate verification of data theft. The campaign ultimately culminated in a full-scale compromise, with attackers achieving their objective of extensive credential harvesting and Active Directory exfiltration.

# Recommendations

- **Block Attacker-Controlled S3 Buckets:** Immediately block all identified attacker-controlled AWS S3 bucket domains at the network perimeter, including service-page-25144-30466-outlook.s3.us-west-2.amazonaws[.]com, cloudfront-021.s3.us-west-2.amazonaws[.]com, and service-page-11369-28315-outlook.s3.us-west-2.amazonaws[.]com.

- **Block SNOWGLAZE C2 WebSocket URL:** Add the hard-coded SNOWGLAZE C2 endpoint wss://sad4w7h913-b4a57f9c36eb.herokuapp[.]com/ws to network blocklists and monitor for WebSocket connections to Heroku subdomains exhibiting tunneling behavior.

- **Restrict External Microsoft Teams Communications:** Configure Microsoft Teams to block or flag chat invitations from external tenants, particularly those impersonating IT helpdesk roles, to prevent the social engineering vector used in this campaign.

- **Audit and Control Browser Extension Installations:** Enforce policies that prevent the sideloading of Chromium browser extensions outside of official stores. Monitor for extensions installed under non-standard directories such as AppData\Local\Microsoft\Edge\Extension Data\SysEvents.

**Monitor for Scheduled Task Abuse:** Establish detection rules for newly created scheduled tasks that invoke Microsoft Edge with headless flags (--headless=new), --load-extension parameters, or non-standard --user-data-dir paths, which are indicators of SNOWBELT persistence.

**Detect AutoHotKey Abuse:** Alert on AutoHotKey binary execution in non-development environments, particularly when AutoHotKey binaries are renamed or executed from user-writable directories such as Downloads or AppData.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1566: Phishing | T1566.002: Spearphishing Link |
| Execution | T1053: Scheduled Task/Job | T1053.005: Scheduled Task |
| | T1059: Command and Scripting Interpreter | T1059.001: PowerShell |
| | | T1059.003: Windows Command Shell |
| | | T1059.006: Python |
| | | T1059.007: JavaScript |
| | | T1059.010: AutoHotKey & AutoIT |
| | T1204: User Execution | T1204.001: Malicious Link |
| | | T1204.002: Malicious File |
| | T1559: Inter-Process Communication | |
| | T1569: System Services | T1569.002: Service Execution |
| Persistence | T1176: Browser Extensions | T1176.001: Browser Extensions |
| | T1543: Create or Modify System Process | T1543.003: Windows Service |
| | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| | | T1547.009: Shortcut Modification |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Privilege Escalation | T1068: Exploitation for Privilege Escalation | |
| Defense Evasion | T1027: Obfuscated Files or Information | T1027.010: Command Obfuscation |
| | T1036: Masquerading | T1036.005: Match Legitimate Resource Name or Location |
| | | T1027.015: Compression |
| | T1070: Indicator Removal | T1070.004: File Deletion |
| | T1112: Modify Registry | |
| | T1134: Access Token Manipulation | T1134.001: Token Impersonation/Theft |
| | T1140: Deobfuscate/Decode Files or Information | |
| | T1202: Indirect Command Execution | |
| | T1564: Hide Artifacts | T1564.001: Hidden Files and Directories |
| | | T1562.001: Disable or Modify Tools |
| | T1622: Debugger Evasion | |
| Credential Access | T1003: OS Credential Dumping | T1003.001: LSASS Memory |
| | | T1003.002: Security Account Manager |
| | | T1003.003: NTDS |
| | T1110: Brute Force | T1110.001: Password Guessing |
| | | T1110.003: Password Spraying |
| | T1552: Unsecured Credentials | T1552.001: Credentials In Files |
| Discovery | T1016: System Network Configuration Discovery | |
| | T1018: Remote System Discovery | |
| | T1046: Network Service Discovery | |
| | T1087: Account Discovery | T1087.001: Local Account |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Discovery | T1007: System Service Discovery | |
| | T1012: Query Registry | |
| | T1033: System Owner/User Discovery | |
| | T1057: Process Discovery | |
| | T1082: System Information Discovery | |
| | T1083: File and Directory Discovery | |
| | T1518: Software Discovery | |
| Lateral Movement | T1021: Remote Services | T1021.001: Remote Desktop Protocol |
| | | T1021.002: SMB/Windows Admin Shares |
| Collection | T1005: Data from Local System | |
| | T1074: Data Staged | |
| | T1113: Screen Capture | |
| | T1560: Archive Collected Data | T1560.001: Archive via Utility |
| Exfiltration | T1567: Exfiltration Over Web Service | T1567.002: Exfiltration to Cloud Storage |
| | T1020: Automated Exfiltration | |
| Command and Control | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1090: Proxy | |
| | T1105: Ingress Tool Transfer | |
| | T1572: Protocol Tunneling | |
| Resource Development | T1608: Stage Capabilities | T1608.002: Upload Tool |
| | | T1608.005: Link Target |
| Impact | T1489: Service Stop | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| URLs | service-page-25144-30466-outlook[.]s3[.]us-west-2[.]amazonaws[.]com, cloudfront-021[.]s3[.]us-west-2[.]amazonaws[.]com, service-page-11369-28315-outlook[.]s3[.]us-west-2[.]amazonaws[.]com, wss[:]//sad4w7h913-b4a57f9c36eb[.]herokuapp[.]com/ws |
| SHA256 | 2fa987b9ed6ec6d09c7451abd994249dfaba1c5a7da1c22b8407c461e62f7e49, c8940de8cb917abe158a826a1d08f1083af517351d01642e6c7f324d0bba1eb8, 7f1d71e1e079f3244a69205588d504ed830d4c473747bb1b5c520634cc5a2477, ca390b86793922555c84abc3b34406da2899382c617f9dcf83a74ac09dd18190, 6e6dab993f99505646051d2772701e3c4740096ff9be63c92713bcb7fcddf9f7, de200b79ad2bd9db37baeba5e4d183498d450494c71c8929433681e848c3807f |
| File Path | C:\ProgramData\log, C:\Users\<user>\AppData\Local\Microsoft\Edge\ExtensionData\SysEvents\background.js, C:\Users\<user>\AppData\Local\Microsoft\Edge\ExtensionData\SysEvents\dream.js, C:\Users\<user>\AppData\Local\Microsoft\Edge\ExtensionData\SysEvents\dream.html, C:\Users\<user>\AppData\Local\Microsoft\Edge\ExtensionData\SysEvents\helper.html |

# References

https://cloud.google.com/blog/topics/threat-intelligence/unc6692-social-engineering-custom-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 demo of **HivePro.**

REPORT GENERATED ON

**April 24, 2026 • 9:00 AM**



More at www.hivepro.com