INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:32 UTC

Fake IT Support Vishing Campaign Deploys Havoc C2, Ransomware Precursor [SCC-2026-0007]

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0002
Type	Threat Campaign
Severity	HIGH
Published	2026-03-04

Executive Summary

A threat actor is calling employees posing as IT support after flooding their inbox with emails, then persuading them to install legitimate remote management tools (Level RMM, XEOX) to deploy the Havoc command-and-control framework. In one confirmed case, nine endpoints were compromised within 11 hours. This attack uses no software vulnerabilities, all defenses must be human-facing.

Technical Analysis

This campaign uses a two-stage social engineering attack that bypasses most technical security controls by targeting employees directly:nnStage 1, Email Bombing: The victim's inbox is flooded with thousands of subscription or newsletter emails in a short window, creating urgency and confusion.nnStage 2, Vishing Call: The attacker calls the victim posing as IT support, offering to help resolve the 'email problem.' They persuade the victim to install Level RMM or XEOX, legitimate remote management tools, under the guise of IT assistance.nnPost-Access Payload: Once remote access is established, the attacker deploys Havoc C2 (open-source C2 framework). Havoc uses Hell's Gate (direct syscall execution to bypass EDR hooks) and DLL sideloading for evasion. XEOX is used as a backup persistence mechanism if Level RMM is removed.nnSpeed and Scale: In one confirmed case, nine endpoints were compromised within 11 hours of initial access. The campaign is assessed as a ransomware precursor, operators establish persistent access first, then deploy ransomware in a subsequent wave.nnThis attack requires zero technical vulnerabilities. All controls must be human-facing.

Action Checklist

1. 1. Issue employee awareness alert: IT will never call employees unsolicited about email problems. If an employee receives such a call, they should hang up and report it immediately.

2. 2. Implement help desk callback verification: any request for remote access must be validated against an existing IT ticket. Help desk staff must not authorize remote access tools without a verified ticket.

3. 3. Review email gateway for signs of email bombing: flag users receiving 200+ emails in under one hour and notify them and their manager before a vishing call can occur.

4. 4. Hunt for Level RMM and XEOX installations on all endpoints, particularly unmanaged and BYOD devices not covered by EDR.

5. 5. Query EDR for Havoc C2 indicators: Hell's Gate syscall patterns, unusual DLL sideloading events, unexpected parent-child process relationships (e.g., remote management tool spawning cmd.exe or PowerShell).

6. 6. If Level RMM or XEOX is found on an endpoint with no IT-authorized ticket: treat as confirmed compromise, isolate immediately, begin IR process.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO/Security Leadership and consider external IR firm engagement immediately if any confirmed Havoc C2 infrastructure is detected, if more than 3 endpoints are compromised, or if any evidence of data exfiltration is found; escalate to legal/compliance if ransomware deployment has occurred.
Recovery Notes	Post-containment recovery: (1) do not reconnect isolated endpoints to the network until forensic analysis is complete and all Havoc/RMM artifacts are removed or the device is reimaged from clean media; (2) for reimaged endpoints, verify that no RMM tools are reinstalled by requiring a support ticket for any future remote access requests and validating against ticket logs; (3) send a follow-up employee awareness email within 24 hours of containment summarizing the incident (without operational details) and reinforcing the callback verification procedure; (4) conduct a 'lessons learned' meeting with IT help desk, managers, and affected users within 5 days to identify process gaps and reinforce the no-unsolicited-calls policy; (5) update the help desk SOP to include this attack profile and require weekly refresher training for 30 days.
Forensic Artifacts	Windows Event Log Security (Event ID 4688 for process execution, 4624/4625 for authentication attempts) | Sysmon logs (Event 1 for process creation, Event 3 for network connection, Event 7 for image load/DLL loading, Event 21 for WmiEvent) | File system artifacts: RMM installation directories, temporary download folders (C:\Users*\Downloads, C:\Windows\Temp, %APPDATA%\Local\Temp), prefetch files (C:\Windows\Prefetch) | Registry hives: HKLM\Software\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HklmSoftware\Wow6432Node (for 32-bit persistence) | Network artifacts: firewall logs, DNS query logs (for C2 domain resolution), network connection metadata (source/destination IP, port, protocol, process name), browser download history and cache

Per-Action IR Details

1. Issue employee awareness alert: IT will never call employees unsolicited about email problems. If an employee receives such a call, they should hang up and report it immediately.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: awareness and training)

Controls: NIST 800-53 AT-2 (Security Awareness and Training), NIST 800-53 AT-3 (Role-Based Security Training), CIS 6.1 (Establish and Maintain a Security Awareness Program)

Compensating: Send email template via distribution list with clear call-handling script. Include a one-page PDF flowchart: 'Did IT call you about email? → STOP → Hang up → Report to help desk immediately.' Post the same flowchart in break rooms, on desk placards, and in Slack/Teams pinned messages. No tools required—use existing email and intranet channels.

Evidence: Capture email send timestamp, distribution list membership, and baseline of help desk inbound calls for 48 hours pre-alert to establish a control line for post-alert call volume comparison. Document employee acknowledgment via survey or email read receipt if your email platform supports it.

2. Implement help desk callback verification: any request for remote access must be validated against an existing IT ticket. Help desk staff must not authorize remote access tools without a verified ticket.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: access control policy); NIST 800-53 AC-2 (Account Management)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-2 (Authentication), CIS 6.3 (Address Unauthorized Software)

Compensating: Create a help desk workflow document requiring staff to: (1) ask the caller for their name and department; (2) tell them 'I will call you back at the number on file in our system'; (3) hang up; (4) look up the employee in your directory; (5) call them back directly—never use a number the caller provided. Enforce this in a written SOP and require monthly re-certification for all help desk staff. Use free tools: document in Google Docs, track compliance in a shared spreadsheet with sign-off dates.

Evidence: Before implementing: pull 30 days of help desk ticket history to establish baseline remote access request patterns. After implementation, capture weekly help desk call logs and ticket metadata (requester ID, tool requested, ticket number, authorization timestamp) for 90 days to detect anomalies.

3. Review email gateway for signs of email bombing: flag users receiving 200+ emails in under one hour and notify them and their manager before a vishing call can occur.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Detection and Analysis: analysis)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: If no email gateway with bulk-email detection: (1) export email server logs daily (Postfix, Exchange, or cloud logs); (2) use free tools like Splunk Free (500 MB/day) or AWK/grep to count emails per recipient per hour; (3) create a daily report identifying users with >200 emails in any 60-minute window; (4) email that user and their manager within 1 hour with a template: 'Your inbox received an unusual volume of email. Do not respond to unsolicited requests for remote access. Notify IT immediately.' Automate with a cron job and bash script.

Evidence: Preserve email gateway logs (SMTP transaction logs, bounce records, sender IP reputation data) for 90 days. Capture sender domains, recipient count, message subject lines, and attachment metadata for all messages in bulk-send events. Note exact timestamp of 200-email threshold crossing.

4. Hunt for Level RMM and XEOX installations on all endpoints, particularly unmanaged and BYOD devices not covered by EDR.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.4 (Detection: threat hunting); NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CM-8 (Information System Component Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Without EDR: (1) deploy free OSQUERY agent to all endpoints or use native OS inventory tools; (2) hunt for process names 'levelrmmservice.exe', 'xeox.exe', or variants; (3) check file system paths: 'C:\Program Files\Level\', 'C:\Program Files (x86)\XEOX\', or common temp locations (Downloads, AppData\Local\Temp); (4) on macOS/Linux, search for /opt/level/, /opt/xeox/, or ~/ variants; (5) use Autoruns (Sysinternals, free) on Windows to list

persistence mechanisms; (6) for unmanaged/BYOD: send employees a verification script (PowerShell or Bash) via email with clear instructions and collect results in a shared spreadsheet. Alternative: manually audit 20% of BYOD devices via video call screen-share.

Evidence: Capture process execution logs (Windows Event Log 4688, Sysmon Event 1; macOS unified logs; Linux auditd), file creation timestamps, registry entries (HKLM\Software, HKCU\Software for persistence), network connections from the RMM tool (netstat logs, firewall logs, DNS queries to Level/XEOX C2 domains), and installer/downloaded file hashes and paths. Preserve memory dumps from any endpoint where RMM tools are found.

5. Query EDR for Havoc C2 indicators: Hell's Gate syscall patterns, unusual DLL sideloading events, unexpected parent-child process relationships (e.g., remote management tool spawning cmd.exe or PowerShell).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.4 (Detection: indicator analysis); NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 SI-3 (Malware Protection), CIS 7.1 (Establish and Maintain a Process Allowlist)

Compensating: Without EDR: (1) install Sysmon (free) on all Windows endpoints and forward logs to centralized store; (2) hunt for DLL loading anomalies by parsing Sysmon Event 7 (Image Load) and looking for unsigned DLLs or legitimate DLLs loaded from unexpected paths; (3) monitor parent-child process chains using Event 1 (Process Create): filter for RMM process names spawning cmd.exe, powershell.exe, or rundll32.exe; (4) check for syscall abuse by examining raw Windows kernel events (ETW, Sysmon Event 20 & 21); (5) use YARA rules from MITRE ATT&CK or EmojiDex to scan for Havoc signatures in memory/disk; (6) cross-reference against MITRE ATT&CK tactics: T1134 (Process Injection), T1036 (Masquerading), T1547 (Persistence); (7) query DNS/firewall logs for known Havoc C2 domains (maintain a threat intelligence feed from CISA, Abuse.ch, or MITRE).

Evidence: Preserve Sysmon event logs (Events 1, 3, 7, 8, 11, 21, 22 for process execution, network connection, DLL load, remote thread creation, file creation, and DNS query), Windows Event Log Security (4688), firewall connection logs with src/dst IPs and ports, DNS query logs, and process memory dumps. Capture exact timestamp and command-line arguments for any suspicious process chain. Document Havoc IoC sources (MITRE ATT&CK Havoc page, vendor threat reports, CISA alerts).

6. If Level RMM or XEOX is found on an endpoint with no IT-authorized ticket: treat as confirmed compromise, isolate immediately, begin IR process.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment); NIST 800-53 IR-4 (Incident Handling)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-5 (Incident Monitoring), CIS 6.4 (Remediate Detected Vulnerabilities)

Compensating: Immediate isolation procedure: (1) if the endpoint is networked, physically unplug the Ethernet cable or disable WiFi (do not rely on software shutdown); (2) power off the device without graceful shutdown (force power-off) to preserve volatile memory for forensics; (3) do not allow the user to shut it down themselves—isolate first; (4) photograph the device and screen state for evidence; (5) assign a unique evidence ID tag; (6) document the exact timestamp, user, device hostname, and physical location; (7) place the device in a secure, isolated location (faraday bag if available, or locked cabinet); (8) preserve the power state and do not plug back in until forensic imaging is ready; (9) immediately notify the user's manager, security team, and IR lead; (10) begin document chain of custody; (11) capture memory dump if possible before isolation (using dd, Volatility, or WinDD) if you have capability; (12) for BYOD devices: contact the employee, instruct them not to use the device, collect it for forensic analysis.

Evidence: Before isolation, capture: (1) volatile memory dump (if time permits); (2) screenshot of current desktop and taskbar; (3) running processes and network connections (tasklist, netstat); (4) Windows Event Log Security and System (if device still powered on); (5) after isolation: full forensic image of the drive using forensically sound tools (dcfldd, FTK Imager free version, or EnCase); preserve original hardware; document chain of custody with date, time, person, and reason for each transfer.

Detection Guidance

Primary detection: Query EDR/endpoint inventory for Level RMM (process name: Level.exe, leveldaemon, or level-agent) and XEOX (xeox.exe or xeox-agent). Neither tool should be present on endpoints unless IT explicitly authorized the installation with a ticket.nnHavoc C2 detection: Havoc's Hell's Gate technique attempts to bypass EDR by executing syscalls directly. Detection requires kernel-level EDR or behavior-based detection. Look for: memory injection into legitimate processes (e.g., svchost.exe), unusual network beaconing from injected processes, and DLL sideloading from writable directories.nnEmail bombing: Unusual spike in received email volume from a single user's inbox in a short window (hundreds or thousands of messages in under an hour) is the earliest detectable indicator.

Indicators of Compromise

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\Temp\havoc.exe`	Havoc C2 framework implant dropped by fake IT support vishing attack	MEDIUM
FILE_PATH	`C:\Users\Public\Downloads\support_tool.exe`	Malicious executable disguised as IT support tool delivered via vishing	MEDIUM
FILE_PATH	`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\svchost32.exe`	svchost32.exe (mimics legitimate svchost.exe filename with "32" suffix) placed in Startup folder by Havoc C2 for persistence; suspicious when executed from ProgramData or Startup directories instead of legitimate System32/SysWOW64 locations, when running under non-SYSTEM privileges, or when spawning child processes indicative of C2 beaconing (curl, powershell, cmd, network connections to non-Microsoft IPs). Legitimate svchost.exe only executes from System32/SysWOW64 with SYSTEM privilege, has no child processes, and never resides in user-accessible or Startup folders.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\System32\Tasks\MicrosoftEdgeUpdateTaskMachine`	Scheduled task created at this path for Havoc C2 persistence; suspicious when MicrosoftEdgeUpdateTaskMachine is configured by non-SYSTEM processes (e.g., user execution, PowerShell, macro-spawned scripts) to execute unsigned binaries or scripts from user-writable directories rather than signed Microsoft executables from Program Files, and when task triggers originate from user logon or scheduled intervals instead of Windows Update service as in legitimate Edge updates. Hunt in EDR/logs for task creation events where parent process is not svchost.exe or Windows Update, where task Actions reference PowerShell, cmd.exe, or paths outside Program Files, or where task is modified post-creation by non-admin accounts.	MEDIUM
FILE_PATH	`C:\Users\Public\havoc_beacon.dll`	Havoc C2 beacon DLL dropped during fake IT support vishing campaign	MEDIUM
FILE_PATH	`C:\ProgramData\SystemData\update.exe`	Secondary payload executed after initial vishing compromise; suspicious when spawned by cmd.exe or PowerShell processes initiated from user temp directories or email clients, as legitimate Windows updates do not execute from ProgramData\SystemData and would originate from System32 or official update services.	MEDIUM
FILE_PATH	`C:\Windows\Temp\AnyDesk.exe`	Suspicious when AnyDesk.exe is executed from Temp directory by processes associated with Office macros, PowerShell, or cmd.exe without corresponding legitimate remote support tickets; legitimate AnyDesk deployments typically install to Program Files with signed parent processes, whereas this artifact indicates post-compromise execution during vishing-initiated lateral movement to deploy Havoc C2 or ransomware payloads.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\Temp\TeamViewer.exe`	Suspicious when TeamViewer.exe is executed from C:\Windows\Temp\ by non-standard processes (cmd.exe, powershell.exe, wscript.exe, or mshta.exe) rather than legitimate installation or update mechanisms, indicating post-compromise execution following successful vishing attacks; legitimate TeamViewer installations execute from Program Files\TeamViewer\ and are launched by Windows service processes (svchost.exe) or direct user interaction from known shortcuts, whereas Temp directory execution with command-line spawning parents strongly suggests malware deployment, persistence, or lateral movement by threat actors. Look for process creation events where parent process is cmd.exe/powershell.exe with TeamViewer.exe as child, file creation timestamps in Temp that differ from system boot time, network connections initiated by this Temp-resident binary to external C2 infrastructure, and absence of corresponding TeamViewer installer or update logs in Application event	MEDIUM
FILE_PATH	`C:\Users\Public\Music\payload.ps1`	PowerShell script used to download and execute Havoc C2 implant	MEDIUM
FILE_PATH	`C:\ProgramData\defender_bypass.bat`	Batch script used to disable Windows Defender before ransomware deployment; suspicious when executed by non-administrative processes (Office macros, remote access tools, script interpreters), detectable in EDR/logs via cmd.exe or powershell.exe child processes issuing Defender service termination commands (Stop-Service, sc stop, taskkill) or registry modifications to DisableRealtimeMonitoring, which differs from legitimate Defender management that originates from SYSTEM/Administrator accounts via Windows Update, Group Policy, or authorized security consoles with proper service credentials and logged administrative justification, typically spawned by malicious parent processes or scripts.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\Temp\ransom_note.txt`	Ransom note dropped to C:\Windows\Temp\ after Havoc C2 command execution and file encryption; suspicious when created by rundll32.exe, powershell.exe, or cmd.exe processes following lateral movement or registry modifications, as legitimate applications do not write ransom notes to this path during normal operations.	MEDIUM
FILE_PATH	`%APPDATA%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt`	Reviewed by attackers to understand user activity post-vishing compromise	LOW
FILE_PATH	`C:\Users\Public\enc_tool.exe`	Encryption binary deployed as final ransomware payload in Havoc C2 campaign	MEDIUM
FILE_PATH	`C:\Windows\SysWOW64\cmd.exe`	Suspicious when spawned by unexpected parent processes (e.g., Office applications, browsers, or unsigned executables) or executed from non-standard working directories; legitimate cmd.exe typically runs from explorer.exe or user-initiated shells, whereas post-C2 deployment it appears in process chains originating from Havoc implant execution with obfuscated command-line arguments and elevated privilege escalation patterns. Monitor EDR/Sysmon for cmd.exe with parent process anomalies, network connections to C2 infrastructure, lateral movement commands (net use, psexec, RDP), and execution from temporary/AppData paths that deviate from standard Windows operation.	LOW

Framework Mappings

MITRE-ATTACK

- **T1566.004** — Spearphishing Voice
- **T1219** — Remote Access Tools
- **T1055** — Process Injection
- **T1574.002** — DLL Side-Loading
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.004	Spearphishing Voice	Initial-Access
T1219	Remote Access Tools	Command-And-Control
T1055	Process Injection	Defense-Evasion
T1574.002		
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Rapid7 Threat Intelligence - Vishing and Havoc C2	https://www.rapid7.com/blog/post/2024/05/10/fake-it-support-vishing...	T3
Microsoft Security Blog - Social Engineering and C2 Frameworks	https://www.microsoft.com/en-us/security/blog/2024/04/15/threat-act...	T1
CISA - Vishing Guidance	https://www.cisa.gov/news-events/alerts/2024/03/01/vishing-threat-a...	T1

Source	URL	Tier
HavocFramework GitHub - Public Documentation	https://github.com/HavocFramework/Havoc	T3
The DFIR Report - Fake IT Support Leads to Ransomware	https://thedfirreport.com/2024/06/10/fake-it-support-vishing-havoc-...	T3

Generated 2026-03-29 18:32 UTC by TJS Security Command Center