INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 18:53 UTC

Parallel Persistence: How a Low-Skill Attacker Survived C2 Takedown Using Tailscale and OpenSSH

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0503
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows workstations; Tailscale VPN client; OpenSSH for Windows; Havoc C2 framework; RustDesk; DuckDNS; Backblaze B2; IONOS VPS
Published	2026-06-17T12:00:56
Discovery Source	Rss

Executive Summary

An unidentified French-speaking attacker compromised a small automotive business by deploying the Havoc C2 framework alongside a secondary persistence channel built from legitimate tools: OpenSSH and Tailscale VPN. When the primary command-and-control server was taken offline, the Tailscale/OpenSSH channel kept the attacker inside the network for 18 additional days, undetected. This case demonstrates that removing malware or disrupting C2 infrastructure is not sufficient for remediation when attackers embed themselves using trusted commercial software.

Technical Analysis

The attacker established initial access via the Havoc C2 framework on a Windows workstation, then deployed a parallel persistence layer using OpenSSH for Windows (T1021.004) and Tailscale mesh VPN (T1572), enrolling the compromised host into an attacker-controlled Tailscale network (T1133). This created an encrypted, authenticated tunnel independent of Havoc. Additional tooling included RustDesk for remote desktop access (T1219), DuckDNS for dynamic DNS C2 resolution (T1568.001), and Backblaze B2 for potential data staging or exfiltration (T1567). Scheduled tasks (T1053.005) and Windows services (T1543.003) were used to maintain persistence across reboots. Keylogging (T1056.001), process injection via portable executable injection (T1055.002), and PowerShell execution (T1059.001) were observed. The attacker created local accounts (T1136) and used valid accounts (T1078) to sustain access. Security tool tampering is indicated by T1562.001. CWEs present include CWE-311 (missing encryption of sensitive data at rest), CWE-522 (insufficiently

protected credentials), and CWE-494 (download of code without integrity check). No CVE is associated with this campaign. The Havoc C2 server went offline and returned 18 days later; throughout the outage, the Tailscale/SSH channel remained active, demonstrating that a parallel persistence channel had been established and functioned independently of the primary C2 framework. The attacker is assessed as low-sophistication based on observed tradecraft. Source quality score is 0.64; primary reporting is from The Hacker News (T3) with corroborating community and vendor discussion threads.

Action Checklist

1. Step 1: Containment, Immediately audit all Windows hosts for unauthorized Tailscale client installations and active Tailscale network enrollments. Isolate any host found enrolled in an unrecognized Tailscale network from the corporate network. Block outbound connections to Tailscale coordination servers (controlplane.tailscale.com) at the perimeter firewall for all hosts not explicitly authorized to use Tailscale (CIS 4.4, CIS 4.5, firewall on servers and end-user devices).
2. Step 2: Detection, Query Windows Event Logs for OpenSSH service installation (Event ID 7045, service name 'sshd'), Tailscale service creation, and RustDesk process execution. Search EDR telemetry for processes spawning from OpenSSH or Tailscale binaries. Review scheduled tasks (schtasks /query) and Windows services (sc query type= all) for entries referencing OpenSSH, Tailscale, RustDesk, or DuckDNS update clients. Check DNS query logs for *.duckdns.org resolution. Review Backblaze B2 API traffic for outbound large transfers from non-authorized hosts (NIST AU-2, Event Logging; NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 8.2, Collect Audit Logs).
3. Step 3: Eradication, Uninstall OpenSSH for Windows, Tailscale, RustDesk, and any DuckDNS updater clients from affected hosts that are not explicitly authorized. Remove associated scheduled tasks and Windows services. Delete any attacker-created local accounts identified during investigation (NIST AC-2, Account Management; CIS 5.3, Disable Dormant Accounts). Rotate all credentials on affected hosts, including local administrator passwords and any service account credentials accessible from those hosts (NIST AC-6, Least Privilege; D3-CRO, Credential Rotation). Revoke the compromised host from any Tailscale network it was enrolled in via the Tailscale admin console.
4. Step 4: Recovery, After eradication, confirm no residual Tailscale or OpenSSH processes remain via EDR process inventory. Verify scheduled tasks and services are clean. Re-image affected hosts if forensic confidence is low, as the attacker had extended dwell time and used process injection. Post-remediation, monitor for re-enrollment attempts to Tailscale networks and new SSH service installations for a minimum of 30 days (NIST SI-4, System Monitoring implied via AU-6; CIS 7.1, Vulnerability Management Process). Confirm Backblaze B2 outbound traffic has ceased.
5. Step 5: Post-Incident, This incident exposed a control gap in software allowlisting and outbound network egress filtering. Implement application allowlisting to prevent installation of unauthorized remote access tools including commercial VPN clients (CIS 2.3, Address Unauthorized Software; CIS 4.6, Securely Manage Enterprise Assets and Software). Establish a policy requiring MFA for all remote access channels and administrator accounts (CIS 6.3, CIS 6.4, CIS 6.5; D3-MFA, Multi-factor Authentication). Update incident response playbooks to include enumeration of LotL persistence channels (mesh VPN, SSH, commercial RMM tools) as a required step in all C2 takedown procedures. The core lesson: C2 disruption alone does not constitute remediation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal counsel immediately if forensic analysis confirms data staging or confirmed exfiltration to Backblaze B2 buckets, if the attacker's Tailscale node was enrolled in a tailnet shared with other organizations, or if PII or automotive customer data was accessible from the compromised workstations, triggering potential breach notification obligations under applicable data protection regulations.
Recovery Notes	Given the attacker's 18-day undetected dwell time and confirmed use of process injection associated with the Havoc C2 framework, forensic confidence on affected hosts must be treated as low — re-imaging is the recommended recovery path rather than relying on malware removal alone. Post-recovery monitoring must specifically watch for Tailscale re-enrollment events (new outbound connections to controlplane.tailscale.com or the 100.64.0.0/10 CGNAT range), new OpenSSH service installation events (Windows System Event ID 7045 with service name 'sshd'), and any resumed Backblaze B2 outbound traffic, maintained for a minimum of 30 days given the attacker's demonstrated patience and persistence methodology. Verify the integrity of all local administrator and service account credentials rotated during eradication by confirming no successful authentications occurred against the old credential hashes using Windows Security Event ID 4624 logon success records from the post-rotation window.
Forensic Artifacts	Windows System Event Log (System.evtx) — Event ID 7045 entries for service name 'sshd' (OpenSSH) and 'Tailscale', with binary paths and install timestamps that establish the attacker's initial persistence timeline on each affected host | OpenSSH authorized_keys file at C:\ProgramData\ssh\administrators_authorized_keys and C:\Users\\.ssh\authorized_keys — attacker's RSA/ED25519 public key used to maintain SSH access through the Tailscale tunnel after Havoc C2 takedown | Tailscale local state file at C:\Users\\AppData\Local\Tailscale\tailscaled.state — contains the node private key, tailnet enrollment domain, and peer list that identifies the attacker's mesh VPN infrastructure and any other enrolled nodes | Windows Prefetch files for TAILSCALE.EXE, SSHD.EXE, RUSTDESK.EXE, and HAVOC.EXE (or beacon process name) at C:\Windows\Prefetch\ — provide execution timestamps and run counts confirming the parallel persistence channel activity during the 18-day post-C2-takedown period | Firewall and proxy logs showing outbound HTTPS connections to Backblaze B2 endpoints (f000.backblazeb2.com, s3.us-west-004.backblazeb2.com) and DNS query logs for *.duckdns.org resolutions — establish the data exfiltration timeline and the DDNS-based C2 resolution mechanism used to reach the IONOS VPS

Per-Action IR Details

Step 1: Containment — Immediately audit all Windows hosts for unauthorized Tailscale client installations and active Tailscale network enrollments. Isolate any host found enrolled in an unrecognized Tailscale network from the corporate network. Block outbound connections to Tailscale coordination servers (controlplane.tailscale.com) at the perimeter firewall for all hosts not explicitly authorized to use Tailscale (CIS 4.4, CIS 4.5 — firewall on servers and end-user devices).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), NIST AC-4 (Information Flow Enforcement)

Compensating: Run `Get-Service -Name 'Tailscale'` and `Get-Process -Name tailscale` on all reachable hosts via PowerShell remoting; enumerate installed programs with `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Where-Object {$_.DisplayName -like '*Tailscale*'}`.

On the perimeter firewall or Windows Defender Firewall via GPO, add an outbound block rule for controlplane.tailscale.com (100.64.0.0/10 is the Tailscale CGNAT range — block at both DNS and IP layer). Use `netstat -ano` filtered on established connections to 100.64.0.0/10 to confirm active Tailscale tunnels before isolation.

Evidence: Before isolating any host, capture: (1) full RAM image using WinPmem or DumpIt to preserve injected shellcode and decrypted Havoc C2 artifacts in memory; (2) `Get-NetTCPConnection | Where-Object {$_.RemoteAddress -like '100.64.*'}` output to document active Tailscale peer connections; (3) `netstat -ano` full snapshot; (4) `tasklist /svc` to map PIDs to services including the OpenSSH sshd process; (5) Tailscale local state file at `C:\Users\\AppData\Local\Tailscale\` including node key and network enrollment data. These are volatile and destroyed upon network isolation or service termination.

Step 2: Detection — Query Windows Event Logs for OpenSSH service installation (Event ID 7045, service name 'sshd'), Tailscale service creation, and RustDesk process execution. Search EDR telemetry for processes spawning from OpenSSH or Tailscale binaries. Review scheduled tasks (schtasks /query) and Windows services (sc query type= all) for entries referencing OpenSSH, Tailscale, RustDesk, or DuckDNS update clients. Check DNS query logs for *.duckdns.org resolution. Review Backblaze B2 API traffic for outbound large transfers from non-authorized hosts (NIST AU-2 — Event Logging; NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with the SwiftOnSecurity config (minimum: Event ID 1 process creation, Event ID 3 network connection, Event ID 7 image load) targeting sshd.exe, tailscale.exe, and rustdesk.exe as parent/child process relationships. Query with: `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045 -and $_.Message -like '*sshd*'}` for OpenSSH service install. For DuckDNS beacon detection, parse Windows DNS client cache with `ipconfig /displaydns | findstr duckdns` and review DNS server query logs or Wireshark capture on UDP/53 filtered for `.duckdns.org`. Use Wireshark with display filter `tcp.port == 443 and ip.dst == 180.209.0.0/16` (Backblaze B2 ASN ranges) to identify bulk exfiltration sessions.

Evidence: This is an analysis step that does not alter live state, but volatile artifacts should already have been captured in Step 1 containment. Key evidence sources for this campaign: (1) Windows System Event Log Event ID 7045 at `%SystemRoot%\System32\winevt\Logs\System.evtx` — service name 'sshd' with binary path pointing to `C:\Windows\System32\OpenSSH\sshd.exe` or a non-standard path; (2) Sysmon Event ID 1 logs showing Tailscale or RustDesk process creation with unusual parent processes; (3) Scheduled task XML files under `C:\Windows\System32\Tasks\` referencing DuckDNS updater scripts or Tailscale autostart; (4) OpenSSH `authorized_keys` file at `C:\ProgramData\ssh\administrators_authorized_keys` containing attacker-controlled public key; (5) Backblaze B2 network flows in firewall or proxy logs showing outbound HTTPS to `f000.backblazeb2.com` or `s3.us-west-004.backblazeb2.com` from workstations.

Step 3: Eradication — Uninstall OpenSSH for Windows, Tailscale, RustDesk, and any DuckDNS updater clients from affected hosts that are not explicitly authorized. Remove associated scheduled tasks and Windows services. Delete any attacker-created local accounts identified during investigation (NIST AC-2 — Account Management; CIS 5.3 — Disable Dormant Accounts). Rotate all credentials on affected hosts, including local administrator passwords and any service account credentials accessible from those hosts (NIST AC-6 — Least Privilege; D3-CRO — Credential Rotation). Revoke the compromised host from any Tailscale network it was enrolled in via the Tailscale admin console.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Remove OpenSSH with `Remove-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0`; uninstall Tailscale via `winget uninstall Tailscale` or `msiexec /x` against the cached MSI. Delete scheduled tasks with `schtasks /delete /tn '' /f` for each identified persistence entry. Enumerate and delete attacker-created local accounts with `net user` and `Remove-LocalUser`. Reset local administrator passwords using `net user Administrator ` or deploy Microsoft LAPS if not already in use. For the Tailscale revocation, log into the Tailscale admin console at admin.tailscale.com, locate the compromised node by hostname or Tailscale IP (100.x.x.x), and select 'Expire key' followed by 'Remove device' — this invalidates the node key and removes it from the tailnet immediately.

Evidence: Before credential rotation, service removal, or Tailscale revocation (all of which alter live authentication state), capture: (1) full dump of `C:\ProgramData\ssh\administrators_authorized_keys` and `C:\Users\\.ssh\authorized_keys` to preserve attacker public key for attribution and IOC sharing; (2) Tailscale local state including node private key at `C:\Users\\AppData\Local\Tailscale\tailscaled.state` — this may allow reconstruction of the attacker's tailnet ID; (3) complete output of `net user`, `net localgroup administrators`, and `Get-LocalGroupMember -Group Administrators` to document all attacker-created accounts before deletion; (4) registry export of `HKLM\SYSTEM\CurrentControlSet\Services\sshd` and `HKLM\SYSTEM\CurrentControlSet\Services\Tailscale` to document service configuration; (5) memory image if not already captured — Havoc C2 reflective injection artifacts will not survive process termination.

Step 4: Recovery — After eradication, confirm no residual Tailscale or OpenSSH processes remain via EDR process inventory. Verify scheduled tasks and services are clean. Re-image affected hosts if forensic confidence is low, as the attacker had extended dwell time and used process injection. Post-remediation, monitor for re-enrollment attempts to Tailscale networks and new SSH service installations for a minimum of 30 days (NIST SI-4 — System Monitoring implied via AU-6; CIS 7.1 — Vulnerability Management Process). Confirm Backblaze B2 outbound traffic has ceased.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Verify process cleanliness with `Get-Process | Where-Object {$_.Name -in @('tailscale','sshd','rustdesk')}` run daily via scheduled PowerShell and output to a monitored log file. Create a Sysmon-based Sigma rule alerting on Event ID 7045 (service install) where ServiceName matches 'sshd' or 'Tailscale' — review matches daily for 30 days. Monitor outbound firewall deny logs for connection attempts to 100.64.0.0/10 (Tailscale CGNAT) or controlplane.tailscale.com as an indicator of re-enrollment attempts. For Backblaze B2 verification, run a one-week Wireshark capture on the egress gateway filtered for connections to Backblaze ASN (AS394560) to confirm cessation. Re-image using a verified clean baseline image and validate file integrity of system binaries with `Get-FileHash` against a known-good baseline before returning host to production.

Evidence: Before re-imaging (which destroys all host state), ensure the following have been collected and archived: (1) complete forensic disk image using FTK Imager or `dd` to preserve all attacker artifacts including any staged data awaiting Backblaze B2 exfiltration in `%TEMP%` or attacker-created directories; (2) all relevant Windows Event Logs exported via `wevtutil epl` for System, Security, Application, and Microsoft-Windows-Sysmon/Operational channels; (3) full scheduled task XML export from `C:\Windows\System32\Tasks\`; (4) network capture of any remaining C2 or Tailscale beacon traffic; (5) prefetch files from `C:\Windows\Prefetch\` for TAILSCALE.EXE, SSHD.EXE, and RUSTDESK.EXE to document execution history and timestamps.

Step 5: Post-Incident — This incident exposed a control gap in software allowlisting and outbound network egress filtering. Implement application allowlisting to prevent installation of unauthorized remote access tools including commercial VPN clients (CIS 2.3 — Address Unauthorized Software; CIS 4.6 — Securely Manage Enterprise Assets and Software). Establish a policy requiring MFA for all remote access channels and administrator accounts (CIS 6.3, CIS 6.4, CIS 6.5; D3-MFA — Multi-factor Authentication). Update incident response playbooks to include enumeration of LotL persistence channels (mesh VPN, SSH, commercial RMM tools) as a required step in all C2 takedown procedures. The core lesson: C2 disruption alone does not constitute remediation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), NIST AC-17 (Remote Access)

Compensating: Implement Windows AppLocker or WDAC (Windows Defender Application Control) policies in audit mode first, then enforcement, blocking execution from `%LOCALAPPDATA%`, `%TEMP%`, and non-standard paths where this attacker staged Tailscale and OpenSSH binaries. Export AppLocker event logs (Event ID 8003/8004 in Microsoft-Windows-AppLocker/EXE and DLL) to detect future bypass attempts. For MFA without enterprise tooling, deploy Authelia or Duo Free tier in front of any RDP gateway. Create a standing Sigma detection rule for Sysmon Event ID 1 where Image path contains 'tailscale', 'sshd', 'rustdesk', or 'ngrok' outside of approved installation directories, and review weekly. Document a formal LotL persistence checklist — covering mesh VPN clients, OpenSSH, commercial RMM tools (AnyDesk, RustDesk, TeamViewer), and DDNS updaters — to be executed at every future C2 takedown before declaring remediation complete.

Evidence: No live-state-altering actions occur in this phase; evidence collection is retrospective. Archive for lessons-learned and threat intelligence sharing: (1) attacker SSH public key from `administrators_authorized_keys` — submit to VirusTotal and share with CISA via their automated indicator sharing feed; (2) Tailscale node ID and tailnet domain used by the attacker, extracted from the Tailscale state file, to allow Tailscale Security (security@tailscale.com) to investigate and revoke the attacker's account; (3) DuckDNS hostname(s) resolved during the 18-day dwell period, extracted from DNS query logs, for IOC dissemination; (4) Backblaze B2 bucket identifiers identified in network traffic or attacker scripts for reporting to Backblaze abuse; (5) Havoc C2 beacon configuration extracted from memory image (profile, sleep timers, jitter, C2 host) for MITRE ATT&CK mapping and future detection rule development.

Detection Guidance

Primary detection targets: (1) Windows Event ID 7045, new service installation with service names 'sshd', 'Tailscale', 'RustDesk', or 'WinSSHD'. (2) Scheduled task creation via schtasks referencing OpenSSH, Tailscale, or RustDesk binaries, query with: schtasks /query /fo LIST /v | findstr /i 'tailscale rustdesk ssh'. (3) Outbound DNS queries to *.duckdns.org from workstation-class hosts (non-server assets). (4) Outbound TCP 41641 (Tailscale default UDP/TCP) or HTTPS traffic to controlplane.tailscale.com, login.tailscale.com. (5) Outbound port 22 from workstations to any external IP, particularly to IONOS VPS address ranges (AS8560). (6) PowerShell execution with encoded commands (Event ID 4104, Script Block Logging) or invocations of Invoke-Expression. (7) Process injection indicators: svchost or legitimate process spawning unexpected child processes. (8) Backblaze B2 API traffic (b2api.us-west-002.backblazeb2.com or similar) from hosts with no authorized backup agent. Behavioral IOC: a host that shows no Havoc beacon activity for an extended period but continues to generate outbound SSH or Tailscale traffic is a strong indicator of parallel persistence surviving C2 disruption.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`*.duckdns.org`	DuckDNS dynamic DNS used for C2 resolution; workstation DNS queries to this domain are anomalous	MEDIUM

Type	Value	Context	Confidence
DOMAIN	`controlplane.tailscale.com`	Tailscale coordination server; outbound connections from unauthorized hosts indicate possible mesh VPN enrollment	MEDIUM
DOMAIN	`login.tailscale.com`	Tailscale authentication endpoint; enrollment of attacker-controlled Tailscale node	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1053** — Scheduled Task/Job
- **T1056.001** — Keylogging
- **T1055.002** — Portable Executable Injection
- **T1136** — Create Account
- **T1562.001** — Disable or Modify Tools
- **T1133** — External Remote Services
- **T1059.001** — PowerShell
- **T1071.001** — Web Protocols
- **T1021.004** — SSH
- **T1572** — Protocol Tunneling
- **T1568.001** — Fast Flux DNS
- **T1053.005** — Scheduled Task
- **T1567** — Exfiltration Over Web Service
- **T1543.003** — Windows Service
- **T1059.005** — Visual Basic
- **T1078** — Valid Accounts
- **T1027.009** — Embedded Payloads

NIST-800-53R5

- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1219	Remote Access Tools	Command-And-Control
T1053	Scheduled Task/Job	Execution
T1056.001	Keylogging	Collection
T1055.002	Portable Executable Injection	Defense-Evasion
T1136	Create Account	Persistence
T1562.001	Disable or Modify Tools	Defense-Evasion
T1133	External Remote Services	Persistence
T1059.001	PowerShell	Execution
T1071.001	Web Protocols	Command-And-Control
T1021.004	SSH	Lateral-Movement
T1572	Protocol Tunneling	Command-And-Control

Technique ID	Technique Name	Tactic
T1568.001	Fast Flux DNS	Command-And-Control
T1053.005	Scheduled Task	Execution
T1567	Exfiltration Over Web Service	Exfiltration
T1543.003	Windows Service	Persistence
T1059.005	Visual Basic	Execution
T1078	Valid Accounts	Defense-Evasion
T1027.009	Embedded Payloads	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/junior-hacker-used-tailscale-and....	T3
Security and experience on Rustdesk server - Reddit	https://www.reddit.com/r/rustdesk/comments/1tsdo1j/security_and_exp...	T3
Security Issues, Virustotal marked as malicious Software #7146	https://github.com/rustdesk/rustdesk/discussions/7146	T3
Rustdesk-server-pro CVEs and Security Vulnerabilities - OpenCVE	https://app.opencve.io/cve/?vendor=rustdesk-server-pro	T3
ChromeLoader, Telegram, RustDesk, & Tailscale: Incident Analysis	https://blackpointcyber.com/blog/chromeloader-telegram-rustdesk-tai...	T3

Generated 2026-06-17 18:53 UTC by TJS Security Command Center