INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 08:39 UTC

CloudZ RAT Abuses Windows Phone Link to Intercept OTPs Without Touching the Mobile Device

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0277
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows 10, Microsoft Windows 11, Microsoft Phone Link application; ConnectWise ScreenConnect (abused as delivery/access vector)
Published	2026-05-06T04:34:00
Discovery Source	Rss

Executive Summary

A newly identified remote access trojan called CloudZ exploits the legitimate Windows Phone Link application to silently harvest one-time passwords synced from paired Android devices, bypassing SMS-based two-factor authentication without touching the mobile device. Organizations using Windows 10 or 11 with Phone Link enabled are exposed to credential theft that most endpoint detection tools will not catch. The business risk is account takeover across any system protected by SMS-based MFA, including email, banking portals, VPNs, and enterprise SaaS platforms.

Technical Analysis

CloudZ is a previously undisclosed remote access trojan, active since at least January 2026 per Cisco Talos research, that deploys a custom plugin named Pheno to query the local SQLite database maintained by the Windows Phone Link application. Phone Link syncs SMS messages from paired Android devices to the Windows host; CloudZ reads OTPs from this database without network interaction with the mobile device. ConnectWise ScreenConnect is referenced as an abused or spoofed delivery/access vector, consistent with broader RMM-abuse patterns documented by Microsoft (T1219). No CVE has been assigned. Applicable CWEs: CWE-522 (Insufficiently Protected Credentials), CWE-312 (Cleartext Storage of Sensitive Information), CWE-494 (Download of Code Without Integrity Check). MITRE ATT&CK techniques include T1555/T1555.003 (Credentials from Password Stores), T1005 (Data from Local System), T1083 (File and Directory Discovery), T1539 (Steal Web Session Cookie), T1219 (Remote Access Software), T1036/T1036.005 (Masquerading),

T1059/T1059.001 (Command and Scripting Interpreter: PowerShell), T1053.005 (Scheduled Task), T1056/T1056.001 (Keylogging), T1113 (Screen Capture), T1105 (Ingress Tool Transfer), T1574 (Hijack Execution Flow), T1071.001 (Web Protocols C2), and T1132.001 (Standard Encoding). The SQLite read path is not monitored by most EDR or AV solutions, making detection with conventional signature-based defenses unlikely. No patch is available; mitigation is configuration- and detection-based. Attribution: unknown as of 2026-05-06.

Action Checklist

1. Step 1: Containment, Audit all Windows 10/11 endpoints for active Windows Phone Link pairings. Disable or unpair Phone Link on systems that do not have a documented business requirement for it, particularly on privileged workstations and systems with access to sensitive accounts. Block ScreenConnect binaries from unauthorized sources using application control, EDR, or allowlisting policies.
2. Step 2: Detection, Query endpoint telemetry for SQLite database reads targeting the Phone Link data path (%LOCALAPPDATA%\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState\) by non-Microsoft processes. Hunt for execution of unsigned binaries with ScreenConnect-lookalike names (T1036.005). Review scheduled task creation events (Windows Event ID 4698) and PowerShell script block logging (Event ID 4104) for anomalous activity. Alert on outbound connections from Phone Link-adjacent processes to non-Microsoft infrastructure.
3. Step 3: Eradication, Remove CloudZ and Pheno binaries if identified; no vendor-issued removal tool is available as of this writing. Disable the Windows Phone Link feature via Group Policy (User Configuration > Administrative Templates > Windows Components) on endpoints where it is not required. Revoke and rotate any credentials or session tokens accessible via accounts that rely on SMS-based OTP on affected systems.
4. Step 4: Recovery, Confirm Phone Link is disabled or unpaired on affected hosts and verify via Group Policy Results or endpoint management console. Monitor previously exposed accounts for unauthorized access attempts for at least 30 days post-remediation. Re-validate MFA enrollment for affected users and migrate from SMS-based OTP to TOTP apps or hardware tokens (FIDO2/WebAuthn) where feasible.
5. Step 5: Post-Incident, Document the detection gap: many EDR tools lack native detection for SQLite reads from cross-device sync applications, creating a detection gap. Submit a use-case request to your EDR vendor for coverage of this data path. Review RMM tool allowlists to ensure only approved ScreenConnect instances are permitted. Assess broader MFA strategy: SMS-based OTP should be treated as a weak second factor per NIST SP 800-63B, and migration to phishing-resistant authenticators should be prioritized.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to CISO and legal/privacy counsel if forensic analysis of the Phone Link SQLite database or Windows Security Event logs confirms that SMS-based OTPs were successfully read by CloudZ on any host with access to financial systems, healthcare records, PII, or privileged administrative accounts — any confirmed OTP interception on such systems triggers breach notification assessment obligations under applicable regulations (HIPAA, PCI DSS, state breach notification laws) and constitutes an active account takeover risk requiring emergency credential rotation across all downstream systems.
Recovery Notes	After completing eradication, verify Phone Link disablement on 100% of in-scope endpoints via 'gpresult /r' and confirm no Microsoft.YourPhone AppX package processes are running using 'Get-Process | Where-Object {$_.Name -like "*YourPhone*"}'. Monitor all accounts whose SMS-based OTPs were accessible on affected hosts for a minimum of 30 days post-remediation, specifically watching for impossible-travel logins, off-hours access, and MFA prompt fatigue patterns in identity provider logs, since OTPs intercepted prior to containment may have already been used to establish persistent session tokens. Treat SMS OTP migration to TOTP or FIDO2 as a time-bound remediation action, not a deferred improvement, given that CloudZ demonstrates an active threat actor capability to silently harvest SMS-based second factors from Windows endpoints without any mobile device interaction.
Forensic Artifacts	Phone Link LocalState SQLite databases at %LOCALAPPDATA%\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState\ (e.g., FantasyPhone.db) — will contain message records including intercepted OTP SMS content with timestamps that can be correlated against account access logs to confirm which OTPs were harvested | Windows Prefetch files at C:\Windows\Prefetch\ for CloudZ and Pheno binary names — will record execution timestamps and loaded DLLs even if the attacker deleted the primary binaries post-exfiltration | Sysmon Event ID 11 (FileCreate) and Event ID 10 (ProcessAccess) logs targeting the Microsoft.YourPhone_8wekyb3d8bbwe package directory — will identify the non-Microsoft process name and full path used by CloudZ to access the Phone Link SQLite database | Windows Security Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) logs — will reveal CloudZ persistence mechanism including the command line, trigger type, and run-as account used to maintain access across reboots | Network connection logs from Sysmon Event ID 3 (Network Connection) or Windows Firewall logs filtered on processes adjacent to Phone Link or bearing ScreenConnect-lookalike names — will expose CloudZ C2 infrastructure IPs and domains used to exfiltrate harvested OTPs and receive RAT commands

Per-Action IR Details

Step 1: Containment — Audit all Windows 10/11 endpoints for active Windows Phone Link pairings. Disable or unpair Phone Link on systems that do not have a documented business requirement for it, particularly on privileged workstations and systems with access to sensitive accounts. Block ScreenConnect binaries from unauthorized sources at the endpoint firewall or application control layer.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and block ongoing attacker access vectors before eradication begins

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality) — restrict Phone Link to documented business use only, NIST SI-4 (System Monitoring) — establish visibility into ScreenConnect binary execution at the endpoint layer, CIS 4.4 (Implement and Manage a Firewall on Servers) — block unauthorized ScreenConnect binaries via host-based application control, CIS 2.3 (Address Unauthorized Software) — treat unapproved ScreenConnect instances as unauthorized software requiring immediate removal, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — prioritize Phone Link disablement on privileged workstations first

Compensating: For teams without enterprise MDM or SCCM: run the following PowerShell one-liner across all endpoints via PSRemoting to enumerate active Phone Link pairings — 'Get-AppxPackage -Name Microsoft.YourPhone | Select-Object Name,PackageFullName,InstallLocation'. To block ScreenConnect lookalikes without EDR, deploy a Software Restriction Policy or AppLocker rule denying execution of any binary matching the ScreenConnect naming convention (ScreenConnect.ClientService.exe, ScreenConnect.WindowsClient.exe) from %TEMP%, %APPDATA%, or user-writable paths. Use Sysmon Event ID 1 (Process Create) with a filter on Image paths outside of the approved ScreenConnect installation directory to detect masquerading binaries (MITRE T1036.005).

Evidence: Before disabling Phone Link, capture a forensic snapshot of the Phone Link local SQLite database at %LOCALAPPDATA%\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState\ — specifically the 'FantasyPhone.db' and any .db files present — to preserve evidence of OTP messages that may have been harvested. Also collect a timestamped registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Uninstall and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall to document ScreenConnect installation artifacts before removal. Capture running process list (tasklist /v /fo csv) and active network connections (netstat -bno) to correlate Phone Link-adjacent processes with outbound C2 connections prior to containment.

Step 2: Detection — Query endpoint telemetry for SQLite database reads targeting the Phone Link data path (%LOCALAPPDATA%\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState\) by non-Microsoft processes. Hunt for execution of unsigned binaries with ScreenConnect-lookalike names (T1036.005). Review scheduled task creation events (Windows Event ID 4698) and PowerShell script block logging (Event ID 4104) for anomalous activity. Alert on outbound connections from Phone Link-adjacent processes to non-Microsoft infrastructure.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across endpoint telemetry, log sources, and network traffic to establish scope of CloudZ compromise

Controls: NIST SI-4 (System Monitoring) — monitor file system access to the Phone Link LocalState path by non-Microsoft processes, NIST AU-2 (Event Logging) — ensure Windows Security, Sysmon, and PowerShell operational logs are enabled and capturing the relevant event IDs, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — actively review logs for CloudZ-specific IOC patterns rather than waiting for automated alerting, NIST IR-5 (Incident Monitoring) — track and document all confirmed and suspected CloudZ-related events across the environment, CIS 8.2 (Collect Audit Logs) — validate that audit logging is enabled on all Windows 10/11 endpoints prior to hunt, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — integrate CloudZ IOCs into ongoing threat hunt cadence

Compensating: Without a SIEM, deploy Sysmon with SwiftOnSecurity's config (minimum) and add a custom rule targeting FileCreate and RawAccessRead events on the path '*\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState*' by Image paths not matching '*\WindowsApps*' or '*\Microsoft.YourPhone*'. Use the following PowerShell to hunt locally for recent SQLite access to the Phone Link path: 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Message -like "*YourPhone*" -and $_.Id -eq 11}'. For scheduled task hunting without a SIEM, run 'schtasks /query /fo LIST /v | findstr /i "Task Name\|Status\|Run As User\|Task To Run"' and flag any tasks executing from %TEMP% or %APPDATA%. Use the community Sigma rule for T1036.005 (Masquerading: Match Legitimate Name or Location) converted to Windows Event Log format as a manual hunt query against Sysmon Event ID 1 logs.

Evidence: Collect Windows Security Event Log entries for Event ID 4698 (Scheduled Task Created) and 4104 (PowerShell Script Block) from the suspected compromise window before any remediation clears volatile state. Export Sysmon Event ID 1 (Process Create), Event ID 11 (FileCreate), and Event ID 3 (Network Connection) filtered on processes accessing the Phone Link LocalState directory or bearing ScreenConnect-lookalike binary names. Capture the Windows Prefetch files (C:\Windows\Prefetch\) for CloudZ and Pheno binary names — prefetch entries will record execution timestamps and file paths even if the binaries have been deleted. Pull DNS client cache ('ipconfig /displaydns') and browser history from affected hosts to identify any C2 domains contacted by CloudZ during the OTP exfiltration phase.

Step 3: Eradication — Remove CloudZ and Pheno binaries if identified; no vendor-issued removal tool is available as of this writing. Disable the Windows Phone Link feature via Group Policy (User Configuration > Administrative Templates > Windows Components) on endpoints where it is not required. Revoke and rotate any credentials or session tokens accessible via accounts that rely on SMS-based OTP on affected systems.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all components of the CloudZ RAT from the environment, eliminate the Phone Link attack surface, and invalidate any credentials compromised via OTP interception

Controls: NIST IR-4 (Incident Handling) — execute eradication as a documented phase with verification steps, not ad hoc binary deletion, NIST SI-2 (Flaw Remediation) — treat the absence of Phone Link Group Policy hardening as a configuration flaw requiring remediation, NIST SI-3 (Malicious Code Protection) — scan for CloudZ and Pheno binaries using updated signatures or YARA rules across all endpoints in scope, NIST IA-5 (Authenticator Management) — revoke and rotate credentials and session tokens for all accounts whose SMS OTPs may have been intercepted, CIS 4.6 (Securely Manage Enterprise Assets and Software) — enforce Phone Link disablement via Group Policy as a configuration management action, CIS 5.2 (Use Unique Passwords) — force password rotation on all accounts where SMS-based OTP was the second factor on affected hosts

Compensating: Without enterprise AV with current CloudZ signatures, write a YARA rule targeting CloudZ and Pheno binary characteristics (PE header anomalies, known strings, or import hash if available from threat intel) and scan using YARA from the command line: 'yara -r cloudz_rule.yar C:\Users\'. For scheduled task persistence removal, enumerate and diff all scheduled tasks against a known-good baseline using 'schtasks /query /fo CSV > current_tasks.csv' and compare against pre-incident exports. To disable Phone Link via GPO without enterprise tooling, use Local Group Policy Editor (gpedit.msc) on each host: navigate to User Configuration > Administrative Templates > Windows Components > Phone Link and set 'Turn off Phone Link' to Enabled. For credential rotation without a PAM tool, use 'net user [username] [newpassword] /domain' for domain accounts and force re-enrollment of MFA factors through the identity provider admin console.

Evidence: Before deleting CloudZ and Pheno binaries, collect full file hashes (SHA-256) using 'Get-FileHash -Algorithm SHA256 [filepath]', capture file metadata (creation, modification, access timestamps via 'fsutil usn readjournal'), and create forensic copies to a write-protected external drive or isolated network share for later analysis. Preserve any scheduled task XML definitions associated with CloudZ persistence before deletion ('schtasks /query /xml > [taskname].xml'). Document all accounts whose sessions were active on the affected host during the suspected compromise window by reviewing Windows Security Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) logs — these define the mandatory scope for credential rotation.

Step 4: Recovery — Confirm Phone Link is disabled or unpaired on affected hosts and verify via Group Policy Results or endpoint management console. Monitor previously exposed accounts for unauthorized access attempts for at least 30 days post-remediation. Re-validate MFA enrollment for affected users and migrate from SMS-based OTP to TOTP apps or hardware tokens (FIDO2/WebAuthn) where feasible.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to verified-clean operational state, confirm Phone Link attack surface is eliminated, and validate that OTP interception capability has been neutralized

Controls: NIST IR-4 (Incident Handling) — verify recovery actions are complete and documented before closing the incident, NIST IA-5 (Authenticator Management) — re-validate MFA enrollment and enforce migration away from SMS-based OTP per NIST SP 800-63B guidance, NIST CA-7 (Continuous Monitoring) — maintain 30-day post-remediation monitoring window on previously exposed accounts for unauthorized access indicators, NIST SI-6 (Security and Privacy Function Verification) — verify Phone Link Group Policy enforcement is applied and effective via 'gpresult /h report.html', CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce TOTP or FIDO2 MFA re-enrollment for all accounts previously protected by SMS-based OTP on affected systems, CIS 7.2 (Establish and Maintain a Remediation Process) — document the SMS-to-TOTP migration as a tracked remediation item with assigned ownership and deadline

Compensating: Without an enterprise identity platform, verify Phone Link GPO enforcement by running 'gpresult /r' on each remediated host and confirming the 'Turn off Phone Link' policy appears under Applied Group Policy Objects. For 30-day account monitoring without a SIEM, configure Windows Security audit policy on domain controllers to log Event

ID 4625 (Failed Logon) and 4776 (Credential Validation) and export these daily via scheduled PowerShell task to a centralized CSV for manual review. For MFA migration without an enterprise SSO platform, use free authenticator apps (Microsoft Authenticator, Google Authenticator) or low-cost FIDO2 hardware tokens (YubiKey Security Key NFC) and re-enroll affected users through each application's MFA settings directly.

Evidence: Run 'gpresult /h gpresult_report.html' on each remediated host and archive the output as verification evidence that Phone Link policy is applied. Collect Windows Security Event ID 4624 and 4625 logs from domain controllers covering the 30-day monitoring window and flag any successful or failed logons from geographic locations, IP ranges, or time-of-day patterns inconsistent with the affected user's baseline. Document the pre- and post-remediation MFA method for each affected account in the incident record to demonstrate the SMS-to-TOTP migration was completed and to support any regulatory reporting obligations.

Step 5: Post-Incident — Document the detection gap: most EDR tools do not alert on SQLite database reads from cross-device sync applications. Submit a use-case request to your EDR vendor for coverage of this data path. Review RMM tool allowlists to ensure only approved ScreenConnect instances are permitted. Assess broader MFA strategy: SMS-based OTP should be treated as a weak second factor per NIST SP 800-63B, and migration to phishing-resistant authenticators should be prioritized.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned analysis focused on the Phone Link SQLite monitoring gap and the ScreenConnect delivery vector, and use findings to drive detection engineering and MFA policy improvements

Controls: NIST IR-4 (Incident Handling) — update the incident response plan to include Phone Link and cross-device sync app data paths as monitored attack surfaces, NIST IR-8 (Incident Response Plan) — revise IR plan to add CloudZ/Phone Link detection use case and ScreenConnect RMM abuse scenario, NIST SI-5 (Security Alerts, Advisories, and Directives) — formalize intake of threat intel on RAT campaigns abusing legitimate Windows features into the advisory review process, NIST RA-5 (Vulnerability Monitoring and Scanning) — incorporate Phone Link attack surface into ongoing risk assessment and configuration review cycles, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — add SQLite access monitoring for cross-device sync application data paths as a standing hunt use case, CIS 6.3 (Require MFA for Externally-Exposed Applications) — document SMS OTP deprecation plan referencing NIST SP 800-63B AAL2 requirements and set a target completion date

Compensating: Without an EDR vendor support portal, submit the Phone Link SQLite monitoring gap as a public feature request or community detection rule: author a Sigma rule targeting Sysmon Event ID 11 (FileCreate) and Event ID 10 (ProcessAccess) on the path '%LOCALAPPDATA%\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState\' by non-Microsoft-signed processes and publish to the SigmaHQ community repository for peer validation. For ScreenConnect allowlisting without enterprise tooling, maintain a plaintext registry of approved ScreenConnect instance URLs and relay codes in your asset management system and audit quarterly using 'Get-WinEvent' queries against Sysmon process creation logs. Use osquery with the scheduled_tasks and processes tables to build a standing post-incident hunt query for future ScreenConnect masquerading attempts: 'SELECT name, action, enabled FROM scheduled_tasks WHERE action LIKE "%ScreenConnect%"'.

Evidence: Archive the complete incident timeline, all forensic artifacts collected during Steps 1-4, EDR alert (or non-alert) records for the compromise window, and the GPO verification reports as the post-incident evidence package — this package supports both internal lessons-learned and any regulatory breach notification assessment. Document the specific EDR product version and configuration that failed to alert on the Phone Link SQLite reads, including the detection policy settings active at the time, to provide concrete data for the vendor use-case submission. Retain the YARA scan results and Sysmon log exports for a minimum of 12 months per NIST AU-11 (Audit Record Retention) requirements to support any subsequent legal, regulatory, or threat intelligence sharing needs.

Detection Guidance

Primary detection path: monitor for file read access to the Phone Link SQLite database at %LOCALAPPDATA%\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalState\ by processes other than Microsoft.YourPhone or Windows system processes. In environments with Sysmon deployed, Event ID 11 (FileCreate) and ID 23 (FileDelete) combined with process ancestry analysis can surface anomalous database access. Use Sysmon Event ID 1 (Process Create) to flag execution of ScreenConnect-named binaries not originating from approved installation paths. Windows Event ID 4698 flags new scheduled task creation, relevant to T1053.005 persistence. PowerShell script block logging (Event ID 4104) should be enabled and reviewed for encoded or obfuscated execution consistent with T1059.001. Network-layer: alert on outbound HTTP/S traffic from processes with no established network baseline, particularly those with ScreenConnect-adjacent names. No confirmed public IOC list (IPs, domains, hashes) has been released as of the item date; treat absence of published IOCs as a gap, not clearance.

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery
- **T1555** — Credentials from Password Stores
- **T1059** — Command and Scripting Interpreter
- **T1059.001** — PowerShell
- **T1132.001** — Standard Encoding
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1539** — Steal Web Session Cookie
- **T1219** — Remote Access Tools
- **T1005** — Data from Local System
- **T1105** — Ingress Tool Transfer
- **T1113** — Screen Capture
- **T1574** — Hijack Execution Flow
- **T1071.001** — Web Protocols
- **T1056** — Input Capture
- **T1036** — Masquerading
- **T1555.003** — Credentials from Web Browsers
- **T1056.001** — Keylogging
- **T1053.005** — Scheduled Task

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

- **CM-3** — Configuration Change Control
- **IA-5** — Authenticator Management

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1555	Credentials from Password Stores	Credential-Access
T1059	Command and Scripting Interpreter	Execution
T1059.001	PowerShell	Execution
T1132.001	Standard Encoding	Command-And-Control
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1219	Remote Access Tools	Command-And-Control

Technique ID	Technique Name	Tactic
T1005	Data from Local System	Collection
T1105	Ingress Tool Transfer	Command-And-Control
T1113	Screen Capture	Collection
T1574	Hijack Execution Flow	Persistence
T1071.001	Web Protocols	Command-And-Control
T1056	Input Capture	Collection
T1036	Masquerading	Defense-Evasion
T1555.003	Credentials from Web Browsers	Credential-Access
T1056.001	Keylogging	Collection
T1053.005	Scheduled Task	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/windows-phone-link-exploited-by-c...	T3
CISA Flags Actively Exploited ScreenConnect, Windows Flaws	https://britec.com/2026/04/cisa-flags-actively-exploited-screenconn...	T3
U.S. CISA adds Microsoft Windows Shell and ConnectWise ...	https://securityaffairs.com/191442/security/u-s-cisa-adds-microsoft...	T3
Screenconnect / connectwise was installed by a scammer - Reddit	https://www.reddit.com/r/ConnectWise/comments/wlx2xu/screenconnect_...	T3
Signed malware impersonating workplace apps deploys RMM ...	https://www.microsoft.com/en-us/security/blog/2026/03/03/signed-mal...	T1

Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-06 08:39 UTC by TJS Security Command Center