INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

Tax Season RMM Abuse: Threat Actors Pivot to Persistent Access as 29,000 Users Hit in Coordinated IRS Phishing Wave

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0085
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft 365, ConnectWise ScreenConnect, Datto RMM, SimpleHelp, Amazon SES (abused for delivery), SmartVault (impersonated), Cloudflare (abused for evasion)
Published	2026-03-23
Discovery Source	Rss

Executive Summary

A coordinated IRS-themed phishing campaign documented by Microsoft Threat Intelligence on February 10, 2026, targeted more than 29,000 users across 10,000 organizations during tax season. Attackers harvested Microsoft 365 credentials and then installed legitimate remote monitoring and management tools, ConnectWise ScreenConnect, Datto RMM, and SimpleHelp, to maintain persistent backdoor access without deploying traditional malware. The business risk is significant: compromised RMM tools grant attackers ongoing remote control of affected endpoints, bypassing most endpoint and email security controls, and the signed nature of these tools means they are whitelisted in many environments.

Technical Analysis

Campaign origin: Microsoft Threat Intelligence, first documented February 10, 2026. Attack chain uses two PhaaS platforms, Energy365 and SneakyLog/Kratos, for credential harvesting against Microsoft 365 accounts. Initial delivery abuses Amazon SES for high-reputation email sending; lures impersonate IRS communications and SmartVault branding. Credential-harvesting pages exploit Cloudflare anti-bot features (CWE-1021: UI Redressing; CWE-345: Insufficient Verification of Data Authenticity) to obstruct automated analysis and evade URL reputation scanning. Post-credential theft, attackers deploy signed RMM binaries, ConnectWise ScreenConnect, Datto RMM, SimpleHelp, via user-executed links or attachments (T1204.001, T1204.002), establishing persistent remote access (T1219) through tools already whitelisted in most enterprise environments. Valid account abuse (T1078, CWE-290) allows lateral movement without triggering

authentication anomaly alerts. Web protocols are used for C2 (T1071.001). Additional observed techniques: spearphishing link (T1566.001), spearphishing attachment (T1566.002), external remote services (T1133), web credential forging (T1598.002), keylogging/input capture (T1056.003), PowerShell execution (T1059.001), masquerading via signed binaries (T1036.005), session cookie theft (T1539), obfuscation (T1027), adversary-in-the-middle (T1557), and establishment of email accounts and infrastructure (T1585.002, T1583.001). No CVE assigned. Relevant CWEs: CWE-1021, CWE-287, CWE-345, CWE-290. Huntress reports a 277% year-over-year increase in RMM tool abuse as context for the broader trend. No patch applicable; this is a tool-abuse and social engineering campaign.

Action Checklist

1. Step 1, Immediate: Audit authorized RMM tools across your environment. Identify any ConnectWise ScreenConnect, Datto RMM, or SimpleHelp instances not provisioned by your IT or security team. Terminate unauthorized sessions and isolate affected endpoints.
2. Step 2, Detection: Query email gateway and Microsoft 365 logs for messages delivered via Amazon SES containing IRS, SmartVault, or tax-related lures. Search endpoint logs for execution of ScreenConnect, Datto RMM, or SimpleHelp binaries not launched from approved management infrastructure. Review sign-in logs for Microsoft 365 accounts showing successful authentication followed by RMM tool installation within the same session window.
3. Step 3, Assessment: Inventory all RMM software present on endpoints using EDR telemetry or asset management tooling. Confirm each instance is authorized, managed, and connected only to your organization's approved tenant or relay. Cross-reference against your approved software list and flag any gaps.
4. Step 4, Communication: Notify affected users whose credentials may have been harvested. Issue a targeted security awareness alert to all staff about IRS-themed phishing during tax season. Escalate to legal and compliance if credential compromise is confirmed, given potential data access implications.
5. Step 5, Long-term: Implement application allowlisting or software restriction policies to block unauthorized RMM binary execution. Enforce phishing-resistant MFA (FIDO2/hardware token) on all Microsoft 365 accounts. Establish a formal RMM governance policy defining approved tools, approved tenants, and mandatory enrollment procedures. Review Cloudflare-proxied URL handling in your secure email gateway configuration.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to C-suite and external incident response firm if credential harvest affects >500 users, if RMM persistence is detected on domain controllers or sensitive file servers, or if forensic analysis reveals lateral movement to restricted data repositories.

Recovery Notes	Post-containment: (1) Force password reset for all affected M365 accounts via Azure AD Bulk Operations and require MFA re-enrollment. (2) Revoke all active Microsoft 365 sessions for compromised accounts via 'Revoke-AzureADUserAllRefreshToken' PowerShell cmdlet to terminate any residual attacker access. (3) Audit M365 delegated admin access and app consent grants for the 14-day window around compromise; remove any suspicious OAuth app registrations via 'Remove-AzureADApplication'. (4) Conduct forensic analysis of isolated endpoints to confirm RMM removal and absence of additional persistence mechanisms (scheduled tasks, WMI event subscriptions, registry run keys); rebuild from known-good backup if evidence of lateral movement is found.
Forensic Artifacts	Windows Event Log Security (Event ID 4624 logons, 4688 process creation, 4720 user creation) — extract via 'wevtutil qe Security /f:text > security_log.txt' | Windows Event Log System (Event ID 7034 service unexpected termination, 7045 new service installation) — document legitimate vs. suspicious RMM service installations | Registry HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall and HKCU\Software\Microsoft\Windows\CurrentVersion\Uninstall — identify RMM GUIDs, install dates, uninstall strings | M365 Azure AD sign-in logs and audit logs (Azure Portal > Azure AD > Audit logs) — correlate successful logons with RMM binary execution timestamps | RMM application logs in C:\ProgramData\[Vendor]\logs\ or %APPDATA%\[Vendor]\logs\ — document connection timestamps, user names used to connect, relay server addresses, session duration | Email gateway message trace logs and mail flow records — identify phishing source IP, SES-spoofed sender addresses, recipient count, keyword matches | Network traffic capture (PCAP) from RMM processes — document C&C domain names, IP addresses, TLS certificate details, HTTP User-Agent strings for attribution | File system timeline (MFT analysis) — establish file creation/modification times for RMM binaries and supporting files to correlate with phishing delivery date | Browser history and download artifacts (%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\, %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History) — document phishing link clicks and RMM installer download sources

Per-Action IR Details

Step 1 — Immediate: Audit authorized RMM tools across your environment. Identify any ConnectWise ScreenConnect, Datto RMM, or SimpleHelp instances not provisioned by your IT or security team. Terminate unauthorized sessions and isolate affected endpoints.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3

Controls: NIST IR-4(1), CIS 2.4, NIST 800-53 SI-7

Compensating: Without EDR: query Windows Registry HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall for ScreenConnect, Datto, or SimpleHelp GUIDs; cross-reference against IT-maintained approved software spreadsheet. Use 'tasklist /v' and 'wmic process list full' to capture running processes; isolate endpoints by unplugging network cable or disabling NIC via BIOS if no network control available. Manually terminate process via Task Manager or 'taskkill /PID [pid] /F' command.

Evidence: Capture before isolation: (1) Registry export of HKLM\Software\Microsoft (reg export command); (2) Active process list with parent process ID and command line via 'wmic process list full > process_snapshot.txt'; (3) File metadata for RMM binaries (creation time, modification time, digital signature via 'sigcheck -nobanner [binary_path]'); (4) Network connections via 'netstat -anob' or 'Get-NetTCPConnection | Select-Object LocalAddress, LocalPort, RemoteAddress, RemotePort, State, OwningProcess'; (5) RMM application logs if present (typically C:\ProgramData\[RMM_vendor]\logs\).

Step 2 — Detection: Query email gateway and Microsoft 365 logs for messages delivered via Amazon SES containing IRS, SmartVault, or tax-related lures. Search endpoint logs for execution of ScreenConnect, Datto

RMM, or SimpleHelp binaries not launched from approved management infrastructure. Review sign-in logs for Microsoft 365 accounts showing successful authentication followed by RMM tool installation within the same session window.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1

Controls: NIST 800-53 AU-12, NIST 800-53 CA-7, CIS 8.2, CIS 8.8

Compensating: M365 alternative (no SIEM): export Azure AD sign-in logs via Azure Portal > Azure AD > Sign-in logs > filter by date range, apply filter 'ResourceDisplayName equals Office 365 Exchange Online' and 'Status equals Success', export to CSV. Cross-reference timestamps with Windows Event Log 4688 (process creation) on target endpoints for RMM binary execution within 15 minutes. Email gateway alternative (no SIEM): enable mail flow logs in Exchange admin center, search message trace for 'from:*amazonaws.com' OR 'from:amazon.com' combined with keyword 'IRS' or 'tax' or 'refund'; export results to CSV. For on-premises mail: query Exchange message tracking logs via 'Get-MessageTrackingLog -Start [date] -End [date] -Sender *@*.amazonaws.com -ResultSize unlimited'.

Evidence: Capture before analysis: (1) M365 Azure AD sign-in logs for 14 days prior to detection (export via Azure Portal or Graph API); (2) Windows Event Log Security (4624 logons, 4688 process creation) filtered for RMM binary names — export via 'wevtutil qe Security /q:"Event[System[(EventID=4688)]] and Event[EventData[Data[@Name='CommandLine'] and (contains(., 'ScreenConnect') or contains(., 'Datto') or contains(., 'SimpleHelp'))]]" /f:text'; (3) Email gateway message trace logs (14-day retention minimum); (4) DNS query logs for resolution of ScreenConnect, Datto, or SimpleHelp command-and-control domains (query via 'Get-DnsClientQueryPolicy' or firewall logs); (5) File download history from user profiles (%USERPROFILE%\Downloads\, %USERPROFILE%\AppData\Local\, Application Data folders).

Step 3 — Assessment: Inventory all RMM software present on endpoints using EDR telemetry or asset management tooling. Confirm each instance is authorized, managed, and connected only to your organization's approved tenant or relay. Cross-reference against your approved software list and flag any gaps.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2

Controls: NIST 800-53 CM-8, NIST 800-53 CA-7, CIS 1.1, CIS 2.1

Compensating: Without EDR/CMDB: deploy PowerShell inventory script across endpoints via GPO or manual execution: 'Get-WmiObject Win32_Product | Where-Object {$_.Name -match "ScreenConnect|Datto|SimpleHelp"} | Select-Object Name, Version, InstallDate, Vendor > software_inventory.csv'. For each identified instance, query registry HKLM\Software\[Vendor] for tenant URL or relay address and compare against IT-maintained approved tenant list. For Linux/Mac: execute 'sudo find / -name "*ScreenConnect*" -o -name "*datto*" -o -name "*simplehelp*" 2>/dev/null' and 'sudo ps aux | grep -E "ScreenConnect|datto|simplehelp"' and cross-reference process connections via 'lsof -p [PID]' or 'netstat -tunap | grep [PID]'.

Evidence: Capture before inventory: (1) Complete software inventory export from asset management tool (Excel format with Name, Version, InstallDate, Publisher, RegistryPath columns); (2) Registry exports for all identified RMM vendors: 'reg export HKLM\Software\[Vendor] [vendor_reg_export.reg]'; (3) RMM application configuration files typically stored in C:\ProgramData\[Vendor]\config.xml or C:\Windows\System32\config\[vendor_service].ini — export entire directories; (4) Network connection telemetry for RMM processes (source IP, destination IP, destination port, protocol, certificate CN if TLS) via 'netstat -anob' or EDR API; (5) File metadata (hash, signature, path, creation/modification time) for all RMM binaries via 'Get-FileHash' and 'Get-ItemProperty'.

Step 4 — Communication: Notify affected users whose credentials may have been harvested. Issue a targeted security awareness alert to all staff about IRS-themed phishing during tax season. Escalate to legal and compliance if credential compromise is confirmed, given potential data access implications.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.3

Controls: NIST 800-53 IR-4(4), NIST 800-53 AU-6(1), CIS 17.1, CIS 19.7

Compensating: No compensating control — this is a procedural requirement. Use email distribution lists filtered from M365 sign-in log analysis to notify affected users directly. Template: 'Your Microsoft 365 account credentials were harvested in a phishing attack on [date]. Mandatory actions: (1) Reset password immediately via account.microsoft.com; (2) Review recent sign-in activity at https://account.microsoft.com/security; (3) Contact IT at [email] if you see unfamiliar activity.' Send org-wide phishing alert via email and security awareness portal highlighting IRS/tax-themed lures, with screenshot examples from the campaign. Log all notifications with timestamps for compliance audit trail.

Evidence: Capture before communication: (1) Complete list of affected users from M365 sign-in log analysis (usernames, email addresses, sign-in timestamp, RMM installation event timestamp if correlated); (2) Email message samples from the phishing campaign (raw EML files, including headers with X-Originating-IP, DKIM, SPF alignment data); (3) RMM installation logs showing affected endpoints and timestamps; (4) Confirmation email delivery receipts for user notifications (archived in legal hold); (5) Legal/compliance sign-off document authorizing disclosure and communication approach.

Step 5 — Long-term: Implement application allowlisting or software restriction policies to block unauthorized RMM binary execution. Enforce phishing-resistant MFA (FIDO2/hardware token) on all Microsoft 365 accounts. Establish a formal RMM governance policy defining approved tools, approved tenants, and mandatory enrollment procedures. Review Cloudflare-proxied URL handling in your secure email gateway configuration.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4.1

Controls: NIST 800-53 CM-6, NIST 800-53 IA-2(1), NIST 800-53 SI-7(1), CIS 2.3, CIS 5.4, CIS 6.1

Compensating: Without enterprise endpoint control: (1) Deploy Windows AppLocker via GPO with rules blocking execution of ScreenConnect, Datto, SimpleHelp binaries except from C:\Program Files\[approved_path]\; policy XML example: 'New-AppLockerPolicy -RuleCollectionType Exe -RuleCollection (Get-AppLockerPolicy -Local -RuleCollectionType Exe).RuleCollections | Set-AppLockerPolicy'. (2) For FIDO2 alternative without hardware tokens: enforce passwordless sign-in via Windows Hello for Business or Microsoft Authenticator app (requires Windows 10+ or mobile device). (3) RMM governance policy document: define approved vendors (ConnectWise official tenant URL, Datto official domain, SimpleHelp official relay), require IT approval for any new RMM deployment, mandate encryption in transit (TLS 1.2+), and quarterly audit of all RMM instances. (4) Email gateway: review allow-list for Cloudflare IP ranges (1.1.1.0/24, etc.) and add additional scrutiny rule: 'Flag for review if message Header contains Cloudflare and Body contains IRS/tax/refund keywords'.

Evidence: Capture post-incident: (1) Baseline AppLocker or software restriction policy configuration (XML/GPO export); (2) FIDO2 enrollment baseline report (number of users enrolled, device types, backup authentication method data); (3) RMM governance policy document (signed, version-controlled, dated); (4) Email gateway configuration export showing Cloudflare-specific rules and keyword filters; (5) Pre- and post-implementation detection rule testing results (e.g., test execution of ScreenConnect binary from non-approved path to confirm block).

Detection Guidance

Microsoft 365 / Entra ID: Query sign-in logs for successful authentications originating from unusual ASNs or geolocations followed within 30 minutes by new device registrations or OAuth application consent grants. Look for service principal activity from unfamiliar RMM application IDs. Endpoint telemetry (EDR): Alert on execution of ScreenConnect.Client.exe, DattoRMM agent binaries, or SimpleHelp binaries (server.exe, remote.exe) where the parent process is a browser, email client, or user-launched installer, not your approved management platform. Flag outbound connections from these binaries to relay domains not registered in your RMM tenant. Email gateway: Search for messages with Amazon SES sending infrastructure (mail from: amazonses.com) containing keywords: IRS, tax refund, SmartVault, Form W-2, tax document. Flag URLs proxied through Cloudflare Workers or Pages domains (workers.dev, pages.dev) that redirect to Microsoft 365 login clones.

Network: Monitor for RMM relay traffic (ConnectWise relay: relay.screenconnect.com; Datto: concord.centrastage.net) originating from endpoints where your team did not deploy an agent. Flag any SimpleHelp relay connections to non-corporate SimpleHelp server IPs. Behavioral indicators: User account logs into Microsoft 365 from a known IP, then within the same session a new device or app is registered; shortly after, an RMM binary executes on that same endpoint. This sequence, credential use, new registration, RMM launch, is the core behavioral chain to detect.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`relay.screenconnect.com`	ConnectWise ScreenConnect relay domain — flag unexpected outbound connections from endpoints not enrolled in your approved ScreenConnect tenant	MEDIUM
DOMAIN	`concord.centrastage.net`	Datto RMM relay domain — flag connections from endpoints not provisioned by your RMM team	MEDIUM
DOMAIN	`workers.dev`	Cloudflare Workers subdomain pattern abused to host credential-harvesting pages; flag in email URL analysis and proxy logs	MEDIUM
DOMAIN	`pages.dev`	Cloudflare Pages subdomain pattern used for phishing page hosting; flag alongside workers.dev in gateway rules	MEDIUM
URL	`https://www.microsoft.com/en-us/security/blog/2026/03/19/when-tax-season-becomes-cyberattack-season-phishing-and-malware-campaigns-using-tax-related-lures/`	Primary source — Microsoft Threat Intelligence campaign analysis (T1 source, search-retrieved, recommend human validation)	HIGH
URL	`https://www.microsoft.com/en-us/security/blog/2026/03/03/signed-malware-impersonating-workplace-apps-deploys-rmm-backdoors/`	Primary source — Microsoft analysis of signed RMM backdoor deployment (T1 source, search-retrieved, recommend human validation)	HIGH

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1078** — Valid Accounts
- **T1583.001** — Domains
- **T1566.001** — Spearphishing Attachment
- **T1204.001** — Malicious Link

- **T1133** — External Remote Services
- **T1598.002** — Spearphishing Attachment
- **T1056.003** — Web Portal Capture
- **T1059.001** — PowerShell
- **T1566.002** — Spearphishing Link
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1585.002** — Email Accounts
- **T1539** — Steal Web Session Cookie
- **T1027** — Obfuscated Files or Information
- **T1557** — Adversary-in-the-Middle
- **T1204.002** — Malicious File
- **T1219** — Remote Access Tools

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

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

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **2.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1583.001	Domains	Resource-Development
T1566.001	Spearphishing Attachment	Initial-Access
T1204.001	Malicious Link	Execution
T1133	External Remote Services	Persistence
T1598.002	Spearphishing Attachment	Reconnaissance
T1056.003	Web Portal Capture	Collection
T1059.001	PowerShell	Execution
T1566.002	Spearphishing Link	Initial-Access
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1585.002	Email Accounts	Resource-Development
T1539	Steal Web Session Cookie	Credential-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1557	Adversary-in-the-Middle	Credential-Access
T1204.002	Malicious File	Execution

Technique ID	Technique Name	Tactic
T1219	Remote Access Tools	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/microsoft-warns-irs-phishing-hits...	T3
Phishing and malware campaigns using tax-related lures - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/03/19/when-tax-s...	T1
Signed malware impersonating workplace apps deploys RMM ...	https://www.microsoft.com/en-us/security/blog/2026/03/03/signed-mal...	T1
Hackers Ramp Up Abuse of ScreenConnect, Other RMM Tools	https://www.msspalert.com/news/hackers-ramp-up-abuse-of-screenconne.. .	T3
When Security Tools Are Turned Against Us: Cloudflare Anti Bot ...	https://coesecurity.com/when-security-tools-are-turned-against-us-c...	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center