INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

Tax Season as Attack Surface: RMM Deployment and PhaaS Infrastructure Converge in Multi-Vector IRS Impersonation Campaign

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0091
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	ConnectWise ScreenConnect, Datto RMM, SimpleHelp, Microsoft 365, Microsoft Azure Monitor, SmartVault (impersonated), Amazon SES, Cloudflare
Published	2026-03-23
Discovery Source	Rss

Executive Summary

On February 10, 2026, Microsoft Threat Intelligence documented a coordinated IRS-impersonation phishing campaign that reached 29,000 users across 10,000 organizations in a single day, with financial services, technology, and retail sectors bearing the highest exposure. Attackers used industrialized phishing-as-a-service platforms to harvest credentials, then deployed legitimate remote management tools (ConnectWise ScreenConnect, Datto RMM, SimpleHelp) to establish persistent access that bypasses standard endpoint controls. The business risk is significant: compromised RMM access grants attackers the same trusted foothold as internal IT staff, enabling data exfiltration, ransomware staging, or prolonged undetected presence across the enterprise.

Technical Analysis

Microsoft documented this campaign on February 10, 2026 (full analysis published March 19, 2026). Attackers used two PhaaS platforms, Energy365 and SneakyLog/Kratos, to industrialize credential harvesting via adversary-in-the-middle (AiTM) and web form-based techniques. Lures were delivered through Amazon SES to abuse sender reputation and routed through Cloudflare infrastructure to evade URL-based filtering. IRS and SmartVault branding supplied social engineering legitimacy for document-retrieval and tax-filing lures targeting accounting workflows. Post-credential-harvest, attackers deployed RMM binaries (ConnectWise ScreenConnect, Datto RMM, SimpleHelp) as persistence mechanisms, exploiting the signed, trusted status these tools hold in most enterprise environments to evade EDR detection. Microsoft Azure Monitor alert

notification emails were abused as a callback phishing vector, embedding malicious links within communications that visually blend with legitimate platform telemetry, constituting spearphishing by trusted service abuse (T1566.001, T1583.008). Additional techniques mapped to MITRE ATT&CK include: T1219 (Remote Access Software), T1539 (Steal Web Session Cookie), T1056.003 (Web Portal Capture), T1059.001 (PowerShell execution), T1105 (Ingress Tool Transfer), T1036/T1036.005 (Masquerading), T1114 (Email Collection), T1078 (Valid Accounts), T1547 (Boot/Logon Autostart Persistence), T1027 (Obfuscated Files), T1071.001 (Web Protocols for C2), T1199 (Trusted Relationship), T1204.001/T1204.002 (User Execution). Relevant weaknesses: CWE-345 (Insufficient Verification of Data Authenticity), CWE-451 (User Interface Misrepresentation), CWE-290 (Authentication Bypass by Spoofing), CWE-940 (Improper Verification of Source of Communication Channel). No CVE is assigned; this is a campaign-level threat, not a specific software vulnerability. The 277% YoY increase in RMM abuse reflects a structural shift in post-compromise persistence tradecraft (Microsoft Threat Intelligence, March 2026). Source quality note: Primary sourcing is Microsoft Security Blog (T1 tier); supporting sources are T3 tier and should be treated as corroborating context only.

Action Checklist

1. Step 1, Immediate: Audit all RMM tool installations (ConnectWise ScreenConnect, Datto RMM, SimpleHelp) across the environment. Identify any instances not provisioned by IT, paying particular attention to installations appearing in user-writable directories or tied to accounts that received IRS-themed email in the February-March 2026 window. Remove unauthorized instances.
2. Step 2, Detection: Query email gateway and SIEM logs for messages originating from Amazon SES infrastructure containing IRS, SmartVault, or Azure Monitor branding delivered between February 1 and the present. Flag any users who clicked links within those messages and cross-reference against RMM process launch events on the same endpoints.
3. Step 3, Detection: Search endpoint telemetry for RMM binaries executed from non-standard paths or by user-level processes rather than system or IT provisioning accounts. In Microsoft Defender XDR, hunt for ScreenConnect, Datto, or SimpleHelp client processes spawned by Office applications, browsers, or scripting engines (PowerShell, cmd.exe).
4. Step 4, Assessment: Review Azure Monitor alert notification delivery settings and audit which accounts received alert emails in the February-March period. Confirm no alert notification templates have been modified to include external URLs. Check for OAuth app consents or mail forwarding rules (T1114) added to accounts in the same window.
5. Step 5, Communication: Notify security-sensitive user populations (finance, accounting, tax, IT helpdesk) of the IRS and SmartVault lure patterns. Provide concrete examples of the lure format. Escalate any confirmed RMM implants to incident response immediately, treat as active compromise until ruled out.
6. Step 6, Long-term: Deploy an allowlist policy for approved RMM tools and block unapproved RMM binaries via application control (e.g., WDAC, AppLocker). Review PhaaS indicator feeds (Energy365, SneakyLog/Kratos infrastructure) and subscribe to Microsoft Threat Intelligence updates for ongoing IOC coverage. Implement conditional access policies requiring phishing-resistant MFA (FIDO2 or certificate-based) to reduce AiTM credential-harvest impact.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to external IR firm immediately if Step 1 or Step 3 confirms RMM implant on a financial system, email server, or identity management system; if mail forwarding rules or OAuth consents are confirmed in Step 4; or if more than 5 endpoints show RMM execution from non-standard paths by user-level processes.
Recovery Notes	Post-containment: rebuild affected systems from clean backups or re-image if RMM implant confirmed; reset passwords for all users who received IRS-themed lures with forced MFA re-enrollment; audit all email forwarding rules, delegated mailbox access, and OAuth consents across the organization with focus on modifications in February–March 2026 window; implement post-incident review with security team to refine detection rules and update employee phishing training with exact lure samples observed in this campaign.
Forensic Artifacts	Windows Event Log Security (4688 process creation, 4657 registry modification, 4688 child process spawning from Office/browser/PowerShell) | Windows Registry: HKLM\Software\ConnectWise, HKLM\Software\Datto, HKLM\Software\SimpleHelp; HKCU\Software\Microsoft\Windows\CurrentVersion\Run; HKLM\Software\Microsoft\Windows\CurrentVersion\Run | O365 Unified Audit Log: AzureActiveDirectory (Add service principal, Consent to application), Exchange (New-InboxRule, Set-InboxRule events showing mail forwarding) | Email gateway logs (Proofpoint, Mimecast, O365 Message Trace): originating IP, SES infrastructure confirmation, recipient, click timestamp, landing URL | Browser history and downloads: Chrome/Edge/Firefox SQLite database showing phishing link clicks, file download records with timestamps | Sysmon Event Log (if deployed): Event 3 (network connections from RMM binary to C2), Event 6 (driver loaded — check for unsigned drivers used by RMM) | Azure Monitor alert rule definitions and modification history (Azure activity log showing 'write' operations on metricAlerts) | File system artifacts: MFT entries for RMM binary installation directory, file timestamps, hash (SHA-256), digital signature verification results

Per-Action IR Details

Step 1 — Immediate: Audit all RMM tool installations (ConnectWise ScreenConnect, Datto RMM, SimpleHelp) across the environment. Identify any instances not provisioned by IT, paying particular attention to installations appearing in user-writable directories or tied to accounts that received IRS-themed email in the February–March 2026 window. Remove unauthorized instances.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §4.2 (detection and analysis)

Controls: NIST 800-53 SI-2 (flaw remediation), NIST 800-53 SI-7 (software, firmware, and information integrity), CIS 2.3 (address unauthorized software)

Compensating: On Windows, query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall and check registry for ScreenConnect (HKLM\Software\ConnectWise), Datto (HKLM\Software\Datto), SimpleHelp installation keys. Cross-check against IT-maintained approved software list. On Linux/Mac, use `ls -la /opt/ /Applications/ /usr/local/` and `brew list` for installation paths. Correlate against IT provisioning tickets (ServiceNow, Jira tickets tagged 'RMM approval'). For file-based hunt: `Get-ChildItem -Path 'C:\Users\*\AppData' -Filter '*ScreenConnect*' -Recurse | Select-Object FullName,CreationTime`

Evidence: Before removal: capture full process tree of RMM process (WMI query `Get-WmiObject Win32_Process -Filter 'Name like %ScreenConnect%'`), registry hives (HKLM\Software, HKCU\Software for all detected RMM keys), MFT entry for installation directory, Windows Event Log 4688 (process creation) for 48 hours prior to detection showing parent process of RMM binary, file creation timestamps via `Get-Item -Path 'C:\path\to\rmm.exe' | Format-List CreationTime,LastAccessTime,LastWriteTime`. If installed to user-writable path: preserve directory structure and file hash (SHA-256) before deletion.

Step 2 — Detection: Query email gateway and SIEM logs for messages originating from Amazon SES infrastructure containing IRS, SmartVault, or Azure Monitor branding delivered between February 1 and the present. Flag any users who clicked links within those messages and cross-reference against RMM process launch events on the same endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §4.2.2 (log analysis and data correlation)

Controls: NIST 800-53 SI-4 (information system monitoring), NIST 800-53 CA-7 (continuous monitoring), CIS 8.5 (deploy endpoint detection and response)

Compensating: If SIEM unavailable, export email logs from gateway (Proofpoint, Mimecast, Office 365 Message Trace) filtering `From:*@ses.amazonaws.com OR SPF/DKIM mismatch` and keywords 'IRS|SmartVault|Azure Monitor' to CSV. Cross-reference recipient addresses against endpoint logs manually: grep Windows Event Log 4688 on each user's machine for RMM binary execution within 2 hours of email click timestamp. Use `Get-MsolUser -All | Where-Object {$_.UserPrincipalName -in $lure_recipients} | Select-Object DisplayName,LastDirSyncTime` to identify affected O365 accounts.

Evidence: Email Message-ID, originating IP, SES infrastructure confirmation (reverse DNS lookup, SMTP logs showing 'amazon.com' mail server), email click tracking log timestamp (exact second), recipient email address. Endpoint: Windows Event Log Security event 4688 (process creation) showing RMM binary name, ParentImage, CommandLine, TargetUserName, LogonGUID; browser history (Chrome/Edge SQLite database at `C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\History` or `C:\Users\*\AppData\Local\Microsoft\Edge\User Data\Default\History`) showing click timestamp and landing page URL. Network: proxy/firewall logs showing HTTP GET to phishing URL within 120 seconds of email delivery.

Step 3 — Detection: Search endpoint telemetry for RMM binaries executed from non-standard paths or by user-level processes rather than system or IT provisioning accounts. In Microsoft Defender XDR, hunt for ScreenConnect, Datto, or SimpleHelp client processes spawned by Office applications, browsers, or scripting engines (PowerShell, cmd.exe).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §4.2.3 (anomaly detection)

Controls: NIST 800-53 SI-4(1) (system monitoring – system-generated alerts), NIST 800-53 SI-4(11) (system monitoring – analyze traffic and event patterns), CIS 8.8 (implement endpoint detection and response)

Compensating: Without Defender XDR: query Windows Event Log Security (4688 process creation) via PowerShell: `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4688; StartTime=(Get-Date).AddDays(-30)} | Where-Object {$_.Message -match '(ScreenConnect|Datto|SimpleHelp)'} | Select-Object TimeCreated,Message | Export-Csv rmm_detections.csv`. Filter for ParentImage matching 'OUTLOOK.EXE|CHROME.EXE|firefox.exe|powershell.exe|cmd.exe'. For non-standard paths, flag Image field not matching 'C:\Program Files\' or approved IT deployment directory. Cross-reference NewProcessName (RMM binary) and SubjectUserName (who launched it) — if user account rather than SYSTEM or approved service account, escalate.

Evidence: Windows Event Log 4688 (process creation): Image (full path to RMM binary), ParentImage (parent process), CommandLine (full command executed), TargetUserName (account that spawned process), LogonGuid, ParentProcessId, ProcessId, CreationTime. File signature: digital signature check via `Get-AuthenticodeSignature -FilePath 'C:\path\to\rmm.exe' | Select-Object *`. Registry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run or HKCU\Software\Microsoft\Windows\CurrentVersion\Run for persistence mechanisms. Network: Sysmon event 3 (network connection) showing RMM binary establishing outbound connection to C2 infrastructure.

Step 4 — Assessment: Review Azure Monitor alert notification delivery settings and audit which accounts received alert emails in the February–March period. Confirm no alert notification templates have been modified to include external URLs. Check for OAuth app consents or mail forwarding rules (T1114) added to accounts in the same window.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §4.2.4 (initial compromise assessment)

Controls: NIST 800-53 AC-2(2) (account management – removal of privileged access), NIST 800-53 AC-3 (access enforcement), CIS 5.4 (restrict administrative privileges to dedicated accounts)

Compensating: Export Azure Monitor alert rules via Azure CLI: `az monitor metrics alert list --resource-group --output json > alerts.json` and inspect each rule's 'actions' field for recipient email addresses and external URLs in condition templates. Query O365 audit logs (Office 365 Security & Compliance Center or via PowerShell: `Search-UnifiedAuditLog -StartDate 2026-02-01 -EndDate 2026-03-31 -RecordType AzureActiveDirectory -Operations 'Add service principal', 'Consent to application'`) for OAuth consent grants. Search mailbox forwarding rules: `Get-InboxRule -Mailbox | Where-Object {$_.ForwardingAddress -or $_.ForwardingSmtpAddress}` for each compromised-suspect account. Manually review alert template JSON in Azure portal for suspicious external URLs.

Evidence: Azure Monitor alert rule definitions (JSON export showing AlertCriteria, Actions, NotificationActions sections). Azure AD audit logs: event type 'Consent to application' with AppDisplayName, ResourceDisplayName, InitiatedByUserPrincipalName, Timestamp. O365 mailbox forwarding rules: export via EAC or PowerShell showing ForwardingAddress, ForwardingSmtpAddress, DeliverToMailboxAndForward values. Email gateway logs showing alerts forwarded to external email accounts. Azure activity log showing modifications to alert rule templates: operation name 'Microsoft.Insights/metricAlerts/write' with Timestamp, Caller, InitiatedByUser.

Step 5 — Communication: Notify security-sensitive user populations (finance, accounting, tax, IT helpdesk) of the IRS and SmartVault lure patterns. Provide concrete examples of the lure format. Escalate any confirmed RMM implants to incident response immediately — treat as active compromise until ruled out.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3.5 (containment and eradication notifications)

Controls: NIST 800-53 AT-2(2) (awareness and training – phishing and social engineering), NIST 800-53 CA-2(2) (security assessments – included in incident response plan), CIS 6.1 (establish security awareness program)

Compensating: Create email alert using native messaging: draft a sample phishing email showing actual Subject line, From address (SES spoofed domain), and example malicious link (redacted or pointing to security.example.com educational page). Send via company email distribution lists for Finance, Accounting, Tax, IT Helpdesk. Include reporting procedure: 'Reply-all with SECURITY-ALERT flag or forward to security@example.com.' Document distribution list membership and delivery timestamp for accountability. For escalation: implement automated ticket routing — any endpoint with confirmed RMM binary (from Step 3) auto-creates P1 incident ticket in ticketing system with IR on-call assignment.

Evidence: Email distribution lists used (membership list, timestamps of notifications sent). Helpdesk ticket system entries showing escalated cases with RMM detections flagged, assigned to IR team, timestamps. User awareness survey responses (if post-campaign survey conducted). SIEM/email gateway logs showing number of users who reported phishing email as suspicious prior to detection. Incident ticket history showing chain of custody from detection through escalation.

Step 6 — Long-term: Establish an allowlist policy for approved RMM tools and block unapproved RMM binaries via application control (e.g., WDAC, AppLocker). Review PhaaS indicator feeds (Energy365, SneakyLog/Kratos infrastructure) and subscribe to Microsoft Threat Intelligence updates for ongoing IOC coverage. Implement conditional access policies requiring phishing-resistant MFA (FIDO2 or certificate-based) to reduce AiTM credential-harvest impact.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4.4 (post-incident activities and lessons learned)

Controls: NIST 800-53 SI-7(15) (information system monitoring – code execution in memory), NIST 800-53 AC-3(7) (access enforcement – role-based access control), NIST 800-53 IA-2(1) (authentication – multi-factor authentication), CIS 2.5 (allowlist approved software), CIS 5.2 (implement multifactor authentication)

Compensating: Without WDAC: deploy AppLocker policy via Group Policy to block RMM binaries by file hash or publisher certificate (reference NIST SP 800-53 SI-7). Create policy rule: Path rule blocking '*\ScreenConnect*', '*\Datto*', '*\SimpleHelp*' except for IT-approved installation directory. Test on pilot group before enterprise rollout. For PhaaS feeds: subscribe to free Microsoft Threat Intelligence RSS (microsoft.com/security/intelligence) and MITRE

ATT&CK updates. Query VirusTotal API (free tier) for RMM binary samples to build hash database. For MFA: configure O365 conditional access policy requiring phishing-resistant MFA (FIDO2 registration via security key) for high-risk users (finance, tax, IT admins). For teams without conditional access: enforce FIDO2 requirement in Azure AD MFA server (on-premises) or use third-party MFA provider (e.g., Okta, Duo) with FIDO2 support.

Evidence: AppLocker policy export (XML) showing allowlist rules and RMM binary blocks. WDAC policy binary (if deployed) showing signed binaries allowlist. PhaaS indicator feed subscriptions (confirmation of enrollment in threat intelligence services, delivery logs of IOC updates). Conditional access policy configuration (export from Azure portal showing conditions, MFA requirements, grant controls). MFA enrollment logs showing users registered for FIDO2 (Azure MFA registration history). Pilot deployment testing results (policy applied to test group, verified RMM binary blocked, legitimate RMM allowed). Enterprise rollout timeline and deployment logs.

Detection Guidance

1. RMM abuse detection: Alert on ScreenConnect, Datto, or SimpleHelp client processes launching from user profile directories (%AppData%, %Temp%, Downloads) or spawned by browser/Office parent processes. In Microsoft Defender XDR: DeviceProcessEvents | where FileName in~ ('ScreenConnect.ClientService.exe','SimpleHelpClient.exe','DattoRMM.exe') | where InitiatingProcessFileName in~ ('WINWORD.EXE','EXCEL.EXE','chrome.exe','msedge.exe','powershell.exe','cmd.exe'). 2. AiTM session token theft: Monitor for impossible travel or token replay anomalies in Azure AD / Entra ID sign-in logs. Look for sign-ins with familiar credentials but unfamiliar device IDs or IP geolocation mismatches occurring within minutes of a known-good login. 3. Azure Monitor callback phishing: Review Azure Monitor action group configurations for unexpected webhook URLs or email addresses added as notification targets. Alert on any alert notification emails containing external hyperlinks pointing to non-Microsoft domains. 4. Mail forwarding rule creation (T1114): Query Exchange/M365 audit logs for New-InboxRule or Set-InboxRule events, especially rules forwarding to external addresses, created after any user interacted with a suspect email. 5. PowerShell and ingress tool transfer: Alert on PowerShell commands downloading executables from external hosts (Invoke-WebRequest, Start-BitsTransfer, IEX(New-Object Net.WebClient)) in proximity to RMM binary drops. 6. Behavioral IOC pattern: User receives IRS/SmartVault-branded email via Amazon SES -> user clicks link -> browser spawns PowerShell or downloads executable -> RMM binary executes from user-writable path -> outbound connection to RMM relay infrastructure. Any endpoint matching steps 3-5 of this chain should trigger immediate triage.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Amazon SES sending infrastructure (ses.amazonaws.com relay)`	Campaign emails delivered via Amazon SES to abuse sender reputation and bypass domain-based filtering. Block or closely inspect SES-originated mail claiming to be from IRS, SmartVault, or Azure Monitor.	HIGH

Type	Value	Context	Confidence
URL	`PhaaS platform: Energy365`	Credential harvesting PhaaS platform used in this campaign. Specific domains not publicly confirmed in available T1 source at time of generation. Monitor threat intel feeds for associated infrastructure.	MEDIUM
URL	`PhaaS platform: SneakyLog / Kratos`	Second PhaaS platform used for AiTM credential harvesting. Specific domains not publicly confirmed in available T1 source at time of generation. Monitor threat intel feeds for associated infrastructure.	MEDIUM
DOMAIN	`Cloudflare-proxied phishing domains (pattern: IRS/SmartVault lures)`	Campaign infrastructure routed through Cloudflare to obscure origin IPs. Specific domains not confirmed in available T1 source. Watch for newly registered domains impersonating irs.gov or smartvault.com with Cloudflare nameservers.	MEDIUM
HASH	`[not available in cited sources]`	File hashes for RMM payloads (ScreenConnect, Datto, SimpleHelp installers used in campaign) not published in available T1 source. Check Microsoft Threat Intelligence portal and Microsoft Security Blog for updated IOC releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1547** — Boot or Logon Autostart Execution
- **T1219** — Remote Access Tools
- **T1539** — Steal Web Session Cookie
- **T1056.003** — Web Portal Capture
- **T1059.001** — PowerShell
- **T1105** — Ingress Tool Transfer
- **T1036** — Masquerading
- **T1566.001** — Spearphishing Attachment
- **T1204.002** — Malicious File
- **T1204.001** — Malicious Link
- **T1199** — Trusted Relationship
- **T1027** — Obfuscated Files or Information
- **T1566.002** — Spearphishing Link

- **T1078** — Valid Accounts
- **T1598.002** — Spearphishing Attachment
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1114** — Email Collection
- **T1071.001** — Web Protocols
- **T1583.008** — Malvertising

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
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5**
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

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

SOC2-TSC

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

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
T1547	Boot or Logon Autostart Execution	Persistence
T1219	Remote Access Tools	Command-And-Control
T1539	Steal Web Session Cookie	Credential-Access
T1056.003	Web Portal Capture	Collection
T1059.001	PowerShell	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1036	Masquerading	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access
T1204.002	Malicious File	Execution
T1204.001	Malicious Link	Execution
T1199	Trusted Relationship	Initial-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1566.002	Spearphishing Link	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1598.002	Spearphishing Attachment	Reconnaissance
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1114	Email Collection	Collection
T1071.001	Web Protocols	Command-And-Control
T1583.008	Malvertising	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/microsoft-warns-irs-phishing-hits...	T3
Microsoft Azure Monitor alerts abused for callback phishing attacks ...	https://www.reddit.com/r/technews/comments/1s0cmkv/microsoft_azure_...	T3

Source	URL	Tier
Phishing and malware campaigns using tax-related lures - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/03/19/when-tax-s...	T1
Week in review: ScreenConnect servers open to attack, exploited ...	https://www.helpnetsecurity.com/2026/03/22/week-in-review-screencon...	T3
Critical ScreenConnect Vulnerability Exposes Machine Keys	https://www.securityweek.com/critical-screenconnect-vulnerability-e...	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center