FEBRUARY

pellera

THREAT INTEL REPORT 2026

Prepared by: Pellera Threat Intel Team
pellera.com | 800.747.8585

Driving Momentum. Accelerating Change. Empowering IT Transformation.

Pellera Technologies was born out of the combined expertise of Converge Technology Solutions and Mainline Information Systems, two industry leaders with over 35+ years of experience and a shared vision for innovation. Together, we empower businesses to achieve greater efficiency, adaptability, and growth for today and tomorrow.

Our commitment is to reshape what's possible with IT, offering advanced solutions in digital infrastructure, cloud, cybersecurity, and AI. We don't just deliver technology—we partner with you to build tailored strategies designed to simplify complexities, unlock opportunities, and drive transformational outcomes.

At Pellera, momentum builds here through collaborative, people-first technology designed to fuel progress and deliver measurable impact.

pellera

Observations for February 2026

Recent reporting shows a continued shift away from exploiting software flaws and toward abusing trust, identity, and legitimate tools. Threat actors are relying on brand impersonation, social engineering, and authorized administrative software to gain access and maintain control. **The focus is no longer limited to endpoint compromise**; activity is expanding into identity systems, SaaS platforms, and remote management infrastructure.

One campaign used a spoofed 7-Zip domain to distribute a trojanized installer that bundled legitimate software with hidden proxyware. Infected systems were converted into residential proxy nodes running with SYSTEM-level privileges. **The operation relied on trusted branding, search-driven user behavior**, and valid-looking installers rather than vulnerability exploitation. The same infrastructure model appears scalable, with related installers impersonating other well-known consumer applications to grow the proxy network.

In parallel, **ShinyHunters-branded activity** has expanded into coordinated SaaS-focused intrusions using voice phishing, credential harvesting, and MFA device enrollment. Multiple clusters are targeting enterprise identity providers and collaboration platforms, then moving quickly into data theft, outbound phishing, and extortion. The primary access method is valid credentials obtained through social engineering, reflecting a direct focus on identity-layer compromise.

At the enterprise level, **abuse of Remote Monitoring and Management (RMM)** tools has become a primary intrusion method rather than a secondary action. Threat actors are deploying or hijacking legitimate remote administration software to establish persistence, move laterally, and conduct data exfiltration while blending into normal IT activity. Across these incidents, the common theme is the abuse of trusted software, identity systems, and administrative tools to reduce detection and increase operational control.

Executive Overview

HOME NETWORK THREAT INFRASTRUCTURE

Audience

- CISO
- Project Managers
- Cybersecurity Analysts
- Risk Management Professionals
- IT Managers

RISK

GEOGRAPHIC SCOPE

BUSINESS IMPACT

A malicious campaign distributing a trojanized 7-Zip installer through a lookalike domain is enrolling infected systems into a residential proxy network. Victims receive a fully functional 7-Zip application, reducing suspicion, while hidden components establish SYSTEM-level Windows services and persistent outbound proxy communications.

The malware, identified in reporting by Malwarebytes and corroborated by BleepingComputer and SC Media, installs Uphero.exe, hero.exe, and hero.dll into C:\Windows\SysWOW64\hero, modifies firewall rules, profiles host hardware, and retrieves configuration data from rotating "smshero"-themed domains. Communications are encrypted, DNS queries are routed over DNS-over-HTTPS, and traffic is proxied through Cloudflare infrastructure.

The operational risk extends beyond individual endpoints. Residential proxy nodes can be leveraged for credential stuffing, phishing, fraud, ad abuse, and further malware distribution, potentially implicating victim IP addresses in downstream criminal activity. Organizations with unmanaged endpoints, remote users, or BYOD exposure face reputational, legal, and investigative complications if corporate assets are co-opted into proxy networks.

READ MORE: HOME NETWORK THREAT INFRASTRUCTURE

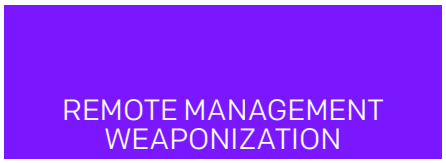
ADVANCES IN RMM THREATS

Audience

- CISO
- IT Operations Managers & Teams
- Risk Management Professionals
- Security Operations Team
- IT Security Managers
- Incident Response Teams
- System Administrators

RISK

GEOGRAPHIC SCOPE



BUSINESS IMPACT

Threat actors across financially motivated and ransomware ecosystems are increasingly weaponizing legitimate RMM platforms as primary access, persistence, and command-and-control mechanisms. This operational pivot reduces reliance on custom malware, bypasses signature-based defenses, and exploits the inherent trust granted to enterprise administration software.

Campaigns observed in early 2026 demonstrate multi-stage intrusion chains involving phishing, SmartScreen bypass, privilege escalation, remote service installation, and data exfiltration through trusted RMM channels. In ransomware-linked cases such as Medusa operations, RMM tools are integrated directly into encryption workflows, lateral movement playbooks, and exfiltration staging.

The operational risk is systemic: environments that permit unrestricted RMM deployment, lack strict service creation monitoring, or fail to differentiate legitimate from malicious remote administration activity remain vulnerable to stealth compromise and rapid attacker scaling.

READ MORE: ADVANCES IN RMM THREAT INFRASTRUCTURE

Audience

- **CISO**
- **IT Operations Managers & Teams**
- **Risk Management Professionals**
- **Security Operations Team**
- **IT Security Managers**
- **Incident Response Teams**
- **System Administrators**

SHINY HUNTERS

RISK

GEOGRAPHIC SCOPE

BUSINESS IMPACT

ShinyHunters-linked threat clusters are conducting coordinated SaaS extortion operations using vishing and real-time credential harvesting to bypass MFA and compromise enterprise SSO environments. The attacks rely on social engineering rather than software vulnerabilities and have successfully targeted Okta customer accounts and other identity providers.

Once access is obtained, attackers exfiltrate sensitive corporate data from multiple SaaS platforms to support 72-hour ransom demands, data leak site exposure, and secondary extortion tactics. The campaign reflects a systemic identity security risk for organizations relying on push-based MFA and SSO without phishing-resistant controls.

READ MORE: SHINY HUNTERS

HOME NETWORK THREAT INFRASTRUCTURE

Overview & Impact

The infection chain begins with domain impersonation. The fraudulent 7zip[.]com site mimics the legitimate 7-zip.org project, replicating site structure and content to deceive users. Distribution vectors include search engine results and YouTube tutorials that incorrectly reference the malicious domain.

Technical execution includes:

- Authenticode-signed installer (certificate issued to Jozeal Network Technology Co., Limited, later revoked)
- Silent drop of malicious binaries to a privileged directory
- Creation of Windows services for Uphero.exe and hero.exe
- SYSTEM-level execution on reboot
- Firewall manipulation via netsh to permit inbound and outbound connections
- Collection of hardware, CPU, disk, memory, and network characteristics
- Configuration retrieval from domains such as hero-sms[.]co and smshero[.]vip
- XOR-encoded control messages (key 0x70)
- Outbound proxy connections on non-standard ports (1000, 1002)
- Cloudflare-fronted infrastructure with TLS encryption
- DNS-over-HTTPS via Google resolver
- Virtualization and debugger detection mechanisms

The infrastructure enables third-party traffic routing through infected IP addresses, consistent with commercial residential proxy services used for fraud, scraping, ad abuse, phishing, and credential stuffing operations.

- SYSTEM-level persistence with auto-start services.
- Firewall rule tampering that reduces network-level containment controls.
- Enrollment of endpoints into monetized residential proxy networks.
- Potential downstream abuse of victim IP addresses in criminal operations.
- Increased legal, reputational, and investigative exposure for impacted organizations.
- Detection challenges due to encrypted C2 traffic and DNS-over-HTTPS usage.

Observations

- Domain impersonation targeting high-trust utility software.
- Bundling of legitimate binaries with concealed proxyware payloads.
- Authenticode signing used to reduce user suspicion.
- Deployment to SysWOW64 for privileged persistence.
- Firewall manipulation via netsh commands.
- DNS-over-HTTPS implementation to evade traditional DNS logging.
- XOR-encoded control protocol over non-standard ports.
- Shared infrastructure across multiple trojanized software brands.

Guidance

Strategic Intelligence

- **Trend**
  - Brand impersonation combined with legitimate application bundling is being operationalized as a scalable proxyware distribution model.
  - Residential proxy monetization is increasingly decoupled from traditional exploit-driven intrusion activity.
  - Campaign structure indicates sustained infrastructure investment rather than short-lived opportunistic malware distribution.

Operational Intelligence

- **Threat Vectors**
  - Domain impersonation (7zip[.]com vs 7-zip.org)
  - Search engine and tutorial-driven user redirection
  - Digitally signed but trojanized installers
  - Bundled legitimate software masking malicious components
- **Monitoring & Detection Gaps**
  - Limited inspection of SysWOW64 subdirectories for non-standard services
  - Inadequate monitoring of Windows service creation events
  - Lack of firewall rule change auditing
  - Insufficient DNS-over-HTTPS visibility
  - Overreliance on signature trust without certificate reputation validation
- **Response Actions**
  - Identify systems that executed installers from 7zip[.]com
  - Audit Windows services for Uphero.exe and hero.exe
  - Review firewall rule modifications via netsh logs
  - Block known hero/smshero domains and related infrastructure
  - Rotate credentials and review outbound traffic logs for anomalous proxy behavior
  - Consider OS reinstallation for high-risk or sensitive endpoints

Tactical Intelligence

- **Mitigation Strategies**
  - Enforce application allowlisting for trusted software sources
  - Monitor Windows Event ID 7045 (service creation)
  - **Alert on execution from C:** Windows\SysWOW64\hero\
  - Inspect firewall configuration changes
  - Restrict outbound traffic on uncommon ports (1000, 1002)
- **Preventive Measures**
  - Conduct user awareness campaigns regarding official download domains
  - Validate code-signing certificates against revocation status
  - Deploy DNS-over-HTTPS detection controls where feasible
  - Implement EDR-based service and persistence anomaly detection
  - Regularly audit endpoints for unauthorized proxy behavior

Threat Hunting Hypotheses

Unauthorized Proxyware Service Deployment

Hypothesis: A system has been enrolled into the upStage Proxy infrastructure through a trojanized installer.

Investigation Steps

- Review Windows Event ID 7045 for creation of services referencing Uphero.exe or hero.exe.
- **Inspect C:**\Windows\SysWOW64\hero\ for unauthorized binaries.
- Correlate service creation timestamps with user download activity.
- Identify outbound connections to hero/smshero-themed domains.
- Validate compromise if SYSTEM-level services align with unusual outbound proxy traffic.

Firewall Rule Manipulation to Enable Persistent C2

Hypothesis: The malware modified firewall rules to permit unrestricted proxy communications.

Investigation Steps

- Audit netsh command execution logs.
- Compare current firewall rules against baseline configurations.
- Identify recently created inbound or outbound allow rules referencing hero binaries.
- Correlate rule creation with service installation times.
- Confirm compromise if rule changes coincide with new SYSTEM services.

DNS-over-HTTPS Evasion Activity

Hypothesis: The infected host is using DNS-over-HTTPS to conceal C2 resolution.

Investigation Steps

- Identify outbound HTTPS traffic to known DoH providers (e.g., Google resolver endpoints).
- Correlate DoH traffic with hero.exe process execution.
- Compare DNS resolution patterns to baseline user behavior.
- Inspect TLS SNI data for hero/smshero-related domains.
- Validate compromise if DoH activity aligns with proxy port traffic (1000/1002).

Sources

- **Malwarebytes: Fake 7-Zip downloads are turning home PCs into proxy nodes**
- **SC Media: Fake 7-Zip website distributes trojanized installer, turns PCs into proxy nodes**
- **BleepingComputer: Malicious 7-Zip site distributes installer laced with proxy tool**
- **CyberInsider: Laced 7-Zip installers turn home PCs into residential proxy nodes**
- **CyberSecurityNews: Hackers Weaponizing 7-Zip Downloads to Turn Your Home Computers into Proxy Nodes**

ADVANCES IN RMM THREAT INFRASTRUCTURE

Overview & Impact

The intrusion lifecycle frequently begins with phishing or vulnerability exploitation targeting exposed RMM infrastructure or file transfer platforms. Observed exploitation paths include:

- CVE-2024-1709 (ConnectWise ScreenConnect)
- CVE-2025-10035 (GoAnywhere MFT)
- CVE-2024-57726/57727/57728 (SimpleHelp)
- CVE-2025-31161 (CrushFTP)
- CVE-2021-34473 (ProxyShell)
- CVE-2023-48788 (Fortinet EMS)

Post-compromise activity includes:

- Silent installation of RMM agents via MSI or encoded PowerShell.
- Disabling Windows SmartScreen and removing Mark-of-the-Web attributes.
- Service creation masquerading under benign or modified names.
- Lateral movement using RDP, SMB, NTLM, and RPC.
- Data staging via Robocopy and exfiltration over HTTPS or SSH tunnels.
- Use of residential proxies and geographically inconsistent infrastructure.
- Ransomware deployment following extended remote control access.

In ransomware-linked incidents such as Medusa operations, attackers edited RMM server configurations to redirect legitimate agents to malicious servers, enabling centralized attacker control across multiple endpoints.

- Stealth persistence through trusted administrative software, reducing detection by signature-based controls.
- Lateral movement and privilege escalation via legitimate Windows service and management channels.
- Large-scale data exfiltration staged through encrypted RMM sessions, complicating network-layer inspection.
- Encryption of enterprise systems following prolonged dwell time.
- Expanded blast radius due to RMM trust relationships across MSP-managed environments.
- Elevated compliance exposure in healthcare, financial services, government, and technology sectors.

Observations

- 277% year-over-year increase in malicious RMM deployments reported.
- Decline in traditional RAT and malware usage corresponding to increased RMM abuse.
- ScreenConnect, AnyDesk, LogMeIn Rescue, Atera, PDQ Deploy, SimpleHelp, and MeshCentral commonly leveraged.
- Binary and service name modification used to bypass Sigma and Elastic detection rules.
- SmartScreen and security control tampering observed prior to RMM installation.
- Use of Rclone, Robocopy, and encrypted RMM channels for data exfiltration.
- Redundant RMM installation to preserve attacker access if one tool is removed.
- Residential proxy and geographically inconsistent outbound connections following compromise.

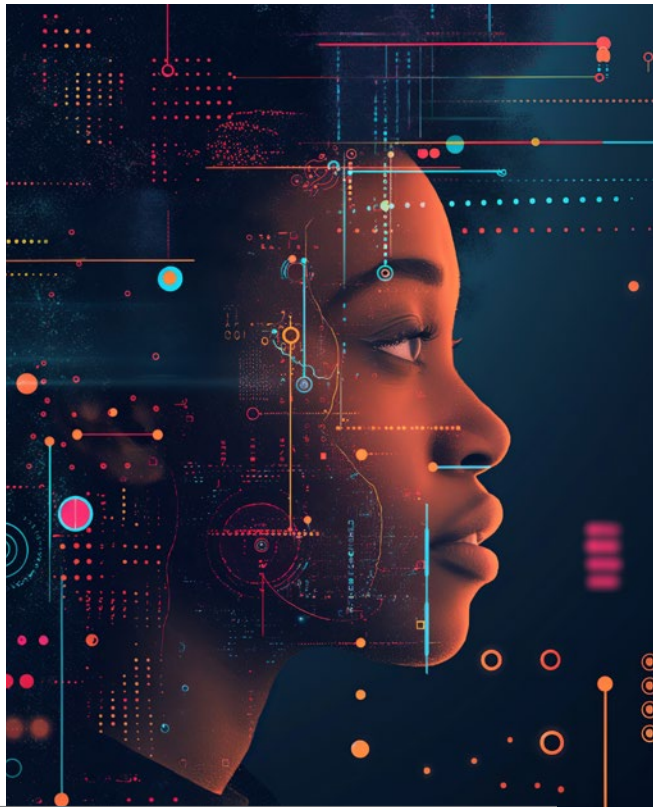
Guidance

Strategic Intelligence

- **Trend**
  - RMM abuse is becoming the preferred command-and-control architecture across ransomware and phishing ecosystems.
  - Attackers are prioritizing trust exploitation over exploit development, reducing reliance on custom malware.
  - The convergence of ransomware operators and initial access brokers around RMM platforms suggests sustained operational standardization rather than isolated campaigns

Operational Intelligence

- **Threat Vectors**
  - Phishing emails delivering RMM installers or encoded scripts
  - Social engineering phone calls convincing users to install remote tools
  - Exploitation of unpatched RMM and file transfer platforms
  - MSI-based silent installations
  - Service creation under modified names
- **Monitoring & Detection Gaps**
  - Lack of allowlisting for RMM binaries
  - Insufficient monitoring of Windows Event ID 7045 (service creation)
  - Limited telemetry around SmartScreen registry changes
  - No correlation between RMM installation and anomalous outbound connections
  - Overreliance on static filename-based detection
- **Response Actions**
  - Immediately inventory all authorized RMM tools
  - Remove unauthorized remote administration software
  - Rotate credentials associated with compromised hosts
  - Revoke active sessions and investigate lateral movement paths
  - Validate integrity of exposed RMM management servers



Tactical Intelligence

- **Mitigation Strategies**
  - Enforce strict RMM allowlists with binary hash validation
  - Restrict outbound connectivity from RMM agents to approved servers only
  - Monitor for renamed or relocated RMM binaries
  - Alert on registry modifications disabling SmartScreen
  - Implement network-based anomaly detection for unusual outbound HTTPS or SSH transfers
- **Preventive Measures**
  - Patch all externally facing RMM and file transfer systems
  - Require MFA and IP restrictions for RMM management consoles
  - Conduct purple-team simulations focused on RMM abuse
  - Validate detection rules against modified service names and binary paths
  - Audit MSP remote access permissions and segmentation controls

Threat Hunting Hypotheses

Unauthorized RMM Service Installation

Hypothesis: An attacker installed an RMM agent under a modified binary or service name to evade detection.

Investigation Steps

- Review Windows Event ID 7045 logs for recent service installations.
- Identify services with uncommon install paths or temp directory origins.
- Correlate service creation with PowerShell execution or MSI installs.
- Compare service names against approved RMM inventory.
- Confirm malicious intent if outbound connections follow service creation within short time windows.

SmartScreen and Security Control Tampering Prior to RMM Deployment

Hypothesis: An attacker disabled SmartScreen protections before installing RMM tooling.

Investigation Steps

- Review registry modifications under SmartScreen-related keys.
- Identify Explorer restarts following registry changes.
- Correlate with elevated PowerShell sessions.
- Search for removal of Mark-of-the-Web attributes on downloaded files.
- Validate by linking registry tampering with subsequent MSI installation events.

Lateral Movement and Data Staging via Legitimate Administrative Tools

Hypothesis: RMM-controlled hosts were used to stage and exfiltrate sensitive data.

Investigation Steps

- Review SMB logs for large file transfers between internal servers.
- Identify Robocopy or Rclone execution.
- Monitor outbound traffic spikes to rare domains or IPs.
- Correlate RMM beaconing with high-volume outbound transfers.
- Validate by establishing deviation from user or server baseline activity.

Detection Rule Evasion Through Binary Renaming

Hypothesis: An attacker renamed MeshAgent or other RMM binaries to evade filename-based detection rules.

Investigation Steps:

- Identify unsigned or recently written executables in Windows Temp directories.
- Extract embedded configuration data from suspected RMM binaries.
- Search for outbound connections to non-approved RMM servers.
- Compare binary hashes against known RMM releases.
- Validate if service creation events reference modified executable paths.

Sources

- **DarkReading: RMM Abuse Explodes as Hackers Ditch Malware**
- **Forcepoint: ScreenConnect Attack: SmartScreen Bypass and RMM Abuse**
- **Darktrace: Medusa Ransomware 2025: RMM Abuse in Ransomware Campaigns**
- **Immersive Labs: RMM Tools Under Attack: Exploring More Effective Detections**
- **CyberProof: Inside the Latest PayPal Scam: RMM Abuse and Credential Theft**

SHINY HUNTERS

Overview & Impact

The intrusion chain begins with voice-based social engineering. Threat actors impersonate internal IT personnel and claim MFA reconfiguration is required. Victims are guided to spoofed SSO portals using domains structured as <company>sso[.]com or <company>internal[.]com, frequently registered through NICENIC or Tucows.

Real-time phishing infrastructure enables attackers to proxy authentication sessions, observe MFA challenge types, and dynamically adjust phishing workflows. This allows bypass of push-based MFA and number-matching techniques by verbally instructing victims during authentication.

Following credential capture, attackers:

- Register attacker-controlled devices for MFA
- Establish OAuth authorizations
- Delete security notification emails
- Move laterally through accessible SaaS environments
- Use PowerShell to extract SharePoint and OneDrive data
- Search cloud repositories using targeted keywords such as "confidential," "internal," "proposal," "vpn," and "salesforce"

In at least one case, compromised email accounts were used to launch additional phishing campaigns targeting cryptocurrency entities, with outbound messages later deleted to reduce detection.

The activity does not exploit vendor vulnerabilities. It exploits identity trust chains, MFA implementation weaknesses, and insufficient helpdesk verification procedures.

- Compromise of SSO credentials enabling full SaaS ecosystem access, effectively bypassing perimeter security controls and shifting compromise to the identity control plane.
- Unauthorized MFA device enrollment enabling persistent access and token-based session continuation even after password resets.
- Exfiltration of sensitive data including PII, internal documents, proposals, and potentially regulated information, increasing compliance exposure and breach notification obligations.
- Secondary operational disruption through DDoS threats, employee harassment, and public data leak site exposure, increasing reputational damage and executive pressure.
- Potential downstream partner compromise through phishing launched from trusted internal mailboxes.

Observations

- Consistent use of vishing to socially engineer MFA enrollment changes.
- Deployment of victim-branded credential harvesting domains mimicking SSO portals.
- Real-time session orchestration to defeat push-based MFA.
- Targeting of Okta customer accounts and broader identity provider environments.
- PowerShell-based SharePoint and OneDrive data extraction.
- Use of Tox for ransom negotiations and Limewire for proof-of-data hosting.
- Escalation to harassment and DDoS threats following extortion noncompliance.
- Infrastructure leveraging residential proxy networks and commercial VPN services.

Guidance

Strategic Intelligence

- **Trend**
  - Identity-layer compromise via social engineering is replacing exploit-driven initial access in SaaS extortion operations.
  - Extortion groups are consolidating around cloud control-plane targeting rather than single-application breaches.
  - The campaign reflects maturation of hybrid phishing operations combining automation with live social engineering, reducing reliance on malware and increasing evasion of traditional endpoint detection.

Operational Intelligence

- **Threat Vectors**
  - Voice phishing impersonating internal IT staff
  - Real-time credential harvesting portals
  - MFA push and number-matching manipulation
  - OAuth abuse and unauthorized device enrollment
- **Monitoring & Detection Gaps**
  - Lack of visibility into MFA enrollment changes
  - Insufficient alerting on new device registrations
  - Inadequate logging correlation between identity provider and SaaS platforms
  - Overreliance on push-based MFA
- **Response Actions**
  - Immediately revoke active session tokens and OAuth grants
  - Disable compromised accounts and revalidate MFA enrollment
  - Temporarily restrict MFA self-service enrollment
  - Enforce high-assurance identity verification for helpdesk interactions
  - Audit SaaS application access logs for bulk download activity

Tactical Intelligence

- **Mitigation Strategies**
  - Implement phishing-resistant MFA (FIDO2 security keys or passkeys)
  - Restrict identity provider administrative privileges
  - Monitor and alert on new MFA device registrations
  - Block known malicious domains and review DNS telemetry
- **Preventive Measures**
  - Conduct simulated vishing exercises
  - Harden helpdesk authentication protocols with out-of-band verification
  - Restrict SaaS access via conditional access policies
  - Educate users on live MFA manipulation tactics

Threat Hunting Hypotheses

Unauthorized MFA Enrollment Following Helpdesk-Themed Calls

Hypothesis: An attacker successfully enrolled an unauthorized MFA device after socially engineering an employee via phone.

Investigation Steps

- Review identity provider logs for new MFA device registrations.
- Correlate MFA enrollment events with recent password resets or helpdesk tickets.
- Identify logins from new IP addresses or residential proxy ASNs following enrollment.
- Compare enrollment timestamps with off-hours activity patterns.
- Correlate OAuth authorization events with MFA changes.
- Confirm success if enrollment is followed by SaaS data access from anomalous geolocation.

Real-Time Phishing Portal Session Proxying

Hypothesis: A user authenticated through a phishing proxy that relayed credentials to a legitimate SSO endpoint.

Investigation Steps

- Analyze web proxy and DNS logs for access to lookalike SSO domains.
- Identify login attempts immediately followed by successful authentication from different IP addresses.
- Review user-agent inconsistencies between login initiation and token issuance.
- Examine IdP logs for simultaneous authentication flows.
- Validate by confirming login token issuance from infrastructure associated with residential proxies.

Bulk SaaS Data Exfiltration Post-SSO Compromise

Hypothesis: Compromised SSO sessions were used to download sensitive SaaS data.

Investigation Steps

- Review SharePoint, OneDrive, Slack, and Salesforce logs for bulk file download activity.
- Search for keyword-based document access patterns.
- Identify PowerShell invocation tied to cloud data export.
- Correlate file download spikes with anomalous IP addresses.
- Validate by establishing volume thresholds exceeding user baselines.

Compromised Email Accounts Used for Secondary Phishing

Hypothesis: An attacker used a compromised mailbox to send outbound phishing before deleting evidence.

Investigation Steps:

- Review email audit logs for sent-message deletions.
- Identify outbound messages to external cryptocurrency or high-risk domains.
- Correlate with login sessions from new IP addresses.
- Examine mailbox rule creation or OAuth app authorizations.
- Confirm if suspicious outbound messages align with compromised session windows.

Sources

- Cloud.google.com: Tracking the Expansion of ShinyHunters-Branded SaaS Data Theft
- DarkReading: ShinyHunters Expands Scope of SaaS Extortion Attacks
- The Hacker News: Mandiant Finds ShinyHunters-Style Vishing Attacks Stealing MFA to Breach SaaS Platforms
- SecurityWeek: ShinyHunters-Branded Extortion Activity Expands, Escalates
- Barracuda Networks Blog: BreachForums Disclosure Surfaces Falling Out Among ShinyHunters Thieves
- Cybersecurity Dive: ShinyHunters Escalates Tactics in Extortion Campaign Linked to Okta Environments
- CSO Online: ShinyHunters Ramp Up New Vishing Campaign with 100s in Crosshairs

pellera

Contact the Pellera Threat Intel Group at getsecure@pellera.com

pellera.com