MARCH

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 March 2026

March 2026 was defined by three threat patterns that share a common thread: attackers are exploiting trust rather than breaking through defenses. Whether it was North Korean operatives exploiting the trust employers place in remote hiring, Iranian-linked groups weaponizing the trust organizations place in their own endpoint management tools, or cybercriminals using phone calls to exploit the trust employees place in their IT departments, the consistent theme was that the people and systems designed to enable business became the attack surface.

The most consequential event was the **Stryker Corporation wiper attack** on March 11. An Iranian-linked group called Handala used Microsoft Intune's built-in wipe command to reset roughly 80,000 endpoints across 79 countries at a Fortune 500 medical technology company. No malware was involved. The attackers got in through administrator credentials that had been harvested by infostealer malware months earlier, created a new Global Admin account, and turned the company's own device management against it. CISA, the White House, FBI, and HHS all engaged directly. The attack has changed how the industry should think about endpoint management security.

On the workforce infiltration front, the **U.S. Treasury sanctioned six individuals and two entities tied to North Korean IT worker fraud networks** that generated nearly $800 million in 2024. DTEX named specific operatives, GitLab banned 131 accounts linked to the Contagious Interview malware campaign, and KELA reported that North Korean workers have expanded beyond IT into architecture and industrial design. The scale of the operation is now visible in a way it was not before.

At the same time, social engineering continued its rise as a primary initial access method. **ShinyHunters ran vishing campaigns against more than 100 organizations** including Workday, Optimizely, and Aura. Microsoft DART documented an attacker who impersonated IT support through Teams voice calls and used Quick Assist to deploy malware. Ericsson disclosed that a single vishing call to a vendor employee exposed data for over 15,000 people. The Payroll Pirates group kept stealing employee paychecks through phished payroll credentials. Across all of these incidents, no software vulnerability was required. The attackers just needed someone to answer the phone.

Executive Overview

IRAN-RELATED CYBER ACTIVITY

Audience

- CISO
- Security Operations Tesms
- Risk Management Professionals
- IT Operations Managers & Teams
- IT Security Managers
- Incident Response Teams

RISK

GEOGRAPHIC SCOPE

BUSINESS IMPACT

On February 28, the U.S. and Israel launched coordinated strikes against Iran. Iranian internet connectivity collapsed almost immediately. Despite this, hacktivist groups based outside Iran launched sustained cyber campaigns against Israeli, American, and allied targets. At least 60 groups were active within days, many coordinating through an "Electronic Operations Room" on Telegram.

The Stryker attack on March 11 was the most consequential incident. Handala claimed to have wiped over 200,000 devices and stolen 50 terabytes of data. BleepingComputer reported that the attackers compromised an administrator account, created a new Global Admin, and used Intune's wipe command on roughly 80,000 managed endpoints. Stryker confirmed no ransomware or malware was found on its systems.

In the aftermath, CISA issued an advisory urging organizations to harden their Intune environments. Microsoft published administrative hardening guidance. The White House National Cyber Director, FBI, CISA, and HHS all engaged directly with Stryker. The government seized domains linked to Handala's infrastructure. Forbes reported on March 18 that two senior Iranian cyber operations leaders were killed in airstrikes.

READ MORE > IRAN-RELATED CYBER ACTIVITY

NORTH KOREAN IT WORKER FRAUD AND INFILTRATION

Audience

- CISO
- Security Operations Teams
- IT Managers
- Incident Response Teams
- Risk Management Professionals
- Human Resources Leadership

RISK

GEOGRAPHIC SCOPE

BUSINESS IMPACT

On March 12, OFAC sanctioned six individuals and two entities operating out of Vietnam, Laos, and Spain for facilitating North Korean IT worker fraud. Treasury identified a key facilitator who converted roughly $2.5 million into cryptocurrency for DPRK workers between 2023 and 2025. The sanctions designated 21 cryptocurrency addresses across Ethereum and Tron networks.

DTEX published research the same week identifying two operatives using the personas "Naoki Murano" and "Jenson Collins." Both were traced to a cell that operated from Laos before relocating to Russia. The Murano persona was previously linked to a $6 million theft from crypto firm DeltaPrime. DTEX also released over 1,000 email addresses connected to North Korean IT worker operations.

GitLab disclosed banning 131 North Korean accounts, most tied to JavaScript repositories that served as loaders for BeaverTail and Ottercookie malware as part of the Contagious Interview campaign. GitLab identified one eight-person cell that earned $1.64 million over roughly three years. KELA separately reported that North Korean workers are now operating in architecture and industrial design roles, not just IT.

READ MORE > NORTH KOREAN IT WORKER FRAUD AND INFILTRATION

Audience

- **CISO**
- **IT Managers**
- **IT Security Managers**
- **Security Operations Teams**
- **Risk Management Professionals**
- **Human Resources Leadership**

SOCIAL ENGINEERING, VISHING, AND HR-TARGETED ATTACKS

RISK

GEOGRAPHIC SCOPE

BUSINESS IMPACT

ShinyHunters, a cybercrime group connected to The Com collective, conducted vishing campaigns against Workday, Optimizely, and Aura during the reporting period. The Workday breach compromised a third-party vendor's customer support system, exposing customer names, emails, and phone numbers across its 11,000-plus client base. Optimizely disclosed on February 11 that a vishing attack compromised internal systems including Zendesk, Salesforce CRM, and internal documents. Aura confirmed on March 18 that approximately 900,000 records were exposed, including 35,000 actual customers. ShinyHunters leaked the data after Aura declined to pay.

Microsoft DART documented a separate November 2025 vishing campaign where the attacker impersonated IT support through Teams voice calls. After two failed attempts, the attacker convinced a third employee to grant Quick Assist remote access, then deployed encrypted loaders and proxy-based C2 connectivity. Ericsson disclosed that a vishing attack against a third-party vendor in April 2025 exposed names, Social Security numbers, financial data, and medical information for 15,661 individuals. The Payroll Pirates continued targeting payroll systems using phishing and malicious search ads to redirect employee direct deposits.

READ MORE > SOCIAL ENGINEERING, VISHING, AND HR-TARGETED ATTACKS

Tactical Guidance

IRAN-RELATED CYBER ACTIVITY

Overview & Impact

The conflict produced two distinct threat categories. The first was the broad hacktivist response. Groups including Handala, APT Iran, Cyber Islamic Resistance, Dark Storm Team, and dozens of others claimed attacks ranging from DDoS and defacement to data theft and SCADA access. Many organized under an Electronic Operations Room established on Telegram on February 28. Pro-Russian hacktivist groups actively collaborated with pro-Iranian collectives, broadening the coalition.

The second was the Stryker wiper attack, which was in a different league. Coalition Inc.'s analysis found that infostealer malware had harvested Stryker administrator credentials for SSO, ITSM, and password management platforms months before the attack. Those credentials were sitting in underground logs, apparently never rotated. The attackers used them to access Microsoft Intune, created their own Global Administrator account, and issued remote wipe commands that reset laptops, desktops, servers, and mobile devices to factory settings across the globe. The attack launched shortly after midnight on March 11.

The attack chain broke down as follows:

- Initial access through compromised credentials from infostealer logs, including SSO and ITSM platforms
- Privilege escalation to Intune administrator, then creation of a new Global Administrator account
- No malware deployed – the attacker used Intune's native wipe and reset commands
- Approximately 80,000 managed endpoints wiped to factory settings across 79 countries
- Stryker employees found devices reset when they arrived at work; some were sent home
- 80,000 to 200,000 endpoints wiped across 79 countries at a Fortune 500 medical technology company.
- Order processing, manufacturing, and shipping disrupted globally.
- Patient-specific surgical cases rescheduled due to supply chain delays.
- Stryker confirmed it does not carry cyber insurance.
- California DFPI and New York DFS issued bulletins to financial institutions warning of heightened cyber risk.
- Fitch Ratings warned that hacktivists and state-sponsored groups may target critical infrastructure and U.S. public entities.
- All Stryker medical products remained safe and operational, as they run independently of the corporate Microsoft environment.

Observations

- Handala used Intune's native wipe functionality instead of deploying custom wiper malware. This bypasses endpoint detection entirely and applies to any MDM or endpoint management tool.
- Infostealer-sourced credentials provided the likely initial access. Credentials for SSO, ITSM, and password management platforms were available in underground logs months before the attack.
- The attackers created a new Global Administrator account after initial compromise, showing they understood the target environment well enough to establish their own persistent administrative access.
- Over 60 hacktivist groups were active within days of the military strikes, many coordinating through Telegram channels established on February 28.

- Unit 42 identified a phishing campaign using a fake Israeli Home Front Command RedAlert app to deliver mobile surveillance malware.
- Cybercriminals in the UAE exploited the conflict for vishing scams impersonating the Ministry of Interior to steal identification numbers.
- INC Ransomware listed an Israeli industrial company on its leak site and replaced the logo with a swastika, weaponizing the conflict for ideological purposes.

Guidance

Strategic Intelligence

- **Trend**
  - Iran has spent over fifteen years building cyber capabilities as a force multiplier alongside kinetic operations. The current conflict has activated those capabilities, though not entirely as expected. The loss of internet connectivity inside Iran has degraded state-sponsored groups, but proxy groups operating outside the country continue with apparent tactical autonomy.
  - The killing of Yahya Hosseiny Panjaki, who reportedly oversaw the MOIS unit controlling Handala, could fragment command and control. It could also result in less restrained activity from groups that are no longer receiving centralized guidance.
  - The Stryker attack demonstrated that the bar for destructive operations has dropped significantly. The attackers did not need zero-days or custom malware. They needed valid credentials and knowledge of how Intune works. Any organization with centralized endpoint management, which is most large enterprises, should treat this attack path as immediately relevant to their own environment.

Operational Intelligence

- **Threat Vectors**
  - Spearphishing with credential-harvesting attachments and links
  - Exploitation of public-facing applications including Fortinet FortiOS, Exchange ProxyShell, and VMware Horizon
  - Password spraying against cloud identity platforms
  - Abuse of legitimate RMM tools such as ScreenConnect and Atera
  - Exploitation of VPN and RDP endpoints with stolen credentials
  - Weaponization of Microsoft Intune through compromised administrative credentials
- **Monitoring & Detection Gaps**
  - No multi-admin approval requirement for Intune wipe commands
  - Credentials available in infostealer marketplaces without forced rotation
  - Lack of alerting on new Global Administrator account creation
  - Insufficient correlation between identity platform authentication and Intune administrative actions
  - Limited monitoring of hacktivist Telegram channels for targeting claims

- **Response Actions**
  - Immediately audit all Global Administrator and Intune administrator accounts
  - Check infostealer marketplaces for any corporate credentials and force rotation on anything found
  - Verify that no new administrative accounts have been created outside of approved change windows
  - Review Intune audit logs for any wipe or reset commands issued in the past 90 days
  - Block known hacktivist infrastructure and domains linked to Handala

Tactical Intelligence

- **Mitigation Strategies**
  - Require phishing-resistant MFA on all administrative accounts, especially those with access to endpoint management and identity platforms
  - Implement multi-admin approval for sensitive Intune actions including device wipes and RBAC modifications
  - Restrict and monitor creation of new Global Administrator accounts
  - Deploy conditional access policies with risk-based signals for administrative sessions
- **Preventive Measures**
  - Patch all internet-facing infrastructure, prioritizing entries in the CISA KEV catalog
  - Disable unused remote access tools and ports
  - Implement geographic IP blocking for regions where the organization does not conduct business
  - Rebuild business continuity plans around total-loss wiper scenarios, not just recoverable ransomware
  - Establish out-of-band communications that do not depend on corporate Microsoft infrastructure
  - Review DDoS mitigation playbooks given the volume of hacktivist activity

Threat Hunting Hypotheses

Compromised Credentials Targeting Endpoint Management

Hypothesis: An attacker with infostealer-sourced credentials has accessed our identity platform and is positioning to escalate to endpoint management administrative roles.

Investigation Steps

- Query identity platform logs for authentication from unusual locations, devices, or times.
- Cross-reference corporate domains against known infostealer marketplace exposure.
- Look for sequences where an account authenticates to the identity platform and then accesses Intune administration within the same session.
- Review whether any new administrative accounts have been created in the past 90 days outside of approved changes.
- Check for changes to RBAC assignments in Intune that were not part of documented change requests.
- If validated, immediately disable the compromised account, revoke all sessions, and conduct a full review of Intune administrative actions performed by that account.

Hacktivist Reconnaissance Against Public Infrastructure

Hypothesis: Pro-Iranian hacktivist groups have conducted reconnaissance or initial access attempts against our public-facing infrastructure in response to the ongoing conflict.

Tactical Guidance

Investigation Steps

- Review WAF and firewall logs for increased scanning or exploitation attempts from Middle Eastern or Eastern European IP ranges since February 28.
- Look for spikes in DDoS traffic or connection attempts against public-facing services.
- Check whether the organization or its industry has been mentioned in hacktivist Telegram channels.
- Search for exploitation attempts targeting Fortinet, Exchange ProxyShell, and Log4Shell vulnerabilities.
- If confirmed, block source infrastructure, increase monitoring, and verify patching on targeted systems.

Sources

- Banking Dive: Bank regulators warn of increased cyber risk from Iran war (March 12, 2026)
- ABC News: Iran-linked hackers take aim at US and other targets (March 12, 2026)
- Cybersecurity Dive: US entities face heightened cyber risk related to Iran war (March 10, 2026)
- SentinelOne: Intelligence Brief – Iranian Cyber Activity Outlook (February 28, 2026)
- Unit 42: Threat Brief – March 2026 Escalation of Cyber Risk Related to Iran (March 3, 2026)
- Sophos: Initial access techniques used by Iran-based threat actors (March 13, 2026)
- BleepingComputer: CISA urges US orgs to secure Microsoft Intune systems after Stryker breach (March 19, 2026)
- SecurityWeek: Iranian Hackers Likely Used Malware-Stolen Credentials in Stryker Breach (March 18, 2026)
- Stryker: Customer Updates – Stryker Network Disruption (March 11–19, 2026)
- Coalition Inc: How Infostealers May Have Opened the Door to the Stryker Wipe (March 12, 2026)
- SecurityWeek: MedTech Giant Stryker Crippled by Iran-Linked Hacker Attack (March 11, 2026)
- Dark Reading: Why Stryker's Outage Is a Disaster Recovery Wake-Up Call (March 12, 2026)

NORTH KOREAN IT WORKER FRAUD AND INFILTRATION

Overview & Impact

North Korea runs what amounts to a state-backed staffing agency. Thousands of IT workers are placed at Western companies under fabricated identities, and their salaries flow back to fund weapons programs. DTEX researcher Michael Barnhart has described it as a "state-sanctioned crime syndicate" spanning multiple North Korean government organizations including the Munitions Industry Department, the Reconnaissance General Bureau, and Bureau 39.

The workers typically operate from China, Russia, Hong Kong, or Southeast Asia. They use VPNs, virtual private servers, and laptop farms to mask their locations. Some work multiple jobs at once, juggling four to six positions under different personas. The earnings get converted to cryptocurrency through facilitators and routed back through layered wallets. Chainalysis traced one facilitator who moved $2.5 million in crypto between mid-2023 and mid-2025.

Running alongside the employment fraud is the Contagious Interview campaign. North Korean actors pose as recruiters and trick real developers into running malicious code during fake technical interviews. GitLab found that most of the 131 banned accounts were tied to JavaScript repositories acting as obfuscated loaders for malware. Once a developer runs the code, BeaverTail and Ottercookie payloads give the attackers access to credentials, cryptocurrency wallets, and browser data.

Flare and IBM X-Force published a joint report documenting how these operations use infostealer malware to harvest credentials from compromised machines. The stolen credentials appear on underground marketplaces and cover platforms like Indeed, Upwork, LinkedIn, and Fiverr, giving the operatives ready access to job platforms and enabling further identity fraud.

- Nearly $800 million generated for DPRK weapons programs through IT worker fraud in 2024 alone.
- Microsoft estimates over 10,000 North Korean IT workers active globally.
- Fortune 500 companies have unknowingly hired North Korean operatives.
- $6 million stolen from DeltaPrime by an operative linked to the Murano persona.
- $1.5 billion stolen from Bybit in February 2026 by North Korean hackers, the largest crypto heist on record.
- One eight-person cell earned $1.64 million across three years of GitLab-based activity.
- Workers with corporate access have introduced malware, stolen proprietary data, and extorted their employers when confronted.
- Operations have expanded into architecture and industrial design, creating potential access to U.S. infrastructure designs.

Observations

- Personas are reused across multiple employers, sometimes for years, with some operatives holding four to six concurrent positions.
- AI tools are being used to generate synthetic identities, create custom code obfuscators, and modify facial features for video interviews.
- Infostealer logs from suspected DPRK worker machines contain compromised credentials for Indeed, Upwork, LinkedIn, Fiverr, and freelancing platforms.
- The Contagious Interview campaign uses GitLab JavaScript repositories as obfuscated loaders for BeaverTail and Ottercookie malware.
- Workers live and work under physical surveillance by North Korean state security, with cameras in their workspaces and minders tracking output quotas.
- Cryptocurrency addresses sanctioned by OFAC span both Ethereum and Tron, indicating a multi-chain laundering approach designed to complicate tracing.

Guidance

Strategic Intelligence

- **Trend**
  - This is not a conventional cyber threat. It is a revenue generation program that happens to create espionage access as a side effect. The North Korean government has organized thousands of workers into a global workforce that funds weapons development through legitimate employment.

- The expansion into non-IT fields like architecture and industrial design suggests a deliberate effort to access physical infrastructure plans, which has intelligence value beyond financial gain.
- Enforcement is having some effect. The OFAC sanctions, GitLab bans, and DTEX exposure are forcing operatives to adopt more sophisticated identity management. But the fundamental vulnerability remains: remote hiring processes that cannot reliably confirm who is actually doing the work.

Operational Intelligence

- **Threat Vectors**
  - Fabricated resumes and stolen identities submitted through standard hiring channels
  - Consumer VPNs and VPS infrastructure for location masking
  - Laptop farms enabling multiple simultaneous remote positions
  - AI-generated profile photos and deepfake video modifications
  - Contagious Interview campaign using fake recruiter personas to deliver malware
  - Cryptocurrency facilitators converting earnings across Ethereum, Tron, and Bitcoin
- **Monitoring & Detection Gaps**
  - Background verification processes that rely on documents without independent confirmation of identity
  - No systematic screening of remote contractor email addresses against known DPRK indicators
  - Lack of device-level controls to detect laptop farm configurations
  - Insufficient monitoring of code repository activity for Contagious Interview patterns
  - Limited visibility into cryptocurrency payment flows for contractor compensation
- **Response Actions**
  - Cross-reference current remote contractors against the 1,000+ email addresses published by DTEX
  - Audit code repository activity for accounts matching known Contagious Interview patterns
  - Review payroll and contractor payments for cryptocurrency-related indicators
  - Flag any remote workers whose employment history cannot be independently verified
  - Report suspected DPRK workers to the FBI before taking any action that might alert the operative

Tactical Intelligence

- **Mitigation Strategies**
  - Require live, unscripted video interviews with real-time identity verification for all remote hires
  - Implement enhanced background checks that go beyond document review to include digital footprint analysis
  - Use sandboxed environments for any code exercises during technical interviews
  - Screen cryptocurrency transactions against OFAC sanctions lists, including the 21 newly designated addresses

- **Preventive Measures**
  - Deploy device management controls capable of detecting laptop farm setups including multiple user sessions and VPN patterns
  - Monitor GitHub and GitLab for newly created accounts pushing JavaScript repositories with obfuscated loaders
  - Cross-reference candidate information against indicators published by DTEX, GitLab, KELA, and government advisories
  - Verify freelance platform profiles have authentic work history that can be independently confirmed
  - Include HR and recruiting teams in security awareness training focused specifically on DPRK IT worker tradecraft

Threat Hunting Hypotheses

North Korean Operative in Contractor Workforce

Hypothesis: A current remote contractor or freelancer is a North Korean IT worker operating under a fabricated identity and generating revenue for the DPRK weapons program.

Investigation Steps

- Review remote contractors hired in the past 24 months against DTEX's published email list and known DPRK worker patterns.
- Check VPN connection logs for access from Laos, Russia (Khabarovsk, Vladivostok), China, or Southeast Asia.
- Look for contractors working unusual hours that align with East Asian time zones rather than their claimed location.
- Verify identity documents match a real person with employment history that can be independently confirmed.
- Flag any contractor managing code repositories with characteristics matching Contagious Interview loaders.
- If indicators are found, engage legal and HR before taking action. Report to the FBI. Do not alert the suspected operative.

Contagious Interview Malware Execution

Hypothesis: A developer in our environment has been targeted by the Contagious Interview campaign and may have executed malicious code from a fake technical interview.

Investigation Steps

- Search endpoint telemetry for execution of JavaScript projects from recently created GitLab or GitHub repositories.
- Look for BeaverTail or Ottercookie indicators in EDR data.
- Check for outbound connections to known Contagious Interview C2 infrastructure.
- Review developer email for recruitment messages directing them to code repositories or take-home coding tests.
- Correlate any suspicious repository clones with subsequent credential access or browser data exfiltration.
- If validated, isolate the affected endpoint, collect forensic images, and scan for lateral movement.

Sources

- U.S. Department of the Treasury: Treasury Sanctions Facilitators of DPRK IT Worker Fraud Targeting U.S. Businesses (March 12, 2026)
- WIRED: North Korean IT Workers Are Being Exposed on a Massive Scale (May 14, 2025)
- Flare / IBM X-Force: Inside the North Korean Infiltrator Threat (March 18, 2026)
- CSO Online: North Korean fake IT worker tradecraft exposed (March 12, 2026)
- KELA: Hidden Threat – North Korean IT Workers Exposed (October 10, 2025)
- Chainalysis: OFAC Targets DPRK IT Workers Using Crypto (March 12, 2026)

SOCIAL ENGINEERING, VISHING, AND HR-TARGETED ATTACKS

Overview & Impact

Several distinct threat streams converged this month, all exploiting the human element.

ShinyHunters has been running a sustained vishing campaign since 2025, targeting SSO platforms including Okta, Microsoft, and Google along with downstream SaaS applications. Their toolkit includes phishing pages that match the specific authentication flow of each victim organization, harvesting both credentials and MFA codes in real time. Mandiant warned in January 2026 that the group was expanding to more cloud platforms and seeking more sensitive data for extortion. They have also started harassing employees and business partners to pressure organizations into paying.

The Microsoft DART case illustrated a different pattern. The attacker used Teams voice calls to impersonate IT support, failed twice with different employees, and succeeded on the third attempt. Once the target granted Quick Assist access, the attacker pivoted to deploying an MSI package that sideloaded a malicious DLL, established C2 through proxied connections, and began session hijacking. Everything was designed to look like normal enterprise activity.

The Payroll Pirates represent the financial crime side. They use phishing and malvertising to capture employee payroll credentials, then change direct deposit routing. They create email rules to suppress change notifications, so employees often do not realize their pay has been stolen until it is gone. The group started in education and manufacturing but is expanding across sectors. With 200 interfaces and over 500,000 users targeted, this is a growing operation.

- Workday vendor breach exposed customer support data for organizations across the Fortune 500 (Workday serves over 60% of Fortune 500 companies).
- Optimizely internal systems compromised including Zendesk, Salesforce CRM, and internal documents. The attacker was unable to escalate further or install persistent malware.
- Aura breach exposed 900,000 records including names, emails, home addresses, and phone numbers for 35,000 customers. ShinyHunters leaked the data publicly.
- Ericsson vendor breach affected 15,661 individuals with exposed data including SSNs, driver's licenses, passport numbers, financial data, and medical information.
- Microsoft Teams vishing campaign compromised a corporate environment through a single successful call, though DART contained it quickly.
- Payroll Pirates targeted over 500,000 users across 200 interfaces, stealing wages directly from employee paychecks.

Observations

- Vishing attacks are pairing live phone calls with real-time credential harvesting pages that dynamically match the victim's specific authentication flow. Generic phishing awareness training does not prepare employees for this.
- Microsoft Teams is being used as an initial access vector. Attackers impersonate IT support through voice calls placed directly within the platform, exploiting the inherent trust employees place in internal communication tools.
- Quick Assist, a built-in Windows remote access tool, was weaponized for initial access. Once the attacker had remote control, they deployed payloads via MSI packages with DLL sideloading.
- ShinyHunters is escalating beyond data theft into employee harassment and extortion. When Aura declined to pay, the group leaked the data publicly.
- Third-party vendor employees remain a primary target. Both the Ericsson and Workday breaches started with vendor compromise, not a direct attack on the target organization.
- Payroll Pirates create email suppression rules after changing direct deposit details, hiding notification emails so employees do not discover the theft until payday.

Guidance

Strategic Intelligence

- **Trend**
  - Technical exploits are still used, but when an attacker can pick up the phone, impersonate IT support, and walk away with credentials and remote access in under 30 minutes, there is less incentive to hunt for zero-days. ShinyHunters has effectively industrialized vishing as a scalable initial access method across more than 100 organizations.
  - HR and payroll systems are becoming a distinct attack category. These systems hold sensitive personal and financial data. The Payroll Pirates campaign shows attackers can monetize access directly through payroll diversion without needing to exfiltrate and sell data on the dark web.
  - The third-party vendor problem is not new, but vishing has made it worse. An organization can enforce MFA, train employees, and implement monitoring, but none of that matters if a vendor's help desk employee falls for a phone call. The Ericsson breach is a clear example: one call exposed data for over 15,000 people, and Ericsson did not learn about it for seven months.

Operational Intelligence

- **Threat Vectors**
  - Voice phishing impersonating internal IT staff or vendor support personnel
  - Real-time credential harvesting portals that match the victim's specific SSO flow
  - MFA push manipulation and number-matching social engineering
  - OAuth abuse and unauthorized device enrollment following credential capture
  - Malicious search engine ads redirecting to fake payroll login pages
  - Microsoft Teams voice calls from external unverified accounts
- **Monitoring & Detection Gaps**
  - Lack of visibility into MFA enrollment changes and new device registrations
  - Insufficient logging correlation between identity providers and downstream SaaS platforms
  - Overreliance on push-based MFA that can be manipulated through social engineering
  - No monitoring of email rule creation for suppression of payroll notifications
  - Limited controls on inbound Teams communications from external accounts
- **Response Actions**
  - Revoke active session tokens and OAuth grants for any suspected compromised accounts
  - Disable compromised accounts and revalidate MFA enrollment
  - Temporarily restrict MFA self-service enrollment during active investigation
  - Audit SaaS application access logs for bulk download or data export activity
  - Review email rules for any suppressing payroll or HR notifications

Tactical Intelligence

- **Mitigation Strategies**
  - Deploy phishing-resistant MFA using FIDO2 security keys for all SSO and privileged access
  - Disable Quick Assist and audit all remote access tools across the environment
  - Restrict inbound Microsoft Teams communications from unmanaged external accounts
  - Require dual approval from HR and payroll for any direct deposit or routing changes
- **Preventive Measures**
  - Enforce out-of-band verification for all credential reset or access change requests
  - Require third-party vendors to demonstrate MFA enforcement and provide breach notification within contractually defined timeframes
  - Monitor for new email forwarding rules, especially those suppressing notifications from payroll or IT systems
  - Conduct vishing-specific awareness training covering IT impersonation through collaboration platforms, not just email phishing
  - Include vendor security requirements in procurement contracts with regular compliance verification

Threat Hunting Hypotheses

Credential Theft via Vishing for SaaS Access

Hypothesis: An attacker used a vishing call to obtain employee SSO credentials and is accessing internal SaaS platforms under the guise of a legitimate user.

Investigation Steps

- Identify user accounts that authenticated to multiple SaaS platforms from a new device or location within a short window.
- Look for access to CRM, support, or document systems that the user does not normally access.
- Review whether any data exports or bulk queries occurred from those sessions.
- Check for new device enrollment in the identity provider following a recent password reset or MFA change.
- Correlate with any reports of suspicious phone calls received by employees.
- If validated, revoke SSO sessions, reset credentials, review all SaaS activity from the compromised session, and notify affected customers if data was accessed.

Payroll Diversion Through Compromised Credentials

Hypothesis: An attacker has compromised a payroll system credential through phishing or malvertising and is modifying direct deposit information for one or more employees.

Investigation Steps

- Query payroll system logs for recent direct deposit changes.
- Cross-reference with email rule creation events for the same users, especially rules suppressing payroll notifications.
- Look for payroll login from devices or locations that do not match the employee's normal pattern.
- Check web proxy logs for access to known malvertising landing pages mimicking payroll providers.
- If validated, freeze the affected changes, contact the employee, reset credentials, remove malicious email rules, and report to financial institutions for potential fund recovery.

Sources

- SBAM: Payroll Pirates – How Cybercriminals Are Hijacking Paychecks (January 19, 2026)
- HR Dive: Hackers target Workday in social engineering attack (August 21, 2025)
- Cyber Security News: Microsoft Teams Support Call Leads to Quick Assist Compromise (March 18, 2026)
- The Register: Ericsson breach blamed on third-party vendor vishing attack (March 10, 2026)
- CPO Magazine: Suspected ShinyHunters Vishing Attack Hits Optimizely (March 3, 2026)
- BleepingComputer: Aura confirms data breach exposing 900,000 marketing contacts (March 18, 2026)
- Aura: Statement on Exposure of Customer Information (March 19, 2026)
- DynaFile: Healthcare HR Under Siege (2026)

pellera

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

pellera.com