COLORTOKENS

ColorTokens Threat Advisory

Threat Intelligence Brief #7

August 31, 2025

Threat Intelligence Brief

August 16 - 31, 2025

Executive Summary

Cyber Threat Intelligence (CTI) is critical in understanding and mitigating the evolving threats faced by various industries, like healthcare, finance & manufacturing industry.

- Healthcare organizations are frequent targets for cybercriminals due to the high value of patient data and the critical nature of their services. Ransomware attacks and data breaches can disrupt operations and risk patient safety by shutting down medical devices or hospital networks. CTI in healthcare helps identify threat actors, vulnerabilities in connected medical devices, and the latest attack tactics. By integrating CTI, healthcare providers can proactively strengthen defenses, protect sensitive data, and maintain patient care continuity

- The finance sector faces continuous threats, including ransomware, Distributed Denial of Service (DDoS), and phishing attacks. Cybercriminals often target financial institutions to access valuable data or to extort money. CTI assists financial organizations in identifying emerging threats, such as new phishing tactics or advanced DDoS methods. By leveraging CTI, these organizations can better protect sensitive financial information, comply with regulations, and maintain trust with clients by preventing data breaches and financial losses.

- Effective CTI helps these sectors stay ahead of adversaries by identifying threat actors, tactics, and indicators of compromise (IOCs).



Section 1 - Critical Vulnerability Information

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2025-43300	Apple Image I/O out-of-bounds write (RCE via malicious image)	8.8 (CVSS v3.1)	Processing a crafted image can corrupt memory and allow code execution; Apple notes targeted in-the-wild exploitation.	iOS/iPadOS ≤ 18.6.1; iPadOS 17 ≤ 17.7.9; macOS Sequoia < 15.6.1, Sonoma < 14.7.8, Ventura < 13.7.8 (see NVD CPEs)	Update to iOS/iPadOS 18.6.2, iPadOS 17.7.10, macOS 15.6.1 / 14.7.8 / 13.7.8.	https://www.cve.org/CVERecord?id=CVE-2025-43300
CVE-2025-7775	Citrix NetScaler ADC/Gateway memory overflow – exploited in the wild	9.2	Memory overflow can lead to RCE/DoS when configured as Gateway/AAA; Citrix and CISA confirm active exploitation on disclosure (Aug 26).	NetScaler ADC/Gateway 14.1 < 14.1-47.48, 13.1 < 13.1-59.22; 13.1-FIPS/NDcPP < 13.1-37.241-FIPS/NDcPP; 12.1-FIPS/NDcPP < 12.1-55.330-FIPS/NDcPP	Upgrade to 14.1-47.48+, 13.1-59.22+, 13.1-37.241-FIPS/NDcPP+, 12.1-55.330-FIPS/NDcPP+.	https://www.cve.org/CV ERecord?id=CVE-2025-7775
CVE-2025-7776	Citrix NetScaler ADC/Gateway memory overflow (Gateway with PCoIP profile)	8.8	Authenticated attacker can trigger memory overflow causing DoS/erratic behavior on Gateways with bounded PCoIP profile.	Same NetScaler release families as above prior to fixed builds	Upgrade to fixed builds per Citrix bulletin (same versions as above).	https://www.cve.org/CVERecord?id=CVE-2025-7776
CVE-2025-8424	Citrix NetScaler improper access control (Mgmt interface)	8.7	Improper access control on management interfaces (NSIP/Cluster/GSLB/SNIP with mgmt access) can allow unauthorized access.	Same NetScaler release families as above prior to fixed builds	Upgrade to fixed builds per bulletin; restrict mgmt access.	https://www.cve.org/CVERecord?id=CVE-2025-8424
CVE-2025-57819	Sangoma FreePBX Endpoint module auth bypass SQLi RCE (actively exploited)	10.0 (CVSS v4)	Insufficient input sanitization lets unauthenticated attackers reach the Admin UI, manipulate DB, and chain to RCE; exploitation observed since Aug 21.	FreePBX 15 < 15.0.66, 16 < 16.0.89, 17 < 17.0.3	Update Endpoint module to 15.0.66 / 16.0.89 / 17.0.3 and lock down Admin access/ACLs.	https://www.cve.org/CVERecord?id=CVE-2025-57819

Critical Vulnerability:

Apple fixes new zero-day flaw exploited in targeted attacks

Apple has issued emergency security updates to address a newly discovered zero-day vulnerability exploited in what it describes as an “extremely sophisticated attack.”

Identified as CVE-2025-43300, the flaw stems from an out-of-bounds write issue in the Image I/O framework, which handles reading and writing various image formats. This type of vulnerability occurs when attackers manipulate input so the program writes data outside the intended memory buffer, potentially causing crashes, data corruption, or even remote code execution.

According to Apple’s advisory, the issue “may have been exploited in a highly targeted attack.” The company fixed the flaw by improving bounds checking, noting that “processing a malicious image file could lead to memory corruption.”

The patch is available in iOS 18.6.2, iPadOS 18.6.2, iPadOS 17.7.10, macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8.

Devices affected include:

- iPhone XS and later
- iPad models: iPad Pro 13-inch, iPad Pro 12.9-inch (3rd gen and later), iPad Pro 11-inch (1st gen and later), iPad Air (3rd gen and later), iPad (7th gen and later), iPad mini (5th gen and later), and older
- Macs running macOS Sequoia, Sonoma, and Ventura

Apple has not disclosed details about the attackers or the exact nature of the exploitation but recommends installing the updates immediately.

Note:

- The details provided about CVE vulnerabilities are based on publicly available sources, security advisories, and threat intelligence feeds. While efforts are made to ensure accuracy, the information may change over time.
- The severity scores (CVSS) and descriptions are for general reference. Organizations must conduct their own risk assessments based on their unique environment, configurations, and security posture.
- While patching and mitigation recommendations are provided, implementation decisions should be made based on an organization’s security policies, compatibility testing, and vendor guidance.
- CVEs may be updated with new exploitation techniques or patches over time. Regular monitoring of official sources (e.g., NVD, MITRE, vendor advisories) is recommended.

FortiWeb Version	Affected Releases	Recommended Action
FortiWeb 8.0	Not affected	Not applicable
FortiWeb 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiWeb 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
FortiWeb 7.2	7.2.0 through 7.2.10	Upgrade to 7.2.11 or above
FortiWeb 7.0	7.0.0 through 7.0.10	Upgrade to 7.0.11 or above

References:

- https://www.marketwatch.com/press-release/sanderling-healthcare-data-breach-under-investigation-by-levi-korsinsky-llp-faef116f
- https://www.classactionlawyers.com/blog/sanderlinghealth

Section 2 - Reported Cyber Breaches

Title: Healthcare Services Group data breach impacts 624,000 people

Impacted Sector: Healthcare

Attack Summary:

The Healthcare Services Group (HSGI) is alerting more than 600,000 individuals that their personal information was exposed in a security breach last year.

The healthcare services provider stated that it detected unauthorized access to its network on October 7, 2024, and subsequently discovered that the intrusion had begun on September 27. The investigation that followed revealed that the intruders had exfiltrated data from the systems they had accessed.

"The investigation concluded that an unauthorized actor may have accessed and copied specific files from our computer systems between September 27, 2024, and October 3, 2024," the notification states.

"Consequently, we conducted a thorough review of the affected files to identify whether they contained sensitive information—and whose data may have been involved."

This comprehensive process took approximately ten months, with affected individuals receiving breach notifications only on August 25, 2025.

Healthcare Services Group—a publicly traded Pennsylvania company—provides support services such as housekeeping, dining, laundry, and maintenance to healthcare facilities nationwide.

The organization has an annual revenue of $1.7 billion, and its services are of strategic importance to the safe and smooth functioning of thousands of healthcare facilities in the country.

The types of data compromised in this incident, varies per individual, and may include:

- **Full name**
- **Social Security number**
- **Driver's license number**
- **State identification number**
- **Financial account information**
- **Account access credentials**

The organization stated that, as of now, there's no evidence of any misuse of the stolen information.

HSGI offers 12 and 24-month credit monitoring and identity theft protection services coverage to individuals affected by the breach, depending on the severity of the exposed data.

In addition to this, the company recommends that people remain vigilant for phishing and scamming attempts and report suspicious activity on their banking accounts to the authorities. As of writing, no ransomware groups have claimed the attack on HSGI.

References:

- https://www.bleepingcomputer.com/news/security/healthcare-services-group-data-breach-impacts-624-000-people/
- https://www.scworld.com/brief/toll-of-healthcare-services-group-breach-exceeds-624k
- https://www.show.it/en/healthcare-services-group-data-breach-impacts-624000/

Title: Pharma firm Inotiv says ransomware attack impacted operations

Impacted Sector: Healthcare

Attack Summary:

American pharmaceutical company Inotiv has disclosed that some of its systems and data have been encrypted in a ransomware attack, impacting the company's business operations. In a filing to the U.S. Securities and Exchange Commission (SEC), Inotiv says that the cyberattack occurred on August 8 and took action to contain the breach.

"On August 8, 2025, Inotiv, Inc. became aware of a cybersecurity incident affecting certain of its systems and data," Inotiv informs.

"The Company's preliminary investigation determined that a threat actor gained unauthorized access to, and encrypted certain of, the Company's systems."

Inotiv started an investigation with the help of external security experts and notified law enforcement authorities of the incident.

The attack was claimed by the Qilin ransomware gang, who alleges to have stolen around 162,000 files amounting to 176GB. The threat actor has also published data samples on their leak site.



Inotive listed on the Qilin ransomware website

Source: BleepingComputer

Inotiv is an Indiana-based contract research organization specializing in drug development, drug discovery and safety assessment, as well as live animal research modeling.

The company employs around 2,000 specialists and has an annual revenue of more than $500 million.

The organization said that the cybersecurity incident has caused disruptions to certain business operations and expects the adverse effects to persist for some time.

Specifically, the incident impacted certain networks and systems that include databases and internal applications used in business processes.

Inotiv's IT team is working to restore these systems and migrated some of the affected operations to offline alternatives in order to mitigate the impact of the outages caused by the cyberattack.

No estimation has been provided for a return to normal operations.

References:

- https://www.bleepingcomputer.com/news/security/pharma-firm-inotiv-says-ransomware-attack-impacted-operations/

Title: Storm-0501 hackers shift to ransomware attacks in the cloud

Impacted Sector: Generic

Attack Summary:

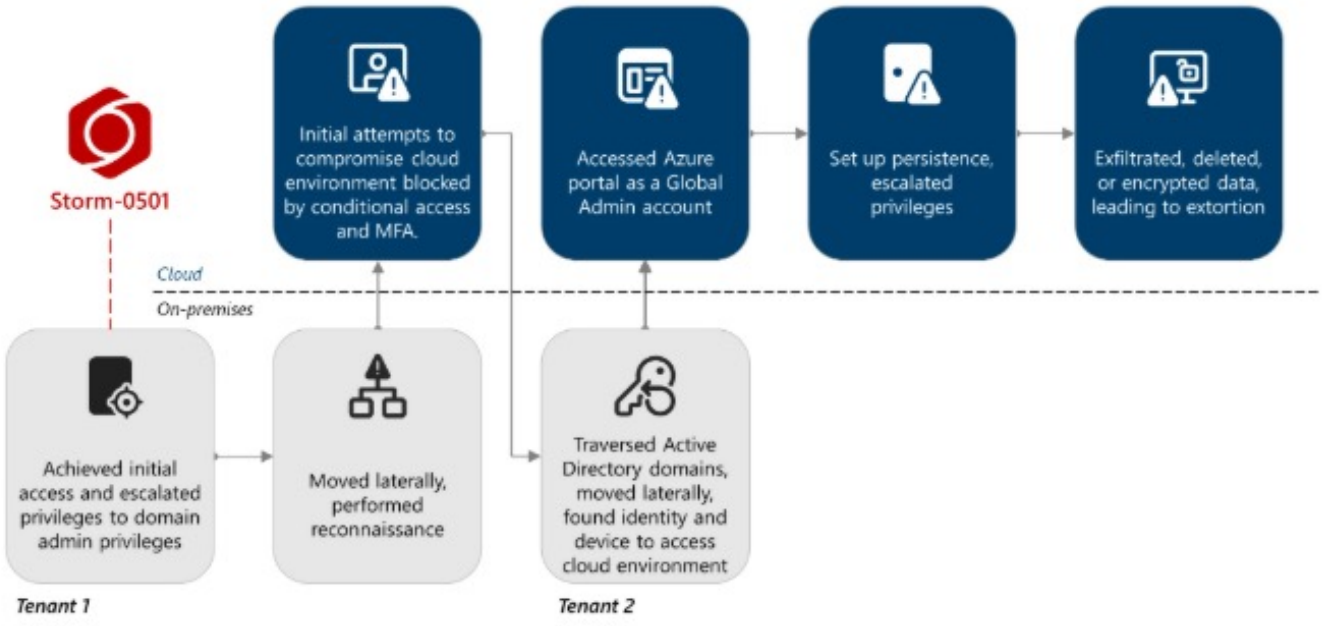
Microsoft has issued a warning about Storm-0501, a threat actor that has shifted its tactics from traditional ransomware attacks to cloud-based operations involving data theft, destruction, and extortion.

Instead of deploying ransomware to encrypt on-premises devices, the group now exploits native cloud features to steal data, delete backups, and destroy storage accounts, pressuring victims to pay ransoms without using conventional encryption tools.

Active since at least 2021, Storm-0501 initially used Sabbath ransomware and later adopted various RaaS platforms, including Hive, BlackCat (ALPHV), Hunters International, LockBit, and more recently, Embargo ransomware. In September 2024, Microsoft reported that the group expanded into hybrid cloud environments, moving from Active Directory compromises to Entra ID tenant attacks, where they either planted persistent backdoors via malicious federated domains or encrypted on-premises devices with ransomware.

Microsoft's latest analysis highlights a significant evolution in their strategy: abandoning on-prem encryption and conducting attacks entirely in the cloud.

"Unlike traditional on-premises ransomware attacks, which deploy malware to encrypt files and then negotiate for decryption keys, cloud-based ransomware represents a major shift. Storm-0501 leverages cloud-native tools to rapidly exfiltrate large amounts of data, delete backups, and demand ransom—all without deploying traditional malware."



Overview of Storm-0501 cloud-based ransomware attack chain
Source: Microsoft

After gaining control of the cloud environment, Storm-0501 disabled security measures and exfiltrated sensitive data from Azure Storage accounts. The attackers also targeted storage snapshots, restore points, Recovery Services vaults, and storage accounts, aiming to eliminate any possibility of free data recovery.

When they were unable to delete recovery data, the group resorted to cloud-based encryption by creating new Key Vaults and generating customer-managed keys, effectively locking the data and making it inaccessible unless the victim paid the ransom.

Following data theft, backup destruction, or encryption, the threat actors initiated the extortion phase, contacting victims via Microsoft Teams using compromised accounts to deliver ransom demands.

Microsoft's report provides defensive guidance, Microsoft Defender XDR detections, and hunting queries to help organizations detect and respond to these tactics.

As ransomware executables are increasingly blocked before encryption occurs, Microsoft warns that more threat actors may adopt similar cloud-based data theft and encryption strategies, which are harder to detect and prevent.

Recommendations:

- Enforce Multi-Factor Authentication (MFA) for all accounts—especially privileged ones like Global Admin—to block credential-based pivots.
- Harden Directory Synchronization Account (DSA) permissions. Microsoft has started restricting DSA roles in Entra Connect and Cloud Sync to reduce privilege escalation risks.
- Apply Zero Trust principles—use just-in-time (JIT) and just-enough-access (JEA) controls, and enforce conditional access policies.
- Enable Defender for Cloud to continuously assess posture and monitor threat activity across your Azure environment.
- Activate Defender for Resource Manager for automated analytics on Azure management operations—this enhances XDR detection.
- Enable immutable storage on Azure Blob accounts to prevent malicious deletions or modifications.
- Enable tamper protection and block mode EDR solutions on endpoints to raise the barrier for unauthorized configuration changes.

References:

- https://www.bleepingcomputer.com/news/security/storm-0501-hackers-shift-to-ransomware-attacks-in-the-cloud/

In line with regulatory requirements, Data I/O has committed to notifying impacted stakeholders, including individuals whose data may have been exposed, in accordance with frameworks like the General Data Protection Regulation (GDPR) or U.S. state breach notification laws.

The ongoing forensic analysis aims to map the attack's kill chain, from reconnaissance to impact, potentially revealing affiliations with known ransomware-as-a-service (RaaS) groups that employ advanced encryption algorithms and double-extortion models.

The response efforts also involved deploying mitigation controls, such as enhanced endpoint detection and response (EDR) tools, network segmentation, and multi-factor authentication reinforcements across the global IT environment.

While some operational functions have been partially restored through workaround measures, the full remediation timeline remains uncertain, reflecting the complexities of decrypting affected assets without paying ransoms a practice discouraged by cybersecurity best practices to avoid funding criminal ecosystems.

This incident aligns with broader industry trends, where manufacturing firms face heightened risks due to their reliance on interconnected operational technology (OT) and industrial control systems (ICS), which can amplify the blast radius of ransomware deployments.

Financial Ramifications

The ransomware attack has caused temporary but notable disruptions to Data I/O's core operations, including internal and external communications, logistics processes like shipping and receiving, manufacturing workflows, and ancillary support functions.

These interruptions stem from the encryption of critical data repositories and the downtime associated with system isolation, potentially delaying product deliveries in the competitive electronics programming market.

Although the company asserts that the incident has not yet materially impacted its overall business operations as of the filing date, the evolving nature of the investigation leaves room for reassessment.

Forward-looking statements in the disclosure highlight uncertainties, such as potential shifts in customer confidence or supply chain partnerships, which could manifest as reputational damage or contractual penalties.

Financially, Data I/O anticipates material costs arising from the breach, encompassing fees for cybersecurity consultants, legal advisors, and system restoration efforts.

These expenditures may strain the company's results of operations and financial condition, particularly if insurance coverage proves insufficient or if litigation ensues from data privacy violations.

Title: Electronics Manufacturer Data I/O Suffers Ransomware Breach

Impacted Sector: Manufacturer

Attack Summary:

Data I/O Corporation, a respected player in the electronics sector—specializing in device programming and security provisioning—has disclosed that it suffered a ransomware intrusion targeting its internal IT infrastructure in mid-August 2025.

The incident, initially identified on August 16, 2025, triggered the company's incident response protocols without delay, underscoring the ongoing ransomware threat to the semiconductor and electronics supply chain sectors. This disclosure was made public through a Form 8-K filing with the U.S. Securities and Exchange Commission on August 21, 2025. According to multiple sources, the ransomware disrupted a range of operational areas, including internal and external communications, shipping, receiving, manufacturing production, and support functions. Data I/O took affected systems offline proactively and engaged external cybersecurity experts to lead the investigation and recovery.

The full scope and long-term impact of the breach remain under investigation. While the company noted that, as of reporting, the incident did not appear to have a material effect on business operations, it cautioned that the related costs—such as advisory and restoration services—could have a material impact on its financial results and condition.

Data I/O has committed to notifying affected parties and relevant regulatory bodies as part of its compliance efforts. Notably, there has been no public attribution to a specific ransomware group, nor any reports of data leaks on extortion platforms. This incident dramatically illustrates how ransomware actors increasingly target specialized manufacturers that serve critical roles in the global supply chain—disrupting operations far beyond the immediate victim. The event reinforces the urgent need for enhanced cyber resilience, including robust segmentation, incident readiness, and third-party risk visibility.

Containment Measures

Upon identifying the ransomware intrusion, Data I/O swiftly implemented containment strategies, including isolating affected systems and taking critical platforms offline to prevent lateral movement by the threat actors.

The company engaged external cybersecurity specialists, likely including digital forensics and incident response (DFIR) teams, to conduct a thorough investigation into the attack vector, payload characteristics, and potential indicators of compromise (IoCs).

Preliminary assessments suggest the ransomware may have leveraged common entry points such as phishing, unpatched vulnerabilities, or supply chain compromises, though the exact initial access technique remains under scrutiny.

The filing invokes safe harbor provisions under the Private Securities Litigation Reform Act of 1995, cautioning that actual outcomes could deviate due to factors like investigation findings, recovery timelines, and external risks outlined in prior SEC reports.

In a sector where intellectual property and proprietary designs are prime targets, this event emphasizes the need for robust defenses, including zero-trust architectures, regular vulnerability scanning via tools like Nessus or OpenVAS, and adherence to standards such as NIST Cybersecurity Framework (CSF) or ISO 27001.

To contextualize the potential scope, consider the following table summarizing key aspects of the incident based on the disclosure:

This ransomware breach at Data I/O serves as a stark reminder of the imperative for electronics manufacturers to bolster their cyber resilience amid rising threats from sophisticated adversaries.

Recommendations:

- Ensure IT and OT environments are isolated to prevent lateral movement.
- Prioritize vulnerabilities linked to ransomware campaigns (e.g., RDP, VPN appliances, web apps).
- Force credential resets for all admin and service accounts; revoke unused accounts.
- Adopt “never trust, always verify” principles for all internal and external connections.
- Extend multi-factor authentication to VPN, privileged accounts, and third-party access.
- Harden manufacturing and ICS environments with firewalls and strict ACLs.
- Monitor on vulnerabilities linked to ransomware exploits.

References:

- https://gbhackers.com/electronics-manufacturer-data/

Title: Google Urges 2.5B Gmail Users to Reset Passwords After Salesforce Breach

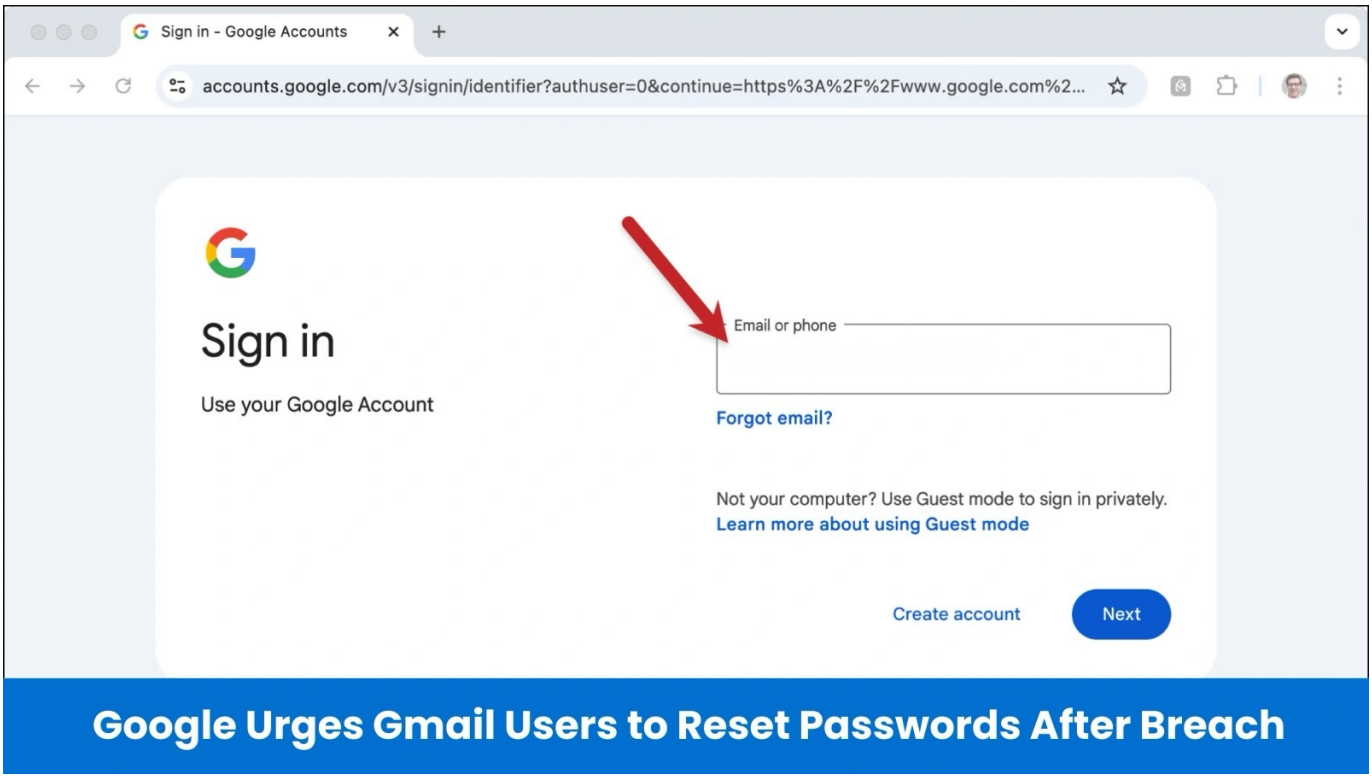
Impacted Sector: Generic

Attack Summary:

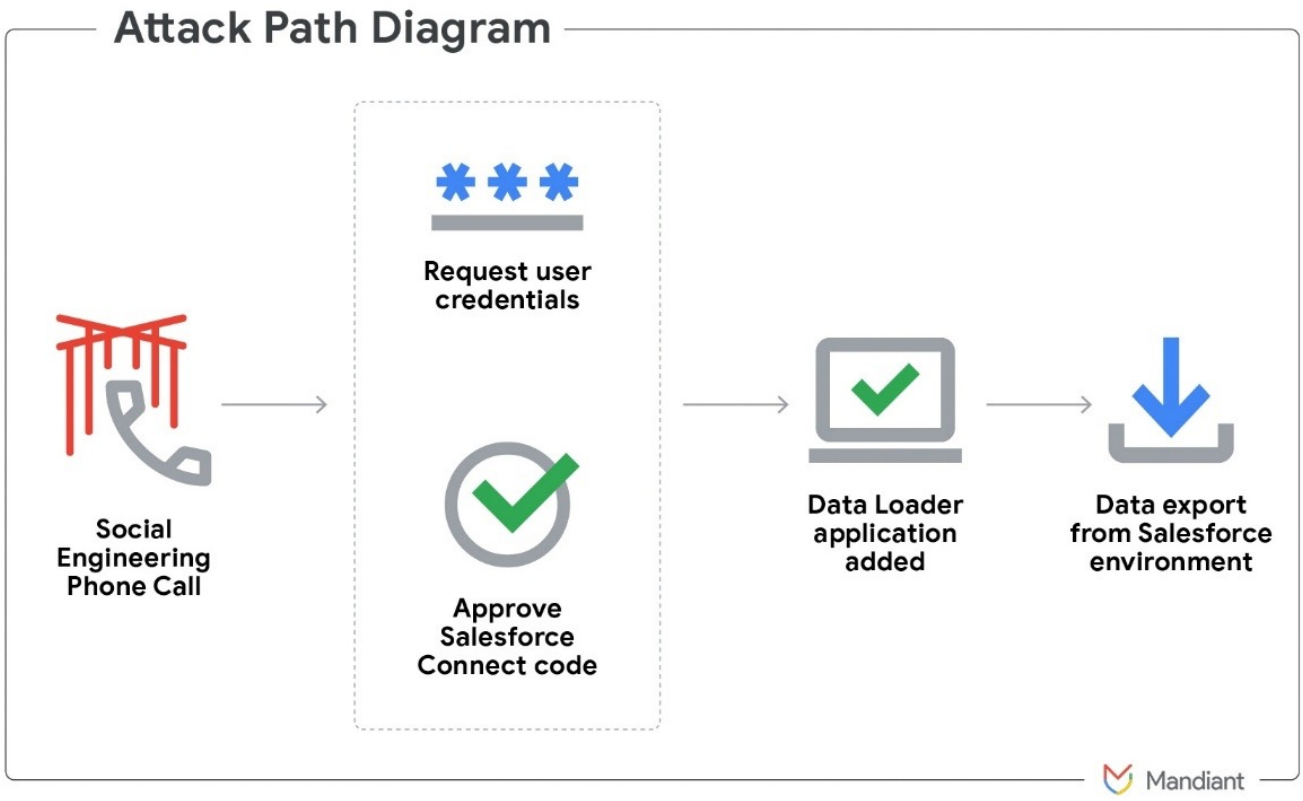
A highly organized voice phishing campaign—tracked by Google's Threat Intelligence Group as UNC6040—has emerged as a serious global threat. Cybercriminals impersonate IT support staff during phone calls to trick employees into granting access to their Salesforce environments. This deceptive tactic typically involves guiding targets to authorize a malicious connected application—often a fake version of Salesforce's Data Loader—which grants extensive access to sensitive CRM data.

The campaign has impacted roughly 20 organizations across sectors like hospitality, retail, and education in Europe and the Americas, resulting in data theft and lateral movement into other cloud services such as Okta and Microsoft 365. In Google's case, basic business contact details were exfiltrated from its Salesforce instance via this method.

After the initial breach, a secondary group—UNC6240, posing as the notorious ShinyHunters—executes extortion campaigns, sometimes delaying ransom demands for months and threatening public data leaks if payments are not made



Google Urges 2.5B Gmail Users to Reset Passwords



Data Loader attack flow

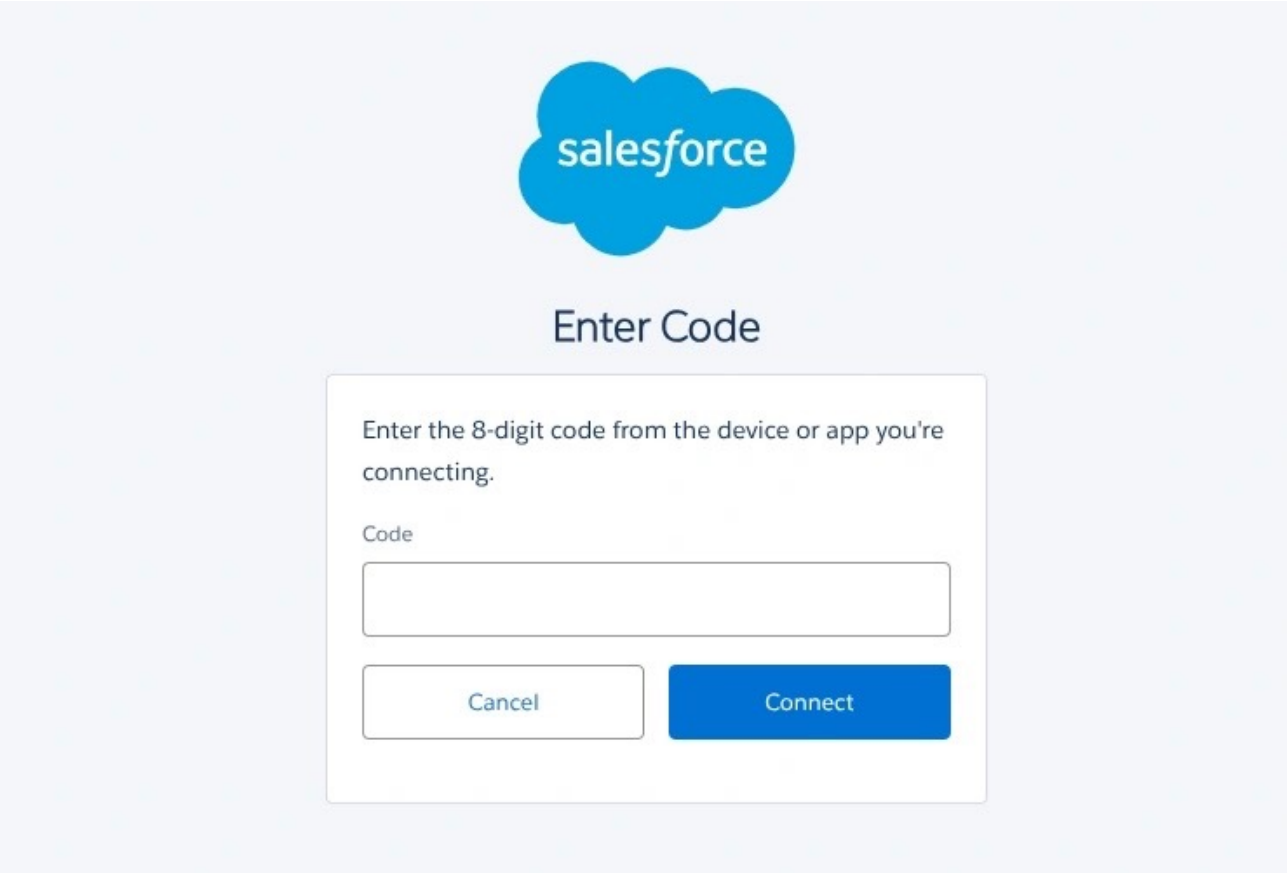
These attackers primarily target English-speaking branches of multinational corporations, exploiting the trust employees place in apparent technical support staff.

During these fraudulent calls, the criminals guide victims through a process that appears legitimate but actually grants unauthorized access to their organization's Salesforce instances.

- Malicious App Authorization: Attackers direct victims to Salesforce's connected app setup page to approve fake Data Loader applications.
- Modified Tools: The criminals use altered versions of legitimate Salesforce Data Loader software with different names or branding.
- Extensive Access: Once authorized, these malicious apps provide broad capabilities to access, query, and steal organizational data.
- Trust Exploitation: The scheme relies on employees' inherent trust in apparent IT support personnel.

The attackers' methodology centers on manipulating victims into authorizing malicious connected applications within their Salesforce portals.

They accomplish this by directing employees to Salesforce's connected app setup page and instructing them to approve what appears to be a legitimate Data Loader application.



The victim needs to enter a code to connect the threat actor controlled Data Loader

However, this application is actually a modified version controlled by the threat actors, bearing different names or branding to avoid detection.

Once authorized, this malicious app provides the criminals with extensive capabilities to access, query, and steal sensitive organizational data directly from the compromised Salesforce environments.

Google's own corporate Salesforce instance fell victim to similar UNC6040 activity in June, affecting contact information for small and medium businesses.

While the company quickly responded and limited the breach to basic business information, the incident demonstrates the campaign's broad reach and effectiveness against even security-conscious organizations.

Following successful data exfiltration, a secondary threat group designated UNC6240 initiates extortion activities, sometimes waiting several months before making contact with victims.

These extortion attempts typically involve direct communication with employees of the targeted organization, demanding bitcoin payments within 72-hour deadlines.

The extortionists consistently claim affiliation with the notorious hacking group ShinyHunters, likely as a psychological tactic to increase pressure on their victims.

Google intelligence reports suggest these threat actors may be preparing to escalate their tactics by launching a data leak site, which would provide a platform for publicly releasing stolen information if ransom demands are not met.

Recommendations:

- For any IT support interactions—especially those involving admin actions—use robust authentication methods such as video ID checks, internal photo databases, and out-of-band confirmation via known corporate channels
- Limit Data Loader and connected-app permissions strictly to a vetted admin group. Approvals for new or existing applications should require explicit review, and unknown or unused apps must be blocked or removed
- Restrict access to Salesforce to authorized IP ranges (e.g., corporate and VPN). Activate Salesforce Shield's Transaction Security Policies to detect unusual actions like bulk data downloads, unexpected app installations, or logins via TOR/VPN
- Train all employees—especially IT staff and helpdesk teams—to recognize vishing tactics, such as urgent requests or imposter IT support calls. Conduct regular simulated vishing exercises to build resilience

References:

- https://gbhackers.com/gmail-users-reset-passwords/

Section 3 - OT/IoT Security Breaches

Title: GeoServer Exploits, PolarEdge, and Gayfemboy Push Cybercrime Beyond Traditional Botne

Impacted Sector: OT (IoT Botnet)

Attack Summary:

Cybersecurity experts have flagged a spate of operations exploiting Redis servers left exposed online and open vulnerabilities for illicit gains—ranging from repurposing compromised devices as IoT botnets and residential proxies to deploying cryptocurrency miners.

A central tactic involves exploiting CVE-2024-36401, a critical remote code execution flaw in OSGeo GeoServer's GeoTools component, carrying a severe CVSS score of 9.8. This vulnerability has been actively exploited since late 2024.

Rather than using overt malware, attackers have adopted a more covert monetization route. They load either legitimate SDKs or slightly modified applications that quietly turn infected machines into sources of passive income by sharing network bandwidth or offering proxy services—akin to benign SDK-based monetization strategies employed by legitimate app developers.

These campaigns, which first became evident in early March 2025, involve systematic scans of GeoServer instances exposed to the internet. Cortex Xpanse, for instance, recorded over 3,700 such instances in early May, underscoring the widespread exposure used for exploitation. The Hacker News further describes these attacks as resource-light schemes designed to evade detection while quietly monetizing bandwidth.

"Once running, the executable operates covertly in the background, monitoring device resources and illicitly sharing the victim's bandwidth whenever possible," Unit 42 said. "This generates passive income for the attacker."

Telemetry data gathered by the company shows that there were over 7,100 publicly exposed GeoServer instances across 99 countries, with China, the United States, Germany, Great Britain, and Singapore taking the top five spots.

"This ongoing campaign showcases a significant evolution in how adversaries monetize compromised systems," Unit 42 said. "The attackers' core strategy focuses on stealthy, persistent monetization rather than aggressive resource exploitation. This approach favors long-term, low-profile revenue generation over easily detectable techniques."

Cybersecurity analysts, including those at Censys, have unveiled the infrastructure behind a sprawling IoT botnet dubbed PolarEdge. This network co-opts both enterprise-grade firewalls and consumer devices—such as routers, IP cameras, and VoIP phones—by exploiting known vulnerabilities. The botnet's true objective remains elusive, though it clearly isn't used for broad network scanning. Upon initial intrusion, attackers implant a custom, TLS-based backdoor built on Mbed TLS (formerly PolarSSL). This implant supports encrypted command-and-control channels, log cleanup, and remote updates. It typically communicates via elevated, uncommon TCP ports to evade conventional network monitoring and detection.

PolarEdge shows hallmarks of an Operational Relay Box (ORB) network—a framework that leverages infected devices as stealthy exit nodes. Censys and Sekoia findings suggest that the campaign began in mid-2023, scaling to approximately 40,000 active devices by August 2025. Infections cluster notably in South Korea, the U.S., Hong Kong, Sweden, and Canada
According to security researcher Himaja Motheram:

"ORBs are compromised exit nodes that forward traffic on behalf of threat actors… They don't need to hijack the host's primary functions—these devices quietly relay traffic while appearing operational, making detection by owners or ISPs unlikely."

Simultaneously, a Mirai-derived botnet known as Gayfemboy has resurfaced with enhanced capabilities. FortiGuard Labs reports it exploits numerous vulnerabilities in devices from DrayTek, TP-Link, Raisecom, and Cisco to establish persistence, deploy XMRig miners, and facilitate DDoS operations.

This campaign spans globally—from Brazil and the U.S. to Germany, Israel, Mexico, Switzerland, France, and Vietnam—and affects diverse sectors such as manufacturing, technology, construction, and media/communications.

Gayfemboy targets multiple system architectures—including ARM, AArch64, MIPS R3000, PowerPC, and Intel 80386—and features modular functionality across four primary roles:

- Monitor: Observes processes, enforces persistence, and detects sandbox environments.
- Watchdog: Binds to UDP port 47272 for operational signaling.
- Attacker: Executes DDoS attacks (via UDP, TCP, ICMP), and opens a backdoor to receive remote commands.
- Killer: Self-destructs if commanded or if sandbox anomalies are detected.

Gayfemboy also employs stealthier techniques such as UPX packing with modified headers to evade signature-based detection, polymorphic downloader scripts named for targeted brands (e.g., “asus,” “zyxel”), and layered obfuscation tactics. FortiGuard Labs has noted this evolution reflects growing malware sophistication that necessitates proactive, intelligence-driven defenses.

Recommendations:

- Patch or mitigate vulnerable IoT edge devices (e.g., CVE-2023-20118 fixes, disable remote management) to block exploitation of known flaws and thwart botnet infiltration.
- Apply strict network segmentation and access controls, isolating IoT and peripheral devices to limit their misuse as relay points or vectors for lateral movement.
- Deploy anomaly-based detection and threat intelligence tools—including SIEMs and AI-enhanced IDS/IPS—to spot stealthy commands, encrypted sessions on high ports, or unusual outbound traffic patterns.
- Enforce strong, unique credentials and replace end-of-life/unpatched devices, especially across routers, firewalls, cameras, and other IoT infrastructure vulnerable to Mirai-derived campaigns.
- Implement threat prevention measures like IPS signatures, C2 domain blocking, and web filtering to disrupt both PolarEdge backdoors and Gayfemboy downloader activity.

References:

- https://thehackernews.com/2025/08/geoserver-exploits-polaredge-and.html

The Indicators of compromise (IOCs) have been attached in an excel sheet based on the categories for IP, Domain, URL & Hash which are involved in attacks & breaches.

Disclaimer

“Cyber threats are constantly evolving, and the tactics, techniques, and procedures (TTPs) described in this report may change over time. Continuous monitoring and threat intelligence updates are recommended to maintain an effective security posture.”

Feedback

“We welcome your feedback to enhance the accuracy, relevance, and effectiveness of our threat intelligence reports. Please share your insights or recommendations to help us improve future editions and better support your security needs.”

Contact us on “Threat Advisory <threatadvisory@colortokens.com>”

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation and breach containment solutions, dedicated to making organizations “breach ready.” By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enabling the enforcement of granular micro-perimeters, swift isolation of critical assets, and effective breach response. Recognized as a Leader in the Forrester Wave™: Microsegmentation Solutions (Q3 2024), ColorTokens delivers proactive security that prevents disruptions and safeguards global enterprises. For more information, visit www.colortokens.com

Copyright 2025 © ColorTokens. All rights reserve