COLORTOKENS

ColorTokens Threat Advisory

Threat Intelligence Brief #15

January 15, 2026

ACCESS BRIEF

Threat Intelligence Brief

December 16, 2025 – January 15, 2026

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-2025-14733	WatchGuard Firebox iked Out of Bounds Write Vulnerability	9.3	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to execute arbitrary code.	Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.5 and 2025.1 up to and including 2025.1.3.	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027	https://www.cve.org/CVERecord?id=CVE-2025-14733
CVE-2025-20393	Cisco Secure Email Gateway and Cisco Secure Email and Web Manager Remote Command Execution Vulnerability	10	Cisco is aware of a potential vulnerability. Cisco is currently investigating and will update these details as appropriate as more information becomes available.	Various version(Total 18 version)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4	https://www.cve.org/CVERecord?id=CVE-2025-20393
CVE-2025-52691	Critical SmarterMail Flaw Allows Attackers to Execute Remote Code	10	the software fails to properly check or restrict the types of files that can be uploaded to the server.	SmarterMail versions Build 9406 and earlier	SmarterMail version Build 9413	https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-124/
CVE-2025-14847	Zlib compressed protocol header length confusion may allow memory read	8.7	An client-side exploit of the Server's zlib implementation can return uninitialized heap memory without authenticating to the server. We strongly recommend upgrading to a fixed version as soon as possible.	Total 9 versions are affected. (Version 3.6 – 8.2.3)	Upgrade to 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, or 4.4.30	https://thehackernews.com/2025/12/mongodb-vulnerability-cve-2025-14847.html
CVE-2025-20393	Cisco Secure Email Gateway and Cisco Secure Email and Web Manager Remote Command Execution Vulnerability	10	A vulnerability in the Spam Quarantine feature of Cisco AsyncOS Software for Cisco Secure Email Gateway and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to execute arbitrary system commands on an affected device with root privileges.	affected at 14.0.0-698, 13.5.1-277, 13.0.0-392, 14.2.0-620, 13.0.5-007, 13.5.4-038 , 14.2.1-020 , 14.3.0-032 , 15.0.0-104 , 15.0.1-030 , 15.5.0-048 , 15.5.1-055, 15.5.2-018, 16.0.0-050, 15.0.3-002, 16.0.0-054, 15.5.3-022 and 16.0.1-017	https://www.cve.org/CVERecord?id=CVE-2025-20393	https://nvd.nist.gov/vuln/detail/CVE-2025-20393

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2026-21267	Adobe Dreamweaver Desktop	8.6	Dreamweaver Desktop versions 21.6 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an attacker. Exploitation of this issue requires user interaction in that a victim must open a malicious file and scope is changed.	Versions 21.6 and earlier	Update to 21.7 version	https://helpx.adobe.com/security/products/dreamweaver/apsb26-01.html

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.

Section 2 - Reported Cyber Breaches

Title: Belgian hospital AZ Monica shuts down servers after cyberattack

Impacted Sector: Healthcare

Attack Summary:

A reported ransomware attack on AZ Monica hospital in Belgium has led to operations being canceled and forced the Red Cross to transfer seven patients requiring critical care to other hospitals.

The hospital, which operates campuses in Antwerp and Deurne, disconnected all servers at 6:32 AM after its systems were hit. The cyberattack also forced the hospital to suspend all scheduled procedures on Tuesday, as the emergency department continues to operate at reduced capacity, even though emergency medical services and intensive care transport units remain offline.

"Due to this situation, no scheduled procedures are possible today. We have informed all patients. The Emergency Department is operating at reduced capacity. The Emergency Department (MUG) and Intensive Care Unit (PIT) services are currently not operational," the hospital said in a press statement.

"Urgent treatment is continuing and of course the patients that were already at the hospital are still being treated. However, non-urgent consultations are being postponed for the time being because we can't retrieve the information contained on the patients' digital medical files," spokeswoman Sofie Braem told VRT News.

Seven patients who required critical care were transferred to other hospitals with Red Cross assistance. Hospital officials added that all remaining patients are staying at AZ Monica and receiving necessary care, but warned that registration procedures for new patients will be slower, since employees "have to register a lot of things on paper."

The hospital has also notified relevant authorities and said that the police and prosecutors are now investigating the cybersecurity incident. It also noted that it continues monitoring the situation and will provide updates as more information becomes available.

"The focus of AZ Monica remains undiminished on the safety and continuity of care for our patients. AZ Monica will continue to monitor the situation closely and will communicate further updates as soon as there is more clarity," it added.

AZ Monica did not specify the nature of the incident or indicate whether it involved ransomware, a common threat targeting healthcare organizations worldwide, seeing that they often store sensitive patient data, making them attractive targets for double-extortion attacks.

However, according to local media, unconfirmed reports from within the hospital suggest the attackers might have demanded a ransom, but these claims are yet to be confirmed by hospital officials and the public prosecutor.

References:

- https://www.bleepingcomputer.com/news/security/belgian-hospital-az-monica-shuts-down-servers-after-cyberattack/
- https://therecord.media/belgium-hospital-cyberattack-antwerp-az-monica•

Title: AllerVie Health Patients Affected by Ransomware Attack

Impacted Sector: Healthcare

Attack Summary:

AllerVie Health, a Frisco, TX-based provider of allergy and immunology services, has announced a security incident that exposed personally identifiable information. Unusual network activity was identified on November 2, 2025, and an investigation was launched to determine the cause of the activity. The investigation confirmed unauthorized access to its network between October 24, 2025, and November 3, 2025, and during that time, "a limited amount of information was subject to unauthorized access."

The file review revealed on November 24, 2025, that names, Social Security numbers, driver's license numbers, and state identification numbers were involved. The affected individuals were notified by mail on December 22, 2025, and have been offered complimentary credit monitoring and identity theft protection services. Allervie Health said it has reviewed its policies and procedures related to data protection. The number of affected individuals has yet to be confirmed.

While not stated by Allervie Health in its notification letters, this appears to have been a ransomware attack by the Anubis ransomware group, which has added Allervie Health to its dark web data leak site along with a copy of the data allegedly stolen in the attack. Anubis claims that the stolen data includes the records of more than 30,000 patients, and the data sample on the website shows first and last names, email addresses, ages, addresses, zip codes, phone numbers, provider names, primary insurer names, and other sensitive data.

AllerVie Health first detected unusual network activity on November 2, 2025, triggering an internal investigation. The review later confirmed that unauthorized actors had access to the organization's systems from October 24 to November 3, 2025. During that period, the attackers accessed and, in some cases, exfiltrated personally identifiable information (PII) stored on the network. The ANUBIS ransomware group is suspected to be responsible for the attack.

The exposed data reportedly included names, Social Security numbers, driver's license or state ID numbers, and other identifiable information.

AllerVie Health notified state attorneys general in New Hampshire and Massachusetts on December 23 and 26, 2025, respectively, and has begun mailing breach notices to impacted individuals. Under U.S. state breach reporting laws, the company is required to alert affected people and regulators once a breach is discovered and evaluated.

In response to the incident, AllerVie has taken several steps:

- Reset affected system credentials and implemented enhanced monitoring.
- Engaged forensic and cybersecurity experts to investigate and secure the environment.
- Contracted Cyberscout, a TransUnion company, to offer complimentary credit monitoring and identity protection services to those affected.

References:

- https://www.hipaajournal.com/allervie-health-data-breach/
- https://www.paubox.com/blog/allervie-health-confirms-ransomware-attack-exposed-patient-data

---

Title: Artemis Healthcare Falls Victim to Ransomware Attack

Impacted Sector: Healthcare

Attack Summary:

Tennessee-based Artemis Healthcare has experienced a ransomware attack involving data theft, and email account breaches have been announced by Greater St. Louis Oral & Maxillofacial Surgery in Missouri and St. John's Riverside Hospital in New York.
Artemis Healthcare in Nashville, Tennessee, has recently announced a data security incident that was identified on May 31, 2025. According to the notification sent to the Vermont Attorney General, Artemis Healthcare confirmed that it was the target of a ransomware group, which accessed its network from May 5, 2025, to May 31, 2025.

The investigation confirmed on September 12, 2025, that the ransomware group accessed personally identifiable and protected health information, including names, addresses, dates of birth, Social Security numbers, and health information. The Crypto24 ransomware group took responsibility for the attack and claimed on its dark web data leak site to have exfiltrated 1 terabyte of data, including image files for millions of patients. The stolen data has been leaked, indicating the ransom was not paid.

Artemis Healthcare said it has updated its security policies and procedures and provided additional training to its workforce to prevent similar incidents in the future. While regulators have been informed, the data breach is not yet shown on the HHS' Office for Civil Rights website, so it is currently unclear how many individuals have been affected.

unauthorized access to Artemis's systems occurred over nearly a month, from May 5 to May 31, 2025. The attackers, identified as a ransomware group, infiltrated the company's network, potentially viewing or exfiltrating files containing confidential data. Shortly after, the cyber threat group, crypto24, took accountability for the breach.

The breach affected an undisclosed number of individuals whose information was handled by Artemis in connection with its healthcare services. The specific types of information exposed vary by individual, but may include names, Social Security numbers, dates of birth, addresses, and other personally identifiable information (PII). For some, protected health information (PHI) may also have been involved, depending on the nature of their relationship with Artemis.

The company completed its investigation on Sept. 12, 2025, and began the notification process soon after. Artemis Healthcare disclosed the data breach to the Attorney General's offices in Vermont on Dec. 29. 2027.

This incident is considered severe due to the length of unauthorized access, the involvement of a ransomware group, and the types of data at risk. The attackers' ability to compromise the network for nearly a month increased the likelihood that sensitive information could be misused for identity theft or fraud.

Artemis Healthcare's response

Artemis Healthcare responded to the breach by immediately securing its systems, force changing passwords, terminating active sessions, and engaging cybersecurity experts to investigate the incident. The company has since reviewed and updated its security policies and procedures, and it is providing additional training to employees to help prevent future incidents.

If you believe your personal information may have been compromised in this breach:

- Carefully review any notice or communication you receive from Artemis Healthcare or a company that does business with Artemis Healthcare.
- Monitor financial accounts and credit reports for signs of identity theft.
- Consider placing fraud alerts or credit freezes with the major credit bureaus.
- Be cautious of unsolicited emails or phone calls requesting personal information.

References:

- https://www.claimdepot.com/data-breach/artemis-healthcare-2025
- https://www.hipaajournal.com/artemis-healthcare-data-breach/
- https://www.paubox.com/blog/artemis-discloses-ransomware-attack-after-weeks-of-unauthorized-access

Title: Central Maine Healthcare breach exposed data of over 145,000 people

Impacted Sector: Healthcare

Attack Summary:

A data breach last year at Central Maine Healthcare (CMH) exposed sensitive information of more than 145,000 individuals.

The hackers persisted on the organization's systems for more than two months last year, between March 19 and June 1, when CMH discovered the intrusion. The CMH integrated healthcare delivery system serves at least 400,000 people and manages hospitals like Central Maine Medical Center (CMMC), Bridgton Hospital, and Rumford Hospital.

Although the organization started notifying affected individuals almost immediately and continued to do so as the investigation advanced and revealed new impacted individuals. The analysis was completed on November 6, 2025, bringing the total number to 145,381.

According to the notification letter, the hackers may have accessed data belonging to CMH patients as well as current and former employees.

On December 29, CMH published a statement informing that the security incident exposed the following data types, which may vary per individual:

- Full names
- Dates of birth
- Treatment information
- Dates of service
- Provider names
- Health insurance information
- Social Security Number (SSN)

As a result of this incident, patients who have received services in the CMH system face an increased risk of phishing, impersonation, and fraud.

"For patients whose information may have been involved in the incident, Central Maine Healthcare recommends that they review the statements they receive from their healthcare providers and health insurance plans," the organization said.

"If they see any services that were not received, they should contact the provider or health plan immediately."

Additionally, a dedicated patient support line has been set up to answer questions, accept data abuse reports, or address concerns.

To keep affected patients safer from financial fraud risk, CMH is offering free credit monitoring services.

BleepingComputer checked for reports of threat actors claiming the attack, but, could not find any at the time of writing.

References:

- https://www.bleepingcomputer.com/news/security/central-maine-healthcare-breach-exposed-data-of-over-145-000-people/
- https://www.scworld.com/brief/central-maine-healthcare-data-breach-affects-over-145000-individuals

---

Title: Microsoft Warns Misconfigured Email Routing Can Enable Internal Domain Phishing

Impacted Sector: Generic

Attack Summary:

Threat actors engaging in phishing attacks are exploiting routing scenarios and misconfigured spoof protections to impersonate organizations' domains and distribute emails that appear as if they have been sent internally.

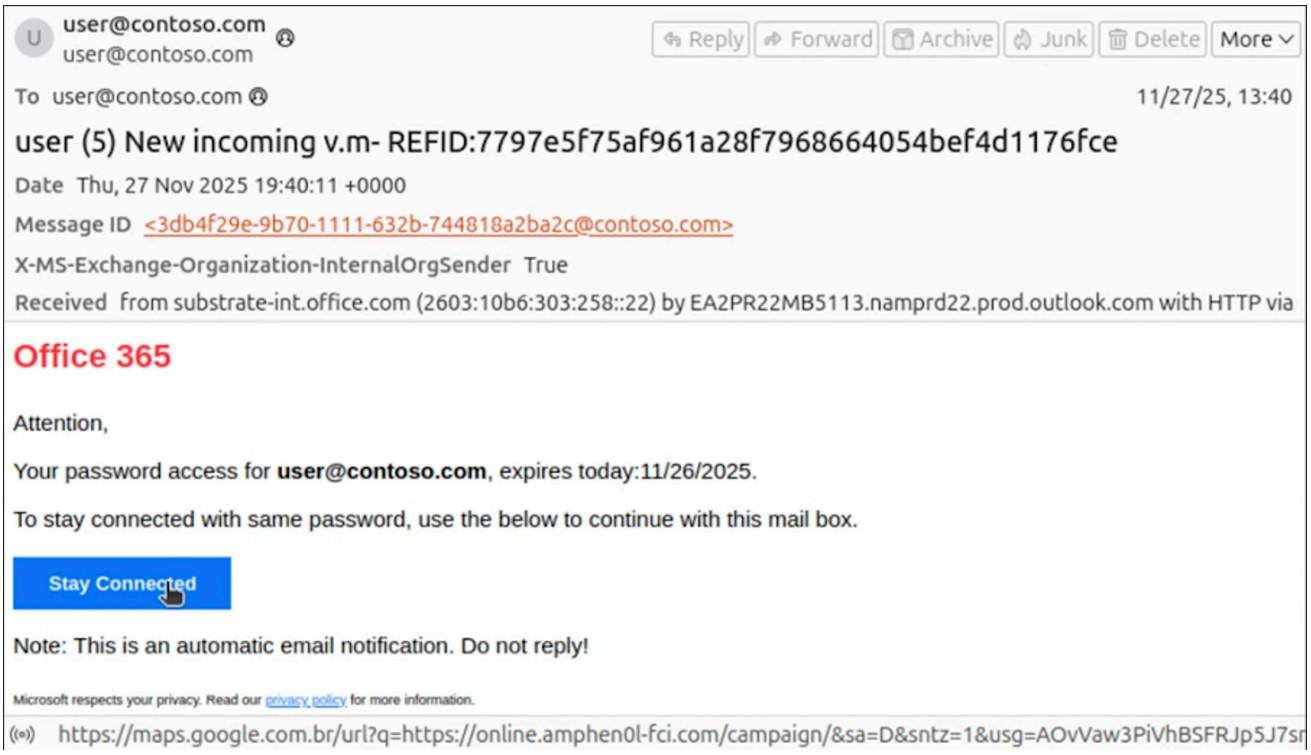
Threat actors have leveraged this vector to deliver a wide variety of phishing messages related to various phishing-as-a-service (PhaaS) platforms such as Tycoon 2FA," the Microsoft Threat Intelligence team said in a Tuesday report. "These include messages with lures themed around voicemails, shared documents, communications from human resources (HR) departments, password resets or expirations, and others, leading to credential phishing.

While the attack vector is not necessarily new, the tech giant said it has witnessed a surge in the use of the tactic since May 2025 as part of opportunistic campaigns targeting a wide variety of organizations across multiple industries and verticals. This includes a campaign that has employed spoofed emails to conduct financial scams against organizations. A successful attack could allow threat actors to siphon credentials and leverage them for follow-on activities, ranging from data theft to business email compromise (BEC).

The problem manifests primarily in scenarios where a tenant has configured a complex routing scenario and spoof protections are not strictly enforced. An example of complex routing involves pointing the mail exchanger record (MX record) to either an on-premises Exchange environment or a third-party service before reaching Microsoft 365

This creates a security gap that attackers can exploit to send spoofed phishing messages that seem to originate from the tenant's own domain. The vast majority of phishing campaigns that leverage this approach have been found to make use of the Tycoon 2FA PhaaS kit. Microsoft said it blocked more than 13 million malicious emails linked to the kit in October 2025.

PhaaS toolkits are plug-and-play platforms that allow fraudsters to create and manage phishing campaigns easily, making it accessible even for those with limited technical skills. They provide features like customizable phishing templates, infrastructure, and other tools to facilitate credential theft and circumvent multi-factor authentication using adversary-in-the-middle (AiTM) phishing.



The Windows maker said it has also spotted emails intended to trick organizations into paying bogus invoices, potentially leading to financial losses. The spoofed messages also impersonate legitimate services like DocuSign or claim to be from HR regarding salary or benefits changes.

Phishing emails propagating financial scams often resemble a conversation between the CEO of the targeted organization, an individual requesting payment for services provided, or the firm's accounting department. They also contain three attached files to lend the scheme a false sense of trust -

- A fake invoice for thousands of dollars to be wired to a bank account
- An IRS W-9 form listing the name and social security number of the individual used to set up the bank account
- A fake bank letter was allegedly provided by an employee at the online bank used to set up the fraudulent account

"They may employ clickable links in the email body or QR codes in attachments or other means of getting the recipient to navigate to a phishing landing page," it added. "The appearance of having been sent from an internal email address is the most visible distinction to an end user, often with the same email address used in the 'To' and 'From' fields."

To counter this risk, organizations are advised to set strict Domain-based Message Authentication, Reporting, and Conformance (DMARC) reject and Sender Policy Framework (SPF) hard fail policies and properly configure third-party connectors, such as spam filtering services or archiving tools.

It's worth noting that tenants with MX records pointed directly to Office 365 are not vulnerable to the attack vector. Additionally, it's recommended to turn off Direct Send if not necessary to reject emails spoofing the organization's domains.

References:

- https://www.bleepingcomputer.com/news/security/cloudflare-blames-todays-outage-on-emergency-react2shell-patch/

Title: DarkSpectre Hackers Infected 8.8 Million Chrome, Edge, and Firefox Users witMalware

Impacted Sector: Generic

Attack Summary:

Researchers have uncovered DarkSpectre, a well-funded Chinese threat actor responsible for infecting over 8.8 million users across Chrome, Edge, and Firefox browsers through a series of highly coordinated malware campaigns spanning seven years.

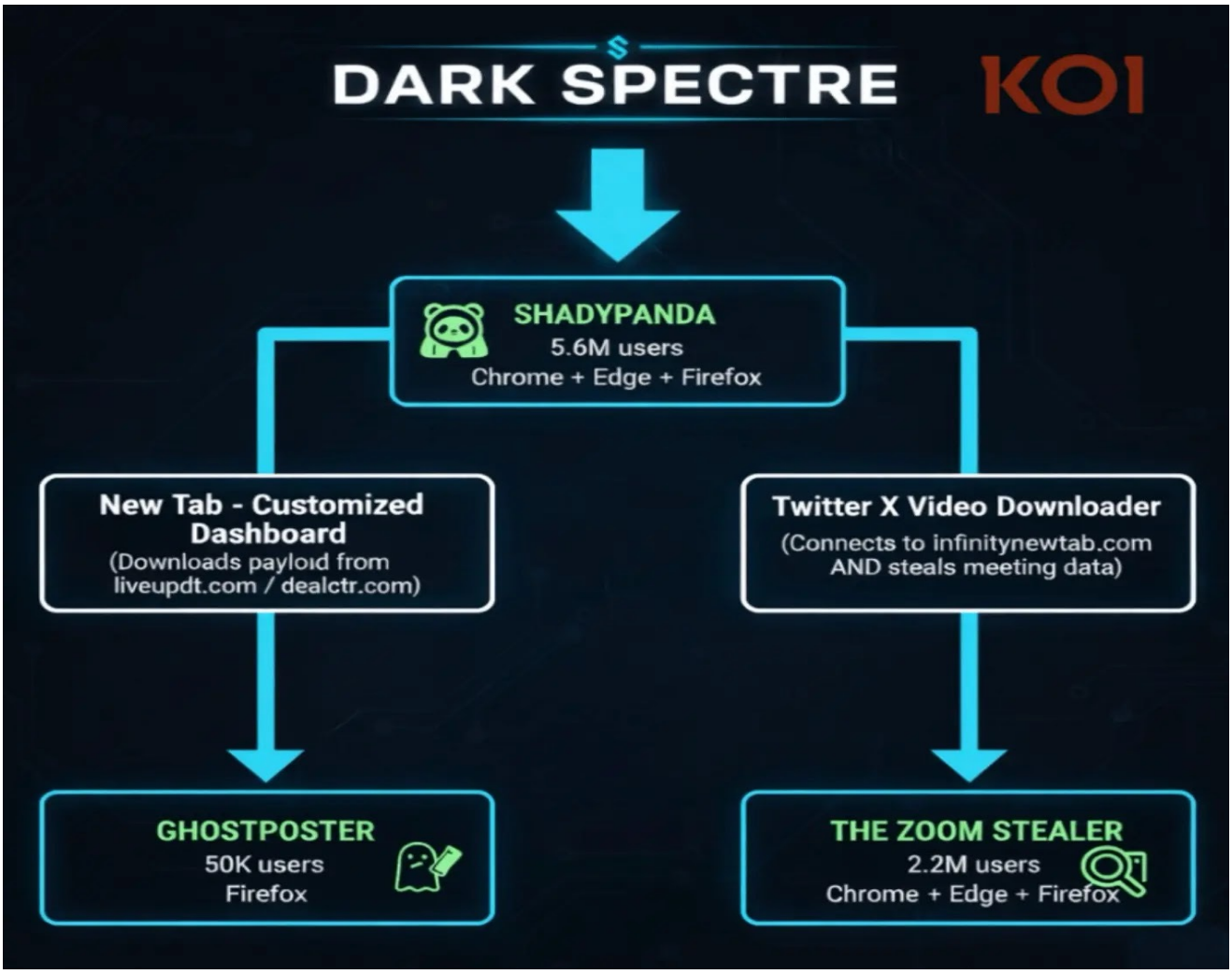
The discovery reveals a level of operational sophistication rarely seen in the threat landscape, with the group running multiple distinct campaigns simultaneously, each targeting different objectives ranging from consumer fraud to corporate espionage.

The operation consists of three major campaigns: ShadyPanda affecting 5.6 million users, the newly discovered Zoom Stealer campaign targeting 2.2 million users, and GhostPoster impacting 1.05 million users. Rather than operating as separate threat actors, investigators confirmed these represent a single, highly organized criminal organization with substantial resources and strategic planning capabilities.

The group demonstrates remarkable patience, maintaining legitimate-appearing browser extensions for five or more years before weaponizing them with malicious payloads. Koi analysts identified the connection between these campaigns while analyzing infrastructure linked to ShadyPanda.

They discovered that while the group used two legitimate domains—infinitynewtab.com and infinitytab.com—to power actual extension features like weather widgets and new tab pages, these same domains connected to entirely different malicious command-and-control infrastructure.

This clever technique of embedding legitimate functionality alongside hidden malicious code became the thread linking all three operations together.



The discovery process resembled following a complex web. One domain led to extensions, which revealed new domains, which connected to additional extensions operated by publishers with dozens of other malicious tools.

The expansion eventually uncovered over 100 connected extensions across multiple browser marketplaces.

As researchers investigated further, they noticed that certain newly discovered extensions communicated with domains already flagged in previous investigations, confirming that ShadyPanda, GhostPoster, and Zoom Stealer represented a single actor operating at nation-state scale.

Time-Bomb Activation and Evasion Tactics

The most alarming aspect of DarkSpectre's methodology lies in their sophisticated persistence and detection-evasion techniques.

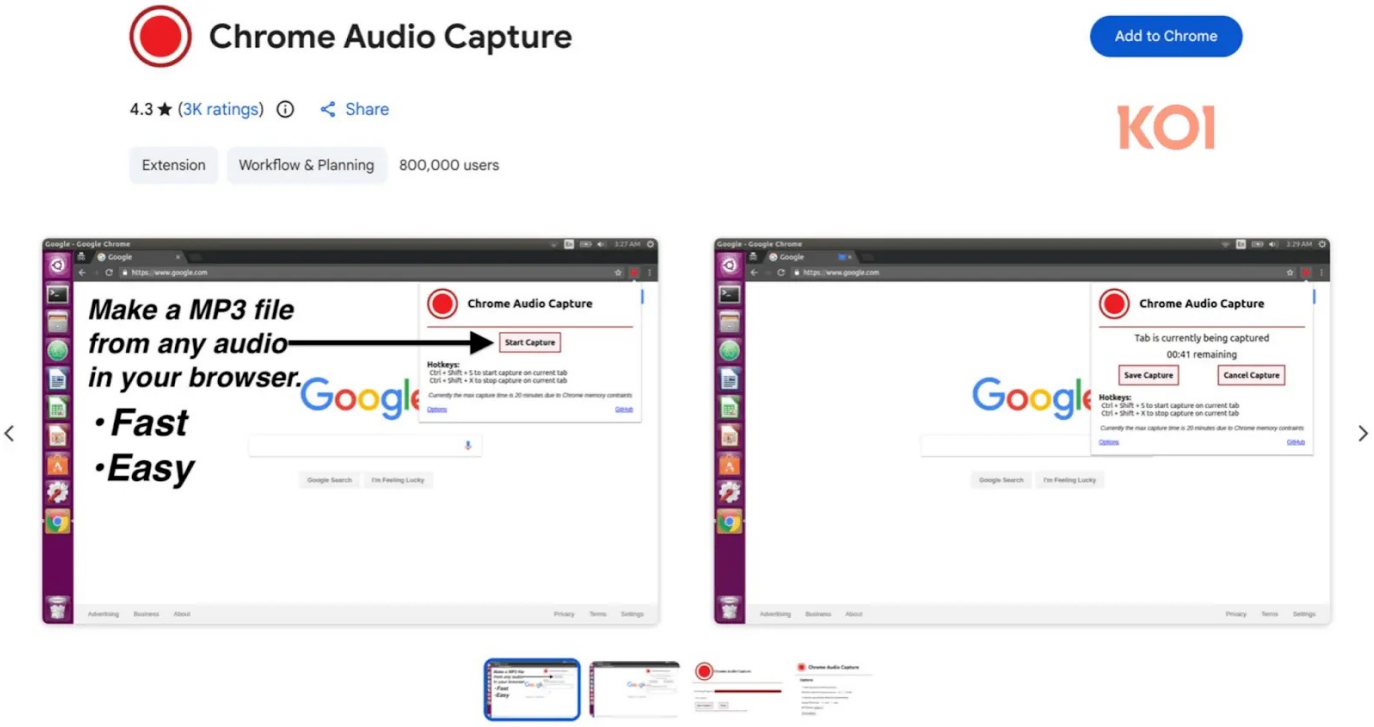
The group employs what researchers term "time-bomb" extensions—malicious tools that remain dormant for extended periods before activating their payload.

One extension called “New Tab – Customized Dashboard” demonstrates this approach by waiting three days after installation before connecting to command-and-control servers to download its actual malicious code.

During the review process when marketplaces evaluate extensions for safety, this extension appears completely legitimate. Browser reviewers cannot detect the malicious behavior because it simply does not activate during testing.

The extension only begins its malicious activities after passing all security checks and reaching a real user’s browser.

To further evade detection, the malware only activates on approximately ten percent of page loads, making it exponentially harder to identify during routine testing or analysis.



The payload delivery itself showcases advanced obfuscation techniques. DarkSpectre disguises malicious code as PNG image files, a method known as steganography.

The extension loads its own logo, extracts the hidden JavaScript code embedded within the image file, and executes it silently in the background.

The JavaScript is wrapped in multiple layers of protection including custom encoding, XOR encryption, and packed code designed specifically to defeat automated detection tools.

Once activated, the extension downloads approximately sixty-seven kilobytes of additional encoded JavaScript from the operators' servers, giving the threat actors complete control over what executes in the user's browser without requiring an extension update that would again trigger the review process.

This configuration-based approach represents the true innovation in DarkSpectre's operation. Instead of pushing updates to change functionality—which would alert reviewers and users—the operators simply modify what their servers return when extensions phone home.

Defenders cannot combat the threat by blocking a single malicious update because the threat actor changes the payload on their backend servers dynamically, maintaining complete operational flexibility.

References:

- https://cybersecuritynews.com/darkspectre-hackers-infected-8-8-million-chrome-users/

Title: Cyberattack knocks offline France's postal, banking services

Impacted Sector: FinTech

Attack Summary:

La Poste, the French national postal service, confirmed on Monday that all its information systems were knocked offline by "a major network incident," disrupting digital banking and online services for millions of customers.

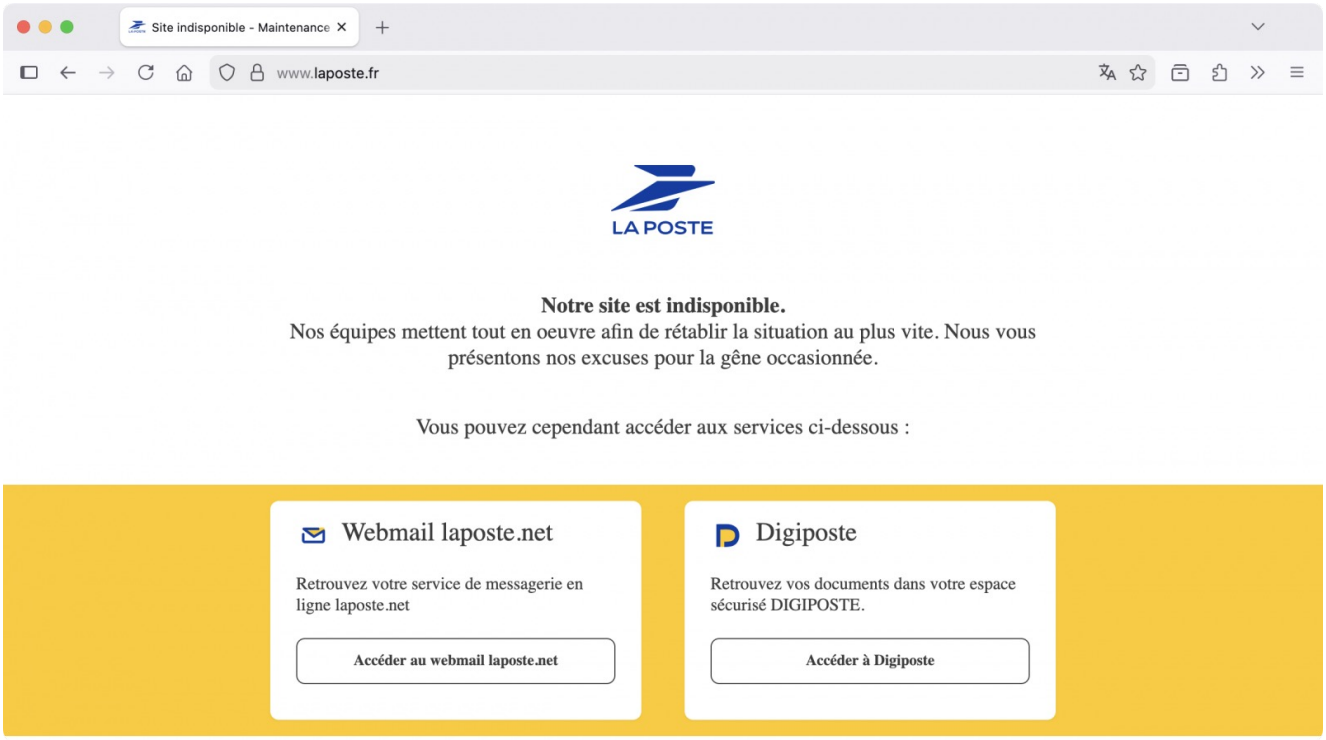
On social media, La Poste announced that the disruption rendered multiple platforms temporarily inaccessible, including its main website, mobile app, digital identity service, and the Digiposte document storage platform.

Some post office locations experienced service disruptions, though officials said customers could still conduct banking and postal transactions at service counters.

"For banking customers, online payments remain possible with SMS authentication. Cash withdrawals from ATMs, card payments at in-store POS terminals, and transfers via WERO are still available," La Poste said.

"In some post offices, service may be temporarily disrupted. However, it is still possible to carry out your banking and postal transactions at the counter."

La Poste's website was still down when this article was published, redirecting customers to its webmail and Digiposte platforms.



La Banque Postale, the banking arm of Groupe La Poste, confirmed that its online and mobile services were also down, but said core banking operations remained functional.

The bank's essential services are not impacted. Payments, interbank exchanges and flow processing are operating normally. Cash withdrawals from ATMs, in-store credit card payments and transfers via WERO remain accessible," it said.

"Online, internet and mobile card payments remain possible with SMS authentication to replace certification via Certicode."

While the postal service has yet to provide a timeline for full service restoration or disclose the nature of the incident, French news outlets reported that the outage was caused by a distributed denial-of-service (DDoS) attack that disrupted the company's operations nationwide.

La Poste is a public-owned company with over 250,000 employees part of the Groupe La Poste, which handles everything from package shipping and mail delivery to banking, insurance, and mobile telecommunications services.

References:

- https://www.bleepingcomputer.com/news/security/cyberattack-knocks-offline-frances-postal-banking-services/

Title: 70,000 bank customers exposed through vendor attack

Impacted Sector: FinTech

Attack Summary:

Texas-based VeraBank has notified the authorities that 37,318 clients were affected by the breach, informing its customers that their names and some other personal information was exposed as part of the incident.

The bank didn't specify what other personal information was potentially retrieved by bad actors, but its data breach notification letter suggests that it varied from client to client.

The Marquis hack also affected 32,344 customers of the Delaware-based Artisans' Bank, which said that the personal information potentially subject to unauthorized access included client names and Social Security numbers.

Both banks said Marquis informed them that it conducted its own investigation and informed law enforcement of the breach that it said happened on August 14th.

The Artisans' Bank said it only learned of the breach in late October and "only recently" that its own customer information may have been compromised. VeraBank said that its own systems were not affected and the attack was limited to Marquis's environment.

In November, Maine's Norway Savings Bank (NSB) informed clients that their personal details were exposed following a ransomware attack on Marquis, its software provider. The breach affected 51,000 NSB clients.

NSB said the breach exposed its clients' names, addresses, dates of birth, Social Security numbers, Tax ID numbers, and financial account information.

Cybernews reported at the time that it appeared Marquis paid the attackers a ransom. While not illegal, it carries a number of risks: there is no guarantee that the attackers wouldn't share the stolen data on the dark web anyway and it also puts the victim in danger of follow-up attacks.

Texas-based Marquis is a digital marketing, compliance solution, and customer relationship manager (CRM) software provider counting over 700 banks in the US as its clients.

According to XLab, both botnets were propagated using the same infection scripts between September and November and were found coexisting on the same group of compromised devices, indicating that they are likely operated by the same threat group.

References:

- https://cybernews.com/news/bank-marquis-software-vendor-attack/

Section 3 - OT/IoT Security Breaches

Title: RondoDox Botnet Exploits Critical React2Shell Flaw to Hijack IoT Devices and Web Servers

Impacted Sector: OT/IoT

Attack Summary:

Cybersecurity researchers have disclosed details of a persistent nine-month-long campaign that has targeted Internet of Things (IoT) devices and web applications to enroll them into a botnet known as RondoDox.

As of December 2025, the activity has been observed leveraging the recently disclosed React2Shell (CVE-2025-55182, CVSS score: 10.0) flaw as an initial access vector, CloudSEK said in an analysis.

React2Shell is the name assigned to a critical security vulnerability in React Server Components (RSC) and Next.js that could allow unauthenticated attackers to achieve remote code execution on susceptible devices.

According to statistics from the Shadowserver Foundation, there are about 90,300 instances that remain susceptible to the vulnerability as of December 31, 2025, out of which 68,400 instances are located in the U.S., followed by Germany (4,300), France (2,800), and India (1,500).

RondoDox, which emerged in early 2025, has broadened its scale by adding new N-day security vulnerabilities to its arsenal, including CVE-2023-1389 and CVE-2025-24893. It's worth noting that the abuse of React2Shell to spread the botnet was previously highlighted by Darktrace, Kaspersky, and VulnCheck.

The RondoDox botnet campaign is assessed to have gone through three distinct phases prior to the exploitation of CVE-2025-55182 -

- March - April 2025 - Initial reconnaissance and manual vulnerability scanning
- April - June 2025 - Daily mass vulnerability probing of web applications like WordPress, Drupal, and Struts2, and IoT devices like Wavlink routers
- July - early December 2025 - Hourly automated deployment on a large-scale

In the attacks detected in December 2025, the threat actors are said to have initiated scans to identify vulnerable Next.js servers, followed by attempts to drop cryptocurrency miners ("/nuts/poop"), a botnet loader and health checker ("/nuts/bolts"), and a Mirai botnet variant ("/nuts/x86") on infected devices.

"/nuts/bolts" is designed to terminate competing malware and coin miners before downloading the main bot binary from its command-and-control (C2) server. One variant of the tool has been found to remove known botnets, Docker-based payloads, artifacts left from prior campaigns, and associated cron jobs, while also setting up persistence using "/etc/crontab."

"It continuously scans /proc to enumerate running executables and kills non-whitelisted processes every ~45 seconds, effectively preventing reinfection by rival actors," CloudSEK said. To mitigate the risk posed by this threat, organizations are advised to update Next.js to a patched version as soon as possible, segment all IoT devices into dedicated VLANs, deploy Web Application Firewalls (WAFs), monitor for suspicious process execution, and block known C2 infrastructure.

References:

- https://thehackernews.com/2026/01/rondodox-botnet-exploits-critical.html

---

Title: IoT Vulnerabilities and BotNet Infections: What Executives Need to Know

Impacted Sector: OT/IoT

Attack Summary:

The Internet of Things (IoT) has revolutionized the way we interact with technology. From smart homes to connected cars, IoT devices have permeated every aspect of our lives. However, the proliferation of these devices has also opened up new avenues for cyber threats, particularly botnet infections.

IoT devices, due to their interconnected nature, present a unique set of vulnerabilities. These devices often lack robust security measures, making them an attractive target for cybercriminals. Furthermore, the sheer number of IoT devices in use amplifies the potential impact of a successful attack.

Botnet Infections in IoT

A botnet is a network of compromised devices, or 'bots', controlled by a malicious actor. Cybercriminals often exploit IoT vulnerabilities to infect devices with malware and incorporate them into a botnet. Once under the attacker's control, these devices can be used to carry out various malicious activities, such as Distributed Denial of Service (DDoS) attacks, data theft, and spamming.

Real-World Examples of Botnet Infections

The Mirai botnet, discovered in 2016, serves as a stark example of the potential scale and impact of IoT botnet infections. Mirai infected hundreds of thousands of IoT devices, including cameras and routers, and used them to launch one of the largest DDoS attacks in history.

In another instance, the Amazon-owned company Ring experienced a security breach where cybercriminals hacked into Ring's home monitoring systems using weak, recycled, and default credentials. This allowed them to access live feeds and communicate remotely with the devices

Preventing IoT Vulnerabilities and BotNet Infections

Given the potential damage caused by these threats, it is crucial to implement measures to prevent them. Here are some recommended steps:

1. **Secure Your Devices:** Ensure all IoT devices are secured with strong, unique passwords. Regularly update device firmware to patch any known vulnerabilities.

2. **Network Segmentation:** Segregate your IoT devices onto a separate network. This can prevent an infected device from compromising your entire network.

3. **Regular Monitoring:** Regularly monitor your network for any unusual activity. Early detection can help mitigate the impact of an attack.

4. **Use Security Software:** Install robust security software that can detect and remove malware from your devices.

5. **Educate Yourself and Your Team:** Stay informed about the latest threats and how to prevent them. Regular security training can help your team recognize and avoid potential threats.

How to Check for Botnet Infections on Your Personal Devices

Are you concerned your device may already have been infected? To check for a botnet infection on your computer or network, you can follow these steps:

1. Review Network Traffic: Look for unusual outgoing traffic, especially to unknown IP addresses. This could indicate that your device is communicating with a command and control server.

2. Check for High Resource Usage: Unusually high CPU or network usage can be a sign of a botnet infection, especially if there is no corresponding user activity. You can monitor this using your operating system's task manager or system monitor.

3. Analyze System Logs: Check system logs for any strange activity, such as unknown programs starting automatically, failed login attempts, or other suspicious entries. This can sometimes indicate the presence of malware.

4. Check for Unusual Software Behavior: If applications start crashing frequently, or if your browser has new toolbars, homepages, or redirects that you didn't set up, it might be due to malware infection.

5. Consult with Cybersecurity Professionals: If you suspect a botnet infection but can't confirm it, consulting with cybersecurity experts can provide more in-depth analysis and mitigation strategies.

References:

- https://blackcloak.io/iot-vulnerabilities-and-botnet-infections-what-executives-need-to-know/

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