COLORTOKENS

ColorTokens Threat Advisory

Threat Intelligence Brief #22

April 30, 2026

ACCESS BRIEF

Threat Intelligence Brief

April 30, 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-2026-20093	Cisco Integrated Management Controller Authentication Bypass Vulnerability	9.8	A vulnerability in the change password functionality of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system as Admin. This vulnerability is due to incorrect handling of password change requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to bypass authentication, alter the passwords of any user on the system, including an Admin user, and gain access to the system as that user.	affected Vesrion and Products Vendor: Cisco Product : Cisco Enterprise NFV Infrastructure Software More than 200 + affected versions. Please check reference tab link for the vesrsions.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn	https://www.cve.org/CVERecord?id=CVE-2026-20093
CVE-2026-41940	WebPros cPanel and WHM Authentication Bypass via Login Flow	9.8	cPanel and WHM versions after 11.40 contain an authentication bypass vulnerability in the login flow that allows unauthenticated remote attackers to gain unauthorized access to the control panel.	Afftected .. Vendor: WebPros Product : cPanel Vendor : WebPros Product : WP Squared Vendor : WebPros Product : WHM Please check reference tab link for the versions	https://docs.cpanel.net/release-notes/release-notes https://docs.wpsquared.com/changelogs/versions/changelog/#13617 https://support.cpanel.net/hc/en-us/articles/40073787579671-cPanel-WHM-Security-Update-04-28-2026	https://www.cve.org/CVERecord?id=CVE-2026-41940
CVE-2026-27681	SQL Injection vulnerability in SAP Business Planning and Consolidation and SAP Business Warehouse	9.9	Due to insufficient authorization checks in SAP Business Planning and Consolidation and SAP Business Warehouse, an authenticated user can execute crafted SQL statements to read, modify, and delete database data. This leads to a high impact on the confidentiality, integrity, and availability of the system.	affected Vendor: SAP_SE Product: SAP Business Planning and Consolidation and SAP Business Warehouse affected at HANABPC 810 affected at BPC4HANA 300 affected at SAP_BW 750 affected at 752 affected at 753 affected at 754 affected at 755 affected at 756 affected at 757 affected at 758 affected at 816	https://url.sap/sapsecuritypatchday https://me.sap.com/notes/3719353	https://www.cve.org/CVERecord?id=CVE-2026-27681
CVE-2026-34621	Acrobat Reader | Improperly Controlled Modification of Object Prototype Attributes	8.6	Acrobat Reader versions 24.001.30356, 26.001.21367 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	Vendor: Adobe Product: Acrobat Reader Affected at , affected from 0 through 26.001.21367	https://helpx.adobe.com/security/products/acrobat/apsb26-43.html	https://www.cve.org/CVERecord?id=CVE-2026-34621

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: Ransomware Attack on Cookeville Regional Medical Center Affected 338K Individu

Impacted Sector: Healthcare

Attack Summary:

Cookeville Regional Medical Center in Cookeville, Tennessee, has recently confirmed that a 2025 ransomware attack exposed the personal and protected health information of 337,917 individuals. Cookeville Regional Medical Center identified the ransomware attack on July 14, 2025, and immediately took action to prevent further unauthorized access to its network. The forensic investigation determined that the ransomware group had access to its computer network between July 11, 2025, and July 14, 2025.

The attack was announced by Cookeville Regional Medical Center promptly, and within a couple of months, when it was confirmed that personal and protected health information had been exposed, a further announcement was made, warning patients about potential data theft. The data breach was reported to the HHS' Office for Civil Rights in August 2025, using a placeholder figure of 500 individuals; however, it has taken several months to review all of the exposed data. On March 16, 2026, the file review was completed, and Cookeville Regional Medical Center obtained the full list of affected individuals. Up-to-date contact information was obtained, and notification letters are now being sent. The types of importation exposed in the incident vary from individual to individual, and may include names in combination with some or all of the following: address, date of birth, Social Security number, driver's license number, financial account number, medical treatment information, medical record number, and/or health insurance policy information.

The affected individuals have been advised to remain vigilant against misuse of their information and should check their accounts and explanation of benefits statements carefully. While no evidence has been found to indicate misuse of the compromised data, Cookeville Regional Medical Center has offered the affected individuals complimentary credit monitoring and identity theft protection services for 12 months, and additional technical security measures have been implemented to prevent similar incidents in the future.

The Rhysida ransomware group claimed responsibility for the attack and added Cookeville Regional Medical Center to its dark web data leak site. Rhysida claims to have exfiltrated 538 gigabytes of data in the attack and has published the data that it has been unable to sell. The data leak site indicates 70% of the data has been leaked, which suggests that the group found a buyer for 30% of the data.

References:

- https://www.hipaajournal.com/hospital-caribbean-medical-center-data-breach/
- https://www.securityweek.com/data-breach-at-tennessee-hospital-affects-337000/

Title: Ransomware Attack on Hospital Caribbean Medical Center Among Three Healthcare Breaches Affecting Patient Data

Impacted Sector: Healthcare

Attack Summary:

Three US healthcare organizations have disclosed data breaches affecting patient and employee information, with the most significant involving a ransomware attack on Hospital Caribbean Medical Center in Fajardo, Puerto Rico.

The Puerto Rico hospital issued a press release on February 8, 2026, disclosing a cyberattack that targeted its information systems. The incident is listed on the HHS Office for Civil Rights breach portal as affecting up to 92,000 individuals. The hospital did not specify what types of data were exposed or confirm the ransomware classification, but a group called The Gentlemen claimed responsibility on February 17, adding the hospital to its dark web leak site and threatening to publish stolen patient data if a ransom was not paid.

Murray County Medical Center in Slayton, Minnesota disclosed in early March 2026 that suspicious activity was detected in its IT systems on August 21, 2025. It took until January 27, 2026, to confirm that patient and employee data had been compromised. Exposed information includes names, dates of birth, Social Security numbers, driver's license numbers, health insurance information, medical treatment details, and medical history. The breach affects 5,073 individuals.

Aligned Orthopedic Partners in Maryland disclosed that an unknown actor accessed its email platform between November 16 and December 16, 2025, with suspicious activity identified on December 8. The compromised data is among the most extensive of the three incidents, spanning names, dates of birth, Social Security numbers, Medicaid and Medicare numbers, financial account numbers, mental and physical condition information, prescription details, diagnosis and clinical information, and medical record numbers. Notification letters were mailed on April 17, 2026. The number of affected individuals has not yet appeared on the HHS breach portal.

Who is affected

Patients and employees across all three organizations face exposure of sensitive personal and health information. The Aligned Orthopedic Partners breach is particularly broad in scope given the range of data categories confirmed as compromised, including financial account numbers and mental health information. The 92,000 figure for Hospital Caribbean Medical Center represents a significant portion of the population in the Fajardo region of Puerto Rico. investigations in response to the data breach and are considering filing class action lawsuits.

Why CISOs should care

The Murray County Medical Center timeline is worth examining closely. Suspicious activity was detected in August 2025, but it took until late January 2026, five months, to confirm that data had actually been compromised. That dwell time and investigation gap is not unusual in healthcare, but it directly affects notification timelines, regulatory exposure, and the window during which affected individuals have no way to protect themselves.

The Aligned Orthopedic Partners breach also illustrates a recurring pattern: email platform compromises in healthcare consistently yield some of the broadest data exposures, because clinical staff use email to share exactly the kind of sensitive, multi-category patient information that makes healthcare breaches so damaging.

3 practical actions

Compress investigation-to-confirmation timelines with better forensic readiness: A five-month gap between detection and confirmed data compromise is a significant liability. Investing in forensic tooling, retained incident response relationships, and log retention policies that support faster investigation will reduce both regulatory risk and patient harm.

Restrict clinical data sharing through email: Email remains one of the most common breach vectors in healthcare precisely because it carries so much sensitive information. Review what categories of patient data are routinely shared via email and whether alternative secure messaging or clinical communication platforms can reduce that exposure.

Monitor ransomware leak sites for listings involving your organization or partners: Hospital Caribbean Medical Center's listing appeared nine days after the hospital's own press release. Proactive monitoring of leak sites can provide earlier warning and more time to assess the credibility of theft claims before they become public.

References:

- https://securityboulevard.com/2026/04/ransomware-attack-on-hospital-caribbean-medical-center-among-three-healthcare-breaches-affecting-patient-data/
- https://www.hipaajournal.com/hospital-caribbean-medical-center-data-breach/

Title: Healthcare Organizations Struggling to Implement Primary Method of Blocking Lateral Movement

Impacted Sector: Healthcare

Attack Summary:

A study of security leaders from the healthcare and manufacturing industries found that while there is an almost universal desire to deploy modern microsegmentation, more than 90% of respondents said they had protected fewer than 80% of critical systems, despite almost half admitting to falling victim to lateral movement attacks in the past year. In healthcare, fewer than 6% of respondents said that their organization had implemented microsegmentation across 80% or more of their critical systems.

Microsegmentation is a cybersecurity technique that divides networks into small, distinct, and isolated zones to secure workloads, applications, or devices. Traditional network segmentation, such as Virtual Local Area Networks (VLANs), creates broad segmented zones, whereas microsegmentation applies security policies at the individual workload or application level. Microsegmentation allows organizations to implement East-West traffic control within their data center, rather than only North-South traffic controls for identifying traffic leaving the network. It provides deep visibility into network traffic flows, including which applications are communicating with each other. Healthcare organizations can enable strict isolation and monitoring of systems that handle sensitive data such as protected health information (PHI), which can simplify HIPAA Security Rule compliance.

Microsegmentation protects internal workloads from applications without authorized access, and can be applied to on-premises and hybrid environments. It reduces the attack surface and greatly limits the potential for lateral movement. In the event of compromise, attackers are contained within a microsegment, limiting the harm they can cause and the data they can access.

The study was conducted on 352 healthcare and manufacturing security leaders by Omdia, on behalf of the network segmentation specialists Elisity. The survey revealed 99% of respondents were implementing or planning to implement microsegmentation, with 57% of respondents ranking microsegmentation as their main initiative to prevent lateral movement; however, they were slow to fully implement it. Only 9% of respondents had implemented it across 80% or more of critical systems, and just 6% in healthcare. While Microsegmentation ranked first among planned priorities, it ranked close to the bottom 24% among currently deployed zero-trust architectures.

There have been challenges with implementing microsegmentation in the past; however, modern identity-based microsegmentation is a different beast, as it requires no agents, no hardware changes, and no VLAN recognition. Instead, the policy is enforced directly on network switches. "Microsegmentation has matured, but many organizations still carry the scars of earlier, complex approaches. What's changed is the architecture. Identity-based microsegmentation lets teams enforce precise policy on the switches they already run, so security becomes an enabler rather than a gate," James Winebrenner, CEO, Elisity, said.

Most organizations still rely on VLANs, ACLs, and agent-based tools, which require constant rework and leave East-West exposure wide open, and progress with implementation has been slow. First-generation tools built around network location rather than identity have slowed real progress to a crawl, as agent-based and firewall-centric designs couldn't uniformly cover IT, IoT, OT, or IoMT. According to Elisity, "These approaches had outdated or unsupported software (56%), high maintenance costs and hardware limitations (50%), and frequent failures or performance issues (43%)."

There have been challenges implementing microsegmentation in healthcare, especially with integrating SIEM, EDR, and SOAR. Respondents said visiting clinicians (74%) and clinical staff (72%) require the most granular policy attention, given the mix of managed and unmanaged devices moving through clinical environments. Many respondents lacked awareness of the ease and speed at which modern identity-based solutions can be deployed. Only 22% of respondents had hands-on experience of implementing microsegmentation, and most teams were still running legacy methods.

There is a clear desire to implement microsegmentation, and awareness of modern-identity-based microsegmentation is improving. "Our data shows the shift is on. Enterprises intend to deploy microsegmentation, and many now see modern solutions as easier and more effective," said Hollie Hennessy, Principal Analyst, Omdia, who points out that with modern solutions, the timeline for implementation has shortened from years to weeks.

References:

- https://www.hipaajournal.com/healthcare-organizations-struggling-to-implement-primary-method-blocking-lateral-movement

Title: 17M Nissan cars impacted by large ransomware attack

Impacted Sector: Tech

Attack Summary:

Nissan has confirmed that a recent cyber incident involved a third-party vendor serving Nissan and Infiniti dealerships in North America, after the Everest ransomware gang claimed it stole 910 GB of data tied to the automaker's dealer ecosystem. In a statement reported by The Record, Nissan said it was aware of a cyber incident affecting an undisclosed vendor earlier this year and that its investigation found the issue was isolated to that vendor and information provided to it. Nissan added that it found "no indication" Nissan systems were compromised or that Nissan customer information was accessed or put at risk.

The attackers, however, described a much broader exposure. Materials reviewed by DataBreach.com identify the affected environment as GCSSD Apps FTP servers operated by GCSSD, an IT contractor that allegedly hosted and processed data on behalf of Nissan. According to the breach materials, the exposed files include customer database dumps, repair-order data, dealer employee records, financial-related extracts, internal business reporting, and source code tied to dealer systems. The most recent file referenced in the materials is dated January 3, 2026.

DataBreach.com reviewed and parsed the leaked data and identified 2,685,720 phone numbers, 2,045,754 email addresses, 4,193,509 full names, 4,055,146 street addresses, 2,736 dates of birth, and 17,119,482 vehicle identification numbers. These figures reflect data elements found in the files, not necessarily unique individuals or vehicles, because the same person, household, or car may appear repeatedly across historical exports and operational records.

A sample file reviewed by DataBreach.com indicates the leak includes row-level dealership service and repair records rather than a simple contact list. In records reviewed, fields included customer names, street addresses, city and ZIP data, VINs, mileage, vehicle year, make and model details, service dates, repair descriptions, parts information, pricing data, and dealership staff names. Some rows also appeared to relate to business accounts, rental fleets, or inventory vehicles, suggesting the dataset mixes consumer, commercial, and operational records.

For consumers, the distinction between Nissan's systems and a Nissan vendor may matter far less than what was actually sitting on the server.

References:

- https://www.bleepingcomputer.com/news/security/american-utility-firm-itron-discloses-breach-of-internal-it-network/

Title: Two major US banks targeted — Citizens Bank and Frost Bank confirms breach

Impacted Sector: Finance

Attack Summary:

The Everest ransomware gang has placed two of America's most prominent financial institutions on its dark web extortion site.

On April 20th, Texas-based Frost Bank and Northeast heavyweight Citizens Financial Group both surfaced on Everest's dark web leak site.

The clock is ticking, with the attackers giving both banks six days before publicly releasing the stolen sensitive data.

This is a very common extortion tactic used by ransomware gangs to pressure victims into negotiating and eventually paying the ransom.

Froze citizen 3

Entry on a leak site

How many bank customers were exposed to the data breach?

Everest claims to hold records for approximately 250,000 Frost Bank clients. The number could not be independently verified. The data visible in the provided samples suggests that the dataset might expose:

1. **Social Security numbers (SSN)**
2. **Tax Identification numbers (TIN)**
3. **Full names**
4. **Interest rate on a mortgage**
5. **Profit gains from investments**
6. **Income**
7. **Taxable amounts**
8. **Home addresses**

However, the gang redacted portions of the preview samples posted on its leak site, so there may be more personal data in the dataset.

"Besides the risk of identity theft and financial fraud, these documents often reveal people's financial status, which can be useful to threat actors when it comes to deciding whom to attack first and to determine their tactics," the Cybernews research team noted.

The Citizens Bank data tells a different story – broader in volume but narrower in severity. The gang claims approximately 3.4 million records, a claim that cannot be proven at this point either.

The Everest listing appears to contain a SQL database dump, with sample entries and screenshots from six internal tables revealing:

1. **Full names**
2. **Home addresses**
3. **Account numbers**
4. **Internal document flags**

According to our researchers, there are no SSNs or TINs in these data samples.

"The mentioned tables do not seem to contain SSNs or TINs as opposed to Frost Bank, that's why the impact here can be more limited to scams and user profiling in general and less likely of identity theft," our team assessed.

Citizens Bank and Frost Bank confirms breach at third-party vendor

Citizens Bank has confirmed to Cybernews an "incident involving data extracted from a third-party vendor" by a known threat actor.

"For Citizens, most of this was masked test data, although a very limited set of customer information was involved," the bank's spokesperson said, adding that there is "no evidence" of unauthorized access to the Citizens network and operations continue as normal.

"We have put enhanced monitoring in place and are in the process of reaching out to impacted customers with additional information and guidance. Customers can also contact Citizens through trusted channels, such as the number on the back of their card or on their statement," the spokesperson highlighted.

"Our security teams are always on, working around the clock to help safeguard customer accounts and information, and watching for unusual activity," the Citizen Bank representative added.

Frost Bank spokesperson stated that they were recently notified by a third-party vendor of an "unauthorized access to their systems" that may have included Frost customer data.

"We have engaged external cybersecurity experts to assist in our investigation, and early findings indicate that the incident may be related to recent claims made by cybercriminals," the spokesperson highlighted.

According to the bank, at this time, there is “no evidence of unauthorized access to the Frost network”.

“Customers can be reassured they’re able to safely use all Frost services,” the Frost Bank’s spokesperson added.

froze citizen

1. **Entry on a leak site**

2. **Everest victims: major American banks**

Everest has gone for the big boys this time. Citizens Financial Group is one of the oldest and largest financial institutions in the United States, reporting $227.9 billion in assets as of March 2026.

The bank operates over 1,000 branches across 14 states, stretching from New England through the Mid-Atlantic and into the Midwest.

Frost Bank, operating under parent company Cullen/Frost Bankers, holds $53 billion in assets and over $67 billion in trust and investment management assets, ranking among the 50 largest US banks.

It operates more than 200 financial centers across Texas’s largest markets – San Antonio, Houston, Dallas-Fort Worth, and Austin.

froze citizen 2

1. **Data sample**

2. **Who is the Everest hacker group?**

The Everest ransomware-as-a-service (RaaS) operation has been active since at least 2020, running a double-extortion model.

This means the Russia-linked attackers steal data, encrypt systems, and threaten to publish everything if the victim doesn’t pay.

References:

- https://cybernews.com/security/everest-ransomware-frost-citizens-bank-breach/

Section 3 - OT/IoT Security Breaches

Title: Researchers Detect ZionSiphon Malware Targeting Israeli Water, Desalination OT Systems

Impacted Sector: OT / IoT

Attack Summary:

Cybersecurity researchers have flagged a new malware called ZionSiphon that appears to be specifically designed to target Israeli water treatment and desalination systems.

The malware has been codenamed ZionSiphon by Darktrace, highlighting its ability to set up persistence, tamper with local configuration files, and scan for operational technology (OT)-relevant services on the local subnet. According to details on VirusTotal, the sample was first detected in the wild on June 29, 2025, right after the Twelve-Day War between Iran and Israel that took place between June 13 and 24.

“The malware combines privilege escalation, persistence, USB propagation, and ICS scanning with sabotage capabilities aimed at chlorine and pressure controls, highlighting growing experimentation with politically motivated critical infrastructure attacks against industrial operational technologies globally,” the company said.

ZionSiphon, currently in an unfinished state, is characterized by its Israel-focused targeting, going after a specific set of IPv4 address ranges that are located within Israel -

- **2.52.0[.]0 - 2.55.255[.]255**
- **79.176.0[.]0 - 79.191.255[.]255**
- **212.150.0[.]0 - 212.150.255[.]255**

Besides encoding political messages that claim support for Iran, Palestine, and Yemen, the malware embeds Israel-linked strings in its target list that correspond to the nation’s water and desalination infrastructure. It also includes checks to ensure that in those specific systems.

“The intended logic is clear: the payload activates only when both a geographic condition and an environment-specific condition related to desalination or water treatment are met,” the cybersecurity company said.

Once launched, ZionSiphon identifies and probes devices on the local subnet, attempts protocol-specific communication using Modbus, DNP3, and S7comm protocols, and modifies local configuration files by tampering with parameters associated with chlorine doses and pressure. An analysis of the artifact has found the Modus-oriented attack path to be the most developed, with the remaining two only including partially functional code, indicating that the malware is still likely in development.

A notable aspect of the malware is its ability to propagate the infection over removable media. On hosts that do not meet the criteria, it initiates a self-destruct sequence to delete itself.

"Although the file contains sabotage, scanning, and propagation functions, the current sample appears unable to satisfy its own target-country checking function even when the reported IP falls within the specified ranges," Darktrace said. "This behavior suggests that the version is either intentionally disabled, incorrectly configured, or left in an unfinished state."

"Despite these limitations, the overall structure of the code likely indicates a threat actor experimenting with multi protocol OT manipulation, persistence within operational networks, and removable media propagation techniques reminiscent of earlier ICS targeting campaigns."

The disclosure coincides with the discovery of a Node.js-based implant called RoadK1ll that's designed to maintain reliable access to a compromised network while blending into normal network activity.

"RoadK1ll is a Node.js-based reverse tunneling implant that establishes an outbound WebSocket connection to attacker-controlled infrastructure and uses that connection to broker TCP traffic on demand," Blackpoint Cyber said.

"Unlike a traditional remote access trojan, it carries no large command set and requires no inbound listener on the victim host. Its sole function is to convert a single compromised machine into a controllable relay point, an access amplifier, through which an operator can pivot to internal systems, services, and network segments that would otherwise be unreachable from outside the perimeter."

Last week, Gen Digital also took the wraps off a virtual machine (VM)-obfuscated backdoor that was observed on a single machine in the U.K. and operated for a year between May 2022 and June 2023, before vanishing without any trace when its infrastructure expired. The implant has been dubbed AngrySpark. It's currently not known what the end goals of the activity were.

"AngrySpark operates as a three-stage system," the company explained. "A DLL masquerading as a Windows component loads via the Task Scheduler, decrypts its configuration from the registry, and injects position-independent shellcode into svchost.exe. That shellcode implements a virtual machine."

"The VM processes a 25KB blob of bytecode instructions, decoding and assembling the real payload – a beacon that profiles the machine, phones home over HTTPS disguised as PNG image requests, and can receive encrypted shellcode for execution."

The result is malware capable of establishing stealthy persistence, altering its behavior by switching the blob, and setting up a command-and-control (C2) channel that can fly under the radar.

"AngrySpark is not only modular, it is also careful about how it appears to defenders," Gen added. "Several design choices look specifically aimed at frustrating clustering, bypassing instrumentation, and limiting the forensic residue left behind. The binary's PE metadata has been deliberately altered to confuse toolchain fingerprinting."

References:

- https://thehackernews.com/2026/04/researchers-detect-zionsiphon-malware.html

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 solutions that operationalize breach readiness across hybrid, cloud, and OT environments. By proactively minimizing lateral movement risk and reducing attack surface, ColorTokens enables organizations to operate in a continuous state of breach readiness — before, during, and after an incident. The Xshield™ platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enforcing adaptive micro-perimeters that dynamically limit blast radius and accelerate response. Recognized as a Leader in The Forrester Wave™: Microsegmentation Solutions (Q3 2024) and the GigaOm Radar for Microsegmentation v3 (March 2026), ColorTokens helps enterprises strengthen operational resilience and maintain security posture as threats evolve. For more information, visit www.colortokens.com.

Copyright 2026 © ColorTokens. All rights reserved.