COLORTOKENS

THREAT INTELLIGENCE BRIEF #30

ColorTokens Threat Advisory

October 31, 2026

ACCESS BRIEF

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

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.

FINANCE

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.

ACROSS SECTORS

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-2026-70229

Windows Active Directory Domain Services Remote Code Execution Vulnerability

9.0 CRITICAL CVSS

Incorrect authorization in Active Directory Domain Services allows an unauthorized attacker to execute code over a network.

AFFECTED VERSIONS

Vendor: Microsoft

Product: Windows 10 Version 1607

Platforms

32-bit Systems, x64-based Systems

Versions 1 Total

Default Status: unknown

affected

affectedfrom 10.0.14393.0before 10.0.14393.9612

And 10+ other MS version.
Please access the given link to understand affected versions.

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70229

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-70229

CVE-2026-70571

Microsoft Exchange Server Remote Code Execution Vulnerability

8.1 HIGH CVSS

Stack-based buffer overflow in Microsoft Exchange Server allows an unauthorized attacker to execute code over a network.

AFFECTED VERSIONS

Vendor: Microsoft

Product: Microsoft Exchange Server 2016 Cumulative Update 23

Platforms: x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 15.01.0.0before 15.01.2507.077

Vendor: Microsoft

Product: Microsoft Exchange Server 2019 Cumulative Update 14

Platforms: x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 15.02.0.0before 15.02.1544.050

Vendor: Microsoft

Product: Microsoft Exchange Server 2019 Cumulative Update 15

Platforms: x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 15.02.0.0before 15.02.1748.055

Vendor: Microsoft

Product: Microsoft Exchange Server Subscription Edition RTM

Platforms: x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 15.02.0.0before 15.02.2562.056

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70571

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-70571

CVE-2026-96951

Windows Shell Security Feature Bypass Vulnerability

8.8 HIGH CVSS

Improper neutralization of special elements used in a command (‘command injection’) in Windows Shell allows an unauthorized attacker to bypass a security feature over a network.

AFFECTED VERSIONS

Vendor: Microsoft

Product: Microsoft Edge (Chromium-based)

Versions 1 Total

Default Status: unknown affected

affectedfrom 1.0.0.0before 154.0.4258.62

Vendor: Microsoft

Product: Outlook.com

Versions 1 Total

Default Status: unknown affected

affectedfrom 1.0.0before 20260925.100

And 10+ other MS version. Please access the given link to understand affected versions.

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-96951

CVE-2026-109618

RCE via OOM corruption

9.3 CRITICAL CVSS

PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).

AFFECTED VERSIONS

Vendor: PHP Group

Product: PHP

Versions 4 Total

Default Status: unaffected affected

affectedfrom 8.2.*before 8.2.35

affectedfrom 8.3.*before 8.3.36

affectedfrom 8.4.*before 8.4.27

affectedfrom 8.5.*before 8.5.12

PATCH DETAILS

https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-109618

CVE-2026-114625

Security Advisory 0199- VeloCloud Orchestrator (VCO) on-prem privileged internal functionality

9.9 CRITICAL CVSS

VeloCloud Orchestrator (VCO) on-prem has a security issue where this issue may allow a remote attacker to access privileged internal functionality and impact the VCO host. Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator and data managed by the orchestrator. On an affected system, any authenticated user can gain operator privileges and masquerade as a local “superuser operator” user. This includes access to functionality that is intended for internal use only and which is not intended to be remotely accessible

AFFECTED VERSIONS

Vendor: Microsoft

Product: Microsoft Entra

PATCH DETAILS

https://cwe.mitre.org/data/definitions/89.html

https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-114625

CVE-2026-59310

vCenter directory-traversal vulnerability

9.9 CRITICAL CVSS

VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code.

AFFECTED VERSIONS

Vendor: VMware

Product: Cloud Foundation

Versions 3 Total

Default Status: unaffected affected

affectedat 9.1.x.x

affectedat 9.0.x.x

affectedat 5.x

Vendor: VMware

Product: vSphere Foundation

Versions 2 Total Default Status: unaffected affected

affectedat 9.1.x.x

affectedat 9.0.x.x

Vendor: VMware

Product: vCenter

Versions 3 Total Default Status: unaffected affected

affectedfrom 9.1.x.xbefore 9.1.0.0300

affectedfrom 9.0.x.xbefore 9.0.2.0100

affectedfrom 8.0before 8.0 U3k

Vendor: VMware

Product: Telco Cloud Infrastructure

Versions 1 Total Default Status: unaffected affected

affectedat 3.0

Vendor: VMware

Product: Telco Cloud Platform

Versions 4 Total Default Status: unaffected affected

affectedat 5.1.x, affectedat 5.0.x

affectedat 4.x, affectedat 3.0

PATCH DETAILS

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-59310

CVE-2026-3382486950

Windows Internet Key Exchange (IKE) Service Extension

9.9 CRITICAL CVSS

Double free in Windows IKE Extension allows an unauthorized attacker to execute code over a network.

AFFECTED VERSIONS

Vendor: Microsoft

Product: Windows 10 Version 1607

Platforms: 32-bit Systems, x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 10.0.14393.0before 10.0.14393.9060

Vendor: Microsoft

Product: Windows 10 Version 1809

Platforms: 32-bit Systems, x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 10.0.17763.0before 10.0.17763.8644

Vendor: Microsoft

Product: Windows 10 Version 21H2

Platforms: 32-bit Systems, ARM64-based Systems, x64-based Systems

Versions 1 Total

Default Status: unknown affected

affectedfrom 10.0.19044.0before 10.0.19044.7184

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-33824

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

HEALTHCARE

Data Breaches Announced by HCA Healthcare; Blossom Health

ATTACK SUMMERY

HCA Healthcare Inc

Nashville, Tennessee-based HCA Healthcare Inc., the operator of 189 hospitals and approximately 2,600 ambulatory sites of care in 19 U.S. states, has disclosed a cybersecurity incident that was first identified on August 12, 2026. Patient and employee data were compromised in the incident.

Suspicious activity was identified within certain IT systems, and the forensic investigation confirmed unauthorized access to those systems on August 12, 2026. HCA Healthcare confirmed that the threat actor obtained copies of certain HR files containing medical resident personal information. The review of the impacted files confirmed that they contained information related to employment, including name, date of birth, email address, phone number, Social Security number, and immigration information.

Patient data was also compromised related to certain affiliated facilities and physician offices. Patient data exposed in the incident included names, email addresses, phone numbers, dates of birth, Social Security numbers, medical information, and health insurance information. The number of affected patients has yet to be disclosed, although 15,096 Texas residents are known to have been affected. The affected individuals have been offered two years of complimentary credit monitoring services.

Blossom Health

Blossom BH Opco Inc., an online telepsychiatry and virtual mental health provider that does business as Blossom Health, has started notifying certain patients about an August 2026 data security incident involving unauthorized access to its electronic health record (EHR) software. According to its October 29, 2026, notification letters, an unauthorized actor gained access to the EHR software and patient data via a phishing attack on a non-employee contractor.

The incident has been investigated, and Blossom Health confirmed that the exposed information included names, contact information, and health insurance information. Blossom Health said financial information and Social Security numbers were not accessible. In its website regulatory disclosure, Blossom Health confirmed that the threat actor downloaded a limited number of patient medical records and a user spreadsheet containing patient information.

The unauthorized access has been blocked, user passwords have been changed, and additional technical security measures have been deployed to reduce the risk of similar incidents in the future. As a precaution against identity theft and fraud, the affected individuals have been offered complimentary single-bureau credit report, credit score, and credit monitoring services. The Texas Attorney General was informed that 2,103 Texas residents have been affected, although the total number of affected individuals has yet to be disclosed.

El Camino Health

El Camino Health, a non-profit health system serving Santa Clara County and the Bay Area in California, has confirmed that an unauthorized individual gained access to its Microsoft 365 environment. Suspicious activity was identified on September 1, 2026, and the forensic investigation confirmed unauthorized access to four Microsoft 365 accounts, which were intermittently accessed between August 26, 2026, and September 2, 2026. Certain documents within those accounts were copied or downloaded.

The review of the affected files has been completed, and they were found to contain contact information, demographic information, Social Security numbers, driver's license numbers, dates of birth, medical record numbers, patient account numbers, diagnoses, treatment information, prescription information, provider names, dates of service, and health insurance information.

A subset of patients also had financial account and routing numbers compromised in the incident. El Camino Health has implemented additional protection and monitoring measures to reduce the risk of similar incidents in the future, and the affected individuals have been offered complimentary credit monitoring and identity theft protection services. The number of affected individuals has not yet been publicly disclosed.

University of Mississippi Medical Center

University of Mississippi Medical Center (UMMC) has started notifying certain patients about unauthorized access to its computer systems. The unauthorized access was identified on February 19, 2026. Third-party cybersecurity experts were engaged to assist with the investigation, and on October 20, 2026, it was confirmed that its network was subject to unauthorized access between February 11, 2026, and February 19, 2026.

UMMC has reviewed the exposed files, but its notice to the California Attorney General does not include details of the types of data involved or the number of affected individuals. There is currently no substitute data breach notice on the UMMC website. This appears to have been a ransomware attack. The Medusa ransomware group claimed responsibility for the attack in March 2026 and demanded payment to prevent the sale or release of the stolen data. The ransom was not paid.

References:

- https://www.hipaajournal.com/labcorp-multistate-settlement-amca/

HEALTHCARE

University of New Mexico Health System Diverts Ambulances Due to Ransomware Attack

ATTACK SUMMERY

The University of New Mexico Health System (UNM Health) has experienced a cyberattack that has prevented access to critical electronic systems. The incident was detected on October 26, 2026, and as a precaution to ensure patient safety, all ambulance traffic was temporarily diverted to alternative hospitals. A decision was made to cancel all appointments at UNM Health facilities on October 26. UNM Health explained in a 2:30 p.m. update on October 26 that it was also temporarily limiting the acceptance of new patients while efforts continued to restore access to key systems.

Other health systems in Albuquerque and Santa Fe have been working with UNM Health to ensure that patients receive the care they need. UNM Health operates UNM Hospital in Albuquerque, the only level 1 trauma center in New Mexico, so the cyberattack had the potential to place patient safety at serious risk. According to UNM Health's announcement, the incident caused a system outage that affected the entire University of New Mexico Health Sciences Center. On October 26, all students at the School of Medicine, College of Pharmacy, College of Nursing, and College of Population Health were requested to leave the campus, and classes were also cancelled on Tuesday.

UNM Health was able to quickly start restoring access to systems, and confirmed in a 10:27 p.m. update that all UNM Health hospitals remain open, and clinics would resume regularly scheduled appointments on October 27, 2026. In the early hours of October 27, 2026, UNM Health confirmed that critical systems had been brought back online at The University of New Mexico Health Sciences Center, and ambulance traffic had returned to normal operations. The divert lasted from 12:30 to 2:30 p.m. on October 26. UNM Health said the cancellation of appointments and outpatient surgeries was necessary while IT teams worked to protect the network.

Containment efforts began at around 11 a.m. on October 26, which were largely successful. While some end user devices were impacted, UNM was able to prevent the threat actor from reaching its core systems and servers. External cybersecurity partners assisted with the remediation efforts, and an investigation has been launched to assess the nature and scope of the unauthorized access.

Law enforcement has been notified, and the incident is under criminal investigation, so limited information about the nature of the attack can be disclosed at this time. It is naturally too early to determine the extent to which patient data was involved. While UNM Health has not disclosed details about the nature of the attack, this appears to have been an attempted ransomware attack. A new ransomware group called Byod has claimed it was responsible. The group's data leak site currently lists 10 victims.

The group's post about the attack suggests that 36,000 systems at the UNM main campus and UNM Health were compromised, and that patient, student, and employee data was exfiltrated, along with payroll information, internal emails, and Cerner EHR rosters. The group later backtracked to a degree, adding a further post stating it was unaware that "[UNM Health] was running machines related to assisting patients in real-time," and offered to provide certain decryption keys for free. "(we would keep it locked if it was appointments, patient information + research data only), we are still going to keep the data, but we will provide the decryption key for the hospital sector only... To any patient that was affected, we will pay you up to $2,500 each for the inconvenience. We are sorry once again. We have morals, and we have a heart, we are not villains, but we will still hold companies responsible for bad security leading to compromise of any customer data."

References:

- https://www.hipaajournal.com/university-new-mexico-health-system-cyberattack/

HEALTHCARE

Ransomware Incident at Paylogix Affects 41K Individuals

ATTACK SUMMERY

Paylogix, New York

Paylogix LLC, a New York-based third-party administrator and software-as-a-service provider, whose solutions are used for enrollment, billing, and managing voluntary employee benefits, has notified the HHS Office for Civil Rights (OCR) about a breach of the protected health information of 41,739 individuals.

Paylogix explained in its breach notification letter that it experienced a network disruption involving certain computer systems and services. The forensic investigation determined that an unauthorized third party had access to its computer network from November 13, 2025, to November 18, 2025. During that time, files containing personal and protected health information were accessed and copied from its network.

The review of the affected files was recently completed. Paylogix determined that the exposed data included dates of birth, Social Security numbers, and voluntary benefit information. A subset of individuals also had their access credentials, electronic signatures, financial account information, health insurance information, medical information, passport numbers, taxpayer identification numbers, and/or U.S. alien identification numbers compromised in the incident. While not mentioned in the notification letters, this appears to have been a ransomware attack by the Akira ransomware group, which claimed to have exfiltrated 185 GB of data.

The Kenaitze Indian Tribe, Alaska

The Kenaitze Indian Tribe in Alaska has notified 9,319 individuals about a data security incident that exposed some of their protected health information. Suspicious activity was identified within its network on July 27, 2026. The investigation concluded that an unauthorized third party had access to its network between July 16, 2026, and July 27, 2026. During that time, files on the compromised parts of the network may have been accessed or acquired.

The review of the affected data was recently completed, and it has been confirmed that the exposed data includes first and last names, dates of birth, Social Security numbers, driver's license numbers/state IDs, financial account numbers, health insurance information, and medical information. The affected individuals started to be notified on September 25, 2026.

Center for Bone and Joint Surgery of the Palm Beaches, Florida

Center for Bone and Joint Surgery of the Palm Beaches in Florida has notified the HHS' Office for Civil Rights about a breach of the protected health information of 5,461 individuals. On July 27, 2026, suspicious activity was identified on its website. The investigation determined that certain forms on its website may have been compromised, potentially allowing an unauthorized third party to obtain data associated with those forms. While data was exposed, the investigation found no proof that patient data was obtained or misused.

The data review determined that the exposed information included names, contact information, appointment request information, and information voluntarily provided through website forms. The affected forms have been removed from its website, security has been strengthened, and additional security measures have been implemented to reduce the risk of similar incidents in the future.

Wichita Family Dental, Kansas

Wichita Family Dental, a dental practice with locations in Wichita and Derby, Kansas, has identified unauthorized access to an employee's email account. The unauthorized access was identified on or around May 4, 2026. The account has been secured, and the investigation and review of the account were completed on July 6, 2026.

The account was found to contain the personal and protected health information of 1,273 individuals. The data involved included names, addresses, dates of birth, Social Security numbers, driver's license numbers/state ID numbers, taxpayer ID numbers, payment card information, financial account information, health insurance information, and dental records. Steps have been taken since the incident to improve email security.

References:

- https://www.hipaajournal.com/data-breach-paylogix-kenaitze-bone-joint-center-wichita-family-dental/

TECH

Pentagon Defense Manpower Data Center (DMDC) Data Breach Exposes Social Security Numbers and Military Personnel RecordsDepartment personnel

ATTACK SUMMERY

Unauthorized users accessed a vulnerable server at the Pentagon's Defense Manpower Data Center, exposing Social Security numbers and other personal data of current and former military personnel. The full number affected has not been disclosed. Affected individuals should monitor credit reports, consider a credit freeze, and watch for phishing attempts referencing military service.

Company	Pentagon Defense Manpower Data Center (DMDC)
Industry	Other Commercial
Data Types Exposed	Social Security Numbers, Military Personnel Records, Personal Identifying Information
People Affected	Not Publicly Disclosed
Attack Method	Unauthorized Network Access
Regulators Notified	Not Publicly Disclosed

What Happened in the Pentagon DMDC Data Breach?
A serious security failure at the Pentagon's Defense Manpower Data Center has put the personal records of military personnel at risk. The DMDC is a massive human resources system that stores data on current and former service members. According to reports, unauthorized users gained access to a vulnerable server tied to this system.

The Pentagon DMDC data breach reportedly began when attackers exploited a weakness in a computer server connected to the agency's network. Because the DMDC holds records for millions of military personnel, the exposure of this server raised immediate alarm among security experts. As a result, officials have flagged the incident as a potential counterintelligence threat, not just a routine data exposure.

The exact discovery date of the intrusion has not been publicly disclosed. However, notification of the breach became public in September 2026. Investigators are reportedly examining how long the unauthorized users had access to the server before the compromise was identified. This kind of forensic review is standard after any confirmed intrusion into a sensitive government system.

Because this involves a defense-related system, the investigation likely includes multiple agencies. In addition, national security experts have pointed out that stolen military personnel data could be misused well beyond ordinary identity theft. This makes the Pentagon DMDC data breach different from many breaches involving retail or healthcare companies.

Who was affected
The breach affects current and former military personnel whose records are stored in the DMDC system. This system is used broadly across the Department of Defense. Therefore, the population affected could include active-duty service members, veterans, and possibly their dependents, though the source material does not specify exact categories.

The total number of individuals affected has not been publicly disclosed. Given the scale of the DMDC, which serves as a central HR repository for the military, the population at risk could be significant. However, no official figure has been released, so speculation about an exact count would be inaccurate.

Because military records often include personnel stationed both domestically and overseas, the geographic scope of this breach could be broad. Meanwhile, it remains unclear whether the exposed data includes information tied to still-active security clearances. This detail matters greatly for assessing the true national security impact of the incident.

What Information Was Potentially Exposed

Reports indicate that the breach exposed Social Security numbers along with other personal information belonging to military personnel. This combination of data is particularly sensitive because of the population involved. Below is a summary of the data categories referenced in connection with this incident.

Social Security numbers

Other personal identifying information tied to military personnel records
Social Security numbers are among the most valuable pieces of data for identity thieves. With a Social Security number, a criminal can potentially open new credit accounts, file fraudulent tax returns, or apply for loans in a victim's name. For military personnel specifically, this risk is compounded by frequent relocations, which can delay a service member's awareness of fraudulent activity.

Beyond conventional identity theft, national security experts have raised concerns about counterintelligence risks. Foreign adversaries could potentially use exposed military personnel data to identify, profile, or target individuals with access to sensitive information. This makes the Pentagon DMDC data breach a matter of both personal financial risk and broader institutional security concern.

References:

- https://databreachrights.com/pentagon-dmdc-data-breach/

SECTION 3

OT/IoT Security Breaches

OT & IOT

Mass Website Compromise Campaign Delivers LunexStealer Through Fake Cloudflare Security Checks

ATTACK SUMMERY

In September 2026, Ukraine's CERT-UA identified over 100 compromised websites injected with malicious JavaScript to distribute LunexStealer malware through fake Cloudflare verification pages. The UAC-0277 threat cluster used ClickFix techniques and EtherHiding methods to selectively target Windows users arriving from search engines, delivering MSI packages that install sophisticated information-stealing capabilities including the LUNARAXE browser extension and NAIVEMESS file system access component.

Attack Path Analysis

UAC-0277 compromised over 100 websites with malicious JavaScript that displayed fake Cloudflare verification pages using ClickFix technique. Victims executed commands downloading MSI packages containing LunexStealer, which bypassed UAC and security controls. The malware installed LUNARAXE browser extension for credential theft and NAIVEMESS for file system access. Command and control used smart contracts on blockchain networks for domain resolution. The attack enabled comprehensive data exfiltration including credentials, browser data, and file system access with potential business disruption.

Kill Chain Progression

This analysis maps confirmed threat intelligence to the full cloud kill chain to show where defensive gaps would emerge as an attack progresses.
Impact

Comprehensive credential theft, browser takeover capabilities, and file system access enabled threat actors to potentially cause business disruption and further compromise organizational assets.
Potential Compliance Exposure

Mapping incident impact across multiple compliance frameworks.

PCI DSS 4.0 – Software Security Framework

Control ID: 6.2.3- Compromised websites hosting payment processing functions could expose cardholder data through malicious JavaScript injection and credential harvesting capabilities of LunexStealer.

NYDFS 23 NYCRR 500 – Cybersecurity Program - Multi-Factor Authentication

Control ID: 500.02(g)- Browser credential theft and session hijacking capabilities bypass authentication controls, compromising secure access to financial systems and customer data.

DORA – ICT Risk Management Framework

Control ID: Article 8- Third-party website compromises demonstrate inadequate supplier risk management and ICT resilience controls for digital operational continuity.

CISA ZTMM 2.0 – Centralized Identity Management

Control ID: Identity – Advanced - Credential harvesting and browser session manipulation undermine identity verification and centralized access control principles in zero trust architecture.

NIS2 Directive – Cybersecurity Risk Management Measures

Control ID: Article 21(2)(a)- Mass website compromise campaign affects essential service availability and demonstrates insufficient incident response and business continuity measures.

GDPR – Security of Processing

Control ID: Article 32 -Personal data exposure through browser credential theft and file system access violates technical and organizational security measures for protecting personal data.

References:

- https://aviatrix.ai/threat-research-center/100-compromised-websites-fake-cloudflare-checks-lunexstealer-2026/

COLORTOKENS

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 2026 © ColorTokens. All rights reserved.