COLORTOKENS

THREAT INTELLIGENCE BRIEF #29

ColorTokens Threat Advisory

September 30, 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-2026-55040

Microsoft SharePoint Server Security Feature Bypass Vulnerability

9.1 CRITICAL CVSS

Weak authentication in Microsoft Office SharePoint allows an unauthorized attacker to bypass a security feature over a network.

AFFECTED VERSIONS

affected

affected from 16.0.0before 16.0.5561.1001

Vendor: Microsoft

Product: Microsoft SharePoint Server 2019

Platforms: x64-based Systems

affected from 16.0.0before 16.0.10417.20175

Vendor: Microsoft

Product: Microsoft SharePoint Server Subscription Edition

Platforms: x64-based Systems

Versions 1 affected from 16.0.0 before 16.0.19725.20434

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55040

Refrence

https://cwe.mitre.org/data/definitions/1390.html

https://www.cve.org/CVERecord?id=CVE-2026-55040

CVE-2026-94127

BIG-IP APM OAuth vulnerability

9.8 CRITICAL
CVSS

When a BIG-IP APM access policy and an OAuth profile are configured on a virtual server, specific malicious traffic can lead to remote code execution (RCE). This vulnerability is only present when BIG-IP APM is configured as an OAuth Authorization Server. Deployments using APM strictly as an OAuth Client / Resource Server (without OAuth authorization server profiles configured) are not affected by this vulnerability. Impact: This vulnerability allows an unauthenticated attacker to perform remote code execution. The BIG-IP system in Appliance mode is also vulnerable. This is a data plane issue; there is no control plane exposure. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

AFFECTED VERSIONS

Vendor: F5

Product: BIG-IP

affected from 21.1.0
before Hotfix-BIGIP-21.1.0.2.0.30.22-ENG

affected from 17.5.0
before Hotfix-BIGIP-17.5.1.9.0.160.12-ENG

affected from 17.1.0
before Hotfix-BIGIP-17.1.3.5.0.41.14-ENG

PATCH DETAILS

https://my.f5.com/manage/s/article/K000162605

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-94127

https://cwe.mitre.org/data/definitions/122.html

CVE-2026-20079

Cisco Secure Firewall Management Center Authentication Bypass Remote Code Execution Vulnerability

10.0 CRITICAL CVSS

A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass authentication and execute script files on an affected device to obtain root access to the underlying operating system. This vulnerability is due to an improper system process that is created at boot time. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute a variety of scripts and commands that allow root access to the device.

AFFECTED VERSIONS

Vendor: Cisco

Product: Cisco Secure Firewall Management Center (FMC)

Versions 72 Total

affected

affected at

7.0.0, 7.0.0.1, 7.0.1, 7.1.0, 7.0.1.1, 7.0.0.1, 7.0.1
7.1.0, 7.0.1.1, 7.1.0.1

PATCH DETAILS

http://seclists.org/fulldisclosure/2026/Aug/80

http://seclists.org/fulldisclosure/2026/Aug/80

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-20079

CVE-2026-69676

Windows Kerberos Remote Code Execution Vulnerability

8.8 HIGH CVSS

Authentication bypass by capture-replay in Windows Kerberos allows an authorized 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 10.0.14393.9512

Vendor: Microsoft

Product: Windows 10 Version 1809

Platforms: 32-bit Systems, x64-based Systems

Versions 1 Total

affected from 10.0.17763.0before 10.0.17763.9245

Vendor: Microsoft

Product: Windows 10 Version 21H2

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

Versions 1 Total

affected from 10.0.19044.0 before 10.0.19044.7725

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69676

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-69676

CVE-2026-83941

Entra ID Elevation of Privilege Vulnerability

10.0 CRITICAL CVSS

Missing authorization in Entra ID allows an authorized attacker to elevate privileges over a network.

AFFECTED VERSIONS

Vendor: Microsoft

Product: Microsoft Entra

PATCH DETAILS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83941

https://cwe.mitre.org/data/definitidef/862.html

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-83941

CVE-2026-93616

Directory Traversal and File upload allows execution of arbitrary script on the Management Server

10.0 CRITICAL CVSS

A directory traversal and file upload vulnerability allows an unauthenticated attacker to upload and execute arbitrary scripts on Check Point Management Server.

AFFECTED VERSIONS

Vendor: checkpoint

Product: Quantum Security Management

Versions 11 Total

Default Status: unknown

affected

affectedat R82.20 with no Jumbo Hotfix

affectedat R82.10 with Jumbo Hotfix Take 44 or below

affectedat R82 with Jumbo Hotfix Take 126 or below

affectedat R81.20 with Jumbo Hotfix Take 166 or below

affectedat R81.10 (EOS) with Jumbo Hotfix Take 190 or below

affectedat R81 (EOS)

affectedat R80.40 (EOS)

affectedat R80.30 (EOS)

affectedat R80.20 (EOS)

affectedat R80.10 (EOS)

affectedat R80 (EOS)

PATCH DETAILS

https://support.checkpoint.com/results/sk/sk1000171

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-18885

CVE-2026-

An out-of-bounds write issue on Apple Products

9.9 CRITICAL CVSS

An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.7.1 and iPadOS 26.7.1, macOS Sequoia 15.8.1, macOS Tahoe 26.7.1. Processing a maliciously crafted file may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 27.

AFFECTED VERSIONS

Vendor: Apple

Product: iOS and iPadOS

Versions 1 Total

Default Status: unknown

affected

affected from 0before 26.7.1

Vendor: Apple

Product: macOS

Versions 2 Total

Default Status: unknown

affected

affectedfrom 0before 15.8.1

affectedfrom 0before 26.7.1

PATCH DETAILS

https://support.apple.com/en-us/149226

https://support.apple.com/en-us/149228

https://support.apple.com/en-us/149229

https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-86950

Refrence

https://www.cve.org/CVERecord?id=CVE-2026-86950

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

Labcorp Settles Multistate Data Breach Investigation for $2.3 Million

ATTACK SUMMERY

A coalition of 44 state attorneys general has agreed to settle a multistate investigation of Laboratory Corporation of America (Labcorp) regarding a 2019 data breach at its debt collection company, American Medical Collection Agency (AMCA). Labcorp has agreed to pay $2,287,455, which will be divided among the 44 states participating in the action.

AMCA is a subsidiary of the debt collection company Retrieval-Masters Creditors Bureau (RMCB) and provides small debt collection services to healthcare organizations, including laboratories and medical testing facilities. The hacking incident was identified by RMCB on March 19, 2029, and the forensic investigation determined that a hacker breached the AMCA network around 8 months before the intrusion was detected. The hacker had access to the network from August 1, 2018, until March 30, 2019, and exfiltrated sensitive data including names, personal information, Social Security numbers, financial information, medical test information, and diagnostic codes.

The AMCA data breach was the largest data breach reported in 2019 by a HIPAA-regulated entity, affecting more than 27.5 million individuals, including more than 10.2 million Labcorp patients. The high cost of remediation forced AMCA to file for bankruptcy protection. AMCA was also investigated by the coalition, led by the Indiana, Texas, Connecticut, and New York attorneys general, and received permission from the bankruptcy court to settle the multistate action, filing for dismissal of the bankruptcy on December 9, 2020.

The investigation of Burlington, NC-based Labcorp was led by the attorneys general of Connecticut, Florida, Indiana, Illinois, Michigan, and Texas and identified potential violations of the Health Insurance Portability and Accountability Act (HIPAA) and state consumer protection and breach notification laws. The Labcorp settlement includes a financial penalty and injunctive relief.

Labcorp must ensure that it does not misrepresent the extent to which it maintains and protects the privacy, security, and confidentiality of personal information (PI) and protected health information (PHI) and must implement a range of security measures, including but not limited to the following:

Review, revise, and update its information security program.

Employ an executive or officer as a CISO to oversee the implementation and maintenance of its information security program.

Provide security awareness training to all personnel who have access to or responsibility for PI and/or PHI.

Implement an incident response plan, which must include a plan for vendor security incidents.

Ensure procedures are implemented for reporting vendor security incidents internally to senior management.

Develop policies and procedures governing the collection, use, disclosure, and retention of PI and PHI, including specific policies and procedures for PI and PHI shared with debt collectors. Minimize the PI and PHI shared with debt collectors.

Develop, implement, and maintain a vendor risk management program; maintain a vendor risk management team; and use security assessment and management tools for vendor assessment and monitoring, with specific requirements for debt collectors.

Require all debt collectors to conduct risk assessments and contractually require debt collectors to conduct penetration tests of systems containing PI and PHI, and annual SOC 2 Type 2 audits.

Labcorp must also engage a third-party assessor to perform an information security assessment, with a focus on vendor risk management.

Labcorp was also named as a defendant in class action litigation against AMCA and other AMCA clients, and agreed to a $35,000,000 settlement earlier this year

References:

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

HEALTHCARE

zHealth Data Breach Affects 118,000 Individuals

ATTACK SUMMERY

A data breach at zHealth, a practice management and EHR software provider, has affected 118,000 individuals. Data breaches have also been announced by Bridgeway Benefit Technologies, Longview ER Operations, and HealthStream.

zHealth

zHealth, Inc., a San Francisco, California-based cloud-based practice management and electronic health records (EHR) software provider, has disclosed a cybersecurity incident that may have involved data being acquired by an unauthorized third party. According to the breach notice provided to the California Attorney General, zHealth became aware that certain information may have been copied on or around June 15, 2026. An investigation was launched, which confirmed that its network had been accessed by an unauthorized third party between January 20 and January 21, 2026. The review of the impacted data was completed on September 3, 2026.

The substitute breach notice on the zHealth website states that the impacted information varies from individual to individual and may include names, medical information, and health insurance information. The affected individuals have been offered single-bureau credit monitoring, credit report, and credit score services for 12 months. Data privacy and security policies and procedures have been reviewed and enhanced to prevent similar incidents in the future. The incident is not currently shown on the HHS' Office for Civil Rights website; however, the Oregon Attorney General has been informed that the data breach affected 118,563 individuals.

Bridgeway Benefit Technologies

Bridgeway Benefit Technologies, a Baltimore, Maryland-headquartered third-party health plan administrator that provides software for managing multiemployer health, welfare, and retirement benefits, has notified the HHS Office for Civil Rights about a breach of the protected health information of 9,268 individuals. The company explained that it experienced a cybersecurity incident involving an employee email account that exposed data provided to the company in connection with the administration services it provides to its clients. The unauthorized activity was identified on May 18, 2026, and the forensic investigation determined that the account was accessed between March 5, 2026, and May 19, 2026.

Bridgeway Benefit Technologies confirmed that the breach was limited to its own email system. No client systems were compromised in the incident. The exact types of data involved are detailed in the individual notification letters. Attorneys General have been notified that the compromised data includes Social Security numbers. Steps have been taken to improve security to prevent similar incidents in the future, and the affected individuals have been offered complimentary credit monitoring and identity theft protection services.

Longview ER Operations

Longview ER Operations, LLC, doing business as Hospitality Health ER, a full-service emergency room operator with facilities in Longview, Tyler, and Galveston, Texas, has experienced a cybersecurity incident that involved patient data. Suspicious network activity was identified on July 22, 2026. Immediate action was taken to secure its systems, and an investigation was launched to determine the nature and scope of the activity, with assistance provided by third-party cybersecurity professionals.

The facilities in Tyler and Galveston were unaffected. The number of affected individuals has not yet been determined. The incident has been reported to the HHS' Office for Civil Rights using an estimate of at least 501 individuals. The total will be updated when the review is completed.

HealthStream

HealthStream Inc., a Nashville, Tennessee-based healthcare technology company that provides software and training solutions for the healthcare industry, has notified the Massachusetts Attorney General about a recent security incident. The letter provides no information about the nature of the data breach, other than stating that some "information" was involved and complimentary credit monitoring and identity theft protection services have been offered for 24 months. "Due to requirements imposed by Massachusetts law, we are unable to provide you with the details about the nature of this incident," states the notification letter.

The notification letters appear to be about a cybersecurity incident reported to the U.S. Securities and Exchange Commission (SEC) on July 29, 2026. According to the Form 8-K filing, the incident involved unauthorized access to corporate file servers and does not appear to have involved protected health information. Data compromised in the incident included employee data, customer and vendor billing data, and legal information. Around 75 of its credentialing customers have been affected. HealthStream said no customer-facing systems were involved, there was no file encryption, operations were not disrupted, and the incident is unlikely to affect its financial position or results.

References:

- https://www.hipaajournal.com/xhealth-data-breach/

HEALTHCARE

American Addiction Centers & Oculus Pathology Disclose Hacking IncidentsImpacted

ATTACK SUMMERY

Two ransomware groups have claimed attacks on the home health care provider Interim Healthcare. Data breaches have been announced by Crystal Coast Pain Management, Golden State Orthopedics & Spine, Gardiner Family Chiropractic, and BestCare Treatment Services.

Interim HealthCare of Oklahoma City

Interim HealthCare, a home healthcare provider operating in 40 U.S. states, has been added to the data leak sites of two ransomware groups. The first listing was added to the Genesis ransomware group's data leak site on August 10, 2026. Genesis claimed to have exfiltrated data in the incident and threatened to publish it if the ransom was not paid. Genesis claims the stolen data relates to Interim Healthcare of Oklahoma and Tulsa, and that 1TB of data was exfiltrated, including medical records, healthcare data, personal data, patient lists, clinical data, and company data. While a list of the compromised files was added to the data leak site, the data allegedly stolen has yet to be published.

Then on August 21, 2026, a second ransomware group listed Interim HealthCare as one of its victims. Anubis claims to have exfiltrated 530 GB of data in the attack, including "financial information about franchisees, details of internal and external audits, discussions of operational issues, as well as memoranda covering all kinds of day-to-day business matters." Samples of the stolen data were added to the listing, and the stolen data has been published, indicating the ransom was not paid.

Crystal Coast Pain Management

Crystal Coast Pain Management in North Carolina, a division of East Carolina Anesthesia Associates ECAA), has started notifying patients that some of their personal and protected health information was obtained by an unauthorized third party in a cybersecurity incident earlier this year.

Suspicious network activity was identified on or around January 11, 2026, and third-party digital forensics and cybersecurity experts were engaged to investigate the activity. On April 20, 2026, it was determined that files containing patient information had been copied by the attackers. The file review was completed on June 24, 2026, when it was confirmed that the stolen data included first and last names, dates of birth, medical information, and Social Security numbers.

The cybersecurity experts confirmed the security of its network; however, as a precaution, all affected systems were wiped and rebuilt, and additional security measures have been implemented. No evidence has been found to indicate any misuse of the affected data, but as a precaution, the affected individuals have been offered single-bureau credit monitoring, credit report, and credit score services. A ransomware group called Devman 2.0 claimed it was behind the attack.

Golden State Orthopaedics & Spine

Golden State Orthopaedics & Spine (GSOS), an orthopaedics practice with 13 locations in the San Francisco Bay Area in California, has announced a recent cybersecurity incident. Suspicious network activity was identified on July 2, 2026, and a third-party team of forensics experts was engaged to assist with the investigation and determine the nature and scope of the activity.

GSOS confirmed that its network had been accessed by an unauthorized third party, who may have viewed or obtained files containing patient information. The data review confirmed that the exposed data included first and last names, addresses, dates of birth, Social Security numbers, health insurance information, and medical diagnosis information.

The review of the affected data is ongoing, and the number of affected individuals has yet to be disclosed. GSOS is reviewing its data security policies, procedures, and practices and is taking steps to prevent similar incidents in the future. This appears to have been a ransomware or data theft and extortion incident. A ransomware group called Brain Cipher claimed responsibility for the attack, in which it alleged that 150 GB of data was stolen.

Gardiner Family Chiropractic

Gardiner Family Chiropractic, a chiropractic clinic in Gardiner, Maine, has notified the HHS' Office for Civil Rights about a network server hacking incident that has affected up to 5,000 patients. Suspicious activity was identified within its computer network on July 17, 2026. An investigation was launched, which confirmed unauthorized network access and the exposure of patient data. Data potentially compromised in the incident includes names, contact information, birth dates, health information, and health insurance/Medicaid information.

According to the substitute breach notice, this was a ransomware attack involving file encryption and data theft. A ransom demand was received; however, the attack was blocked, and the ransom was not paid. The Interlock ransomware group claimed responsibility for the attack. Gardiner Family Chiropractic has taken several steps in response to the attack to strengthen security. In addition to wiping the affected devices and purchasing new computers for its employees, security policies, procedures, and practices have been reviewed, additional security measures have been implemented, and special training has been provided to its workforce on ransomware.

BestCare Treatment Services

BestCare Treatment Services, Inc., an Oregon-based behavioral healthcare provider, has experienced a data security incident involving unauthorized access to parts of its network containing patient information. Unauthorized network activity was identified on June 15, 2026, and a third-party cybersecurity firm was engaged to assist with the investigation and confirm the security of its network.

The investigation confirmed that files had been exposed containing names, dates of birth, contact information, demographic information, medical information, and other patient identifying information. Notification letters were mailed to the affected individuals on August 10, 2026. The data breach was recently reported to the HHS Office for Civil Rights as affecting 4,216 individuals.

References:

- https://www.hipaajournal.com/interim-healthcare-ransomware/

TECH

DoD Social Security Numbers breached in with four million Defense

ATTACK SUMMERY

A data breach affecting civilians is bad enough, but a DoD data breach carries an entirely different level of concern. For military personnel, their SSN is more than just a number; it's intrinsically linked to their service records, their benefits, their security clearances, and in some cases, even their deployment information. The potential implications extend far beyond mere financial fraud. Think about it: an adversary with access to such detailed personal information could potentially use it for blackmail, targeted phishing attacks, or even to compromise individuals in positions of national security importance. This isn't just about losing money; it's about potentially undermining the very fabric of national defense.

Furthermore, military families often operate with unique financial structures, including allotments, specific benefits, and sometimes a spouse deployed overseas. The complexity of managing these finances can make them particularly vulnerable to sophisticated identity theft schemes. A compromised SSN could disrupt paychecks, divert benefits, or create a cascade of financial headaches that are exponentially harder to resolve when one is stationed abroad or dealing with the demands of active duty. The trust placed in the DoD to protect this information is absolute, and when that trust is broken, the fallout is significant.

What exactly happened in this DoD data breach

An estimated four million U.S. Defense Department personnel had their sensitive personal data, including Social Security Numbers (SSNs), compromised by unauthorized users. This means their SSNs and other highly confidential information were accessed by malicious actors.

Furthermore, military families often operate with unique financial structures, including allotments, specific benefits, and sometimes a spouse deployed overseas. The complexity of managing these finances can make them particularly vulnerable to sophisticated identity theft schemes. A compromised SSN could disrupt paychecks, divert benefits, or create a cascade of financial headaches that are exponentially harder to resolve when one is stationed abroad or dealing with the demands of active duty. The trust placed in the DoD to protect this information is absolute, and when that trust is broken, the fallout is significant.

A2: Specific discovery details are often classified for national security reasons. However, official breach notification letters began to be mailed to affected individuals around September 23, 2026. This staggered notification is standard practice but can cause anxiety among those waiting to hear.

DoD data breach severity

While any data breach is serious, a DoD data breach carries unique national security implications. Beyond financial fraud, compromised military data (like SSNs linked to service records or security clearances) could be used for espionage, blackmail, targeted attacks on personnel, or to undermine national defense. Military families also face unique financial vulnerabilities. (See: Data privacy and security.)

Specific personal information compromised
The primary piece of information confirmed to be compromised is the Social Security Number (SSN). However, breach notifications often mention “other sensitive personal information,” which could include names, addresses, dates of birth, and potentially other details that facilitate identity theft.

DoD actions to prevent future breaches

While specific measures are often classified, the DoD typically responds to major breaches by reviewing and enhancing cybersecurity protocols, investing in IT modernization, implementing advanced threat detection, increasing cybersecurity training, and adopting frameworks like zero-trust architectures and multi-factor authentication. Accountability for security failures is also a focus.

References:

- https://www.thetechedvocate.org/dod-social-security-numbers-breached-in-september-2026-approximately-four-million-defense-department-personnel-may-be-affected-r-airforce/

SECTION 3

OT/IoT Security Breaches

OT & IOT

Japan's Keio confirms ransomware attack disrupted business systems

ATTACK SUMMERY

Keio Corporation (Keio), a major private railway operator in Japan, said its network was hit by a ransomware attack over the weekend, disrupting some of its business systems.

Following a system failure in the early hours of Saturday, the company confirmed the attack and shut down its network to prevent additional damage.

The company said it is investigating the extent of the impact and whether the attackers accessed any customer or business partner information.

Keio is a large Japanese railway operator with 85 km of track and 69 stations, as well as a separate hospitality business of 25 hotels. The company has over 2,200 employees and a reported annual revenue of about $2.6 billion.

"In the early hours of September 26, 2026, we confirmed a ransomware attack on our group's servers. We have reported the incident to the police and are conducting an investigation into the attack's route and damage with the cooperation of external experts," Keio says.

The incident appears to have affected only the hospitality side of Keio's business, not train operations.

A separate announcement published on the company's Keio Plaza Hotel Tokyo website is warning of possible delays on some customer-facing services.

Local media outlets have reported that the cyberattack disrupted the firm's payment systems. At the time of writing, Bleeping Computer could not find a ransomware group claiming the attack on Keio. Bleeping Computer has contacted the company to request more information about the incident, and we will update this post with their response once it reaches us.

Tokyo Metro has also disclosed a cyber incident over the weekend in which attackers gained unauthorized access to its systems and accessed 59,000-member email addresses.

Although both Keio and Tokyo Metro are Japanese railway operators, it is unclear if the organizations were targeted in a coordinated campaign by the same threat actor.

References:

- https://www.bleepingcomputer.com/news/security/japans-keio-confirms-ransomware-attack-disrupted-business-systems/

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.