

## Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : bc4b1182

Oct 03, 2025, 06:14 AM



### Today's Headlines:

#### Leading Story

- Clop Extortion Emails Claim Theft of Oracle E-Business Suite Data

#### Data Breaches & Data Leaks

- Red Hat Data Breach - Threat Actors Claim Breach of 28K Private GitHub Repositories
- US Air Force Probes SharePoint Breach by Chinese Threat Actors, Sparking Security Overhaul

#### Cyber Crimes & Incidents

- New DNS Malware Detour Dog Delivers Strela Stealer Using DNS TXT Records

#### Vulnerabilities & Exploits

- PoC Exploit Released for VMware Workstation Guest-To-Host Escape Vulnerability
- Chrome Security Update – Patch for 21 Vulnerabilities that Allow Threat Actors to Crash Browser

#### Trends & Reports

- NIST Publishes Guide for Protecting ICS Against USB-Borne Threats

## Privacy, Legal & Regulatory

- US Shutdown Halts IT Security Projects, Boosts Cyber Vulnerability

## Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – October 28, 2025, 12:00-01:00 PM ET
  - European – October 29, 2025, 03:00-04:00 PM CET
- [European Summit](#) – Rome, Italy – October 14-16, 2025
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

## Additional Information

### Leading Story

#### [Clop Extortion Emails Claim Theft of Oracle E-Business Suite Data](#)

### Summary

- Mandiant and GTIG researchers have revealed a new malicious campaign, seemingly from the Clop ransomware group, that claims to have stolen sensitive Oracle E-Business Suite data from victims.

### Analysis & Action

Mandiant and Google Threat Intelligence Group (GTIG) researchers have identified a new extortion campaign allegedly orchestrated by Clop ransomware. The campaign claims to steal sensitive Oracle E-Business Suite data to lure victims.

According to Mandiant, the malicious activity began on September 29 and is characterized by extortion emails sent from compromised accounts, seemingly owned by threat group FIN11. The extortion emails listed contact information, including the same email addresses listed on Clop's data leak website, indicating that the threat actors might be working together. While there are no reports of stolen data from the Oracle accounts, Mandiant and GTIG advise targeted individuals to review their E-Business Suite environments for potential compromise.

Health-ISAC recommends that its members avoid interacting with suspicious emails, educate staff on social engineering techniques, and actively review account and network logs for suspicious activity that may indicate compromise.

## Data Breaches & Data Leaks

### [Red Hat Data Breach - Threat Actors Claim Breach of 28K Private GitHub Repositories](#)

#### **Summary**

- The Crimson Collective extortion group claims to have breached Red Hat's private GitHub repositories and stolen nearly 570 GB of data.

#### **Analysis & Action**

An extortion group dubbed Crimson Collective claims to have stolen nearly 570GB of compressed data from Red Hat's private GitHub repositories.

The compressed data was allegedly stolen from 28,000 internal repositories, referencing thousands of organizations including major banks, telecoms, airlines, and public-sector institutions. The stolen data includes CI/CD secrets, pipeline configuration files, VPN connection profiles, backup files, exported GitHub configuration templates, infrastructure blueprints, and inventories. Organizations heavily reliant on automated DevOps and Infrastructure-as-a-Code (IaC) paradigms have been warned of exposed credentials resulting in potential business risks. Red Hat has not yet released a public statement to confirm or deny the breach.

Health-ISAC advises its members to encrypt sensitive data, regularly audit systems, and limit data access through strong access controls as mitigations against data breaches and leaks.

### [US Air Force Probes SharePoint Breach by Chinese Threat Actors, Sparking Security Overhaul](#)

#### **Summary**

- The U.S. Air Force is investigating a recent cyber incident that may have exposed PII and PHI after threat actors breached the department's SharePoint instance.

#### **Analysis & Action**

The United States Air Force is investigating a recent breach of its SharePoint instance, which resulted in a service-wide shutdown and the potential leak of sensitive data.

Investigations reveal a potential link to a vulnerability exploit in July by Chinese-affiliated threat groups Linen Typhoon, Violet Typhoon, and Storm-2603. The threat actors are believed to have exploited authentication bypass techniques to breach the SharePoint

collaboration tool. While authorities have yet to confirm the extent of the breach, the incident may have exposed personally identifiable information (PII) and protected health information (PHI). The Air Force immediately shut down all SharePoint systems to prevent further compromise and conduct forensic analysis in partnership with Microsoft.

Health-ISAC recommends that its members encrypt all data, apply all software patches as they are made available, and strengthen user authentication protocols to mitigate potential data breaches.

## **Cyber Crimes & Incidents**

### [New DNS Malware Detour Dog Delivers Strela Stealer Using DNS TXT Records](#)

#### **Summary**

- Cybersecurity researchers are tracking a DNS-based campaign that exploits compromised websites and DNS TXT commands to execute remote code and deploy malware.

#### **Analysis & Action**

Security researchers are tracking a DNS-based malware campaign, Detour Dog, that leverages compromised websites to deliver the Strela Stealer malware.

Detour Dog has been active since August 2023, but has recently been seen targeting primarily European users. The campaign leverages Domain Name Systems (DNS) records to hide command-and-control channels and deliver the Strela malware. The compromised websites communicate with malicious and threat actor-controlled servers through server-side DNS queries to remain undetected. Through DNS TXT commands, the compromised site can be used for remote command execution and as a proxy server to download the malware.

Health-ISAC advises its members to implement DNS security and filtering solutions, actively monitor network activity, and deploy endpoint detection and response (EDR) solutions as mitigation measures.

## **Vulnerabilities & Exploits**

### [PoC Exploit Released for VMware Workstation Guest-To-Host Escape Vulnerability](#)

## Summary

- A critical vulnerability chain impacting VMware Workstation permits threat actors to execute arbitrary code on host operating systems.

## Analysis & Action

A severe vulnerability chain within VMware Workstation allows threat actors to escape guest virtual machines and execute arbitrary code on host operating systems.

Exploitation of the attack occurs in two stages, beginning by exploiting CVE-2023-20870 and CVE-2023-34044 together, leveraging a Use-After-Free (UAF) memory leak, allowing threat actors to leak memory pointers on the host. Afterwards, threat actors exploit a buffer overflow flaw tracked as CVE-2023-20869, triggering a stack-based overflow by sending malicious Service Discovery Protocol (SDP) packets to the guest VM. This permits the threat actors to hijack execution flows, executing custom payloads on the host's system. The chain of attack primarily impacts VMware Workstation versions 17.0.1 and earlier.

Health-ISAC advises its members to consider granting users and applications only the minimum permissions required per the principle of least privilege as mitigation against similar vulnerability exposures.

## [Chrome Security Update – Patch for 21 Vulnerabilities that Allow Threat Actors to Crash Browser](#)

### Summary

- The latest Chrome 141 release addresses 21 recently identified vulnerabilities, which, if exploited, could enable threat actors to execute arbitrary code, exfiltrate sensitive data, and crash the web browser.

### Analysis & Action

In the latest Chrome 141 release, Google has patched 21 identified vulnerabilities affecting Windows, Mac, and Linux platforms.

The update addresses several security flaws, including CVE-2025-11205. Considered the most critical, the vulnerability enables threat actors to execute arbitrary code that could crash the web browser. Another major patched vulnerability is CVE-2025-11206, which affects the video processing component of the web browser. Other medium-severity flaws were patched, such as some in Chrome's V8 JavaScript engine and others that could compromise user data through side-channel methods. Google's Big Sleep AI system identified several of the flaws.

Health-ISAC encourages its members to actively scan for system vulnerabilities, apply all available software patches, and consider automated vulnerability detection solutions to mitigate potential exploits.

## **Trends & Reports**

### [NIST Publishes Guide for Protecting ICS Against USB-Borne Threats](#)

#### **Summary**

- NIST has released a new guide to help organizations reduce risks associated with removable media devices in OT environments.

#### **Analysis & Action**

NIST has published its NIST Special Publication (SP) 1334 guide to aid organizations in reducing cybersecurity risks concerning removable media devices in operation technology (OT) environments.

The guide covers multiple forms of removable media, such as external hard drives and CD/DVD drives. However, it highlights USB flash drives, which are typically used within OT environments for firmware updates or data retrieval. Despite this, USB flash drives are also a frequent source of malware infections, warning of increasingly sophisticated threats targeting OT. If inserted, NIST warns that these infected USBs could spread to industrial control systems, disrupting operations and compromising safety.

It is recommended that organizations store devices in physically secure locations, ensuring they are inventoried and labeled. Additionally, organizations should consider performing data sanitization before disposing of devices to mitigate risks of removable media attacks.

## **Privacy, Legal & Regulatory**

### [US Shutdown Halts IT Security Projects, Boosts Cyber Vulnerabilities](#)

#### **Summary**

- Following the U.S. government shutdown, critical IT security projects and modernization efforts have been halted, leaving agencies vulnerable to growing threats.

## **Analysis & Action**

The U.S. government shutdown, which started on October 1 and was caused by politicians' disagreement over federal funding, has halted critical IT security projects and modernization efforts, leaving agencies vulnerable to growing cyberthreats.

Agencies impacted by the shutdown include the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). The government shutdown coincides with the expiration of the Cybersecurity Information Sharing Act 2015, which facilitates data-sharing between private and government sectors to combat cyber threats. As a resolution to the congressional action has yet to be made at the time of reports, agencies will have to utilize bare minimum defenses, as experts warn that each day of delay on the action increases risks.

Health-ISAC advises its members to ensure patch and vulnerability management continuity and to bolster internal monitoring and detection as mitigative strategies.

### **Health-ISAC Cyber Threat Level**

On September 18, 2025, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level to **Blue (Guarded)**. The Threat Level of **Blue (Guarded)** is due to threats from:

**NPM Worm Impact, QR Code Phishing, Typosquatting Campaigns, Remote IT Worker Fraud, and Job Posting Scams.**

**For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.**

**You must have Cyware Access to reach the Threat Advisory System document.  
Contact [membership@h-isac.org](mailto:membership@h-isac.org) for access to Cyware.**

## Report Source(s)

Health-ISAC

---

## Reference

[cybersecuritynews](#)  
[webpronews](#)  
[bleepingcomputer](#)  
[webpronews 1](#)  
[cybersecuritynews 1](#)  
[securityweek](#)  
[cybersecuritynews 2](#)  
[cybersecuritynews 3](#)

## Tags

VMware Workstation, Detour Dog Malware, Strela Stealer Malware, NIST, Clop ransomware, Data Breaches, Chrome

---

**TLP:WHITE:** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

### Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" [here](#).

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

### Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" [here](#).

### Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact [membership@h-isac.org](mailto:membership@h-isac.org) for access to Health-ISAC Threat Intelligence Portal (HTIP).

### For Questions or Comments:

Please email us at [toc@h-isac.org](mailto:toc@h-isac.org)