SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

October 2025 - VOL.1

The News

IN THE NEWS THIS WEEK

Red Hat OpenShift AI Flaw Exposes Hybrid Cloud Infrastructure to Full Takeover

A critical vulnerability has been uncovered in Red Hat OpenShift AI, a platform for managing GenAI models across hybrid cloud environments. The flaw, CVE-2025-10725, scores 9.9 on the CVSS scale and enables privilege escalation under specific conditions. Although Red Hat labels it "Important" rather than "Critical," the risk remains severe due to the potential for full infrastructure compromise.

An authenticated low-privileged user, such as a data scientist using Jupyter notebooks, could gain cluster administrator rights. This escalation threatens the confidentiality, integrity, and availability of the entire cluster. The root cause lies in an overly permissive ClusterRole that lets authenticated users create jobs in any namespace. Attackers can exploit this to run malicious jobs in privileged namespaces using high-privilege ServiceAccounts.

By exfiltrating tokens, they can pivot across accounts and eventually seize root access on master nodes. Affected versions include OpenShift AI 2.19, 2.21, and RHOAI. Initial mitigation advice involved revoking broad permissions and ClusterRoleBindings. However, Red Hat later admitted these measures fall short of its product security standards for usability and deployment. The flaw exposes all hosted applications to potential breach.

READ MORE

OTHER NEWS HIGHLIGHTS

New WireTap Attack Extracts Intel SGX ECDSA Key via DDR4 Memory-Bus Interposer

Artificial Intelligence ChatGPT Targeted in Server-Side Data Theft Attack

OpenSSL Vulnerabilities Allow Private Key Recovery, Code Execution, DoS Attacks

The News

TOP OF THE NEWS THIS WEEK

Clop extortion emails claim theft of Oracle E-Business Suite data

Mandiant and Google are investigating a new extortion campaign targeting executives with claims of stolen data from Oracle E-Business Suite systems. The campaign began around September 29, 2025, but the legitimacy of the data theft remains unverified. Emails are being sent from hundreds of compromised accounts, one linked to FIN11, a known ransomware group. The extortion messages, attributed to Clop, threaten to sell or leak stolen documents unless payment is made. Clop claims to have exploited a vulnerability in Oracle's software, though they've withheld technical details. Oracle responded by pointing to flaws patched in their July 2025 update and urged customers to apply it. Mandiant and GTIG advise affected organizations to check for signs of compromise. The email addresses used match those on Clop's leak site, suggesting a connection, but evidence of actual data theft is inconclusive. Clop portrays their actions as protective services, demanding payment to avoid reputational damage.
The group has a history of exploiting zero-day vulnerabilities in file transfer platforms. Their MOVEit Transfer breach in 2023 affected over 2,700 organizations globally. In 2024, they exploited Cleo file transfer zero-days in another major campaign. Clop, also known as TA505 and FIN11, began operations in 2019 with CryptoMix ransomware. They've evolved from encryption-based extortion to pure data theft. The U.S. State Department offers a $10 million reward for information linking Clop to foreign governments.

READ MORE

TOP RELATED ARTICLES

Adobe Analytics bug leaked customer tracking data to other tenants

Red Hat confirms security incident after hackers breach GitLab instance

Nearly 50,000 Cisco firewalls vulnerable to actively exploited flaws

Geo-Politics

NEWS FROM AROUND THE WORLD

Chinese APT ‘Phantom Taurus’ Targeting Organizations With Net-Star Malware

Phantom Taurus is a Chinese state-sponsored hacking group active in espionage since at least 2023. Though its tactics differ from typical Chinese APTs, shared infrastructure recently confirmed its origin.

The group targets high-value entities like foreign ministries and embassies, aligning with China’s strategic interests. Its operations are covert and persistent, enabling long-term access to sensitive systems.

Phantom Taurus employs unique malware families such as Specter, Ntospy, and Net-Star. It also uses familiar Chinese hacker tools like China Chopper and Impacket. Attacks have focused on email servers and databases across Africa, the Middle East, and Asia. In 2025, it introduced Net-Star, a .NET suite targeting IIS web servers. Net-Star includes three backdoors, notably IIServerCore, which is fileless and memory-resident. IIServerCore can execute payloads and relay results to its command-and-control server.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Breaches

SECURITY BREACHES THIS WEEK

430,000 Harrods Customer Records Exposed in Supply Chain Attack

Harrods has disclosed a cybersecurity breach affecting around 430,000 customers, stemming from a compromised third-party provider. The exposed data includes names, contact details, and internal marketing labels, though no financial or login credentials were leaked. Harrods emphasized the incident is unrelated to a previous attack in May by Scattered Spider. The breach may be linked to the broader Salesloft OAuth token compromise, which has impacted multiple firms via Salesforce integrations.

Attackers reportedly contacted Harrods directly, suggesting possible extortion attempts. The incident highlights growing risks in digital supply chains and the need for stronger vendor oversight. Harrods has alerted customers and authorities, stressing its internal systems remain secure.

The leaked data, while not overtly sensitive, could still enable phishing or impersonation. This breach joins a wave of recent UK retail cyberattacks, including those at Co-Op and M&S. Harrods continues to focus on containment, transparency, and customer protection.

READ MORE

OTHER SECURITY BREACHES

Ransomware On Collins Aerospace Halts Check-In At Major Airports

Data Breaches 1.2 Million Impacted by WestJet Data Breach

766,000 Impacted by Data Breach at Dealership Software Provider Motility

Red Hat Confirms GitLab Instance Hack, Data Theft

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-10725 - Critical Red Hat Kernel Privilege Escalation Vulnerability

CVSS SCORE 9.9

CVE-2025-10659 - Critical PHP Remote Code Execution Vulnerability

CVSS SCORE 9.3

LAST WEEKS RECAP

CVE-2025-20333 - Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability
CVSS Score: (9.9)

CVE-2025-26399 - SolarWinds unauthenticated AjaxProxy deserialization remote code execution vulnerability
CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

A total of 502 new victims were reported across various ransomware groups this Month.

TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 10% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 251 affected entities.

Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

TOP THREAT ACTORS

Qilin

Qilin is a ransomware-as-a-service operation linked to Russia, encrypting and stealing data for ransom. Active since October 2022, it has targeted organizations like The Big Issue and Yanfeng.

INC. Ransom

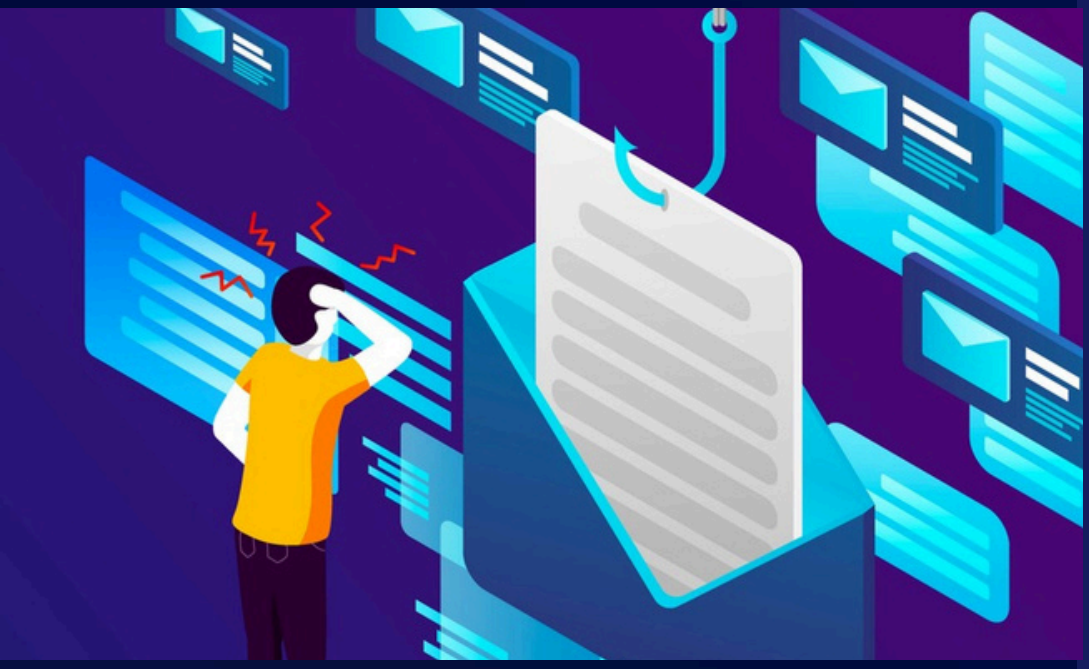
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

Play

Play ransomware was first observed around June of 2022. The ransomware family's name is derived from the .play extension added to files once they have been encrypted by the ransomware.

Phishing

PHISHING NEWS THIS WEEK



Extortion Emails Sent to Executives by Self-Proclaimed Clop Gang Member

A wave of extortion emails has targeted executives since September 29, with senders claiming ties to the Clop ransomware group. The attackers allege they've stolen sensitive data from Oracle's E-Business Suite, prompting investigations by Google's Threat Intelligence Group and Mandiant.

Charles Carmakal, CTO at Mandiant, confirmed the campaign is being launched from hundreds of compromised accounts. One such account has prior links to FIN11, a known ransomware and extortion group. The emails include contact details that match listings on Clop's data leak site, suggesting brand mimicry. However, researchers caution this doesn't confirm Clop's involvement.

Attribution in cybercrime remains complex, with threat actors often impersonating notorious groups to amplify pressure. Organizations are urged to investigate for signs of compromise. The case remains under active analysis, with no definitive link to Clop established yet.

READ MORE

OTHER PHISHING ARTICLES

Phishing Tops EU Threat Landscape, ENISA Report

Hackers Exploit Milesight Routers to Send Phishing SMS to European Users

Smishing Campaigns Exploit Cellular Routers to Target Belgium