SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

October 2025 - VOL.4

The News

IN THE NEWS THIS WEEK

JLR Hack UK's Costliest Ever, Hitting Economy with £1.9bn Loss

The cyber-attack on Jaguar Land Rover (JLR) in August 2025 has been declared the most economically damaging cyber event in UK history, according to the Cyber Monitoring Centre (CMC). In its October 22 report, the CMC estimated a financial impact of £1.9 billion ($2.55 billion), affecting over 5,000 UK organizations. The attack led to a shutdown of JLR's internal IT systems and halted production at major UK plants, disrupting its supply chain and dealership operations for weeks. The CMC classified the incident as a "Category 3 systemic event," citing widespread business interruption and recovery costs.

Experts warn the true cost may be far greater, especially if trade secrets were stolen and exploited by hostile nation states. Ilia Kolochenko of ImmuniWeb cautioned that long-term consequences could include competitive sabotage or even bankruptcy. The incident has reignited calls for stronger government oversight, with cybersecurity leaders urging proactive audits and higher compliance standards for companies of national importance. ESET's Jake Moore emphasized that boards must treat cybersecurity as a strategic risk on par with financial and operational threats, especially amid rising supply chain vulnerabilities.

READ MORE

OTHER NEWS HIGHLIGHTS

Lumma Stealer Vacuum Filled by Upgraded Vidar 2.0 Infostealer

Major Vulnerabilities Found in TP-Link VPN Routers

Lazarus Group's Operation DreamJob Targets European Defense Firms

The News

TOP OF THE NEWS THIS WEEK

Jira Vulnerability Lets Attackers Alter Files Accessible to the Jira JVM Process

Atlassian has disclosed a critical vulnerability in Jira Software Data Center and Server, tracked as CVE-2025-22167, that allows authenticated attackers to perform path traversal with arbitrary file write. With a CVSS v3.1 score of 8.7, this flaw poses a significant risk to system integrity, enabling attackers to overwrite files anywhere the Jira JVM process has write access. The vulnerability affects multiple Jira versions introduced in September 2025, specifically:

- 9.12.0 through 9.12.27
- 10.3.0 through 10.3.11
- 11.0.0 through 11.0.1

Atlassian discovered the issue internally and has released patches to mitigate the threat. Customers are strongly advised to upgrade to 9.12.28, 10.3.12, or 11.1.0, depending on their current version branch. For organizations unable to immediately deploy the latest release, these targeted upgrade paths offer a critical stopgap against potential exploitation.

The vulnerability requires network access and valid authentication, but its impact on confidentiality, integrity, and availability is rated high. In multi-tenant or shared environments, the risk is amplified, making this a priority issue for enterprise deployments. Atlassian's transparency in disclosure gives defenders a head start, but the nature of the flaw demands swift action.

READ MORE

TOP RELATED ARTICLES

Exploitation of Critical Adobe Commerce Flaw Puts Many eCommerce Sites at Risk

Lanscope Endpoint Manager Zero-Day Exploited in the Wild

Hackers Steal Microsoft Teams Chats & Emails by Grabbing Access Tokens

Geo-Politics

NEWS FROM AROUND THE WORLD

Iran-Linked MuddyWater Targets 100+ Organisations in Global Espionage Campaign

Iranian-linked threat group MuddyWater has launched a targeted cyber espionage campaign across the Middle East and North Africa, compromising over 100 government entities. Using a hijacked email account accessed via NordVPN, the attackers sent phishing emails disguised as diplomatic correspondence. These emails contained weaponized Word documents that deployed Phoenix v4, a backdoor capable of system reconnaissance, persistence, and file transfer, once users enabled macros.

The malware was delivered via a loader named FakeUpdate, which decrypted and executed the AES-encrypted payload.

Group-IB researchers linked Phoenix to BugSleep, a Python-based implant previously attributed to MuddyWater, which is believed to operate under Iran's Ministry of Intelligence.

The campaign's infrastructure also hosted remote monitoring tools and a custom credential stealer targeting major browsers, blending custom malware with legitimate software like PDQ and Action1. This hybrid approach highlights MuddyWater's evolving tactics and its focus on stealthy, long-term intelligence gathering.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Ukraine Aid Groups Targeted Through Fake Zoom Meetings and Weaponized PDF Files

North Korean Hackers Lure Defense Engineers With Fake Jobs to Steal Drone Secrets

Chinese Threat Actors Exploit ToolShell SharePoint Flaw Weeks After Microsoft's July Patch

Breaches

SECURITY BREACHES THIS WEEK

Volkswagen Allegedly Hacked in Ransomware Attack as 8Base Claims Data Leak

Volkswagen Group is investigating claims by the 8Base ransomware gang, which alleges it exfiltrated sensitive data from the automaker. While Volkswagen confirmed its core IT systems remain unaffected, the company acknowledged the possibility of a breach via a third-party supplier.
The stolen data, listed on 8Base's dark web portal, reportedly includes financial records, employee contracts, and confidentiality agreements. Although no public leak occurred by the group's stated deadline, the incident raises concerns about supply chain vulnerabilities and regulatory exposure under GDPR.

8Base, linked to the Phobos ransomware family, is known for double-extortion tactics and previously targeted smaller businesses. Despite a Europol-led takedown in early 2025, experts warn that affiliates may continue operations under new identities.
With Volkswagen's global footprint and high-profile brands like Audi and Porsche, the potential impact is significant.

The case underscores the growing threat of third-party breaches and the need for continuous monitoring and risk management across enterprise ecosystems.

READ MORE

OTHER SECURITY BREACHES

Fencing and Pet Company Jewett-Cameron Hit by Ransomware

Data Breaches Hackers Steal Sensitive Data From Auction House Sotheby's

Prosper Data Breach Impacts 17.6 Million Accounts

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-61932 - Lanscope Endpoint Manager Remote Code Execution via Improper Request Origin Verification vulnerability

CVSS SCORE 9.8

CVE-2025-22167 - Jira Software Data Center Path Traversal (Arbitrary Write) vulnerability

CVSS SCORE 8.7

LAST WEEKS RECAP

CVE-2025-61882 - Oracle Critical Remote Code Execution Vulnerability Exploited in the wild
CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

A total of 185 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

The Technology sector was the primary focus, representing 13.3% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 108 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

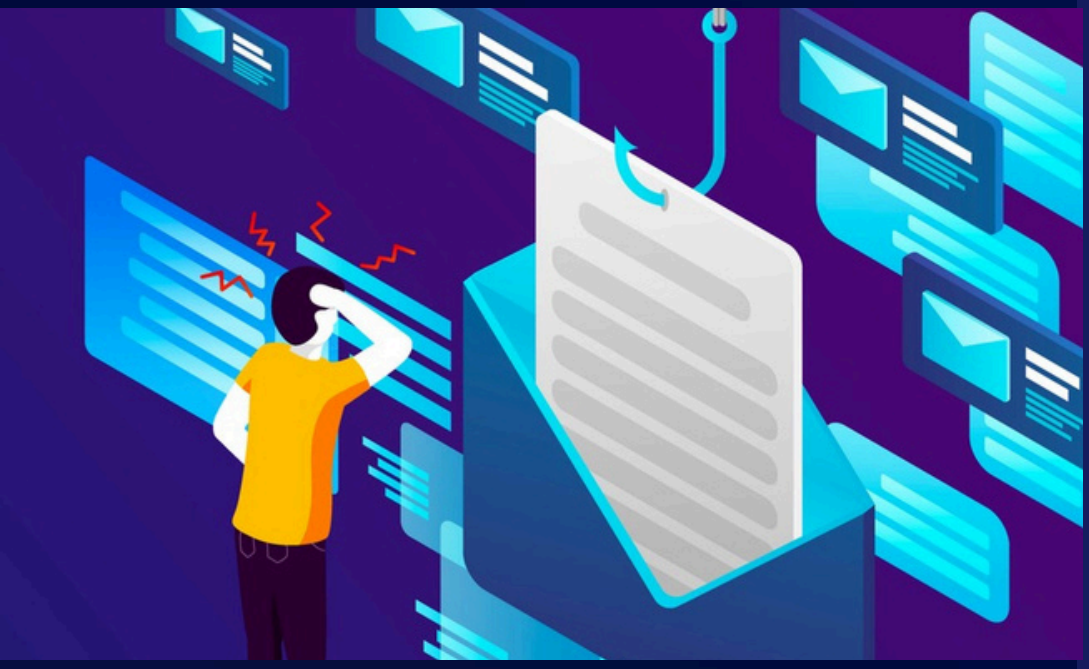
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



MuddyWater Uses Compromised Mailboxes in Global Phishing Campaign

A newly uncovered phishing campaign attributed to Iran-linked threat actor MuddyWater has targeted international organizations across multiple regions, aiming to collect foreign intelligence.

The attackers accessed compromised email accounts via NordVPN and sent phishing emails disguised as legitimate correspondence. These emails contained malicious Word documents that prompted recipients to enable macros, triggering embedded Visual Basic code that deployed Phoenix v4—a backdoor granting remote control over infected systems. Group-IB emphasized that the operation exploited trusted communication channels to bypass defenses and infiltrate high-value targets.

Phoenix v4 introduced enhanced persistence and system reconnaissance features, connecting to a command-and-control server hosted under screenai[.]online. Investigators also discovered the use of legitimate remote monitoring tools (PDQ, Action1, ScreenConnect) and a custom credential stealer named Chromium_Stealer, which harvested browser login data while posing as a calculator app. The infrastructure was briefly active in August 2025 and linked to NameCheap servers. Group-IB tied the campaign to MuddyWater through overlapping code and targeting patterns, warning that similar operations are likely to continue.

Recommended defenses include disabling Office macros, deploying EDR tools, conducting phishing simulations, and monitoring for indicators tied to Phoenix and related domains.

READ MORE

OTHER PHISHING ARTICLES

New Phishing Wave Uses OAuth Prompts to Take Over Microsoft Accounts

Cybercriminals Impersonate Aid Agencies to Lure Victims with Fake Financial Offers

Global SMS Phishing Campaign Traced to China Targets Users Worldwide