SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

September 2025 - VOL.4

The News

IN THE NEWS THIS WEEK

Co-op Records £206m Revenue Loss Following Cyber-Attack

The Co-op has reported a £206m ($277m) revenue loss following a cyber-attack in April 2025, which forced the temporary shutdown of key systems. In its H1 financial report, the UK retailer revealed total losses of £80m ($107m) for the six-month period ending July 5, with further sales impact expected in H2. While a one-off cost of £20m ($27m) was recorded, it's unclear if this relates directly to the incident.

CEO Shirine Khoury-Haq praised the company's resilience in maintaining essential services like funerals and rural food supply during the disruption. She emphasized the need for structural changes, especially in the food division, and announced a partnership with The Hacking Games to address youth disenfranchisement—a factor she linked to rising cyber threats.

The attack has been attributed to the Scattered Spider group, part of The Com criminal network, and coincided with similar breaches at Marks & Spencer and Harrods. UK authorities have arrested four suspects, including three teenagers, in connection with the incidents. M&S reported even greater losses of £300m ($403m) and confirmed its attack involved ransomware, though it declined to disclose if a ransom was paid.

During a Parliamentary hearing, Co-op's general counsel Dominic Kendal-Ward confirmed that member data—names, addresses, and birthdates—was accessed but limited in scope. The events have prompted renewed calls for organizations to strengthen defenses against evolving Scattered Spider tactics.

READ MORE

OTHER NEWS HIGHLIGHTS

Experts Warn of Global Breach Risk from Indian Suppliers

NCA Arrest Man as HardBit Ransomware Blamed for Airport Outages

Attacker Breakout Time Falls to 18 Minutes

The News

TOP OF THE NEWS THIS WEEK

Urgent: Cisco ASA Zero-Day Duo Under Attack; CISA Triggers Emergency Mitigation Directive

Cisco has issued an urgent call for customers to patch two actively exploited zero-day vulnerabilities affecting its Secure Firewall ASA and FTD software. The flaws—CVE-2025-20333 and CVE-2025-20362—allow attackers to execute remote code or bypass authentication via crafted HTTP requests. One requires valid VPN credentials, while the other can be exploited without authentication. Cisco confirmed attempted exploitation but has not disclosed the scope or attribution.

The vulnerabilities are suspected to be chained together to gain privileged access and execute malicious code. Cisco credited multiple national cybersecurity agencies, including those from Australia, Canada, the UK, and the U.S., for assisting in the investigation. In response, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive ED 25-03, mandating federal agencies to mitigate the risks within 24 hours. Both flaws have been added to CISA's Known Exploited Vulnerabilities catalog.

CISA linked the campaign to a sophisticated threat cluster known as ArcaneDoor, attributed to actor UAT4356 (aka Storm-1849). This group has previously targeted perimeter devices from multiple vendors to deploy malware like Line Runner and Line Dancer. The attackers have demonstrated the ability to modify ASA ROM to persist across reboots and upgrades, posing a serious threat to network integrity.

READ MORE

TOP RELATED ARTICLES

Salesforce Patches Critical ForcedLeak Bug Exposing CRM Data via AI Prompt Injection

Hackers Exploit Pandoc CVE-2025-51591 to Target AWS IMDS and Steal EC2 IAM Credentials

SolarWinds Releases Hotfix for Critical CVE-2025-26399 Remote Code Execution Flaw

Geo-Politics

NEWS FROM AROUND THE WORLD

Chinese Hackers RedNovember Target Global Governments Using Pantegana and Cobalt Strike

A global cyber espionage campaign previously tracked as TAG-100 has now been identified as a Chinese state-sponsored threat actor named RedNovember, also known as Storm-2077 by Microsoft. Between June 2024 and July 2025, RedNovember targeted perimeter appliances of high-profile organizations worldwide, using tools like the Go-based backdoor Pantegana, Spark RAT, and Cobalt Strike. Their victims span government and private sectors, including defense, aerospace, law firms, and space agencies, with confirmed breaches in the U.S., Europe, Africa, and Southeast Asia.

The group exploits known vulnerabilities in internet-facing devices from vendors like Check Point, Cisco, Citrix, Fortinet, and Palo Alto Networks to gain initial access. Their tactics include leveraging open-source tools and VPN services such as ExpressVPN and Warp VPN to obscure attribution and maintain persistence. Recent targets include Ivanti Connect Secure appliances linked to U.S.-based media and military contractors, and Outlook Web Access portals of a South American country ahead of a diplomatic visit to China.

RedNovember's activity reflects broad intelligence-gathering goals and a growing trend among Chinese threat actors to compromise security infrastructure like VPNs, firewalls, and email servers. Their operations have concentrated on regions including the U.S., Panama, Taiwan, South Korea, Southeast Asia, and South America, indicating shifting priorities and evolving espionage objectives.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Breaches

SECURITY BREACHES THIS WEEK

Boyd Gaming discloses data breach after suffering a cyberattack

28 properties across ten states, has disclosed a cyberattack in a recent SEC Form 8-K filing. The breach allowed threat actors to infiltrate its systems and steal sensitive data, including employee information and details about a limited number of other individuals. Despite the incident, Boyd Gaming confirmed that its operations remain unaffected and it does not expect any material financial impact, thanks in part to its cybersecurity insurance policy.

The company, which employs over 16,000 people and reported $3.9 billion in revenue for 2024, responded swiftly by engaging external cybersecurity experts and notifying law enforcement. It is also in the process of informing affected individuals and relevant regulatory bodies. The stolen data was confirmed to have been removed from Boyd's IT systems, though the full scope of the breach remains unclear.

As of now, no ransomware group or threat actor has claimed responsibility for the attack, and Boyd Gaming has not issued further public statements. The incident underscores the growing risks faced by large entertainment and hospitality firms, especially those handling vast amounts of personal and financial data.

READ MORE

OTHER SECURITY BREACHES

CISA says hackers breached federal agency using GeoServer exploit

Chinese Hackers Use 'BRICKSTORM' Backdoor to Breach US Firms

Vulnerabilities

VULNERABILITIES & EXPLOITS

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

LAST WEEKS RECAP

CVE-2025-10585 - Chrome Type Confusion 0-Day vulnerability
CVSS Score: (8.8)

CVE-2025-21043 - Samsung Mobile libimagecodec.quram.so Out-of-Bounds Write Remote Code Execution Vulnerability
CVSS Score: (8.8)

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

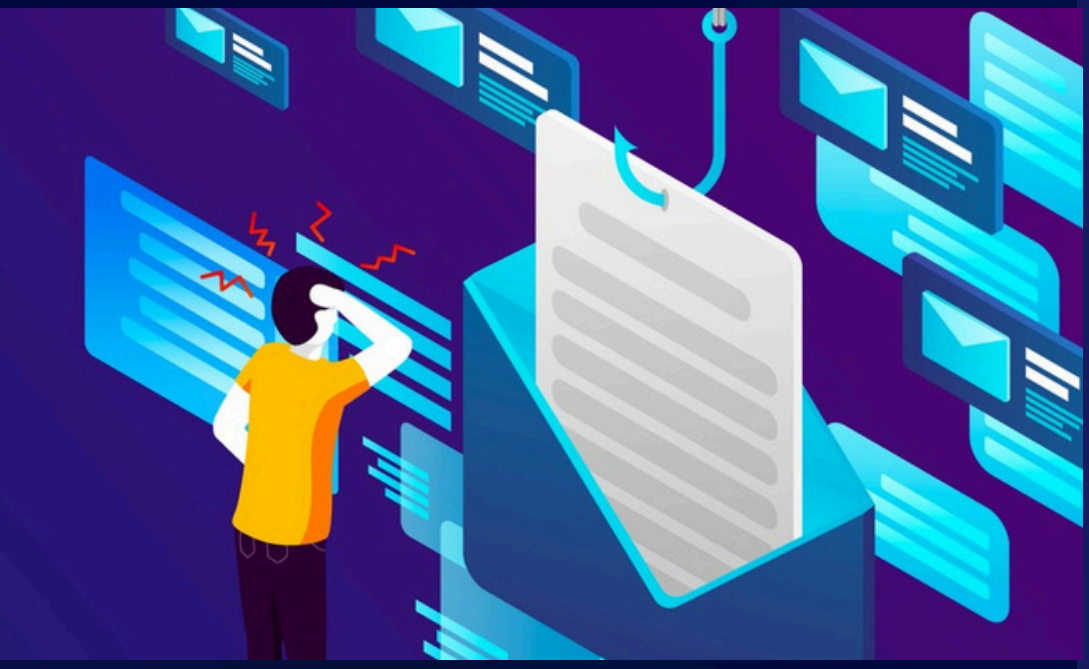
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



Deepfake Attacks Hit Two-Thirds of Businesses

Nearly two-thirds of organizations faced deepfake attacks in the past year, often involving impersonation through video or audio calls or biometric spoofing. These attacks are increasingly paired with social engineering, making them harder to detect and more dangerous. Akif Khan from Gartner emphasizes that employees are now the frontline defense, as automated tools alone aren't enough. He suggests integrating deepfake detection into platforms like Zoom and Teams, though large-scale deployments are still rare.

Some companies are using deepfake simulations in training to raise awareness. Strengthening payment authorization workflows with phishing-resistant MFA is also advised. Meanwhile, 32% of organizations reported attacks on AI applications, mainly via prompt injection.

Although not the top threat, 5% experienced major incidents, signaling a growing concern. Khan recommends managing shadow AI and tightening access controls to mitigate these risks.

READ MORE

OTHER PHISHING ARTICLES

Phishing Campaign Evolves into PureRAT Deployment, Linked to Vietnamese Threat Actors

Attackers Abuse AI Tools to Generate Fake CAPTCHAs in Phishing Attacks

Malicious AI Agent Server Reportedly Steals Emails