SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JULY 2025 - VOL.1

The News

IN THE NEWS THIS WEEK

Hawaiian Airlines Hacked as Aviation Sector Warned of Scattered Spider Attack

Hawaiian Airlines confirmed a cybersecurity incident as authorities warned of rising Scattered Spider attacks on aviation and transportation. The FBI, Mandiant, and Palo Alto Networks urged airlines to watch for social engineering tactics and report breaches quickly. Scattered Spider typically infiltrates systems via trusted vendors and identity infrastructure, prompting calls to tighten MFA and verification protocols. Sources suspect the group may be behind the WestJet breach, while American Airlines also reported tech issues that could be linked. Experts recommend proactive hardening of help desks and identity platforms to counter these coordinated cyber threats.

READ MORE

Cisco Warns of Hardcoded Credentials in Enterprise Software

Cisco has issued a critical security patch for its Unified CM and Unified CM SME platforms to fix a root-level vulnerability (CVE-2025-20309) caused by default development credentials. The flaw allows attackers to execute arbitrary commands with full privileges, affecting Engineering Special versions 15.0.1.13010-1 through 15.0.1.13017-1. The company has released a patch and will roll out a permanent fix in version 15SU3 later this month. Admins are advised to check system logs for root access indicators in /var/log/active/syslog/secure, although no active exploitation has been reported.

READ MORE

OTHER NEWS HIGHLIGHTS

Attackers Impersonate Top Brands in Callback Phishing

Over 40 Malicious Firefox Extensions Target Cryptocurrency Wallets, Stealing User Assets

Chinese Hackers Exploit Ivanti CSA Zero-Days in Attacks on French Government, Telecoms

The News

TOP OF THE NEWS THIS WEEK

Scattered Spider hackers shift focus to aviation, transportation firms

Scattered Spider threat actors have shifted their attacks to aviation and transportation firms, after previously targeting retail and insurance companies. Recent victims include WestJet and potentially Hawaiian Airlines, with tactics involving MFA resets and help desk manipulation to gain unauthorized access. Security experts from Palo Alto Networks and Mandiant warn that these actors use social engineering and target identity systems to breach networks. Scattered Spider is not one group but a loosely connected set of threat actors using shared tactics, some of whom collaborate with Russian ransomware gangs. Past targets include major firms like MGM, Twilio, Coinbase, and Reddit, prompting cybersecurity teams to urgently strengthen identity verification and MFA protocols.

Researchers recommend limiting help desk permissions, securing password reset tools, and monitoring critical infrastructure to counter these attacks. The group typically operates via hacker forums and real-time planning on Telegram or Discord, with motives ranging from financial fraud to data extortion. The campaign against transportation firms marks a dangerous evolution in their strategy, suggesting broader industry risk. Google and Palo Alto have released defensive guides to counteract these advanced attack patterns. Companies are advised to audit their identity systems and prepare for highly targeted and persistent threat activity.

READ MORE

TOP RELATED ARTICLES

Google fixes fourth actively exploited Chrome zero-day of 2025

Over 1,200 Citrix servers unpatched against critical auth bypass flaw

International Criminal Court hit by new 'sophisticated' cyberattack

Geo-Politics

NEWS FROM AROUND THE WORLD

Spain arrests hackers who targeted politicians and journalists

Spanish police arrested two individuals in Las Palmas linked to cyberattacks targeting government officials and journalists. Authorities labeled them a national security threat, citing data leaks aimed at boosting the value of stolen info sold online. Investigators discovered personal data tied to politicians and media figures circulating across social media. One suspect focused on stealing data while the other handled sales, credentials, and cryptocurrency payments. Electronic devices were seized during house raids, possibly revealing buyers and accomplices. This continues

Spain's recent streak of cybercriminal arrests, including hackers targeting defense agencies and global firms. Notably, past operations took down members of the Scattered Spider group and Kelvin Security, tied to hundreds of attacks. The latest case shows growing sophistication in financially motivated cybercrime with political implications. Officials stress vigilance against threats exploiting digital platforms for widespread data exposure. Further investigations may uncover deeper networks behind the breaches and help bolster national cybersecurity.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

US disrupts North Korean IT worker "laptop farm" scheme in 16 states

Russia's throttling of Cloudflare makes sites inaccessible

U.S. warns of Iranian cyber threats on critical infrastructure

Breaches

SECURITY BREACHES THIS WEEK

Switzerland says government data stolen in ransomware attack

Switzerland has reported a ransomware attack on Radix, a federal contractor, which led to the theft and leak of sensitive government-related data on the dark web. The attack was carried out by the Sarcoma group, known for exploiting vulnerabilities through phishing and lateral network movement. Authorities, including the National Cyber Security Centre, are assessing the damage and identifying affected agencies. While over 1.3TB of data was posted online, Radix claims that no partner organizations' sensitive data has been confirmed as compromised. Impacted individuals have been notified.

READ MORE

FBI: Cybercriminals steal health data posing as fraud investigators

The FBI has warned that cybercriminals are impersonating health fraud investigators to steal personal and medical data via emails and texts disguised as official communications. These phishing attempts target both patients and healthcare providers, pressuring victims to reveal sensitive information or repay fabricated charges. The FBI urges caution, recommending strong passwords, Multi-Factor Authentication, and direct verification with health insurers before sharing any personal details. Imposter scams cost Americans nearly $3 billion in 2024, while broader cybercrime led to losses of $16.6 billion.

READ MORE

OTHER SECURITY BREACHES

Kelly Benefits says 2024 data breach impacts 550,000 customers

Esse Health says recent data breach affects over 263,000 patients

Qantas discloses cyberattack amid Scattered Spider aviation breaches

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-6554 - Type confusion in V8 in Google Chrome

CVSS SCORE 8.1

CVE-2025-6543 - Memory overflow vulnerability leading to unintended control flow and Denial of Service in NetScaler ADC and NetScaler Gateway

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2025-49113 - Critical Roundcube Webmail Remote Code Execution Vulnerability
CVSS Score: (9.9)

CVE-2025-20282- Cisco ISE API Unauthenticated Remote Code Execution Vulnerability
CVSS Score: (10)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

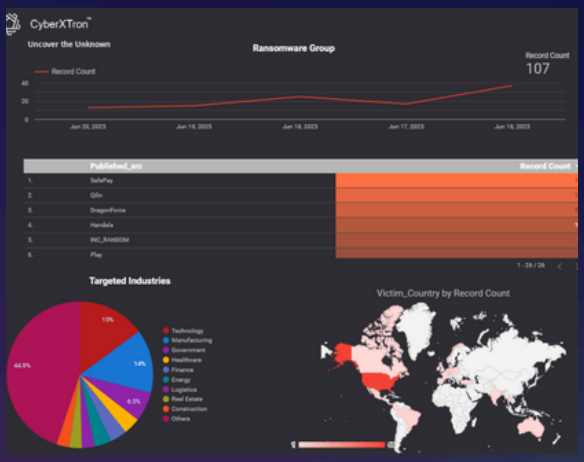
A total of 107 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

The Technology sector was the primary focus, representing 15% of all victims.

TARGET COUNTRY

The USA had the highest number of victims, with 66 in total.



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

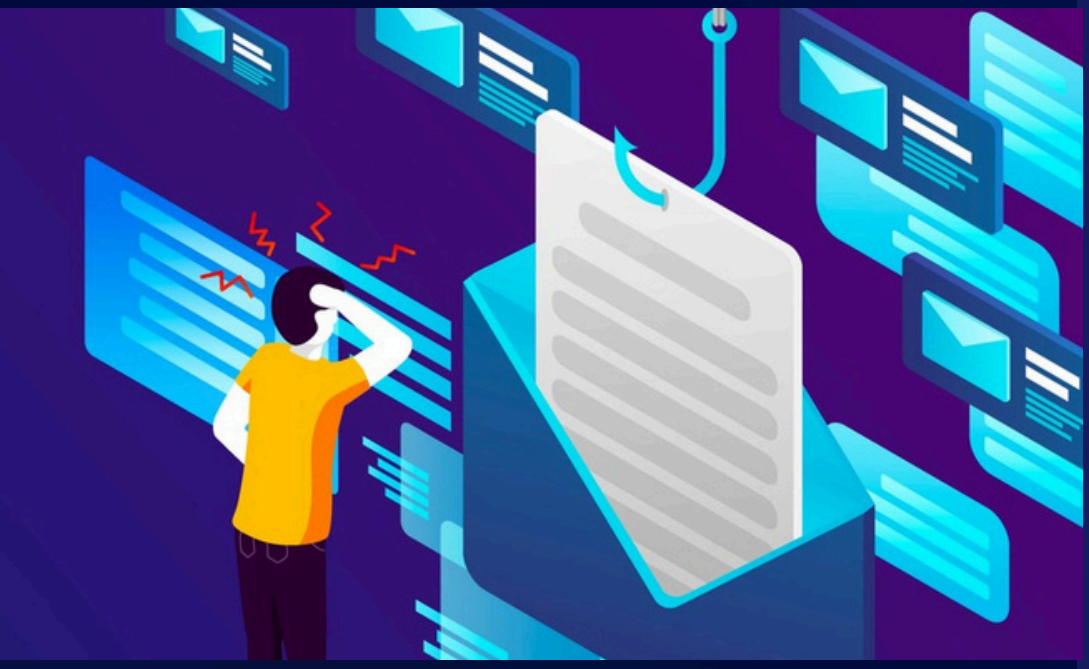
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



Hackers Using PDFs to Impersonate Microsoft, DocuSign, and More in Callback Phishing Campaigns

Phishing campaigns are increasingly exploiting trusted brands like Microsoft, DocuSign, PayPal, and NortonLifeLock to lure victims into Telephone-Oriented Attack Delivery (TOAD) schemes, where emails with PDF attachments persuade recipients to call adversary-operated numbers. These calls are designed to appear like legitimate customer support interactions, with attackers using call center scripts, spoofed IDs, and hold music to steal sensitive information or install malware.

Many PDFs also contain QR codes and hidden annotations linking to credential-harvesting pages disguised as Microsoft 365 or Dropbox. Cisco Talos researchers highlight how VoIP numbers help attackers remain anonymous and execute multi-stage scams. A newer threat uses Microsoft's Direct Send email feature to impersonate internal users and bypass authentication, targeting dozens of organizations.

These attacks combine social engineering, urgency, and brand spoofing, broadening their reach through tactics that blur the lines between phishing, tech support fraud, and business email compromise.

READ MORE

OTHER PHISHING ARTICLES

Vercel's v0 AI Tool Weaponized by Cybercriminals to Rapidly Create Fake Login Pages at Scale

Massive Android Fraud Operations Uncovered: IconAds, Kaleidoscope, SMS Malware, NFC Scams