SCC | DIGITAL

THREAT PULSE

> Amateurs hack systems;
> professionals hack people
> - Bruce Schneier

THREATS

NEWS

PHISHING

MAY 2025 - VOL.2

The News

IN THE NEWS THIS WEEK

Cisco fixed a critical flaw in its IOS XE Wireless Controller

Cisco patched a critical vulnerability (CVE-2025-20188) in its IOS XE Wireless Controller that could allow unauthenticated remote attackers to upload arbitrary files and execute commands with root privileges.

The flaw stems from a hard-coded JSON Web Token (JWT) and is exploitable via crafted HTTPS requests to the AP image download interface but is disabled by default. Cisco advises disabling the affected feature until the fix is applied, and no active exploitation has been observed in the wild.

READ MORE >

UK Cyber Essentials Certification Numbers Falling Short

The UK government acknowledges that Cyber Essentials certification uptake is insufficient, with only 35,000 organizations certified out of 5.5 million businesses. Despite this, reports confirm Cyber Essentials effectively strengthens security. To boost adoption, compliance is required for some government contracts, and funding expansion is being considered. Efforts are underway to make Cyber Essentials more accessible, particularly for small businesses. The scheme offers two certification levels Cyber Essentials and Cyber Essentials Plus both focused on fundamental security controls.

READ MORE >

OTHER NEWS HIGHLIGHTS

Hacker Finds New Technique to Bypass SentinelOne EDR Solution

Cyber-Attacks Have Doubled, UK’s NCSC Reports

Canary Exploit tool allows to find servers affected by Apache Parquet flaw

The News

TOP OF THE NEWS THIS WEEK

Hacking Spree Hits UK Retail Giants

The DragonForce ransomware group orchestrated cyberattacks on UK retailers Co-op, Harrods, and Marks & Spencer, disrupting operations. Marks & Spencer suspended online purchases, while Harrods restricted internet access to mitigate the threat. Co-op confirmed customer data was stolen, including names and contact details but not financial information.

The UK National Cyber Security Centre (NCSC) urged organizations to strengthen cybersecurity measures. DragonForce, initially a hacktivist group, now focuses on financial extortion using phishing emails and known vulnerabilities.

The group employs tools like Cobalt Strike and mimikatz for reconnaissance and ransomware delivery. It exploits vulnerabilities in Apache Log4j2, Windows, and Ivanti VPNs to gain access.

DragonForce ransomware was built using leaked LockBit and Conti code, targeting various operating systems. The group recently launched a "ransomware cartel" branding service to expand its cybercrime ecosystem. SentinelOne warns of its rising influence in the crimeware landscape.

READ MORE >

TOP RELATED ARTICLES

LockBit's Dark Web Domains Hacked, Internal Data and Wallets Leaked

ClickFunnels Investigates Breach After Hackers Leak Business Data

Android fixes 47 vulnerabilities, including one zero-day

Geo-Politics

NEWS FROM AROUND THE WORLD

Russian state-linked Coldriver spies add new malware to operation

Google researchers identified Lostkeys, a new malware used by Coldriver, a Russian state-backed espionage group. Coldriver, also known as Star Blizzard, UNC4057, and Callisto, typically relies on phishing to spy on diplomats, military personnel, and journalists from NATO countries.

Lostkeys steals files and system information and is deployed selectively via a fake CAPTCHA page to bypass email security. Coldriver has operated since 2022, and its previous malware, Spica, was used for targeted document theft. The group has also targeted human rights organizations and independent media in Eastern Europe and the U.S.

READ MORE >

Pakistani Firm Shipped Fentanyl Analogs, Scams to US

The Texas-based firm eWorldTrade was charged with facilitating synthetic opioid distribution and linked to fraudulent operations involving trademarks, book publishing, and app development. Its founder, Azneem Bilwani, previously led Abtach Ltd., accused of trademark fraud before rebranding as Intersys Limited. Investigators connected the network to Axact, a Pakistani firm involved in diploma scams and extortion, with multiple individuals charged in a major money laundering case.

READ MORE >

HIGHLIGHTS FROM AROUND THE WORLD

Polish authorities arrested 4 people behind DDoS-for-hire platforms

Pro-Russia hacktivist group NoName057(16) is targeting Dutch organizations

Pro-Russia collective NoName057(16) launched a new wave of DDoS attacks on Italian sites

Breaches

SECURITY BREACHES THIS WEEK

VC giant Insight Partners confirms investor data stolen in breach

Insight Partners confirmed a data breach from a January 2025 cyberattack, exposing sensitive information from employees and limited partners. The attack, carried out through social engineering, lasted a single day without disrupting operations, but investigations are ongoing. Affected individuals are advised to change passwords, enable 2FA, and monitor financial activity, while the attackers remain unidentified.

READ MORE

LockBit ransomware gang hacked, victim negotiations exposed

The LockBit ransomware gang suffered a data breach, with its dark web affiliate panels defaced and replaced with a message linking to a MySQL database dump.
The leaked database contains details on bitcoin addresses, ransomware builds, victim negotiations, and affiliate accounts, with some plaintext passwords exposed. The attack's origin is unclear, but it resembles a recent breach of Everest ransomware’s site. LockBit, previously hit by Operation Cronos in 2024, has been struggling to maintain operations. This latest breach further damages its reputation in the cybercrime world.

READ MORE

OTHER SECURITY BREACHES

[Ascension discloses new data breach after third-party hacking incident]

[VeriSource now says February data breach impacts 4 million people]

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-49112- Out-of-Band Access Point (AP) Image Download feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs)

CVSS SCORE 10

CVE-2025-27007- Plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation

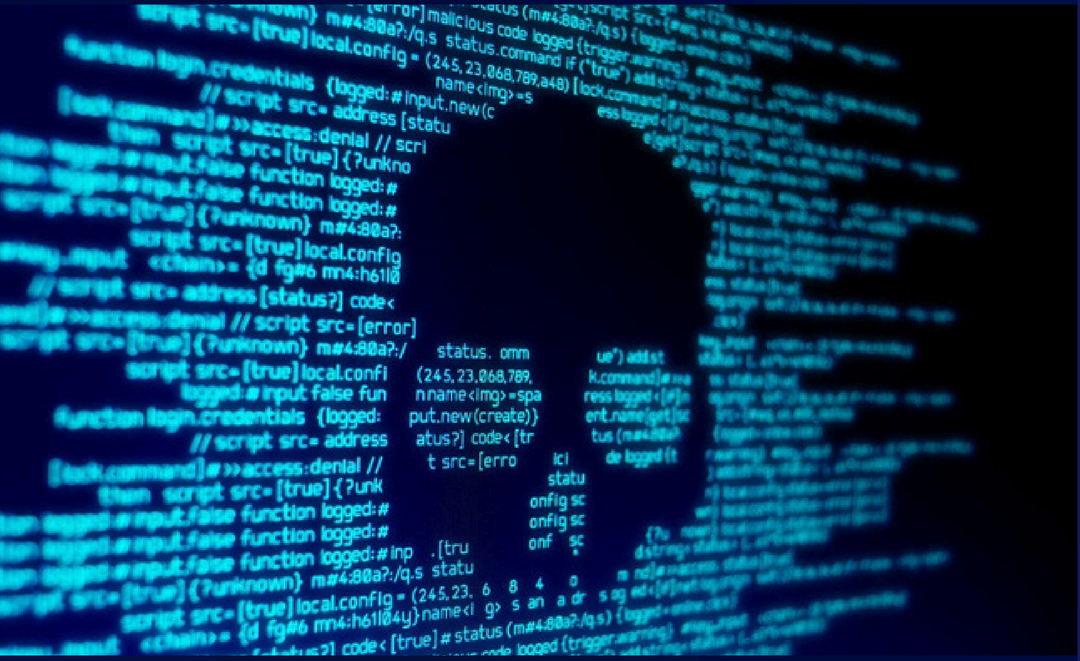
CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2025-34028 - Commvault Remote Code Execution
CVSS Score: (9.0)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS



OVERVIEW

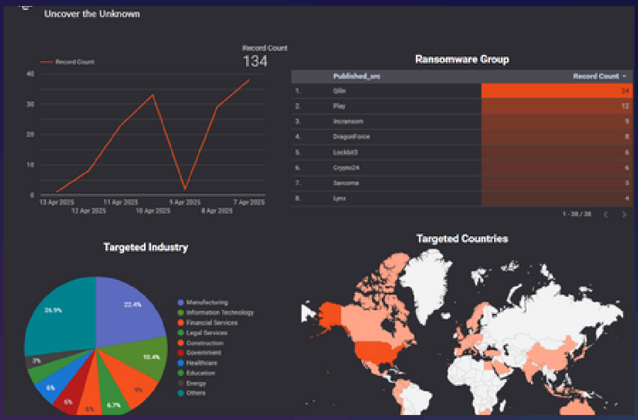
Last week we see Qilin claim the most ransomware victims targeting different sectors cumulating a total of 24 victims.

TARGET INDUSTRIES

Last week saw the most ransomware attacks against the Manufacturing industries followed by the Information Technology industry.

TARGET COUNTRY

The United States has consistently held the top position as the primary target.



	Published_src	Record Count ▾
1.	Qilin	24
2.	Play	12
3.	Incransom	9
4.	DragonForce	8
5.	Lockbit3	6
6.	Crypto24	6
7.	Sarcoma	5
8.	Lynx	4

Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

TOP THREAT ACTORS

RansomHub

RansomHub is a ransomware group that emerged in early 2024. They operate under the Ransomware-as-a-Service (RaaS) model, providing sophisticated ransomware tools to affiliates, including operators from rival groups like LockBit and ALPHV

Funksec

A relatively new ransomware group that emerged in late 2024. They operate under the Ransomware-as-a-Service (RaaS) model, providing their ransomware tools to affiliates. They have claimed 11 victims across various sectors, including media, IT, retail, education, automotive, professional services, and NGOs, in countries like the USA, Tunisia, India, France, Thailand, Peru, Jordan, and UAE.

Black Basta Ransomware Gang

Black Basta is a ransomware group that emerged in early 2022 and quickly became one of the most active Ransomware-as-a-Service (RaaS) threat actors. Black Basta is believed to have connections to the defunct Conti ransomware group, sharing similarities in their approach to malware development and operations

Phishing

PHISHING NEWS THIS WEEK

CoGUI Phish Kit Targets Japan with Millions of Messages

CoGUI is a phishing kit actively targeting Japanese organizations by impersonating well-known consumer and finance brands to steal credentials and payment data. It shares similarities with the Darcula kit, both used by Chinese-speaking threat actors, but employs advanced evasion techniques.

Proofpoint has created detections and Emerging Threats rules to combat CoGUI, aligning with Japan's Financial Services Agency reporting on phishing leading to financial theft.

The campaigns, observed since late 2024, are high-volume and primarily target Japan, although occasional attacks occur in other regions. Best practices include verifying URLs, avoiding urgent-click traps, and implementing strong authentication measures.

READ MORE >

OTHER PHISHING ARTICLES

Cyber criminals impersonate payroll, HR and benefits platforms to steal information and funds

NCSC warns of IT helpdesk impersonation trick being used by ransomware gangs after UK retailers attacked

Python InfoStealer with Embedded Phishing Webserver