SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JUNE 2025 - VOL.4

The News

IN THE NEWS THIS WEEK

Citrix Patches Critical Vulns in NetScaler ADC and Gateway

Citrix has patched a critical vulnerability, CVE-2025-5777, in NetScaler ADC and Gateway, which scored 9.3 on the CVSS scale and is similar to 2023's CitrixBleed. The flaw stems from insufficient input validation, allowing attackers to extract session tokens from device memory using crafted requests.
Although exploitation hasn't yet been observed, experts warn it's only a matter of time.
Citrix urges customers to upgrade to secure versions, especially since older builds like 12.1 and 13.0 are now end-of-life. Another flaw, CVE-2025-5349, was also patched. Admins are advised to kill all active sessions post-upgrade to ensure safety.

READ MORE

China-Nexus 'LapDogs' Network Thrives on Backdoored SOHO Devices

Researchers have uncovered a Chinese-linked ORB network dubbed "LapDogs," infecting over 1,000 SOHO devices across the U.S., Japan, Taiwan, and more for espionage purposes. The network uses a custom backdoor called ShortLeash and spoofed TLS certificates mimicking the LAPD to mask malicious traffic. Over half the infected devices were Ruckus Wireless access points, with others from major vendors like ASUS and Cisco. LapDogs highlights how ORB networks help threat actors evade detection, making compromised nodes potential entry points into broader internal systems.

READ MORE

OTHER NEWS HIGHLIGHTS

Supply Chain Incident Imperils Glasgow Council Services and Data

Jailbroken AIs are helping cybercriminals to hone their craft

Hawaiian Airlines discloses cyberattack, flights not affected

The News

TOP OF THE NEWS THIS WEEK

Cisco warns of max severity RCE flaws in Identity Services Engine

Cisco has issued a critical security advisory for two unauthenticated remote code execution (RCE) vulnerabilities in its Identity Services Engine (ISE) and Passive Identity Connector (ISE-PIC), tracked as CVE-2025-20281 and CVE-2025-20282. Both flaws are rated with a maximum CVSS score of 10.0, indicating their severity. CVE-2025-20281 affects ISE and ISE-PIC versions 3.3 and 3.4, allowing attackers to execute OS commands as root via a specially crafted API request due to insufficient input validation. CVE-2025-20282, affecting only ISE 3.4, enables remote attackers to upload and run arbitrary files in privileged directories because of poor internal API file validation. These vulnerabilities allow full remote system compromise without authentication or user interaction, posing a major risk to organizations using ISE for network access control and policy enforcement.

Cisco also disclosed CVE-2025-20264, a medium-severity authentication bypass flaw impacting all ISE versions up to 3.4. This bug involves improper enforcement of authorization for users authenticated via SAML SSO, which could let attackers modify system settings or initiate a system restart. While there's no known active exploitation of any of these vulnerabilities, Cisco strongly recommends urgent patching. Fixes for the RCE issues are available in ISE 3.3 Patch 6 and 3.4 Patch 2, and the authentication flaw is patched in 3.3 Patch 5 and 3.4 Patch 2. ISE versions 3.1 and earlier remain unsupported, and Cisco advises users to migrate to a supported version as soon as possible.

READ MORE

TOP RELATED ARTICLES

Microsoft nOAuth Flaw Still Exposes SaaS Apps Two Years After Discovery

UK Ransom Payments Double as Victims Fall Behind Global Peers

China-linked LapDogs Campaign Drops ShortLeash Backdoor with Fake Certs

Geo-Politics

NEWS FROM AROUND THE WORLD

Israeli cyber and computer science experts phished by Iran-linked APT42

Iranian state-sponsored hacking group APT42, also known as Charming Kitten or Mint Sandstorm, has launched a targeted phishing campaign against Israeli journalists, cybersecurity experts, and computer science professors. According to researchers at Tel Aviv-based Check Point, the group, which is linked to Iran's Islamic Revolutionary Guard Corps (IRGC), impersonated cybersecurity firm employees to trick victims into revealing email credentials and two-factor authentication codes. The attacks were delivered through email and WhatsApp, using realistic and AI-generated messages that initially contained no links to avoid suspicion. Once trust was established, the attackers sent phishing links disguised as Google Meet invites or Gmail login pages.

APT42 has a history of impersonating high-profile individuals to conduct espionage, including a previous incident where malware was sent under the pretense of a podcast invitation. Amid rising tensions between Iran and Israel, cybersecurity experts warn that such activity is likely to escalate, though a sharp uptick has not yet been observed. Iran's cyber operations often aim to collect intelligence and further political agendas, and may expand to affect infrastructure and supply chains.

The campaign is part of a broader Iranian strategy that also targets adversaries across Europe, as seen in a recent attack on government services in Albania's capital.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Russia-linked APT28 use Signal chats to target Ukraine official with malware

Africa Sees Surge in Cybercrime as Law Enforcement Struggles

Charming Kitten APT Tries Spying on Israeli Cybersecurity Experts

Breaches

SECURITY BREACHES THIS WEEK

184 million passwords leaked across Facebook, Google

A massive unprotected database containing over 184 million account credentials—including usernames, passwords, and emails for major platforms like Google, Apple, and Facebook—was discovered by cybersecurity researcher Jeremiah Fowler. The data, likely stolen by infostealer malware, was stored in plain text with no encryption or security. Some users confirmed their information in the file was real, raising serious privacy and security concerns. Though the database was taken offline, the incident highlights both cybercriminal threats and users' risky data storage habits.

READ MORE

McLaren Health Care says data breach impacts 743,000 patients

McLaren Health Care is notifying 743,000 patients of a data breach caused by a July 2024 ransomware attack attributed to the INC gang. Although the breach was discovered in August 2024, the forensic investigation wasn't completed until May 2025. The attackers had access to McLaren's systems for over two weeks, affecting both McLaren Health Care and the Karmanos Cancer Institute. While full names were confirmed exposed, the complete extent of compromised data remains unclear. This marks McLaren's second major breach in two years, following a 2023 ALPHV/BlackCat attack that leaked sensitive data from 2.2 million individuals.

READ MORE

OTHER SECURITY BREACHES

'Cyber Fattah' Hacktivist Group Leaks Saudi Games Data

Steel Giant Nucor Confirms Data Stolen in Cyberattack

Telecom Giant Viasat Is Latest Salt Typhoon Victim

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-49113 - Critical Roundcube Webmail Remote Code Execution Vulnerability

CVSS SCORE 9.9

CVE-2025-5419 - Google Chrome Out of bounds read and write in V8 Vulnerability

CVSS SCORE 8.8

CVE-2025-20281 - Cisco ISE API Unauthenticated Remote Code Execution Vulnerability

CVSS SCORE 9.8

CVE-2025-20282- Cisco ISE API Unauthenticated Remote Code Execution Vulnerability

CVSS SCORE 10

LAST WEEKS RECAP

CVE-2025-23121 - Critical remote code execution (RCE) vulnerability
CVSS Score: (9.9)

CVE-2025-6019 - Local Privilege Escalation (LPE) vulnerability in libblockdev
CVSS Score: (7.0)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

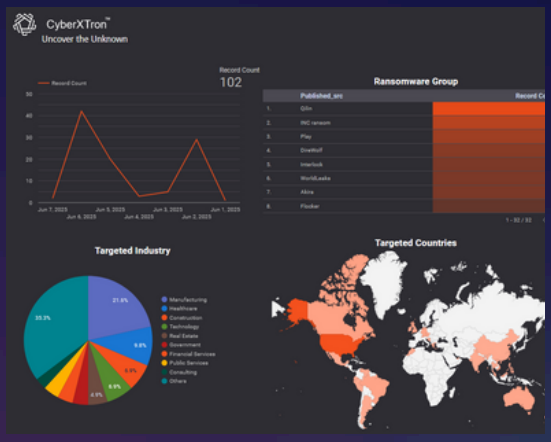
A total of 102 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 21.4% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 53 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

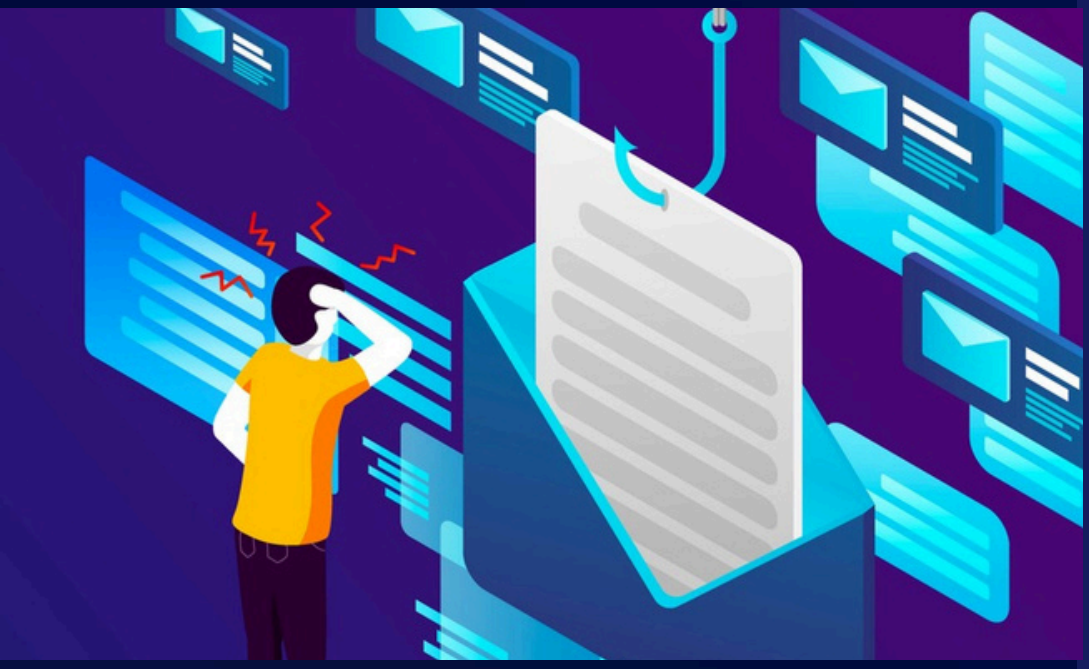
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



Trezor's support platform abused in crypto theft phishing attacks

Trezor has issued a warning about a phishing campaign exploiting its automated support system to send deceptive emails that appear to come from its official address. The system allows anyone to submit a support ticket using any email and subject line, which then triggers an automatic reply from help@trezor.io containing the submitted subject.

Attackers abuse this by crafting subjects with urgent phishing messages, tricking recipients into believing they're receiving legitimate alerts. These emails include links to phishing pages designed to steal users' wallet seed phrases—24-word keys that grant full access to cryptocurrency assets.

Victims who visit the fake sites are prompted to enter their seed, effectively handing over control of their wallets. Trezor, known for its secure hardware wallets, reminds users never to share their seed phrases and is working to strengthen defenses against such abuse. This attack echoes past incidents where Trezor's communication channels were exploited, including breaches involving MailChimp in 2022, impersonation campaigns in 2023, and a support site data breach in early 2024.
Trezor advises users to consult its online guide for protection against phishing threats.

READ MORE

OTHER PHISHING ARTICLES

UNC1151 exploiting Roundcube to steal user credentials in a spearphishing campaign

Ongoing Campaign Abuses Microsoft 365's Direct Send to Deliver Phishing Emails