SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

March 2025 - VOL.2

The News

IN THE NEWS THIS WEEK

Critical Patches Issued for Microsoft Products, March 11, 2025

Microsoft issued patches on March 11, 2025, to address multiple vulnerabilities, including those allowing remote code execution. Exploited vulnerabilities like CVE-2025-24983 highlight risks across various products, such as Windows, Office, Azure, and Edge. Successful attacks could enable unauthorized actions like installing programs or altering data, especially for users with administrative privileges. Affected systems include Windows Kernel, Visual Studio, and more.

READ MORE

iOS 18.3.2 Patches Actively Exploited WebKit Vulnerability

Apple has released iOS 18.3.2 and iPadOS 18.3.2 to address CVE-2025-24201, a critical WebKit vulnerability actively exploited by cybercriminals. This flaw allowed malicious web content to escape the Web Content sandbox, posing a severe security risk. Initially patched in iOS 17.2, a supplementary fix was necessary to fully mitigate the issue.
The vulnerability was used in targeted attacks before iOS 17.2, highlighting its sophistication.

READ MORE

OTHER NEWS HIGHLIGHTS

Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

Multiple Vulnerabilities in Mozilla Products Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

The News

TOP OF THE NEWS THIS WEEK

Ransomware Hits Record High: 126% Surge in Attacks in February 2025

February 2025 saw a record 126% surge in ransomware attacks, with Cl0p ransomware responsible for over a third of the incidents. Cl0p exploited vulnerabilities in file transfer software like MOVEit and Cleo, targeting edge network devices. Despite available patches, many organizations failed to update systems, leaving them vulnerable.

Other trends included FunkSec's new infostealer, Wolfer, which extracts sensitive data, and Black Basta's internal chats revealing deepfake use and operational insights. Ghost ransomware exploited older vulnerabilities, while Akira hijacked webcams to bypass security.

To combat these threats, experts recommend patching vulnerabilities, strengthening email security, and adopting zero-trust architectures. Developed nations remain prime targets due to reliance on connected devices and critical data.

READ MORE

TOP RELATED ARTICLES

Medusa ransomware hit over 300 critical infrastructure organizations until February 2025

Thousands of WordPress Websites Infected with Malware

Chinese Hackers Implant Backdoor Malware on Juniper Routers

Geo-Politics

NEWS FROM AROUND THE WORLD

North Korea-linked APT group ScarCruft spotted using new Android spyware KoSpy

The North Korea-linked APT group ScarCruft (APT37) has deployed a new Android spyware, KoSpy, targeting Korean and English-speaking users. Active since 2012, ScarCruft primarily targets government, defense, military, and media organizations in South Korea. KoSpy disguises itself as utility apps like "File Manager" and "Kakao Security," using Google Play Store and Firebase Firestore for distribution and configuration.

The spyware collects sensitive data, including SMS, calls, and location, and communicates with C2 servers for further exploitation. Researchers found links between KoSpy and North Korean groups APT37 and APT43, suggesting shared infrastructure and broader cyber-espionage operations.

READ MORE

China-linked APT UNC3886 targets EoL Juniper routers

China-linked APT group UNC3886 has been deploying custom backdoors on Juniper Networks' Junos OS MX routers, exploiting outdated hardware and software. These backdoors, based on TinyShell, include features for active and passive access and stealth, such as tampering with logs. UNC3886 bypassed Junos OS's Veriexec file integrity system by injecting malicious code into trusted processes

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Ukraine seeks to bolster offensive cyber capabilities amid rising threats from Russia

Ransomware attack takes down health system network in Micronesia

Two US Army soldiers charged with selling military secrets to China

Breaches

SECURITY BREACHES THIS WEEK

Kansas healthcare provider says more than 220,000 impacted by cyberattack

Sunflower Medical Group, a Kansas healthcare provider, suffered a cyberattack in December 2024, exposing sensitive information of nearly 221,000 patients. Data potentially leaked includes names, Social Security numbers, medical records, and health insurance details. Hackers infiltrated the system on December 15 and accessed files until January 7, 2025, when the breach was discovered.

The company hired a cybersecurity firm to investigate and offered affected individuals one year of credit monitoring. The Rhysida ransomware gang claimed responsibility, threatening to leak the data unless an $800,000 ransom was paid. Sunflower has not reported operational disruptions but did not disclose whether ransomware was used in the attack.

READ MORE

OTHER SECURITY BREACHES

Data breach at Japanese telecom giant NTT hits 18,000 companies

Rivers Casino Philadelphia reaching out to those impacted after data breach

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-26645 - Remote Desktop Client Remote Code Execution Vulnerability

CVSS SCORE 8.8

CVE-2025-24084 - Windows Subsystem for Linux (WSL2) Kernel Remote Code Execution Vulnerability

CVSS SCORE 8.4

CVE-2025-24035 - Windows Remote Desktop Services Remote Code Execution Vulnerability

CVSS SCORE 8.1

CVE-2025-24064 - Windows Domain Name Service Remote Code Execution Vulnerability

CVSS SCORE 7.8

LAST WEEKS RECAP

CVE-2025-25012 - Elastic Kibana Remote Arbitrary Code Execution Vulnerability

CVSS Score: (9.9)

CVE-2025-22224 - VMware ESXi and Workstation Heap-Overflow Vulnerability

CVSS Score: (9.3)

CVE-2025-22225 - VMware ESXi Arbitrary Write Vulnerability

CVSS Score: (8.2)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

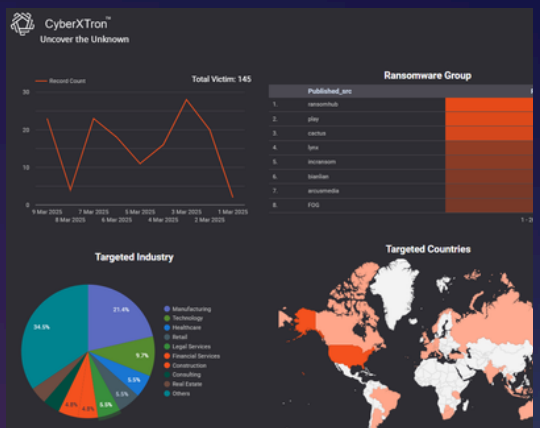
Last week we see Ransomhub claim the most ransomware victims targeting different sectors cumulating a total of 21 victims.

TARGET INDUSTRIES

Last week saw the most ransomware attacks against the manufacturing industries followed by the technology industry.

TARGET COUNTRY

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



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

Play

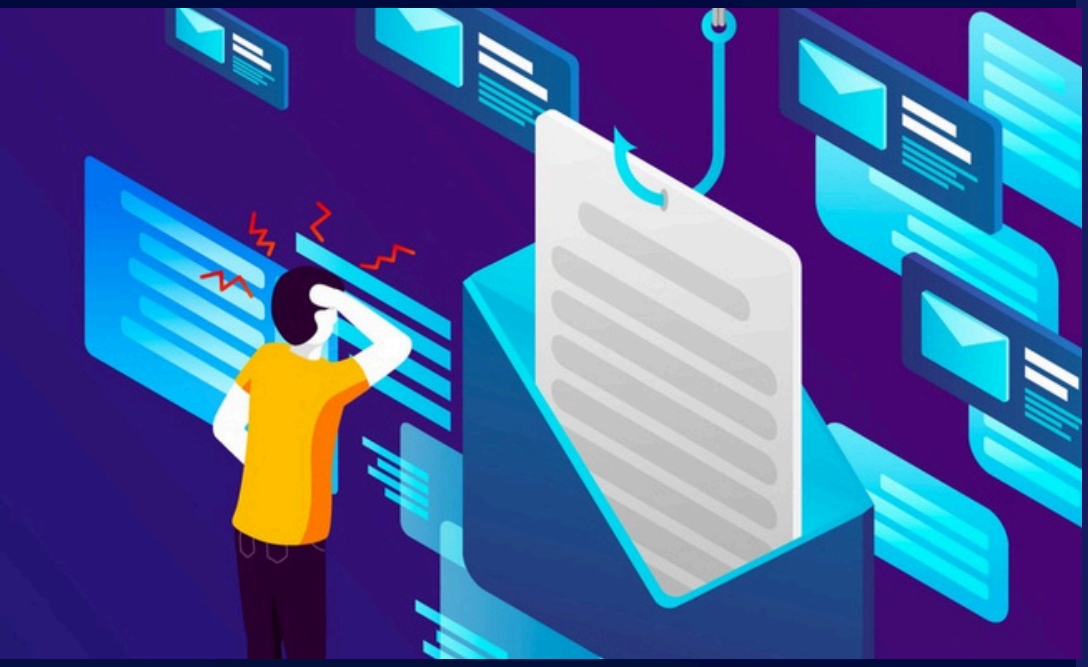
Play is a hacker group responsible for ransomware extortion attacks on companies and governmental institutions. The group emerged in 2022 and attacked targets in the United States, Brazil, Argentina, Germany, Belgium and Switzerland.

Cactus

Cactus is a ransomware-as-a-service (RaaS) group that encrypts victim's data and demands a ransom for a decryption key. Hundreds of organisations have found themselves the victim of Cactus since it was first discovered in March 2023, with their stolen data published on the dark web as an "incentive" to give in to the extortionists' demands.

Phishing

PHISHING NEWS THIS WEEK



'Microsoft Copilot Spoofing: A New Phishing Vector

Phishing campaigns have targeted users of Microsoft Copilot, a Generative AI assistant, by exploiting employee unfamiliarity with the new service. Attackers send spoofed emails resembling invoices, tricking recipients into clicking malicious links. These emails may appear legitimate, leveraging Microsoft branding, but include red flags like unofficial email addresses. Clicking the link directs users to a fake Microsoft Copilot welcome page, imitating a payment dashboard with a convincing layout.

The phishing scheme escalates to a fake login page, collecting credentials from unsuspecting users. One giveaway is the absence of features like "Forgot Password." A subsequent fake multi-factor authentication (MFA) page further misleads users, providing attackers time to exploit stolen data.

To combat such threats, organizations must educate employees on recognizing phishing attempts and provide clear communication about official services. Awareness and training are essential to fortify defenses against spoofing attacks in the workplace.

READ MORE

OTHER PHISHING ARTICLES

Cybercriminals are sending malicious emails to hospitality employees who are likely to work with Booking.com

New OBSCURE#BAT Malware Targets Users with Fake Captchas