SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

March 2025 - VOL.1

The News

IN THE NEWS THIS WEEK

Multiple vulnerabilities have been discovered in VMware ESXi, Workstation, and Fusion which could allow for local code execution.

Multiple vulnerabilities have been discovered in VMware ESXi, Workstation, and Fusion could allow for local code execution.
VMware ESXi, Workstation, and Fusion are all virtualization products that allow users to run virtual machines (VMs) on their computers.
Successful exploitation of these vulnerability could allow for local code execution in the context of the administrator account.
An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

READ MORE

LinkedIn InMail-Spoofing Email Delivers ConnectWise RAT

Cofense Phishing Defense Center identified a LinkedIn-spoofing malware campaign delivering ConnectWise RAT via fake LinkedIn InMail notifications. The campaign mimics older LinkedIn email templates to appear legitimate and creates urgency to prompt recipients to click on embedded links, installing the RAT. The email fails SPF and DKIM checks but bypasses security measures due to improper DMARC settings. The campaign has been active since at least May 2024.

READ MORE

OTHER NEWS HIGHLIGHTS

Over 4,000 ISP IPs Targeted in Brute-Force Attacks to Deploy Info Stealers and Cryptominers

Over 1,000 WordPress Sites Infected with JavaScript Backdoors Enabling Persistent Attacker Access

1 Million Third-Party Android Devices Have a Secret Backdoor for Scammers

Malicious Chrome extensions can spoof password managers in new attack

Mobile Phone SIM Swap Fraud

The News

TOP OF THE NEWS THIS WEEK

Tata Technologies Hit by Hunters International Ransomware, 1.4TB Data at Risk

Tata Technologies, a subsidiary of Tata Motors, was targeted by Hunters International ransomware group, who claim to have stolen 1.4TB of data. This attack follows a previous disclosure by Tata Motors about a ransomware incident.

Hunters International is demanding a ransom to avoid leaking the data. Speculation suggests Hunters International may be a rebranded Hive ransomware gang, previously disrupted by law enforcement. The situation remains unresolved, highlighting the ongoing threat of ransomware to large corporations.

The incident underscores the need for advanced cybersecurity and proactive threat intelligence. Camellia Chan of X-PHY emphasized the high ransom potential of industrial sectors and the importance of multi-layered defense strategies.

READ MORE

TOP RELATED ARTICLES

Malware Infects Linux and macOS via Typosquatted Go Packages

Chinese Silk Typhoon Group Targets IT Tools for Network Breaches

Trojaned AI Tool Leads to Disney Hack

Geo-Politics

NEWS FROM AROUND THE WORLD

The U.S. DoJ charges 12 Chinese nationals for state-linked cyber operations

The U.S. Department of Justice charged 12 Chinese nationals, including PRC security officers, employees of i-Soon, and members of APT27, for state-linked cyber operations. These individuals are accused of hacking targets worldwide under PRC orders, including U.S. agencies, critics, and Asian governments. The hackers exploited vulnerable systems for profit, selling stolen data to the PRC government.
The U.S. has issued indictments and rewards for information leading to their arrests. The case highlights the PRC's use of private firms and freelancers to obscure state involvement in cyber theft. The U.S. continues to combat these malicious cyber activities.

READ MORE

Russian crypto exchange Garantex's website taken down in apparent law enforcement operation

Russian cryptocurrency exchange Garantex was taken down by U.S. and European law enforcement agencies. The U.S. Secret Service seized the domain following a warrant from the U.S. Attorney's Office for the Eastern District of Virginia. Garantex was previously sanctioned by the U.S. Treasury in 2022 for its role in the Russian ransomware ecosystem.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Russia claims Ukraine hacked state youth organizations to recruit minors

Polish Space Agency POLSA disconnected its network following a cyberattack

Chinese Lotus Blossom APT targets multiple sectors with Sagerunex backdoor

Breaches

SECURITY BREACHES THIS WEEK

Millions of stalkerware users exposed again

Stalkerware apps, marketed as parental monitoring tools, enable secret spying on individuals' private lives, often used in domestic abuse situations. These apps are poorly coded and secured, leading to data breaches.

Stalkerware apps allow access to victims' data like messages, photos, and location. Researchers found a vulnerability in three stalkerware apps—Spyzie, Cocospy, and Spyic—that exposed data from victims' devices and millions of users' email addresses. The bug allowed access to 518,643 Spyzie customers, 1.81 million Cocospy customers, and 880,167 Spyic customers' email addresses. Details of the bug were withheld to prevent misuse.

Previous stalkerware apps like mSpy, pcTattleTale, and TheTruthSpy also faced significant security issues and data breaches. mSpy suffered multiple data breaches, while pcTattleTale uploaded victim screenshots to an unsecured server. TheTruthSpy exposed photos of children due to poor cybersecurity practices. The recurring vulnerability in stalkerware apps highlights the risks of using such tools and the potential for exposing both victims and users to significant privacy breaches.

READ MORE

OTHER SECURITY BREACHES

Thousands of public school workers impacted by cyberattack on retirement plan administrator

Vo1d Botnet's Peak Surpasses 1.59M Infected Android TVs, Spanning 226 Countries

The Qilin ransomware group claims responsibility for attacking the newspaper Lee Enterprises, stealing 350GB of data

Hunters International gang claims the theft of 1.4 TB of data allegedly stolen from Tata Technologies

Vulnerabilities

VULNERABILITIES & EXPLOITS

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

LAST WEEKS RECAP

CVE-2025-27364 - MITRE Caldera Remote Code Execution (RCE) vulnerability
CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

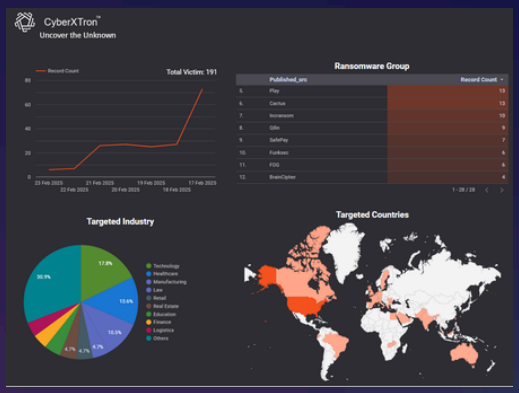
CyberXTron reported a total of 191 ransomware victims. The Play and Cactus groups each claimed 13 victims

TARGET INDUSTRIES

The Technology industry experienced the highest number of attacks at 30.9%, followed by Healthcare at 17.8% and Manufacturing at 13.6%.

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

Funksec

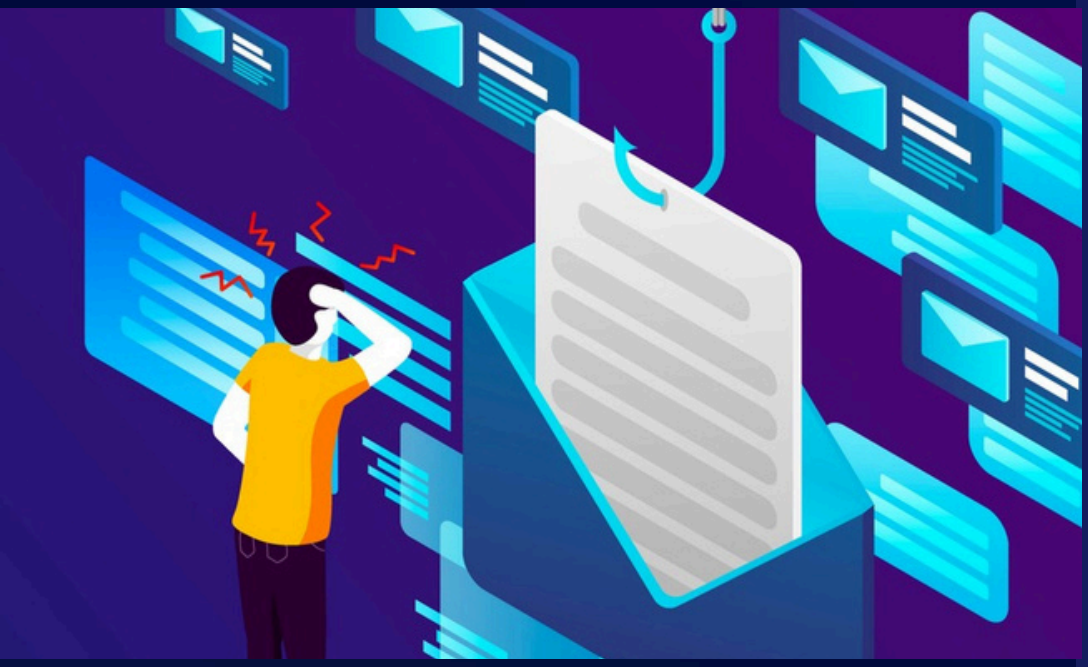
A relatively new ransomware group that emerged in late 2024. They operate under the Ransomware-as-a-Service (RaaS) model, providing their ransomware tools to affiliates. They have claimed 11 victims across various sectors, including media, IT, retail, education, automotive, professional services, and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



PayPal scam abuses Docusign API to spread phishy emails

PayPal scammers are exploiting the Docusign API to enhance the legitimacy of their phishing emails. They create Docusign accounts and use templates to send fake PayPal invoices, bypassing many security filters.

Victims receive emails about unauthorized transactions, prompting them to contact a fraudulent "Fraud Prevention Team." Red flags include a Gmail "From" address and non-existent "To" address. To verify the legitimacy, users should directly visit the Docusign site and enter the security code.

If you suspect fraud, report it to both PayPal and Docusign, review and secure your accounts, and never click on suspicious links in unsolicited emails. Docusign investigates and closes suspicious accounts within 24 hours.

READ MORE

OTHER PHISHING ARTICLES

Fake police call cryptocurrency investors to steal their funds

Nonprofits Face Surge in Cyber-Attacks as Email Threats Rise 35%

Microsoft says malvertising campaign impacted 1 million PCs

Fake CAPTCHA PDFs Spread Lumma Stealer via Webflow, GoDaddy, and Other Domains