SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

October 2025 - VOL.2

The News

IN THE NEWS THIS WEEK

GitHub Copilot 'CamoLeak' AI Attack Exfiltrates Data

A researcher from Legit Security has demonstrated a proof-of-concept attack called “CamoLeak” targeting GitHub’s AI coding assistant, Copilot.
The exploit uses a complex sequence to exfiltrate small but sensitive data like passwords and private keys. Despite GitHub’s improved security, the attack would likely go undetected by users and the platform itself.
Legit Security CTO Liav Caspi confirmed the stealthy nature of the method.
The attack highlights growing risks in embedding agentic AI tools into developer platforms.

Researchers warn that functionality often outpaces security in AI integrations. GitHub has faced past lapses but continues to strengthen Copilot’s defenses. CamoLeak underscores the need for rigorous safeguards in AI-powered environments. Security experts urge vendors to treat AI agents with the same scrutiny as core software.

READ MORE

OTHER NEWS HIGHLIGHTS

13-Year-Old Redis Flaw Exposed: CVSS 10.0 Vulnerability Lets Attackers Run Code Remotely

Medusa Ransomware Actors Exploit Critical Fortra GoAnywhere Flaw

New Quishing Attack With Weaponized QR Code Targeting Microsoft Users

The News

TOP OF THE NEWS THIS WEEK

Hackers Extorting Salesforce After Stealing Data From Dozens of Customers

A newly formed threat group calling itself Scattered LAPSUS$ Hunters has claimed responsibility for stealing data from dozens of Salesforce customers.
The group appears to include members from infamous hacking collectives Lapsus$, Scattered Spider, and ShinyHunters, all previously linked to high-profile cyberattacks.
On a Tor-based leak site, the hackers listed 39 targeted organizations, including Google, Disney, Cisco, FedEx, and Louis Vuitton, threatening to leak stolen data unless Salesforce pays a ransom.
They allege the theft of nearly 1 billion records from Salesforce instances, though additional victims remain unnamed.
Salesforce responded by stating there's no evidence of a platform breach or vulnerability exploitation, and that the claims may relate to past or unverified incidents. The company is working with external experts and authorities to support affected customers.
Lapsus$ has been inactive since 2022, while Scattered Spider and ShinyHunters recently announced their retirement.
The campaign raises concerns about coordinated extortion tactics targeting cloud-based enterprise platforms.
Cybersecurity analysts continue to monitor the situation as Salesforce maintains its stance on platform integrity.

READ MORE

TOP RELATED ARTICLES

Microsoft Warns of Hackers Compromising Employee Accounts to Steal Salary Payments

Google Warns of CL0P Ransomware Group Actively Exploiting Oracle E-Business Suite Zero-Day

SonicWall Confirms Breach Exposing All Customer Firewall Configuration Backups

Geo-Politics

NEWS FROM AROUND THE WORLD

Nation-State Chinese Hackers Breached Law Firm Williams & Connolly via Zero-Day

Chinese Hackers Breach Prominent U.S. Law Firms in Sophisticated Espionage CampaignWashington, D.C. — Williams & Connolly, one of the most prestigious law firms in the United States, confirmed a cyber intrusion linked to state-sponsored Chinese hackers who exploited a zero-day vulnerability to access attorney email accounts.

The firm, known for representing high-profile clients including Barack Obama, the Clintons, and major corporations like Intel and Google, said the breach affected a limited number of accounts and did not compromise confidential client data.
An investigation led by cybersecurity firm CrowdStrike attributed the attack to a nation-state actor targeting legal services, consistent with recent campaigns reported by Google and Mandiant involving China-linked groups.
Sources told The New York Times that Williams & Connolly privately informed clients the stolen data is unlikely to be leaked or sold.

The breach aligns with broader Chinese cyberespionage efforts targeting U.S. entities involved in international trade and policy, often using impersonation tactics and long-term network infiltration.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

North Korean Hackers Have Stolen $2 Billion in Cryptocurrency in 2025

Microsoft, DOJ Dismantle Domains Used by Russian FSB-Linked Hacking Group

Breaches

SECURITY BREACHES THIS WEEK

CL0P-Linked Hackers Breach Dozens of Organizations Through Oracle Software Flaw

A newly disclosed zero-day vulnerability in Oracle's E-Business Suite (CVE-2025-61882) has been exploited since August 9, 2025, impacting dozens of organizations, according to Google Threat Intelligence Group (GTIG) and Mandiant.

The flaw, rated 9.8 on the CVSS scale, enabled attackers to breach networks and exfiltrate sensitive data. Oracle has since released patches to address the issue.

The campaign resembles tactics used by the Cl0p ransomware group, though attribution remains uncertain. Google noted overlaps with FIN11 malware, including GOLDVEIN and GOLDTOMB.

Attackers launched a mass phishing campaign on September 29, targeting executives via compromised third-party email accounts bought on underground forums.

Victims received extortion emails claiming Oracle EBS breaches and demanding ransom, though none have yet appeared on Cl0p's leak site.

The intrusion leveraged SSRF, CRLF injection, authentication bypass, and XSL template injection to gain remote code execution.

Payloads included GOLDVEIN.JAVA and SAGEGIFT, which deployed further malware like SAGELEAF and SAGEWAVE

READ MORE

OTHER SECURITY BREACHES

SonicWall: 100% of Firewall Backups Possibly Breached

Red Hat OpenShift AI Flaw Exposes Hybrid Cloud Infrastructure to Full Takeover

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-61882 - Oracle E-Business Suite Concurrent Processing BI Publisher Integration Unauthenticated Remote Takeover Vulnerability

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2025-10725 - Critical Red Hat Kernel Privilege Escalation Vulnerability
CVSS Score: (9.9)

CVE-2025-10659 - Critical PHP Remote Code Execution Vulnerability
CVSS Score: (9.3)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

A total of 502 new victims were reported across various ransomware groups this Month.

TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 10% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 251 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

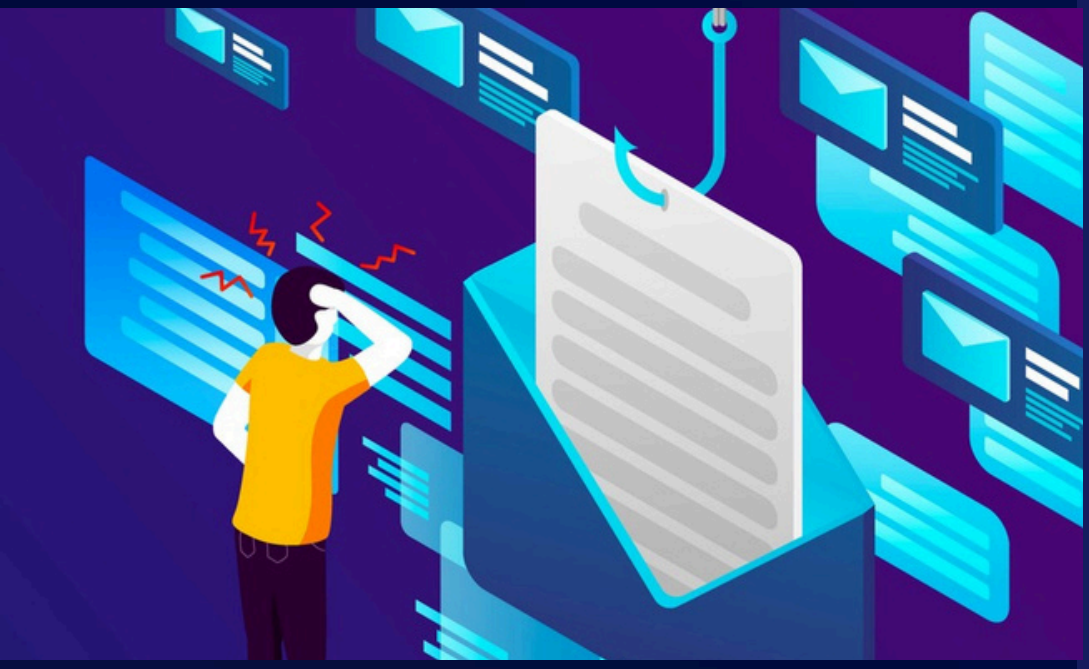
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



Hackers Exploit WordPress Sites to Power Next-Gen ClickFix Phishing Attacks

Cybersecurity researchers have uncovered a malicious campaign targeting WordPress sites through theme file injections that redirect visitors to fraudulent domains. The attack, analyzed by Sucuri, involves modifying the “functions.php” file to load remote JavaScript mimicking legitimate Cloudflare assets, ultimately serving malware via traffic distribution systems like Kongtuke.

The campaign also leverages the IUAM ClickFix Generator—a phishing kit that creates fake browser verification pages to deploy malware such as DeerStealer and Odyssey Stealer. These lures manipulate clipboard data and tailor payloads based on the victim’s operating system.

A newer variant uses “cache smuggling,” storing malware in the browser cache disguised as image files, bypassing traditional download detection. Experts urge site owners to update plugins and themes, enforce strong credentials, and monitor for unauthorized admin access to prevent persistent compromise.

READ MORE

OTHER PHISHING ARTICLES

New ClayRat Spyware Targets Android Users via Fake WhatsApp and TikTok Apps

FTX issues red alert over rising phishing attacks targeting creditors

OpenAI Bans State-Backed Chinese and North Korean Accounts for Malicious AI Use