SCC | DIGITAL

# THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

November 2025 - VOL.4

# The News

## IN THE NEWS THIS WEEK

### KawaiiGPT – Free WormGPT Variant Leveraging DeepSeek, Gemini, and Kimi-K2 AI Models

KawaiiGPT is an open-source project on GitHub that mirrors WormGPT by offering unrestricted AI outputs without API keys, installing quickly on Linux or Termux through simple Python and Git scripts, and using a reverse-engineered API wrapper to access models like DeepSeek, Gemini, and Kimi-K2.

It bypasses guardrails via prompt-injection, producing uncensored responses framed as playful but capable of generating phishing emails, ransomware notes, and exfiltration scripts. Its “kawaii” persona masks serious risks, lowering barriers for novice attackers, and since July 2025 it has evolved to version 2.5 with community-driven enhancements contrasting WormGPT’s paid model.

Obfuscated code raises concerns though the creator denies malware, enforcing MIT licensing against profiteering, while a Telegram community of hundreds fuels its growth. Security experts warn that despite its positioning for ethical pentesting, KawaiiGPT amplifies dual-use AI threats, demanding stronger organizational defenses against AI-aided phishing and automation.

READ MORE

## OTHER NEWS HIGHLIGHTS

Microsoft to Block External Scripts in Entra ID Logins to Enhance Protections

Shai Hulud 2.0 Compromises 1,200+ Organizations, Exposing Critical Runtime Secrets

London Councils’ IT Systems Impacted by CyberAttack, Including Phone Lines

# The News

## TOP OF THE NEWS THIS WEEK


### Salesforce Warns that Customer Data May Have Been Accessed Through Gainsight App

In November 2025, OpenAI disclosed a security incident stemming from its third-party analytics provider Mixpanel, which had fallen victim to a smishing campaign that tricked employees into revealing credentials.

Attackers used this access to export customer analytics data, exposing account names, emails, approximate locations, device and browser details, and internal organization IDs, though no passwords, API keys, chat logs, or payment information were compromised. Once notified on November 25, OpenAI quickly severed ties with Mixpanel, halted all integrations, and began notifying affected API users the following day, while also announcing stricter security requirements for all vendors.

Although the leaked metadata may seem low-sensitivity, experts warn it can fuel highly convincing phishing and impersonation attacks by tailoring messages with real names, locations, and account details.

The breach underscores the risks of third-party dependencies, highlighting that even secure platforms can be undermined by vendor lapses, and reinforces the need for vigilance, multi-factor authentication, phishing awareness, and careful vetting of suppliers to mitigate exposure.

READ MORE

## TOP RELATED ARTICLES

Shai-Hulud v2 Spreads From npm to Maven, as Campaign Exposes Thousands of Secrets

FBI Reports $262M in ATO Fraud as Researchers Cite Growing AI Phishing and Holiday Scams

Malicious Chrome Extension Injects Hidden Solana Transfer Fees

# Geo-Politics

## NEWS FROM AROUND THE WORLD


### Chinese Cyberspies Deploy ‘BadAudio’ Malware via Supply Chain Attacks

APT24, also known as Pitty Panda, has conducted a three-year cyberespionage campaign. The group, active since 2008, evolved from spear phishing into supply-chain compromises. Central to its toolkit is BadAudio, a C++ downloader fetching AES-encrypted payloads. BadAudio collects system data, encrypts it, and executes payloads in memory. It is deployed as a DLL via search order hijacking and script-based sideloading. Some incidents involved Cobalt Strike beacons linked to prior APT24 activity. Since late 2022, at least 20 websites were compromised with malicious JavaScript.Victims were tricked into downloading BadAudio through tailored pop-ups. In July 2024, a Taiwanese marketing firm was infiltrated, affecting 1,000 domains.

Re-compromises in 2025 used modified JavaScript and JSON for mass distribution.APT24 also abused cloud storage and tracking links for victim monitoring.Google Threat Intelligence highlights the campaign as proof of adaptive sophistication.

READ MORE

## HIGHLIGHTS FROM AROUND THE WORLD

MI5 Warns Lawmakers That Chinese Spies Are Trying to Reach Them via LinkedIn

Amazon Details Iran’s Cyber-Enabled Kinetic Attacks Linking Digital Spying to Physical Strikes

Russian Hackers Target US Engineering Firm Because of Work Done for Ukrainian Sister City

# Breaches

## SECURITY BREACHES THIS WEEK


### Qilin Ransomware Turns South Korean MSP Breach Into 28-Victim 'Korean Mass Hack'

A major ransomware incident has struck South Korea, where the Qilin ransomware gang exploited a managed service provider (MSP) to compromise 28 downstream organizations. Attackers reportedly exfiltrated over 1 million files totaling 2 TB of sensitive data, including corporate documents and client records. The breach originated from the MSP's remote management tools, which were leveraged to deploy ransomware payloads across multiple customer environments. This supply-chain style attack underscores the growing risk posed by MSP compromises, as they provide attackers with privileged access to numerous networks simultaneously.

The Qilin group has demanded significant ransom payments and threatened to leak stolen data on dark web forums if victims refuse to comply. Security experts warn that the incident could have cascading effects on critical sectors in South Korea, including finance and healthcare. Recommended mitigations include isolating MSP connections, enforcing multi-factor authentication, and conducting forensic reviews of remote access logs.

The attack highlights the urgent need for MSPs and their clients to adopt zero-trust principles and continuous monitoring to prevent similar large-scale breaches.

READ MORE

## OTHER SECURITY BREACHES

Google Confirms Gainsight Breach Exposed Salesforce Data of 200 Companies

US Banks Scramble After Hackers Breach Financial Tech Firm

DPRK's FlexibleFerret Malware Tightens Grip on macOS Targets

OpenAI User Data Exposed in Mixpanel Hack

OpenAI User Data Exposed in Mixpanel Hack

# Vulnerabilities

## VULNERABILITIES & EXPLOITS

CVE-2025-41115 - Grafana SCIM Provisioning Numeric externalId User Impersonation / Privilege Escalation Vulnerability

**CVSS SCORE 10**

CVE-2025-61757 - Oracle Fusion Middleware Identity Manager REST WebServices Unauthenticated Remote Takeover Vulnerability

**CVSS SCORE 9.8**

## LAST WEEKS RECAP

CVE-2025-13223 - Type Confusion vulnerability in Google Chrome's V8 JavaScript
CVSS Score: (8.8)

# Ransomware

## WEEKLY RANSOMWARE ROUNDUPS

### OVERVIEW

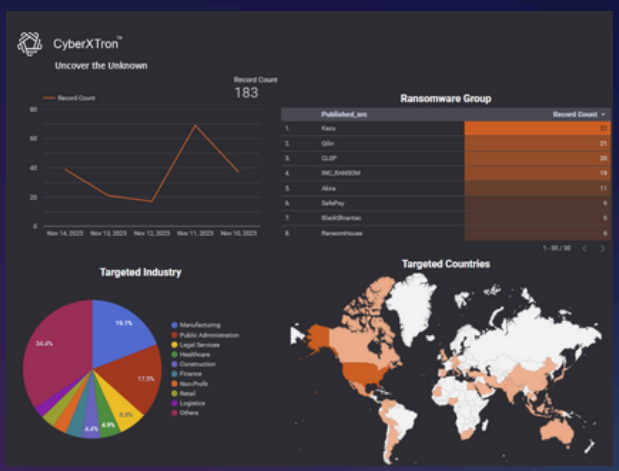
A total of 183 new victims were reported across various ransomware groups this Week.

### TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 19.1% of all victims.

### TARGET COUNTRY

The USA was the top victim country, with a total of 81 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**

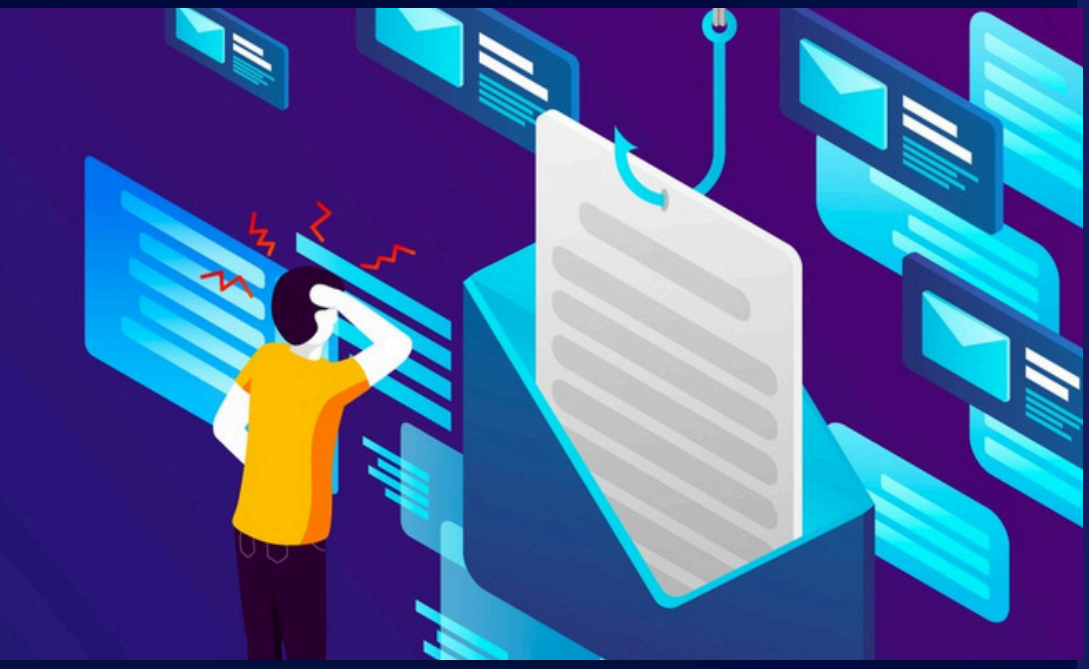
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

**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



### Matrix Push C2 abuses browser notifications to deliver phishing and malware

A new phishing technique called Matrix Push C2 is exploiting browser notifications to deliver malicious links without requiring file downloads. The campaign uses fake alerts and redirects to lure victims into clicking links that lead to credential theft or malware installation. Researchers note that this approach is highly evasive because it leverages native browser features, making detection by traditional security tools difficult.

The attack is cross-platform, targeting Windows, macOS, and Linux users through Chrome, Firefox, and other major browsers. Victims are tricked into enabling notifications, which then serve as the delivery channel for phishing payloads. The infrastructure behind Matrix Push C2 is modular, allowing attackers to update campaigns quickly and scale globally.

Security experts warn that this method could become a preferred tactic for phishing-as-a-service operators due to its low cost and high success rate. Organizations are advised to disable unnecessary browser notifications and educate users about the risks of granting notification permissions.

The broader implication is that phishing is evolving beyond email, exploiting legitimate web features to bypass defenses.

READ MORE

## OTHER PHISHING ARTICLES

DHL-Themed Phishing Emails Surge Ahead of Holiday Season

Alumni, Student, and Staff Information Stolen From Harvard University