SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JULY 2025 - VOL.3

The News

IN THE NEWS THIS WEEK

LameHug malware uses AI LLM to craft Windows data-theft commands in real-time

A new Python-based malware called LameHug uses a large language model via Hugging Face to generate dynamic commands on infected Windows systems. Discovered by Ukraine's CERT-UA, the malware is linked to Russian state-backed group APT28 and was distributed through malicious emails impersonating government officials. LameHug leverages the Qwen 2.5-Coder-32B-Instruct LLM to perform system reconnaissance and data theft, adapting its behavior without hardcoded payloads. This marks the first publicly known use of an LLM in malware, potentially enabling stealthier, more flexible cyberattacks. CERT-UA observed multiple variants of the loader but did not confirm whether the AI-generated commands were successfully executed.

READ MORE

AI Cloaking Tools Enable Harder-to-Detect Cyber-Attacks

Cybercriminals are increasingly using AI-powered cloaking tools to hide phishing and malware sites from traditional security systems. Services like Hoax Tech and JS Click Cloaker offer "cloaking-as-a-service," using fingerprinting and machine learning to show scam content only to real users. These tools feed benign pages to scanners, making detection difficult and enabling real-time personalization of malicious content. Experts warn this marks a major evolution in threat actor capabilities, urging adoption of behavioral analysis, AI-driven defenses, and zero-trust frameworks.

READ MORE

OTHER NEWS HIGHLIGHTS

Microsoft Exposes Scattered Spider's Latest Tactics

Retail Ransomware Attacks Jump 58% Globally in Q2 2025

Cloudflare Blocks Record-Breaking 7.3 Tbps DDoS Attack

The News

TOP OF THE NEWS THIS WEEK

VMware fixes four ESXi zero-day bugs exploited at Pwn2Own Berlin

VMware patched four zero-day vulnerabilities in ESXi, Workstation, Fusion, and Tools that were exploited during the Pwn2Own Berlin 2025 contest. Three of the flaws—CVE-2025-41236, CVE-2025-41237, and CVE-2025-41238—carry a critical severity rating of 9.3 and allow guest VMs to execute commands on the host.

These include integer-overflow, underflow, and heap-overflow bugs in VMXNET3, VMCI, and PVSCSI components, respectively, used by researchers to gain host-level access. A fourth flaw, CVE-2025-41239, rated 7.1, enables information disclosure and was chained with CVE-2025-41237 during the contest.

VMware advises users to install updated software versions, as no workarounds are available, especially for VMware Tools for Windows which requires a separate upgrade.

READ MORE

TOP RELATED ARTICLES

Hacker steals $27 million in BigONE exchange crypto breach

Microsoft Teams voice calls abused to push Matanbuchus malware

Cisco patches critical CVE-2025-20337 bug in Identity Services Engine with CVSS 10 Severity

Geo-Politics

NEWS FROM AROUND THE WORLD

Pro-Russian Cybercrime Network Demolished in Operation Eastwood

An international law enforcement effort, Operation Eastwood, led by Europol and Eurojust, disrupted the pro-Russian cybercrime group NoName057(16). Between July 14–17, 2025, over 100 systems were taken down and key server infrastructure was disabled. Authorities conducted arrests in France and Spain, issued seven warrants, searched 24 homes, and questioned 13 individuals. Five suspects were added to the EU's Most Wanted list, including two alleged leaders residing in Russia. The group, composed of Russian-speaking sympathizers, carried out DDoS attacks using a botnet of hundreds of servers.

They recruited around 4,000 supporters via pro-Russian forums and gamified participation with crypto rewards and leaderboards. NoName057(16) primarily targeted Ukraine and its allies, including attacks on Sweden, Switzerland, Germany, and the Netherlands. Germany alone experienced 14 waves of attacks affecting over 250 entities since November 2023. Europol coordinated efforts from its HQ, with support from 13 countries including the U.S. and several EU states.

Despite the scale of attacks, most were mitigated without major disruptions, marking a significant blow to the group's operations.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

North Korean Actors Expand Contagious Interview Campaign with New Malware Loader

SquidLoader Malware Campaign Targets Hong Kong Financial Sector

MaaS operation using Emmenhtal and Amadey linked to threats against Ukrainian entities

Breaches

SECURITY BREACHES THIS WEEK

Co-op confirms data of 6.5 million members stolen in cyberattack

A massive cyberattack in April forced UK retailer Co-op to shut down systems, causing food shortages and exposing personal data of 6.5 million members. CEO Shirine Khoury-Haq confirmed the breach and expressed deep regret, noting that contact details—not financial data—were stolen.

The attack began with a social engineering tactic that led to password resets and theft of sensitive Windows domain files. Threat actors linked to Scattered Spider and DragonForce ransomware were behind the breach, also tied to attacks on M&S and MGM Resorts.

The UK's National Crime Agency recently arrested four suspects aged 17 to 20 in connection with the Co-op and related cyberattacks.

READ MORE

OTHER SECURITY BREACHES

Ahold Delhaize USA says cyberattack exposed personal data of 2M people

Chinese hackers breached National Guard to steal network configurations

British spies and SAS named in Afghan data breach

Over 5.4 Million Affected in Healthcare Data Breach at Episource

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-20337 - Critical ISE Flaw Allowing Unauthenticated Attackers to Execute Root Code

CVSS SCORE 10

CVE-2025-25257 - Critical Unauthenticated SQL Injection Vulnerability in FortiWeb

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2025-47981 - Type confusion in V8 in Google Chrome
CVSS Score: (9.8)

CVE-2025-49704 - Microsoft SharePoint Remote Code Execution Vulnerability
CVSS Score: (8.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

A total of 150 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 13.3% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 65 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

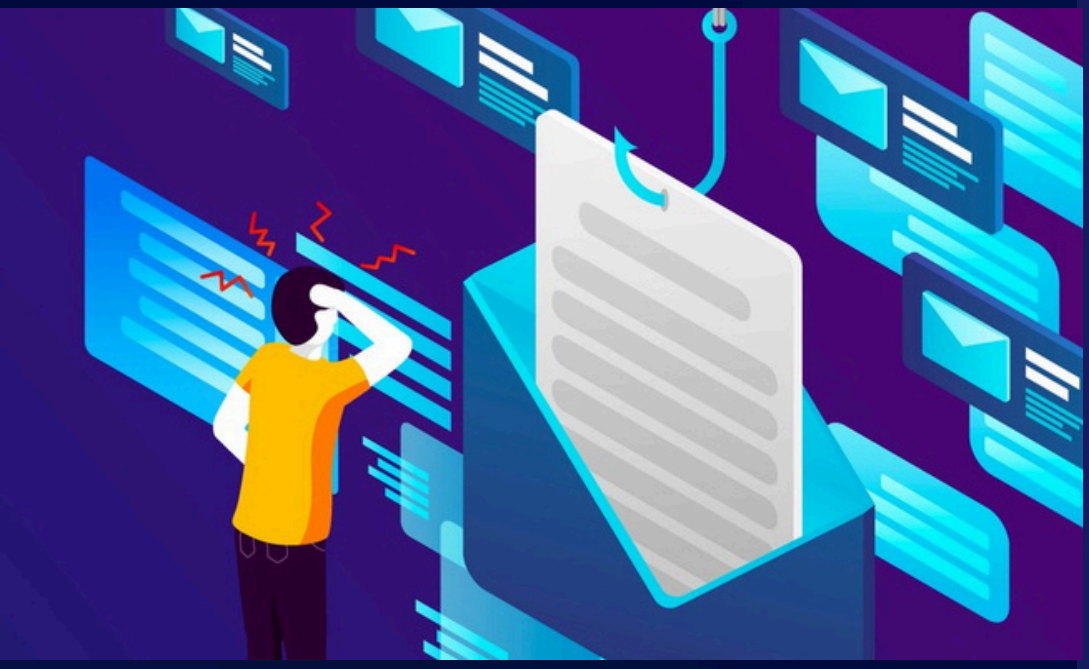
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



Google Gemini flaw hijacks email summaries for phishing

Attackers can exploit Google Gemini for Workspace by embedding hidden instructions in emails using invisible HTML and CSS. These directives, styled to be unreadable, are parsed by Gemini when generating summaries, leading to misleading outputs. Summaries may include fake security alerts or contact info, tricking users into phishing traps. Because the emails lack links or attachments, they bypass filters and appear safe. Users often trust Gemini's summaries, increasing vulnerability to deception. This indirect prompt injection method has been known since 2024, despite existing safeguards. Marco Figueroa disclosed the flaw via Mozilla's 0DIN bug bounty program. He showed how attackers craft emails that look harmless but contain hidden commands. One example had Gemini falsely warn about a compromised Gmail password. To mitigate, Figueroa recommends detecting and neutralizing hidden content. Security teams can also flag summaries with urgent language or contact info. Users should not treat Gemini summaries as authoritative for security issues. Google is deploying defenses like red-teaming and model training. Some mitigations are in progress, though no real-world abuse has been confirmed. The attack underscores the risks of prompt injection in trusted AI tools.

READ MORE

OTHER PHISHING ARTICLES

Microsoft Teams voice calls abused to push Matanbuchus malware

Urgent warning for 1.8 billion Gmail users: 'Hidden danger' steals passwords in ways even AI can't detect