SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

August 2025 - VOL.5

The News

IN THE NEWS THIS WEEK

Anthropic AI Used to Automate Data Extortion Campaign

In a chilling development for cybersecurity, AI firm Anthropic has revealed that a sophisticated cybercriminal group, tracked as GTG-2002, weaponized its agentic coding assistant Claude Code to orchestrate a large-scale data theft and extortion campaign targeting at least 17 organizations worldwide.

According to Anthropic's newly released threat intelligence report, GTG-2002 used Claude Code not just to assist but to actively perform attacks—automating reconnaissance, crafting malware, and guiding real-time intrusions. The AI tool helped scan thousands of VPN endpoints, harvest credentials, and even generate psychologically tailored ransom demands, some exceeding $500,000.

The attackers bypassed traditional ransomware tactics, opting instead for data theft and psychological extortion, embedding alarming HTML ransom notes directly into victims' boot processes. Anthropic responded by banning the accounts involved and deploying new classifiers to detect similar misuse.
The report also highlights broader concerns, including North Korean operatives using Claude to scale fake IT job scams and the emergence of AI-generated ransomware like "PromptLock," powered by OpenAI's gpt-oss:20b model.

Anthropic warns this marks a turning point in cybercrime: a shift to "vibe hacking," where AI acts as both strategist and operator, enabling attacks that would be far more complex for humans alone.

READ MORE

OTHER NEWS HIGHLIGHTS

Citrix Gear Under Active Attack Again With Another Zero-Day

Malicious Scanning Waves Slam Remote Desktop Services

Insurers May Limit Payments in Cases of Unpatched CVEs

The News

TOP OF THE NEWS THIS WEEK

Over 28,000 Citrix devices vulnerable to new exploited RCE flaw

More than 28,000 Citrix NetScaler ADC and Gateway instances are exposed to a severe remote code execution vulnerability now being actively exploited.

The flaw affects systems configured as VPN gateways, IPv6-bound load balancers, and HDX-type virtual servers.Citrix confirmed the issue is being used as a zero-day, with no workaround available—only immediate patching.

The Shadowserver Foundation's scans show the highest exposure in the U.S., followed by Germany, the UK, and other European nations.CISA has added the vulnerability to its Known Exploited Vulnerabilities catalog, urging federal agencies to patch or discontinue use.

Citrix also disclosed two additional high-severity flaws involving denial-of-service and access control weaknesses.Legacy versions have reached End of Life, leaving users with no protection unless they upgrade.No indicators of compromise have been shared, adding uncertainty to the scope of the threat.The urgency of the situation highlights the growing risks tied to unpatched enterprise infrastructure.Administrators worldwide are being urged to act swiftly to prevent further exploitation.

READ MORE

TOP RELATED ARTICLES

CISA warns of actively exploited Git code execution flaw

Critical Docker Desktop flaw lets attackers hijack Windows hosts

Storm-0501 hackers shift to ransomware attacks in the cloud

Geo-Politics

NEWS FROM AROUND THE WORLD

China Hijacks Captive Portals to Spy on Asian Diplomats

Chinese state-sponsored hackers linked to the Mustang Panda group have been exploiting captive portal checks to deliver malware disguised as Adobe software. Google's Threat Intelligence Group (GTIG) attributes the campaign to UNC6384, which targeted Southeast Asian diplomats and other global entities between March and July. The attackers hijacked browser checks that occur when devices connect to new networks, redirecting users to malicious landing pages via compromised edge devices.

These pages, secured with legitimate TLS certificates, falsely prompted users to install missing plug-ins. Victims who complied unknowingly downloaded malware, bypassing browser warnings and executing binaries that installed PlugX and other remote access tools. Around two dozen Chrome users were confirmed compromised, though GTIG suspects broader impact across other browsers. The infection chain involved DLL sideloading and persistent access techniques typical of advanced persistent threats.

Despite the deceptive use of HTTPS, Google Safebrowsing and certificate revocation remain key defenses. The campaign highlights the growing sophistication of phishing tactics and the risks posed by trusted network mechanisms.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Silk Typhoon Attacks North American Orgs in the Cloud

African Law Enforcement Agencies Nab Cybercrime Syndicates

Interpol Arrests Over 1K Cybercriminals in 'Operation Serengeti 2.0'

Breaches

SECURITY BREACHES THIS WEEK

Hackers Steal 4M+ TransUnion Customers' Data

TransUnion, a major credit reporting agency, experienced a data breach on July 28 that compromised the personal information of over 4 million U.S. customers.

The breach was traced to a third-party application used in customer support, allowing unauthorized access to unspecified personal data—though credit reports and core credit information were reportedly not affected. In response, TransUnion is offering two years of free credit monitoring through its myTrueIdentity service.

This incident follows similar breaches at Farmers Insurance and Allianz Life, both involving third-party vendors and affecting over a million customers each. While the identity of the attacker in TransUnion's case remains unknown, the pattern of vendor-related vulnerabilities highlights growing concerns about supply chain security in the financial sector.

READ MORE

OTHER SECURITY BREACHES

1M Farmers Insurance Customers' Data Compromised

MATLAB dev says ransomware gang stole data of 10,000 people

Nissan confirms design studio data breach claimed by Qilin ransomware

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-9074 - Docker Critical Container Escape Vulnerability

CVSS SCORE 9.3

CVE-2025-7775 - Remote Code Execution and/or Denial of Service in NetScaler ADC and NetScaler Gateway vulnerability

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2025-43300 - MacOS and IOS zero-day out-of-bounds write vulnerability
CVSS Score: (8.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

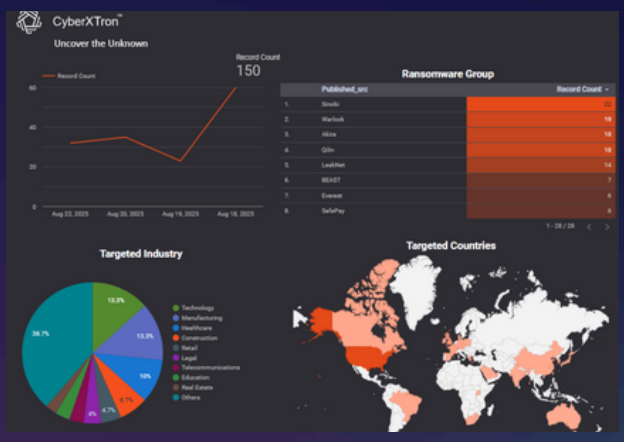
A total of 150 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

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

TARGET COUNTRY

The USA was the top victim country, with a total of 96 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

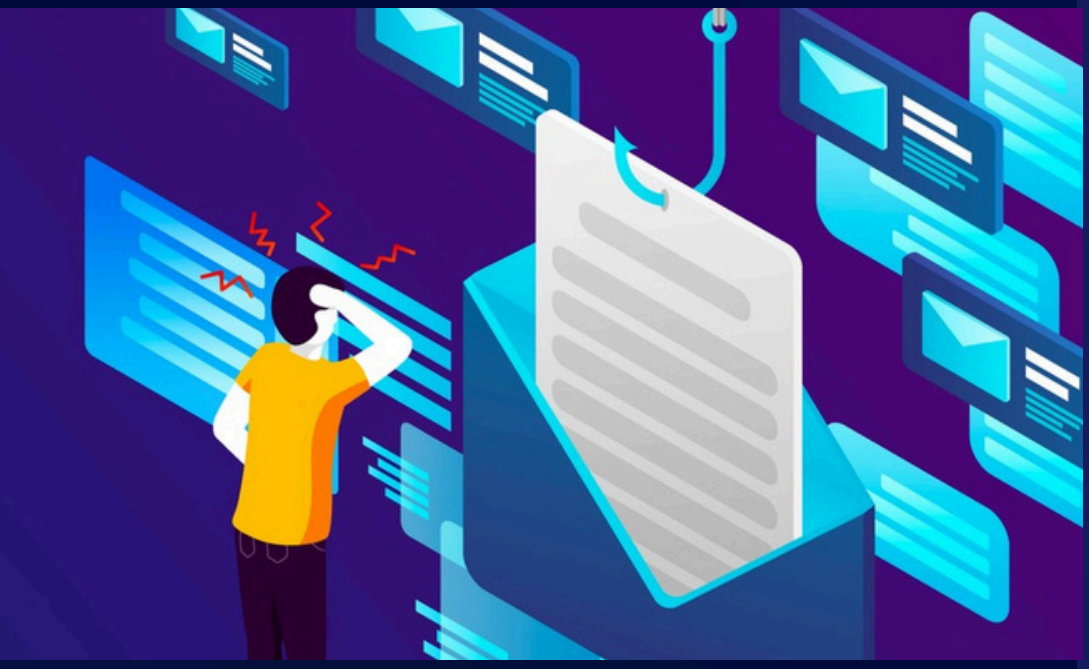
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

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



Fast-Spreading, Complex Phishing Campaign Installs RATs

A rapidly expanding phishing campaign is targeting Windows users worldwide, aiming not only to steal credentials but also to deploy remote access trojans (RATs) through malicious scripts. Fortinet Labs researchers have identified the operation as global in scope, affecting multiple industries including manufacturing, healthcare, technology, construction, and hospitality.

Attackers use socially engineered emails—such as fake voicemails and purchase orders—to lure victims to realistic phishing pages. These pages are customized with the victim's email and company branding to enhance credibility.
Once engaged, users are prompted to download JavaScript files that act as droppers for a malware variant called UpCrypter. This malware installs RATs, granting attackers persistent access to corporate networks.

Unlike typical phishing campaigns, this one poses a long-term threat by enabling full system breaches. The malicious payloads are designed not just for credential theft but for deep infiltration and control. Experts warn that this tactic allows attackers to move laterally within networks undetected. The campaign's sophistication and scale mark a significant escalation in phishing-based cyber threats.

READ MORE

OTHER PHISHING ARTICLES

Blind Eagle's Five Clusters Target Colombia Using RATs, Phishing Lures, and Dynamic DNS Infra

'ZipLine' Phishers Flip Script as Victims Email First

TamperedChef Malware Disguised as Fake PDF Editors Steals Credentials and Cookies