TRACKING RANSOMWARE - FEBRUARY 2025 - CYFIRMA

Archived: 2026-04-05 13:24:19 UTC

Published On : 2025-03-13

EXECUTIVE SUMMARY

February 2025 witnessed a sharp rise in ransomware incidents, with 956 reported victims globally, marking an 87% increase from January. Clop and Play ransomware groups led this surge, while new actors like Anubis and Linkc Pub emerged. The Manufacturing sector faced the highest impact, and the United States remained the most targeted region. This report analyzes key ransomware trends, highlighting the growing sophistication of attacks and the increasing overlap between financial crime and cyber espionage.

INTRODUCTION

The ransomware landscape in February 2025 experienced unprecedented growth, surpassing trends from previous years. This report presents a detailed analysis of ransomware activity, comparing it with past months. It covers the most affected industries, geographical targets, and newly emerging ransomware groups. Additionally, the report explores evolving threat actor tactics, including zero-day exploitation, advanced social engineering techniques,

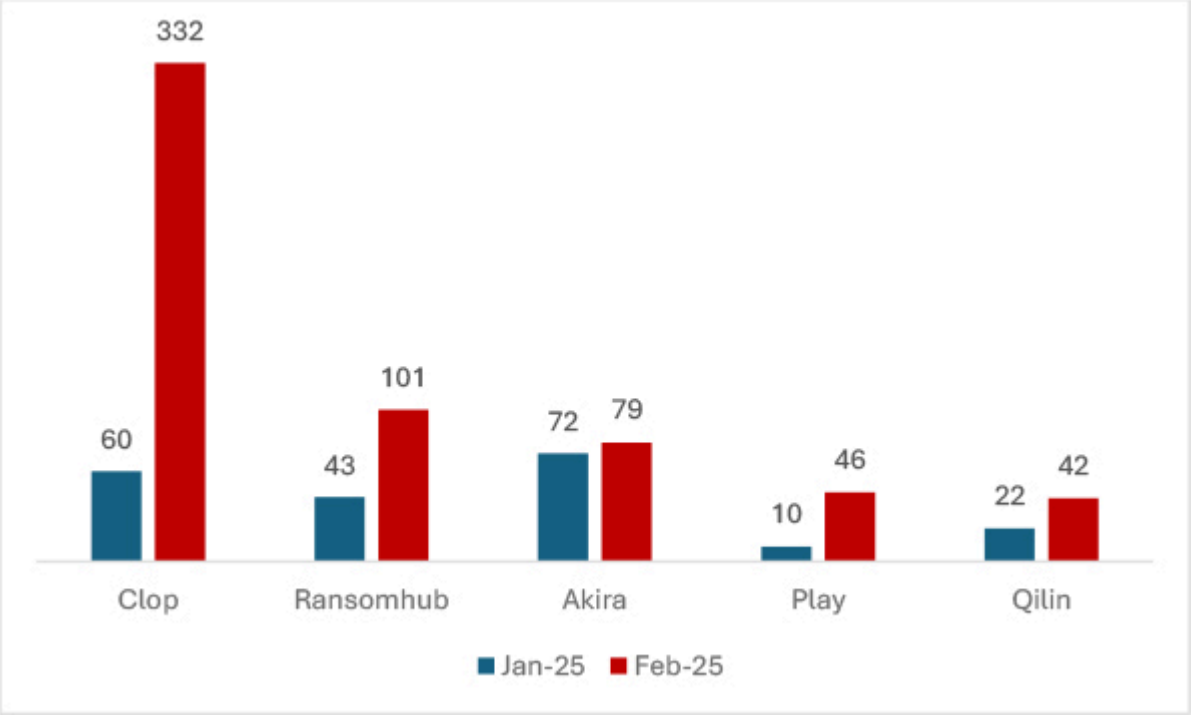
and espionage-linked ransomware attacks, offering valuable insights into the rapidly shifting cyber threat environment.

KEY POINTS

- In February 2025, the Clop ransomware group emerged as a significant threat, leading with a victim count of 332.
- The Manufacturing sector is the primary target of ransomware attacks, experiencing 159 incidents globally in February 2025.
- The USA was the most targeted geography in February 2024.
- Anubis, linkc and RunSomeWares emerged as new threats in the ransomware landscape.

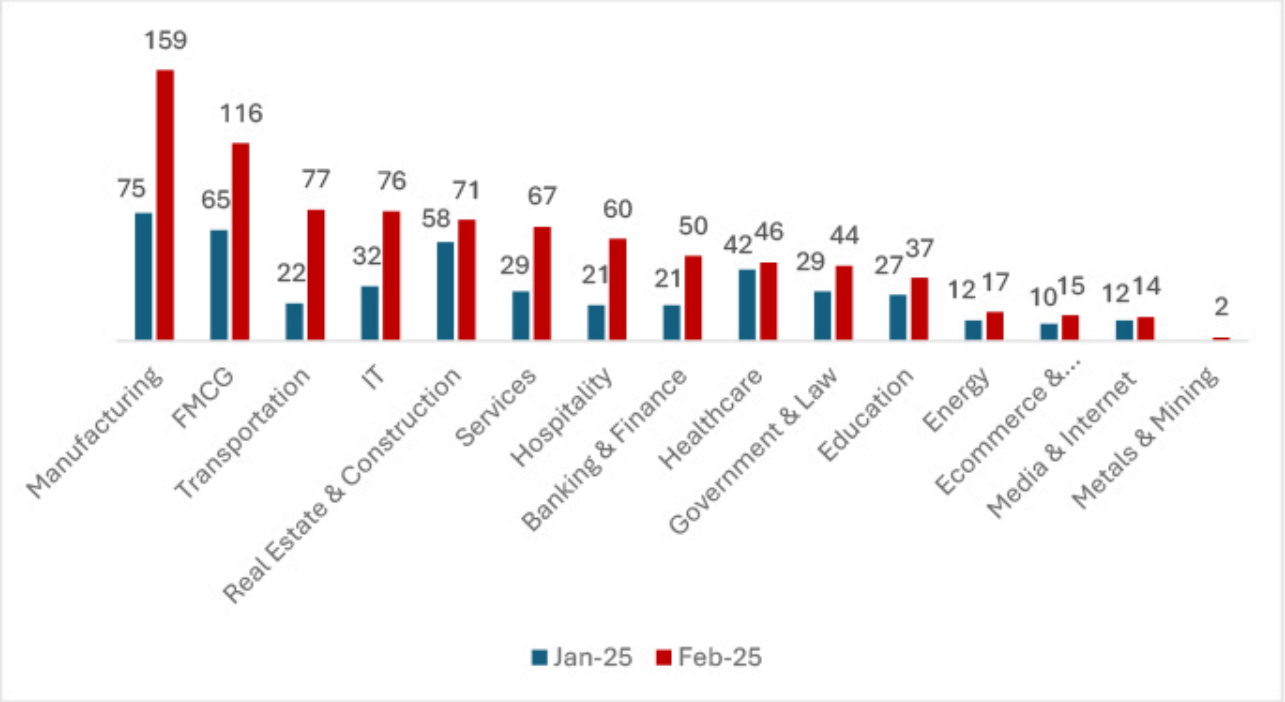
TREND COMPARISON OF FEBRUARY 2025'S TOP 5 RANSOMWARE GROUPS.

Throughout February 2025, there was notable activity from several ransomware groups. Here are the trends regarding the top 5:



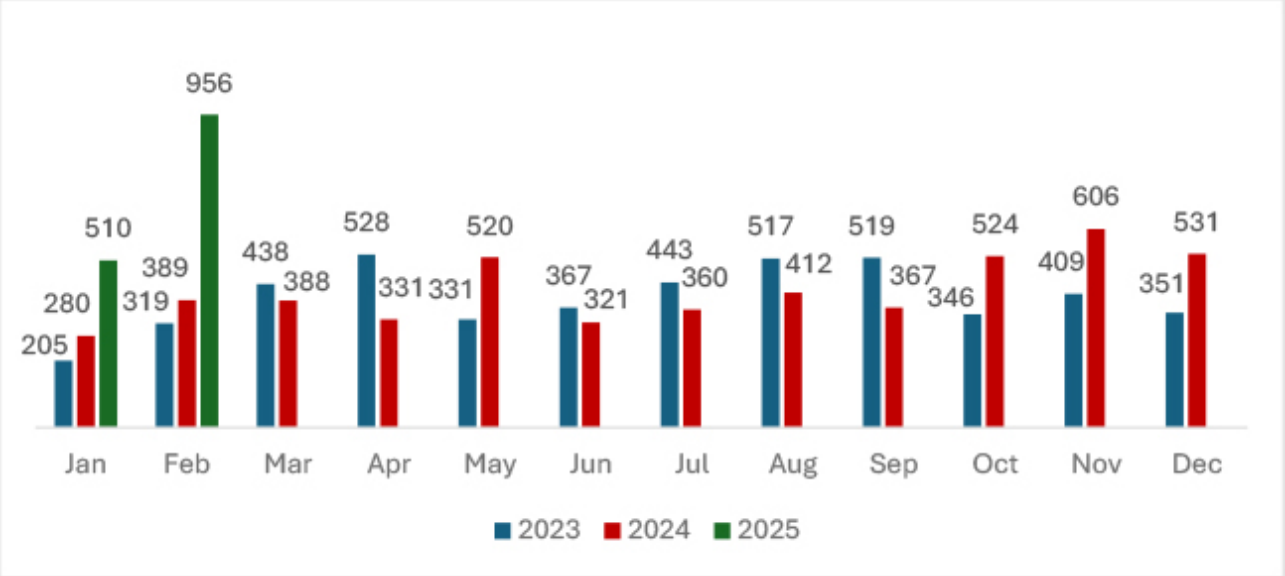
Ransomware activity surged in February 2025 compared to January. Clop saw a staggering 453% increase, while Ransomhub rose by 135%. Play experienced a sharp 360% spike, and Qilin nearly doubled, growing by 91%. Akira showed a moderate 10% rise. The significant uptick, especially in Clop and Play ransomware, underscores the urgent need for enhanced cybersecurity measures to counter evolving ransomware threats.

INDUSTRIES TARGETED IN FEBRUARY 2025 COMPARED WITH JANUARY 2025



In February 2025, cyberattacks surged across industries compared to January 2025, with Manufacturing witnessing the highest increase of 112% (from 75 to 159 incidents). FMCG attacks rose by 78%, while Transportation saw a 250% spike. I.T. and Services industries faced 138% and 131% increases, respectively. Banking & Finance attacks increased 138%, whereas Healthcare rose by 9.2% incidents. Government & Law and Education also saw 51% and 37% growth. Minimal changes were observed in energy, e-commerce, and media. These trends indicate a sharp rise in cyber threats across critical sectors, demanding stronger security measures.

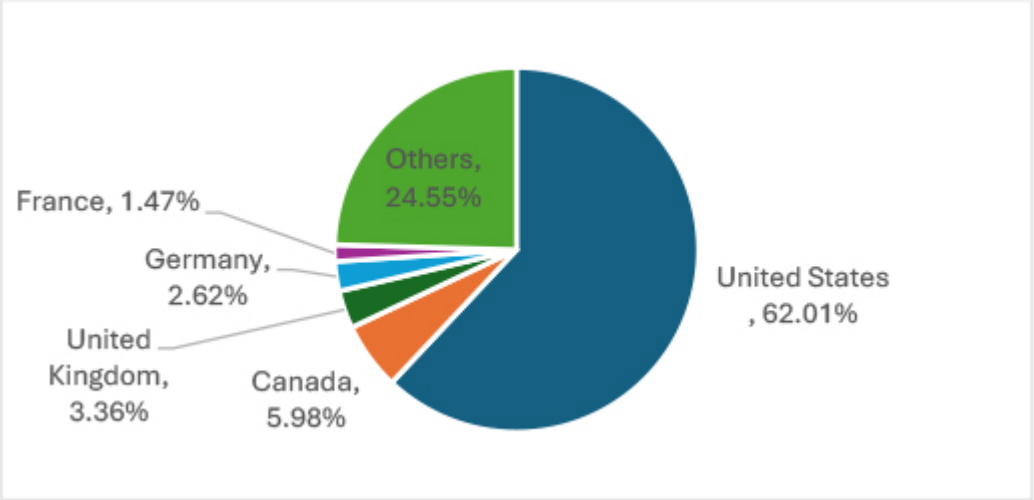
TRENDS COMPARISON OF RANSOMWARE ATTACKS



In February 2025, ransomware attacks surged , marking an 87% increase from 510 in January 2025. This sharp rise highlights a significant escalation in ransomware operations, surpassing trends from 2023 and 2024. The unprecedented spike suggests evolving attacker tactics and increased targeting of vulnerable sectors. This trend

highlights the urgent need for enhanced cybersecurity defenses, proactive threat intelligence, and stronger incident response frameworks to mitigate the growing ransomware threat and minimize business disruptions.

GEOGRAPHICAL TARGETS: TOP 5 LOCATIONS



In February 2025, the United States remained the top ransomware target, with 591 victims—significantly outpacing other regions. Canada followed with 57 attacks, while the United Kingdom (32), Germany (25), and France (14) saw lower but notable ransomware activity. These regions are prime targets due to their strong economies, data-rich enterprises, critical infrastructure, and high ransom-paying potential, making them lucrative for cybercriminals.

EVOLUTION OF RANSOMWARE GROUP IN FEBRUARY 2025

China-linked attackers exploit Check Point flaw, deploy ShadowPad and ransomware

A newly identified threat activity cluster targeted European organizations, particularly in the healthcare sector, deploying PlugX and its successor ShadowPad, before executing **NailaoLocker** ransomware. The attacks leveraged a recently patched vulnerability (CVE-2024-24919 – CVSS score: 7.5) in Check Point network gateway to gain initial access.

Exploiting vulnerable instances enabled credential theft and VPN access using legitimate accounts. The attackers then conducted network reconnaissance, moved laterally via RDP, and escalated privileges. They employed DLL search-order hijacking to sideload ShadowPad and PlugX, enabling persistent remote access. ShadowPad, an advanced malware with obfuscation and anti-debugging techniques, was used for stealthy command-and-control operations.

The final stage involved executing NailaoLocker ransomware via DLL sideloading. The payload encrypted files, appended a “.locked” extension, and dropped a ransom note demanding bitcoin payments. NailaoLocker lacked sophistication, with no capability to scan network shares, stop critical services, or evade debugging.

Attribution indicators, including the use of ShadowPad, sideloading techniques, and tool overlaps with previous campaigns, suggest involvement of a Chinese-aligned group. The attack highlights a potential trend where

espionage-focused actors engage in ransomware for financial gain while maintaining long-term network access for future operations.

ETLM Assessment
Future ransomware campaigns may increasingly blur the lines between espionage and financial crime, with state-linked actors leveraging advanced implants like ShadowPad for persistent access while deploying unsophisticated ransomware for quick profits. More critical sectors could be targeted, and attackers may refine techniques, exploiting zero-days and evading detection with enhanced obfuscation.

XELERA Ransomware Campaign Spreads via Malicious Documents in New Attack
A recent cybersecurity threat has emerged, targeting job seekers with fake employment offers from a prominent Indian public sector organization. The attack begins with a spear-phishing email containing a malicious Word document titled “FCEI-job-notification.doc.” This document appears legitimate, detailing vacancies and eligibility criteria, but harbors an embedded Object Linking and Embedding (OLE) object. Extracting this object reveals a compressed PyInstaller executable named “jobnotification2025.exe,” which serves as the initial stage of the malware.

Upon execution, this executable unpacks Python-compiled files, including “mainscript.pyc,” which contains the core malicious logic. The malware employs libraries such as psutil, aiohttp, and asyncio for system monitoring and network operations. Notably, it utilizes a Discord bot as its command-and-control (C2) server, enabling remote command execution on the victim’s machine. The bot can perform various malicious activities, including privilege escalation, system control (e.g., locking or shutting down the system), credential theft from browsers, and visual disruptions like altering wallpapers.

In its final stage, the malware deploys ransomware that demands payment in Litecoin. It includes functions to terminate Windows Explorer unless a specific executable is running and downloads an MBR (Master Boot Record) corruption tool named “MEMZ.exe.” This tool can render the system unbootable, adding pressure on the victim to comply with the ransom demands.

Given the sophistication of this attack and its exploitation of trusted platforms and services, it is anticipated that similar ransomware campaigns will increase in frequency and complexity. Attackers are likely to continue refining their tactics, making detection and prevention increasingly challenging.

ETLM Assessment
Given the sophisticated nature of this campaign, it’s anticipated that similar attacks will increase, employing advanced social engineering tactics and multi-stage infection processes to exploit job seekers and other vulnerable groups globally.

EncryptHub infiltrates organisations, deploys infostealers, and ransomware.
EncryptHub, also known as Larva-208, is a new sophisticated threat actor targeting organizations globally through spear-phishing and social engineering tactics. Since June 2024, it has compromised over 600 organizations by impersonating IT support and mimicking corporate VPN products. Victims are lured through SMS phishing, voice phishing, and fake login pages, where credentials and MFA tokens are stolen in real time. The group uses over 70 domains that resemble legitimate services to increase credibility. Once access is gained, remote monitoring and management tools are deployed for persistence, followed by information stealers like Stealc and Rhadamanthys to

exfiltrate credentials, browser data, and cryptocurrency wallets. EncryptHub has also been linked to RansomHub and BlackSuit ransomware operations, acting either as an initial access broker or direct affiliate. While it has deployed these ransomware variants in past attacks, it also uses a custom PowerShell-based encryptor that appends a ".crypted" extension to files before deleting originals. A ransom note demands payment in USDT via Telegram. The use of bulletproof hosting, sophisticated obfuscation, and tailored social engineering tactics allows EncryptHub to evade detection and compromise high-value targets. Its connections to established ransomware groups further amplify the threat to global organizations.

ETLM:
EncryptHub and other threat atcors are likely to evolve by refining phishing techniques, leveraging AI for automation, and expanding partnerships with ransomware groups like RansomHub and BlackSuit. Increased use of evasive malware, cloud-based attacks, and multi-platform targeting could escalate global breaches. Strengthened defenses against social engineering and MFA bypass will be critical.

Chinese espionage tools deployed in RA World ransomware attack
A China-based threat actor, Emperor Dragonfly, has been observed conducting ransomware attacks using a toolset previously linked to espionage operations. The attackers deployed RA World ransomware against an Asian software company, demanding a $2 million ransom. This activity suggests a potential overlap between cyber espionage and financially motivated cybercrime.

Between mid-2024 and early 2025, the threat actor targeted government ministries and telecom operators in Southeast Europe and Asia, focusing on long-term persistence. A specific PlugX (Korplug) backdoor was deployed using DLL sideloading, leveraging a legitimate Toshiba executable (toshdpdb.exe) and a malicious DLL (toshdpapi.dll). Additionally, NPS proxy, a covert network communication tool, and RC4-encrypted payloads were used to maintain stealth.

Later, in a separate attack against a South Asian software firm, RA World ransomware was executed following the deployment of Korplug. The attackers initially compromised the network by exploiting CVE-2024-0012, a vulnerability in security appliances. They then used the same sideloading techniques to establish persistence before encrypting systems.

ETLM:
State-backed cybercriminals will likely continue blending espionage with ransomware for financial gain. Future attacks may target critical infrastructure and major enterprises, exploiting zero-days and supply chain vulnerabilities for deeper access.

Overall Trend in Ransomware Evolution

- **Blurring Lines Between Espionage and Financial Crime –** State-linked actors are increasingly engaging in ransomware attacks, not just for financial gain but also to maintain long-term network access. The China-linked group behind the ShadowPad and NailaoLocker campaign exemplifies this hybrid approach, where advanced malware ensures persistence while ransomware serves as a quick monetization tool.
- **Advanced Social Engineering & Multi-Stage Attacks –** Threat actors are refining their social engineering tactics, leveraging phishing, fake job offers, and impersonation to gain initial access. Groups like EncryptHub mimic IT support teams and use real-time MFA interception to bypass security measures

before deploying ransomware. Meanwhile, XELERA campaign is conducting through fake job notifications, utilizing Discord bots for command-and-control before encrypting victims' data.

- **Exploitation of Zero-Days & Evasive Malware –** The increased use of zero-day vulnerabilities and sideloading techniques highlights the evolution of ransomware delivery methods. The exploitation of a Check Point firewall flaw (CVE-2024-24919) allowed China-linked attackers to deploy ShadowPad and ransomware payloads undetected, demonstrating how adversaries rapidly weaponize newly disclosed vulnerabilities.

Ransomware incidents have surged 87.45%, rising from 510 to 956 victims. This sharp increase is largely attributed to the Clop ransomware group, whose victim count skyrocketed by 453%. The group recently disclosed the majority of its compromised victims, exploiting zero-day vulnerabilities (CVE-2024-50623 and CVE-2024-55956) in Cleo software to breach corporate networks.

EMERGING GROUPS

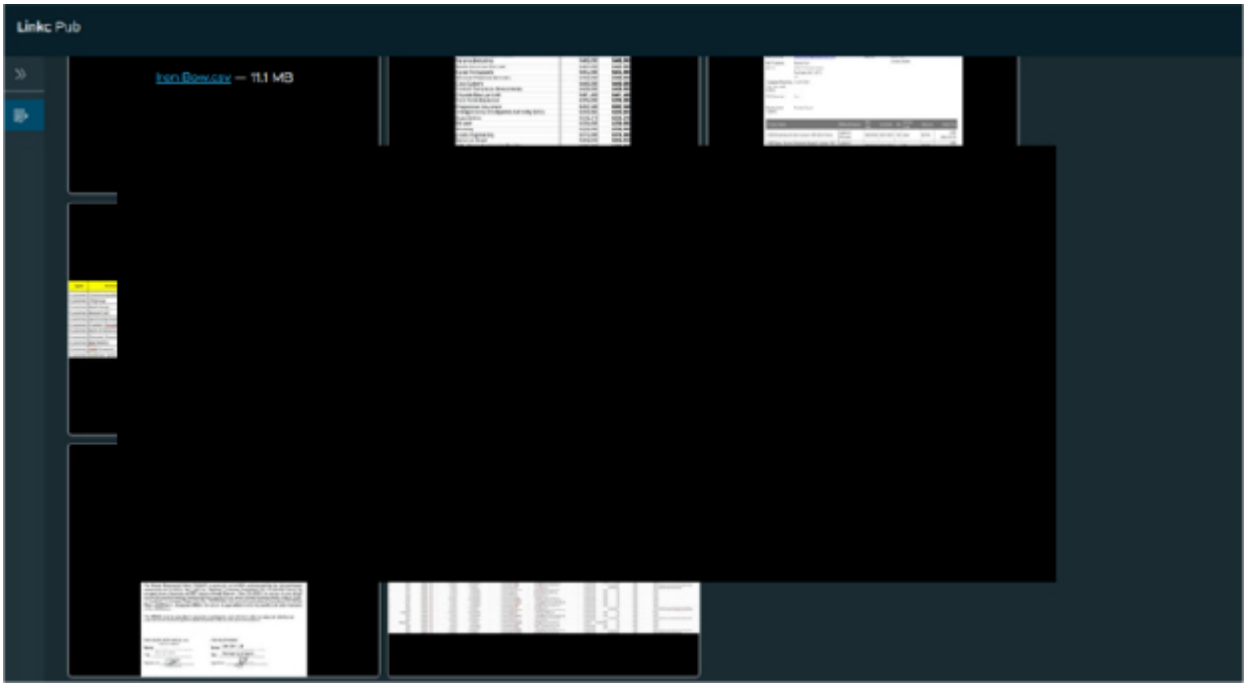
Anubis

Anubis, a new Ransomware-as-a-Service (RaaS) group, suspected to be active since late 2024, comprising experienced cybercriminals with an active dark web presence. The group employs a double extortion strategy and offers three affiliate programs: classic ransomware (providing an 80% share for affiliates targeting Windows, Linux, NAS, and ESXi), data ransom (monetizing stolen data with a 60/40 revenue split), and access monetization (paying brokers 50% for exclusive access in select regions). Tracked through dark web actors like 'superSonic', Anubis launched its dedicated leak site by the end of February 2025, signaling its intent to intensify ransomware operations.

Appearance of the leaksite of ransomware

Linkc Pub

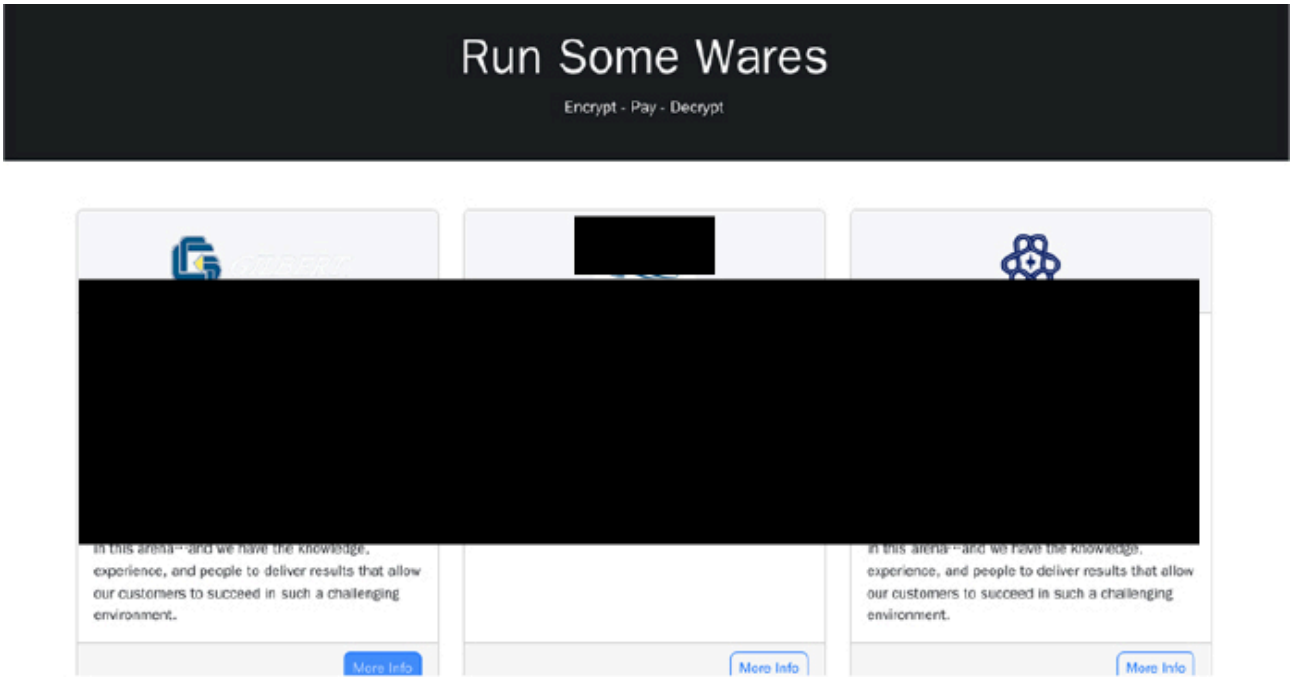
The Linkc Pub ransomware group recently emerged and launched its leak site in mid-February 2025. As of the time of this report, the group has already listed one victim, indicating the beginning of its extortion activities.



Appearance of the leaksite of ransomware

RunSomeWares

Researchers have identified a new ransomware group, RunSomeWares, which launched its leak site in late February 2025. While limited information is available about this group, its emergence poses a serious global threat, given that it has already claimed four victims upon launch. Stay tuned with our reports for more details.



Appearance of the leaksite of ransomware

KEY RANSOMWARE EVENTS IN FEBRUARY 2025

8Base dismanteled

An international law enforcement operation dismantled the 8Base ransomware group, shutting down its dark web data leak and negotiation sites. Authorities arrested four individuals in Thailand for deploying Phobos ransomware, which encrypted data across 17 firms, demanding ransom payments for decryption keys. The suspects allegedly stole approximately $16 million in cryptocurrency from around 1,000 victims worldwide.

Active since 2022, 8Base targeted small and medium-sized businesses across industries such as finance, manufacturing, and IT. In recent campaigns, Phobos ransomware was delivered via encrypted payloads instead of traditional loaders. It executed rapid encryption by fully locking files under 1.5MB and partially encrypting larger ones while storing metadata within the file. The malware scanned network shares, disabled backups, and used registry keys for persistence. It also bypassed security controls, terminated processes holding files open, and reported infections to an external URL. These techniques enhanced stealth, encryption speed, and operational efficiency.

Beware of Ghost CISA and the FBI warns

Ghost ransomware has been an active threat since early 2021, compromising victims across over 70 countries, including critical infrastructure, healthcare, government, education, and manufacturing sectors. According to a joint advisory from CISA and the FBI, the group indiscriminately exploits outdated internet-facing services, leveraging multiple ransomware variants such as Ghost.exe, Cring.exe, and ElysiumO.exe. The attackers frequently modify file extensions, ransom notes, and communication methods to evade detection.

CISA and the FBI highlight that Ghost ransomware operators exploit unpatched vulnerabilities in Fortinet (CVE-2018-13379), ColdFusion (CVE-2010-2861, CVE-2009-3960), and Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207). They deploy credential stealers, CobaltStrike beacons, and ransomware payloads using CertUtil to bypass security measures. Some of these vulnerabilities have also been exploited by state-backed threat actors.

Black Basta ransomware attack cost Southern Water £4.5M

Black Basta ransomware targeted a major UK water supplier Southern Water in February 2024, leading to a data breach and financial impact of £4.5 million ($5.7M). While the attack did not disrupt operations, the ransomware actors stole data from the company’s servers. The victim engaged cybersecurity experts and legal advisors, as well as notified affected individuals.

Leaked internal communications suggest that the attackers initially demanded $3.5 million, but the victim reportedly negotiated a lower ransom offer of $950,000. By the end of February, the victim’s listing was removed from Black Basta’s extortion site, implying a possible settlement. However, no official confirmation of a ransom payment was provided.

IVF giant Genea got hit by Termite ransomware

The Termite ransomware group has claimed responsibility for breaching a major fertility services provider Genea in Australia, exfiltrating 940.7GB of sensitive data. The attack began on January 31, 2025, through a Citrix server, allowing access to critical systems, including patient management, domain controllers, and backup infrastructure. Two weeks later, the attackers transferred the stolen data to a cloud server under their control. The compromised records include personally identifiable information, medical histories, insurance details, and diagnostic test results.

The victim has obtained a court order to prevent further distribution of the leaked data and is working with cybersecurity authorities on the investigation. Termite operators later leaked portions of the stolen data on their dark web portal, showcasing identification documents and patient files. This ransomware group, active since October 2024, leverages a Babuk-based encryptor, conducts data theft, and engages in extortion. Their encryptor has exhibited execution flaws, suggesting ongoing development. The incident underscores the growing risks to healthcare data security.

BUSINESS IMPACT ANALYSIS

Based on available public reports approximately 31% of enterprises are compelled to halt their operations, either temporarily or permanently, in the aftermath of a ransomware onslaught. The ripple effects extend beyond operational disruptions, as detailed by additional metrics:

- A significant 40% of affected organizations are forced into downsizing their workforce due to the financial strain caused by the attack.
- The aftermath sees 35% of businesses experiencing turnover at the executive level, with C-suite members stepping down in the wake of the security breach.
- The financial toll of cyber incidents is staggering, with the average cost burden to companies, irrespective of their size, estimated at around $200,000. This figure underscores the substantial economic impact of cyber threats.
- Alarmingly, 75% of small to medium-sized enterprises (SMEs) face existential threats, admitting the likelihood of closure should cybercriminals extort them for ransom to avoid malware infection.
- The long-term viability of these entities is also in jeopardy, with 60% of small businesses shutting down within six months post-attack, highlighting the enduring impact of such security breaches.
- Even in instances where ransoms are not conceded to, organizations bear significant financial weight in their recovery and remediation endeavors to restore normality and secure their systems.

EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Impact Assessment

Ransomware remains a severe threat to both organizations and individuals, encrypting critical data and demanding payment for decryption. Beyond financial extortion, these attacks impose heavy costs through recovery efforts, operational disruptions, and cybersecurity reinforcements. Victims often face reputational damage, regulatory fines, and market instability, eroding consumer confidence. To protect financial stability and public trust, businesses and governments must prioritize proactive cybersecurity strategies to mitigate ransomware risks effectively.

Victimology

Cybercriminals are intensifying attacks on businesses that manage vast amounts of sensitive data, including personal information, financial records, and intellectual property. Industries like manufacturing, real estate, healthcare, FMCG, e-commerce, finance, and technology are prime targets due to their extensive data assets. Attackers focus on nations with strong economies and advanced digital infrastructures, exploiting vulnerabilities to encrypt critical data and demand high ransoms, aiming to maximize financial gains through calculated and sophisticated tactics.

CONCLUSION

The escalation in ransomware activity in February 2025 highlights the increasing complexity and aggression of cybercriminals. The emergence of state-backed ransomware operations and the weaponization of zero-day vulnerabilities signal a critical need for stronger defenses. Organizations must adopt proactive threat intelligence, robust incident response frameworks, and enhanced cybersecurity measures to counter evolving threats. As ransomware tactics continue to evolve, staying ahead of adversaries through continuous security improvements will be imperative.

STRATEGIC RECOMMENDATIONS:

1. Strengthen cybersecurity measures: invest in robust cybersecurity solutions, including advanced threat detection and prevention tools, to proactively defend against evolving ransomware threats.
2. Employee training and awareness: conduct regular cybersecurity training for employees to educate them about phishing, social engineering, and safe online practices to minimize the risk of ransomware infections.
3. Incident response planning: develop and regularly update a comprehensive incident response plan to ensure a swift and effective response in case of a ransomware attack, reducing the potential impact and downtime.

MANAGEMENT RECOMMENDATIONS:

1. Cyber Insurance: Evaluate and consider cyber insurance policies that cover ransomware incidents to mitigate financial losses and protect the organization against potential extortion demands.
2. Security audits: conduct periodic security audits and assessments to identify and address potential weaknesses in the organization’s infrastructure and processes.
3. Security governance: establish a strong security governance framework that ensures accountability and clear responsibilities for cybersecurity across the organization.

TACTICAL RECOMMENDATIONS:

1. Patch management: regularly update software and systems with the latest security patches to mitigate vulnerabilities that threat actors may exploit.
2. Network segmentation: implement network segmentation to limit lateral movement of ransomware within the network, isolating critical assets from potential infections.
3. Multi-Factor authentication (MFA): enable MFA for all privileged accounts and critical systems to add an extra layer of security against unauthorized access.
