TRACKING RANSOMWARE : JANUARY 2025

cyfirma.com/research/tracking-ransomware-january-2025/

Published On : 2025-02-10

EXECUTIVE SUMMARY

January 2025 saw consistent ransomware incidents, with 510 reported victims globally. Akira led the landscape, while new groups like MORPHEUS and Gd Lockersec emerged. The Manufacturing sector remained the primary target, with Finance and IT also heavily impacted. The USA remained the most targeted region. This report explores key ransomware trends, highlighting the growing sophistication of threat actors and their increasing focus on regions across the globe, emphasizing the need for stronger cybersecurity measures.

INTRODUCTION

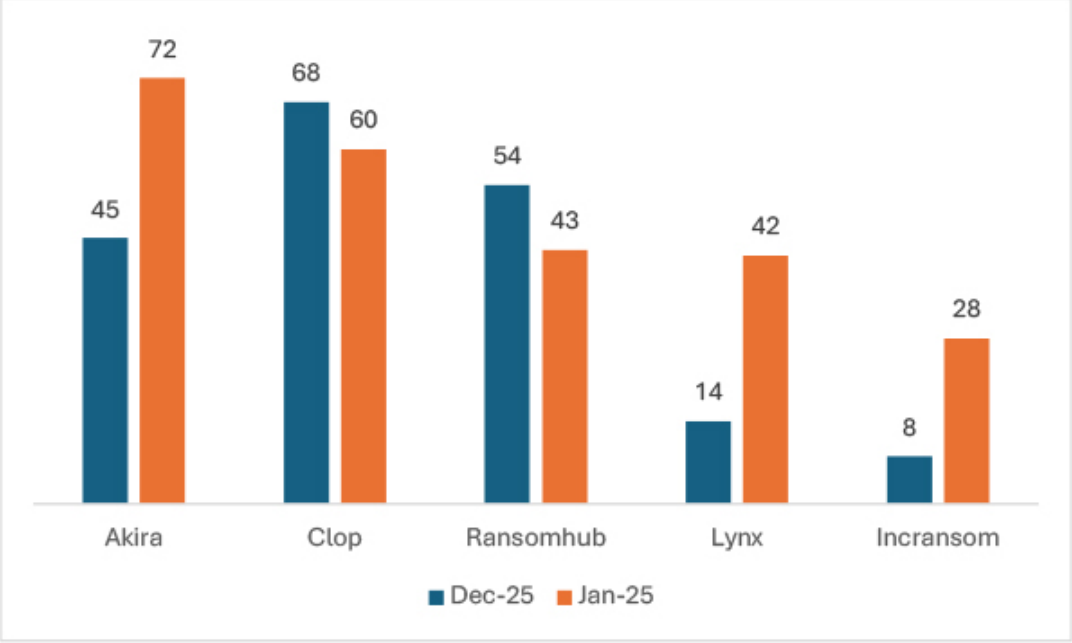
The ransomware landscape in January 2025 showed a slight decline, yet the frequency and complexity of attacks remained consistent. This report provides a comprehensive analysis of ransomware activity, comparing trends from previous months. It highlights the most affected industries, regions, and the emergence of new ransomware groups. Additionally, the report examines the evolving tactics of prominent threat actors, including Python-based malware deployments and VMware ESXi exploitation, offering insights into the shifting cyber threat landscape.

KEY POINTS

- In January 2025, the Akira ransomware group emerged as a significant threat, with a victim count of 72.
- The Manufacturing sector is the primary target of ransomware attacks experiencing 75 incidents globally in January 2025.
- The USA was the most targeted geography in January 2025.
- MORPHEUS and Gd Lockersec emerged as new threats in the ransomware landscape.

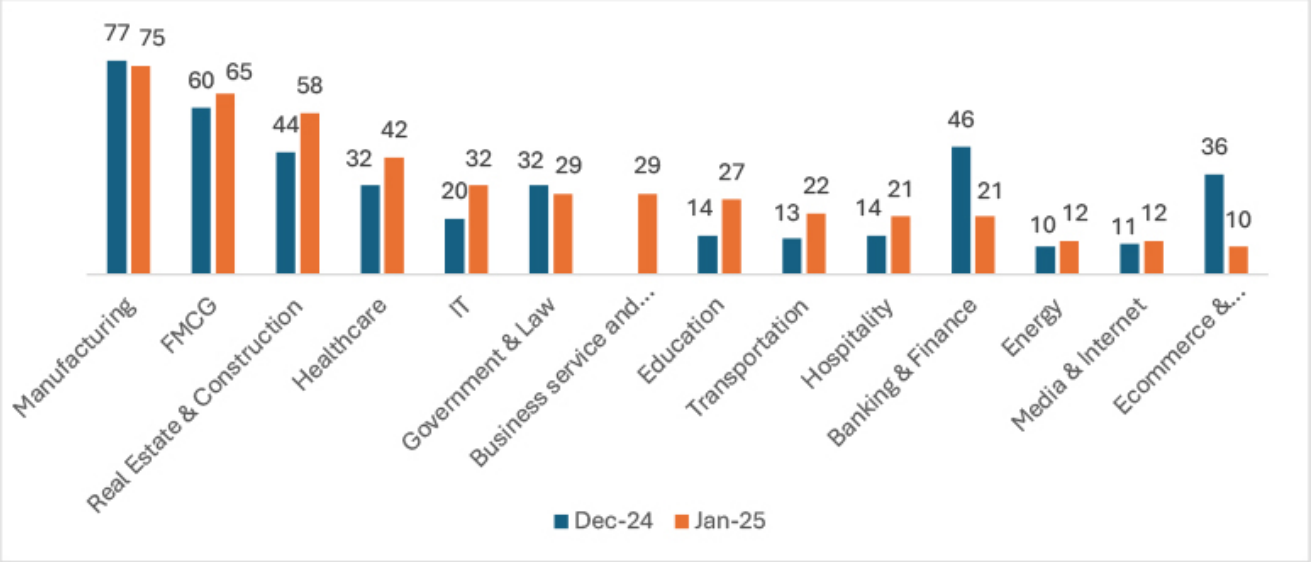
TREND COMPARISON OF JANUARY 2025's TOP 5 RANSOMWARE GROUPS.

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



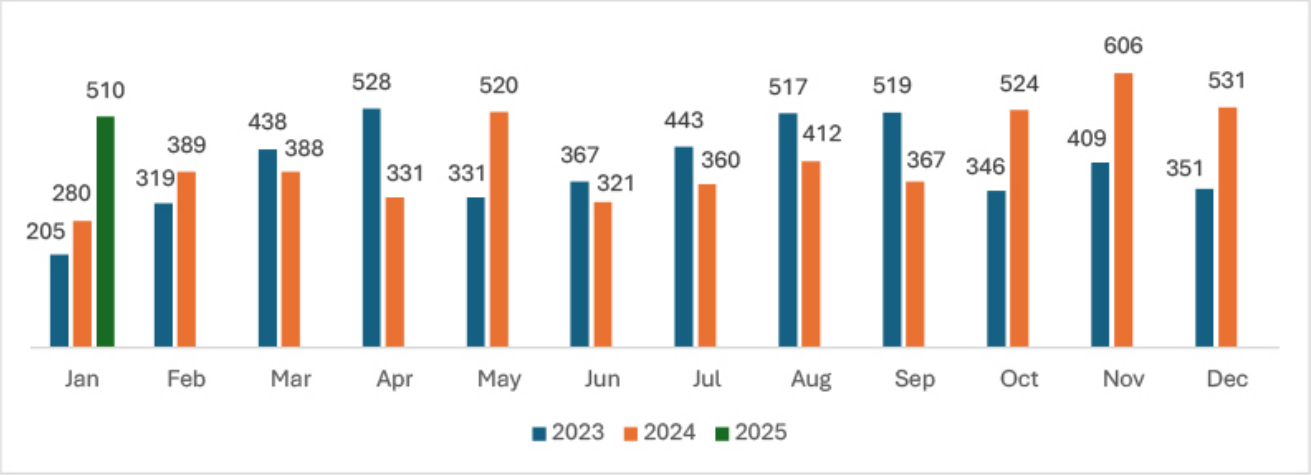
In January 2025, Akira's activity surged by 60%, while Lynx and Incransom saw sharp increases of 200% and 250%, respectively. In contrast, Cl0p experienced a 12% decline, and RansomHub dropped by 20%. These trends highlight the evolving ransomware landscape and the shifting focus of threat actors across industries.

INDUSTRIES TARGETED IN JANUARY 2025 COMPARED WITH DECEMBER 2024



The graph highlights shifting ransomware trends across industries in January 2025 compared to December 2024. IT surged by 60%, driven by its critical data and supply chain access. Healthcare rose by 31.25%, reflecting increased targeting of sensitive medical data. Government & Law saw a 9% downfall, while Education and Transportation spiked by 93% and 69%, respectively, due to their expanding digital footprints. FMCG and Hospitality saw marginal increases of 8% and 5%, respectively. Conversely, Banking & finance dropped by 54%, and Manufacturing declined slightly by 2.6%. These trends highlight the evolving threat landscape, necessitating robust cybersecurity strategies across all sectors.

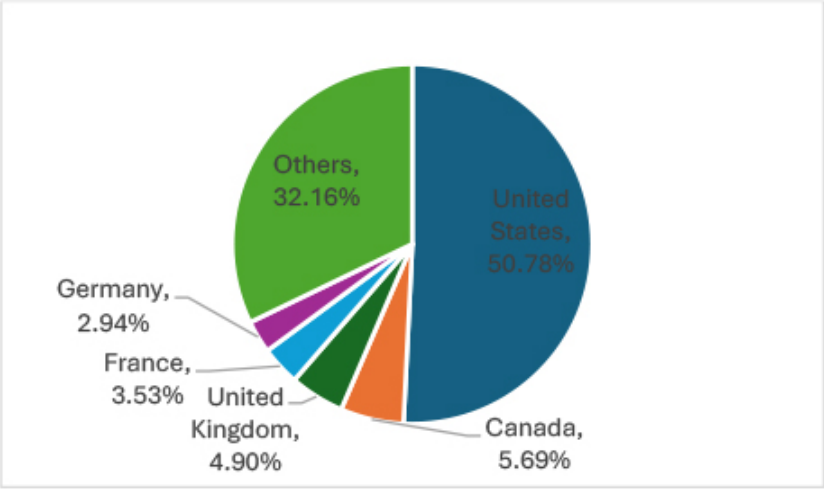
TREND COMPARISON OF RANSOMWARE ATTACKS



January 2025 experienced a 3.95% decline in victims when compared to December 2024.

However, the long-term trend remains alarming. January victims rose from 205 in 2023 to 280 in 2024, then surged to 510 in 2025 – an 82.14% increase in a year. This sharp rise highlights ransomware's growing impact, fueled by evolving tactics, expanded attack surfaces, and heightened targeting of enterprises across critical industries.

GEOGRAPHICAL TARGETS: TOP 5 LOCATIONS



The data reveals that ransomware attacks in January 2025 were heavily concentrated in the United States (259), followed by Canada (29), the United Kingdom (25), France (18), and Germany (15). 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 GROUPS IN JANUARY 2025

Python-Based Malware Fuels RansomHub Ransomware Operations
A recent campaign has been observed utilizing a Python-based backdoor to deploy RansomHub ransomware across compromised networks. Initial access was achieved using SocGholish, a JavaScript-based malware distributed through drive-by downloads and SEO poisoning techniques. SocGholish targeted outdated WordPress SEO plugins like Yoast and Rank Math PRO for exploitation. After the initial infection, the Python backdoor was dropped within 20 minutes and propagated laterally using RDP sessions.

The Python script functions as a reverse proxy, establishing a tunnel based on the SOCKS5 protocol after a C2 handshake. It is highly obfuscated but features distinct classes, detailed method names, error handling, and verbose debugging. These characteristics indicate a sophisticated development process, potentially assisted by AI tools. The backdoor facilitates lateral movement, enabling ransomware deployment while bypassing detection.

ETLM Assessment
Ransomware campaigns will increasingly leverage Python-based backdoors for seamless network infiltration and propagation. These backdoors, combined with advanced obfuscation and lateral movement capabilities, will enable ransomware groups to exploit critical vulnerabilities in cloud infrastructure and legacy systems. This evolution signals a growing focus on targeting enterprises with complex network environments for maximum impact.

Ransomware groups stealthily infiltrate VMware ESXi using SSH tunnels.
Ransomware actors are increasingly targeting VMware ESXi bare-metal hypervisors due to their critical role in virtualized infrastructures, hosting multiple virtual machines on a single physical server.

These appliances are often unmonitored, making them ideal targets for attackers to establish persistence, exfiltrate data, encrypt files, and cripple an organization's operations by rendering virtual machines inaccessible.

A common technique involves abusing ESXi's built-in SSH service, intended for administrative management, to establish stealthy persistence. Threat actors compromise these systems using either administrative credentials or by exploiting known vulnerabilities. Once access is gained, SSH tunneling is configured to create a SOCKS connection to the attackers' command-and-control (C2) server. This allows the attackers to move laterally, deploy ransomware payloads, and maintain a persistent backdoor. The resilience of ESXi appliances, which are rarely shut down, further enhances the stealth of this approach.

Monitoring and detecting these attacks are challenging due to ESXi's distributed logging mechanism, where logs are separated into multiple files instead of a consolidated syslog. Critical logs include /var/log/shell.log (command execution), /var/log/hostd.log (administrative activities), /var/log/auth.log (authentication events), and /var/log/vobd.log (system and security events). Threat actors often manipulate or clear these logs to hide traces of their activity.

ETLM Assessment
Ransomware actors will likely continue exploiting VMware ESXi hypervisors due to their critical role in virtualized environments and limited monitoring. Threat actors may integrate advanced tunneling techniques, log manipulation tactics, and automated persistence mechanisms, emphasizing the need for proactive defenses, centralized logging, and robust access controls to mitigate emerging threats.

Experts discover a shared codebase between Morpheus and HellCat ransomware.
The HellCat and Morpheus ransomware operations, which emerged in October and December 2024, respectively, are employing an identical payload code, suggesting shared development resources or a common builder application. Both ransomware strains utilize 64-bit executable payloads requiring a specified input path. They exclude the \Windows\System32 folder and file extensions like .dll, .sys, .exe, .drv, .com, and .cat from encryption, showcasing targeted file exclusion techniques.

An unusual feature is that neither ransomware alters the extensions or metadata of encrypted files. While the file contents are encrypted, the original filenames and extensions remain intact. Encryption is performed using the Windows Cryptographic API, relying on the BCrypt algorithm for key generation and file encryption.

The ransom notes dropped by both operations share structural similarities, resembling templates used by earlier ransomware schemes, though the payloads differ functionally. Unlike many ransomware families, HellCat and Morpheus do not modify system settings, such as desktop wallpaper, or establish persistence mechanisms on infected systems, focusing solely on encryption and extortion.

ETLM Assessment
The rise of shared ransomware codebases and decentralized affiliate models signals a shift toward more efficient and widespread operations in 2025. Emerging groups like Morpheus and HellCat may drive innovation in stealthy encryption techniques, targeting high-value enterprises. Increased competition among threat actors could also lead to faster adoption of advanced evasion and encryption methods.

TRIPLESTRENGTH targets cloud for cryptojacking and on-premises infrastructures
A financially motivated threat actor, dubbed TRIPLESTRENGTH, has been identified targeting cloud environments and on-premises infrastructures for cryptojacking, ransomware, and extortion. This group leverages a combination of stolen credentials, cookies, and information stealer logs to gain unauthorized access to cloud instances from platforms like Google Cloud, AWS, and Microsoft Azure. Once access is achieved, hijacked environments are exploited to deploy cryptocurrency mining operations using the unMiner application and unMineable mining pools, optimized for CPU and GPU mining.

TRIPLESTRENGTH further escalates by utilizing privileged accounts to add attacker-controlled billing contacts to victim cloud projects, enabling large-scale mining. While cryptojacking targets cloud resources, its ransomware activities focus on on-premises systems, using lockers such as Phobos, LokiLocker, and RCRU64. These operations involve lateral movement, antivirus evasion, and mass encryption on targeted hosts.

The group also advertises access to compromised servers and promotes RCRU64 ransomware-as-a-service on Telegram, actively seeking collaborators for ransomware and extortion campaigns. Observed attacks highlight vulnerabilities in remote access services, which are exploited for initial access, often bypassing security mechanisms like MFA.

ETLM Assessment
TRIPLESTRENGTH and other threat actors are likely to refine their ransomware arsenal, shifting focus toward hybrid cloud environments to exploit their critical role in enterprise operations. Expect advanced ransomware payloads targeting high-value on-premise systems and cloud platforms, with increased use of RaaS models and partnerships to scale extortion campaigns globally.

Ransomware groups impersonate I.T. support in Teams' phishing schemes.
In recent days, ransomware operators have been leveraging email bombing and impersonation in Microsoft Teams calls to infiltrate corporate networks. This tactic was first observed in attacks attributed to Black Basta ransomware. Recent findings reveal similar methods being used by groups that researchers called STAC5143 and STAC5777.

STAC5143 initiated attacks by overwhelming targets with spam emails – 3,000 messages within 45 minutes – followed by external Teams calls from accounts like "Help Desk Manager." Victims were tricked into granting remote access, allowing the attackers to deploy a Java archive (MailQueue-Handler.jar) and RPivot malware. RPivot, previously linked to FIN7 operations, established encrypted command-and-control communication. Although the obfuscation techniques suggest ties to FIN7, the public availability of the tools complicates attribution.

More recent activity from STAC5777 involved similar tactics but used Microsoft Quick Assist for direct access. The group deployed malware that logged keystrokes, harvested credentials, and scanned networks. Evidence suggests STAC5777 attempted to deploy Black Basta ransomware, highlighting potential collaboration or overlap between the groups. These findings demonstrate the evolution of ransomware tactics, emphasizing sophisticated social engineering and tool integration.

ETLM Assessment
Ransomware groups will increasingly adopt these advanced tactics, exploiting collaboration tools like Microsoft Teams. Inspired by methods used by Black Basta, and others, future campaigns will likely

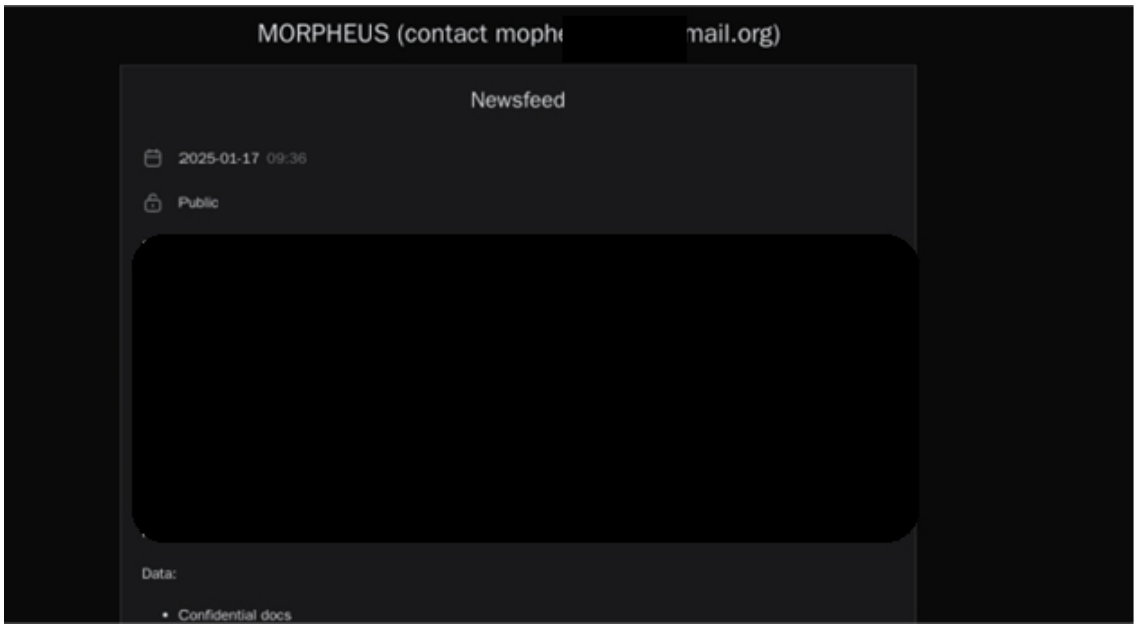
target critical industries with refined approaches to maximize impact.

Ransomware exploits AWS feature and encrypts S3 buckets for ransom demands.
The ransomware campaign by Codefinger targets Amazon S3 buckets by exploiting compromised AWS credentials with ‘s3:GetObject’ and ‘s3:PutObject’ privileges. The attackers use AWS’s Server-Side Encryption with Customer Provided Keys (SSE-C) to encrypt data, generating a custom AES-256 key locally that is unknown to the victim. Since AWS does not store these keys, decryption is impossible without the attacker’s cooperation. Ransom notes are placed in affected directories, demanding Bitcoin payments for the decryption key, while a seven-day file deletion policy is enforced via the S3 Object Lifecycle Management API. Victims are warned against altering account permissions, as doing so results in negotiation termination. The attack leverages AWS’s native services and achieves encryption in a way that is both secure and unrecoverable without their cooperation.

ETLM Assessment
The success of Codefinger’s tactics may encourage more ransomware groups to adopt cloud-native encryption techniques, making data recovery nearly impossible without paying ransom. Future attacks could expand beyond S3 to other cloud storage services, exploiting misconfigured IAM policies and automation tools and increasing the risk of large-scale, undetectable ransomware operations.

EMERGING GROUPS

MORPHEUS
Researchers have identified a new ransomware named Morpheus, this ransomware has potentially been active since the end of December 2024 but only published victims – on a data leak site – since January 2025. By the time of writing this report, the group has claimed 3 victims.

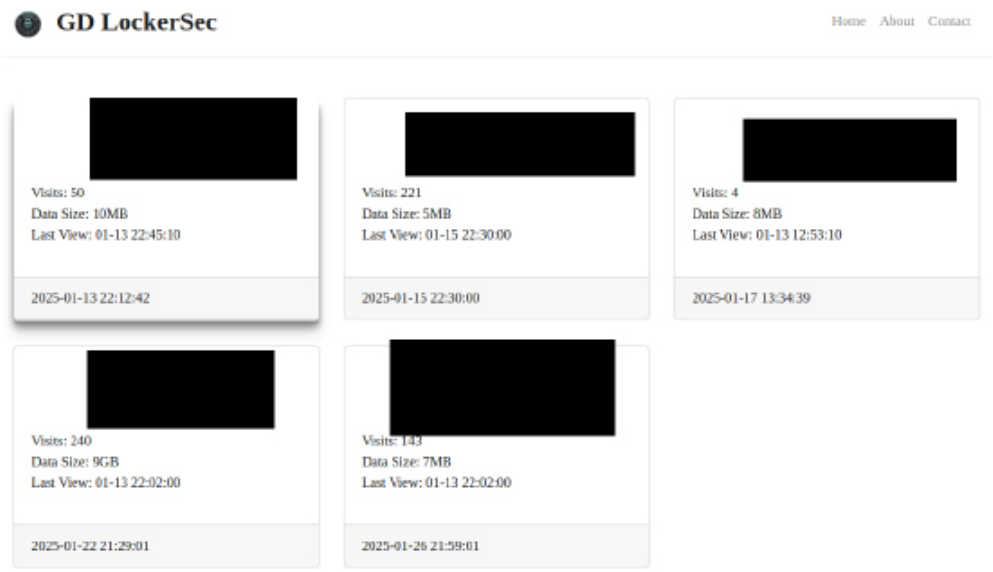


Appearance of the Onion site (Source: Underground Forum)

Gd Lockersec

By the end of January 2025, our researchers observed the launch of a leak site by Gd Lockersec, a newly emerged ransomware group. The group describes itself as being composed of members from various countries, with a sole focus on financial gains. They have outlined specific restrictions, including prohibiting attacks on entities based in CIS countries, Cuba, North Korea, and China. Additionally, Gd Lockersec does not target non-profit hospitals or certain non-profit organizations. They also emphasize that companies that already paid a ransom are exempt from re-attacks.

During the drafting of this report, the group has claimed 5 victims.



Appearance of the Onion site (Source: Underground Forum)

KEY RANSOMWARE EVENTS IN JANUARY 2025

Rhode Island's RIBridges stolen data leaks

The Brain Cipher ransomware gang has initiated the release of data stolen from Rhode Island's RIBridges social services platform, impacting approximately 650,000 individuals. RIBridges, an integrated eligibility system for managing state social assistance programs, was compromised in an attack first detected on December 5, 2024. Confirmation of data theft occurred on December 10, based on evidence provided by the attackers. Malicious code was identified on December 13, prompting the platform's shutdown for remediation.

The leaked data includes personally identifiable information (PII) of adults and minors, such as names, addresses, Social Security numbers, and banking details. The group used an encryptor based on the leaked LockBit 3.0 builder and operates a data leak site for extortion purposes. While the data leak site is currently offline, the Tor negotiation page remains active. Victims are advised to monitor their credit and remain vigilant against phishing scams leveraging the stolen data.

US charges cryptomixer operators for aiding ransomware gangs' activities

Recently, three operators of cryptocurrency mixing services were indicted for aiding ransomware groups and state-sponsored hackers in laundering illicit funds. These mixers facilitated the obfuscation of ransomware proceeds by mixing crypto assets and redistributing them to customer-controlled

wallets. The services, active between 2018 and 2023, were linked to the laundering of over $500 million stolen during major ransomware and hacking campaigns, including operations by North Korean groups.

One service shut down in 2022, was directly tied to laundering funds from a high-profile cryptocurrency bridge hack, while its successor continued similar operations until seized by international law enforcement in 2023. Both services were sanctioned for their role in enabling ransomware gangs and hackers to launder stolen virtual currency.

Two operators were apprehended in December 2024, while a third remains at large. This indictment underscores law enforcement's focus on dismantling financial infrastructures that enable ransomware attacks and cybercrime on a global scale.

Tata Technologies suspended some IT services following a ransomware attack.
The ransomware attack on Tata Technologies resulted in the temporary suspension of select IT services, though client delivery operations remained unaffected. The company has since restored impacted assets and is conducting a detailed investigation with cybersecurity experts. While the attacker's identity remains unknown, no major ransomware groups have claimed responsibility. It is also unclear whether data exfiltration occurred. However, ransomware incidents often involve data theft, even if encryption is prevented. Given Tata Technologies' role in automotive design, aerospace, and R&D, any potential data compromise could expose intellectual property and confidential engineering documents. This incident follows a 2022 attack on Tata Power, where exfiltrated data was leaked.

The attack highlights the ongoing threat to technology firms, particularly those involved in state projects and critical sectors. Without clear attribution, the motive remains uncertain, but data theft remains a key concern. Organizations in similar industries should reinforce cybersecurity to mitigate evolving ransomware tactics.

New York blood donation giant faces ransomware attack
The ransomware attack on the New York Blood Center (NYBC) led to operational disruptions, forcing the rescheduling of some donor appointments and blood drives. The incident was detected on January 26 after suspicious activity was observed on its IT systems. In response, NYBC engaged cybersecurity experts, took affected systems offline, and initiated containment measures. While donation services remain active, ongoing disruptions continue to impact scheduling and logistics. The attack coincided with a severe blood shortage, exacerbating supply challenges. No ransomware group has claimed responsibility, and it is unclear whether donor personal or health data was compromised.

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 poses a significant threat to both organizations and individuals by encrypting critical data and demanding payment for decryption. Beyond the ransom itself, these attacks lead to substantial financial burdens due to recovery efforts and cybersecurity measures, disrupt operations, and erode customer trust. Victims often suffer reputational damage, regulatory penalties, and market instability, further undermining consumer confidence. To safeguard financial stability and public trust, it is crucial for businesses and governments to prioritize proactive measures against ransomware threats.

Victimology

Cybercriminals are increasingly targeting businesses that handle large volumes of sensitive data, including personal information, financial records, and intellectual property. Industries such as manufacturing, real estate, healthcare, FMCG, e-commerce, finance, and technology are particularly vulnerable due to their extensive data repositories. These attackers focus on nations with strong economies and advanced digital infrastructures, exploiting vulnerabilities to encrypt critical data and demand substantial ransoms. Their goal is to maximize financial gains through sophisticated and calculated strategies.

CONCLUSION

January 2025 ransomware activities saw a small decline yet consistency, highlighting the persistent evolution of cyber threats, with increased sophistication in attack methods. Key industries, including manufacturing, healthcare, and finance, remain at heightened risk. Organizations must prioritize robust cybersecurity measures, including regular patching, employee training, and incident response planning, to mitigate risks. Strengthening defenses against ransomware is essential to safeguard operations, protect sensitive data, and ensure resilience against this escalating global cyber threat.

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 the 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.

Copyright CYFIRMA. All rights reserved.