Threat Intelligence Report

2024 Ransomware Trends and Observations

In 2024, the ransomware threat landscape was impacted by the diversification of ransomware strains, proliferation of Ransomware-as-a-Service (RaaS), and the emergence of new cyber criminal groups of varying sophistications. As depicted in Figure 1 below, 2024 saw 4,830 known ransomware incidents compared to 2,919 in 2023, an increase of 65 percent. This increase was accompanied by unprecedented ransom demands and payments, with a record-high victim payment of $75 million occurring in March 2024 and the average extortion demand exceeding $5.2 million in the first half of 2024. These statistics emphasize the continued threat posed by ransomware and the need for organizations to ensure their cybersecurity policies and procedures account for shifts in the ransomware threat landscape.

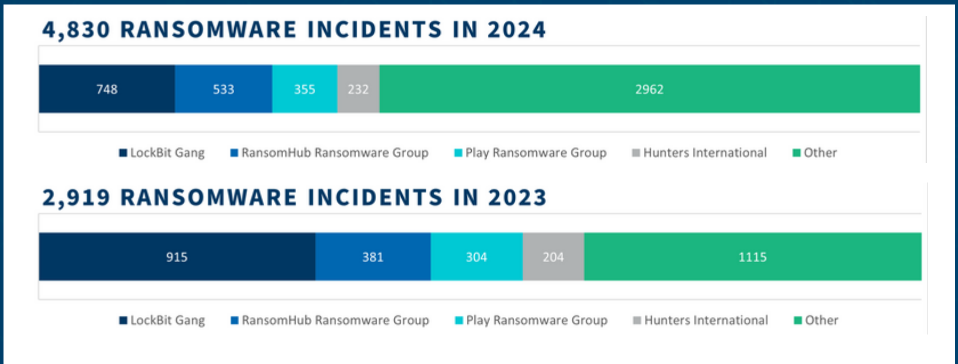

Figure 1: Ransomware Incidents per Group, 2023 and 2024.

Derived in Partnership with Recorded Future.

EMERGING GROUPS

The first quarter of 2024 saw the organized law enforcement takedown of LockBit, one of the most active ransomware groups in the world whose ransom proceeds exceeded $120 million. The takedown significantly impacted the ransomware landscape, creating opportunities for both new and existing ransomware operations to fill the void. In some instances, small ransomware groups pretended to be LockBit, using the LockBit ransomware but altering the ransom note. Despite the growing number of ransomware groups, there is limited evidence suggesting a proportionate rise in victims, possibly indicating increased fragmentation and diversification in the cyber criminal ecosystem. In fact, many of the newer ransomware groups demonstrate a lower level of maturity compared to longstanding groups. Many emerging groups have been observed using ransomware with flawed encryption algorithms, providing victims the opportunity to decrypt their data without paying a ransom.

RansomHub: First detected in February 2024, RansomHub is a RaaS group that debuted its leak site within a week of the LockBit takedown. Likely an updated and rebranded iteration of Knight ransomware, RansomHub is known for employing “big game hunting” tactics targeting large, high-value organizations. The group has quickly emerged as one of the most dominant RaaS groups in 2024. RansomHub’s rapid rise can be attributed to its aggressive RaaS model and its ability to attract affiliates from disrupted platforms, like LockBit 3.0.

Argonauts Group: Argonauts Group claimed responsibility for cyber attacks against 10 victims by late November 2024, predominantly targeting Italian technology and manufacturing organizations. The group employs double extortion tactics, both encrypting victim data and exfiltrating sensitive information to further pressure organizations into paying ransom.

Kairos: Emerging in late 2024, Kairos has already claimed at least 14 victims, with a focus on organizations in the United States. The group is reported to rely on Initial Access Brokers (IABs) to breach victim networks. Kairos has been particularly aggressive in its pressure tactics, exerting significant pressure on victims to pay ransom demands by threatening to notify stakeholders and emphasizing potential legal, financial, and reputational consequences if ransoms are not paid.

FunkSec: Presenting itself as a new RaaS operation, FunkSec claimed more than 80 victims in December 2024 alone, reportedly demanding relatively low ransoms and possibly being linked to hacktivist campaigns. Their operations appear to be supported by Artificial Intelligence (AI) and conducted by inexperienced actors suspected to be using recycled leaked information from previous hacktivist-related breaches.

TARGETED INDUSTRIES AND REGIONS

Ransomware actors have increasingly focused on industries with a low tolerance for downtime in operations, leading to a rise in attacks on critical sectors. As depicted in Figure 2 below, the most heavily targeted industries in 2024 included finance, healthcare, manufacturing, and critical industrial infrastructure like energy, oil, and gas. Meanwhile, attacks on the education sector declined between 2023 and 2024, likely due to limited ability to pay ransoms. Similarly, state and local governments saw a significant decline in ransomware incidents, while attacks on central governments increased. The disparity between federal and local governments is likely due to the increase in political attacks targeting the federal government coupled with state governments' limited ability to pay ransoms.

In terms of number of attacks, the United States, Canada, and the United Kingdom were the top three countries impacted by ransomware in 2024, though attacks on U.S. entities far outpaced those on U.K. or Canadian organizations. These three countries also reported the highest number of attacks in 2023, indicating there has been little change in the global distribution of ransomware attacks in the past year.

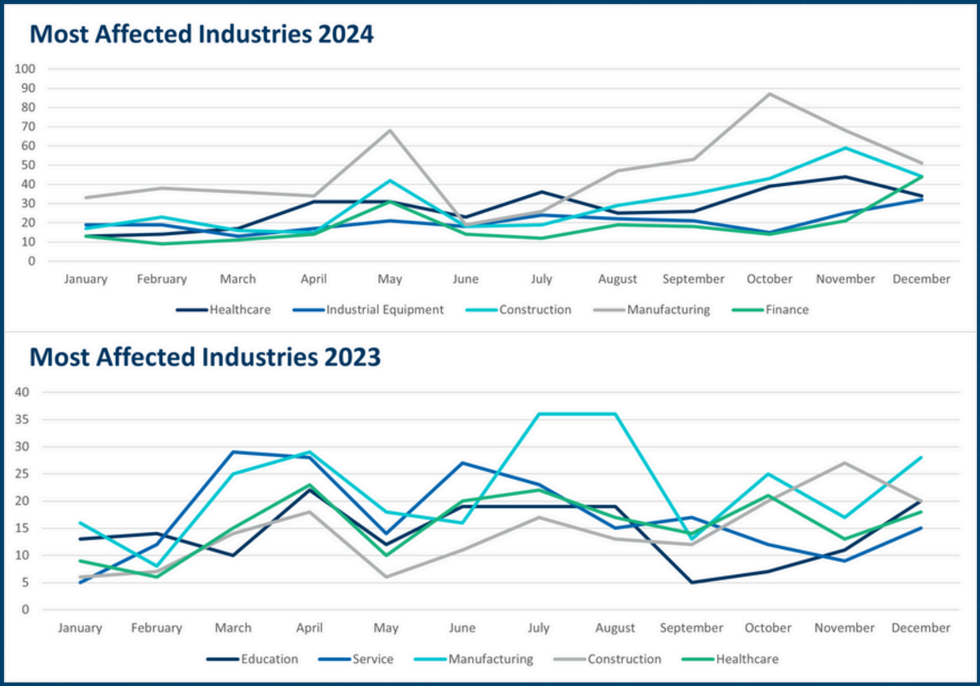

Figure 2: *Most Affected Industries, 2023 and 2024*

Derived in Partnership with Recorded Future.

EVOLVING TACTICS AND TECHNIQUES

Increased Data Theft and Creative Pressure Tactics: FTI Cybersecurity observed threat actors conducting data exfiltration and extortion in a significant number of ransomware cases in 2024. In some instances, attackers did not attempt data encryption at all, instead focusing solely on data exfiltration to remain under the radar as long as possible. Increases in data exfiltration and extortion can also be partially attributed to the adoption of improved cybersecurity and backup/recovery practices, which have reduced the urgency of decrypting ransomed data. As a result, threat actors are exploiting the risk of exposing stolen data to pressure victims into paying ransoms. As part of these new tactics, ransomware groups are weaponizing disclosure rules, financial consequences, and reputational damage by threatening to directly notify stakeholders such as employees, customers, investors, and regulators, at times even before the victim has an opportunity to report the breach themselves.

CASE STUDY

In a particularly aggressive instance, FTI Cybersecurity observed a ransomware group reaching out directly to employees and state authorities to pressure the victim into paying the ransom. The actors took additional time to analyze exfiltrated data and identify Personally Identifiable Information (PII) for VIP contacts, conducting targeted outreach to exert further pressure.

When these pressure tactics did not work, the threat actor began calling the victim daily and made threats to managing directors' physical security. Despite making every effort to pressure victims into paying a ransom for the stolen data, the threat actor can still profit from the compromise even if the victim refuses to pay, often pivoting to selling the stolen data on underground markets.

CASE STUDY

FTI Cybersecurity was engaged in late 2024 to investigate a ransomware case where the threat actor leveraged existing RMM tools and compromised accounts to stay in the organization's infrastructure for 40 days without detection. The intrusion was discovered only after the ransomware was deployed, by which time the ransomware actors had already exfiltrated sensitive data. By using remote access tools that were already part of the organization's legitimate operations, the threat actor was able to minimize their footprint and avoid detection. FTI Cybersecurity has observed malicious use of RMM tools in almost every ransomware intrusion it has investigated in the past year.

Exploitation of Zero-Day Vulnerabilities: Zero-day exploitation, particularly against network-edge devices like VPN gateways and firewalls, remote monitoring and management (RMM) tools, file transfer applications, and enterprise software, also became more pronounced in 2024. In a few high-profile incidents, ransomware actors exploited zero-day vulnerabilities to compromise victims. In December 2024, Cl0p ransomware gang claimed responsibility for exploiting a zero-day vulnerability for identified managed file transfer (MFT) products to conduct data theft attacks against more than 100 victims. Similarly, Black Basta and Bl00dy ransomware gangs were observed exploiting vulnerabilities in a widely used RMM tool to gain footholds in victim networks.

Living Off the Land (LOTL) Tactics: Threat actors engaged in more widespread use of LOTL tactics in 2024, which involve exploiting existing, legitimate software and applications that exist natively within an organization's environment to carry out attacks. LOTL attacks are more successful than traditional malware attacks because they are often not detected by traditional security tools, which only detect inherently malicious scripts or files and are reliant on indicators of compromise (IOCs) instead of indicators of attack (IOAs). These approaches to detection tend to ignore "weak signals," which may be an early indicator of an attack in progress. The rise of these tactics prompted the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) to release joint guidance on identifying and mitigating LOTL attacks. RMM tools in particular are extensively relied upon by threat actors to "live off the land" and remain undetected in a victim environment.

CONCLUSION AND OUTLOOK:

Despite improved awareness across industries regarding cybersecurity best practices, including implementation of data loss prevention protocols, least-privilege access controls, and multi-factor authentication, ransomware continues to pose a pervasive threat to organizations, with threat actors constantly finding new ways to compromise victims and increase financial payouts. FTI Cybersecurity expects the ransomware threat landscape in 2025 to be more sophisticated and disruptive than ever before. Based on trends observed in 2024, ransomware attacks are projected to reach an all-time high, with a record number of victims reported in the last quarter of 2024 alone. Ransomware groups are likely to employ a variety of tactics, including social engineering, exploitation of unpatched vulnerabilities, and brute-forcing remote access services to compromise victims. The use of artificial intelligence in cyber criminal operations is expected to increase as cyber criminals develop their own generative AI systems devoid of ethical safeguards. These could be used to generate more convincing phishing material and synthetic media, compile credentials from dark web listings, and more. The resilience of the RaaS model, despite law enforcement disruptions, suggests that ransomware will continue to be a persistent and evolving threat in 2025.

Threat actors' effective tactics for compromising, pressuring, and extorting victims underscore the importance of implementing robust security measures, including zero-trust architectures, regular system updates, and comprehensive incident response plans to better defend against ransomware attacks and minimize the impact of extortion tactics. Further, the use of LOTL techniques highlights the urgency of securing and monitoring native systems and tools, and instituting behavior-based detection systems to more effectively recognize anomalous activity.

RECOMMENDATIONS

- Limit the use of RMM software to one validated, legitimate tool. Block and monitor for the use of other non-validated RMM tools.
- Regularly test your incident response playbook (e.g., crisis exercises that test the technical, organizational, and communication aspects of a ransomware incident).
- Conduct attack surface monitoring to improve your visibility on the external perimeter.
- Conduct dark web monitoring to identify instances of leaked credentials, data, or other relevant mentions by threat actors.
- Regularly review privileged account use.
- Regularly review your detection rules to ensure they capture anomalous activity.
- Adopt an intelligence-driven approach to threat detection that leverages IOAs, monitoring specifically for unusual network activities, anomalous user behavior, and system-level changes.
- Implement detection and monitoring of weak signals to identify LOTL attacks.

SOURCES:

- U.S. and U.K. Disrupt LockBit Ransomware Variant
- 31 New Ransomware Groups Join the Ecosystem in 12 Months
- The State of Ransomware 2024
- Joint Guidance: Identifying and Mitigating Living Off the Land Techniques
- 2024 Threat Hunting Report
- Securing the Artificial Future: Trend Micro Security Predictions for 2025
- Ransomware Victims and Threat Groups Have Reached an All-Time High, GuidePoint Security Finds
- Threat Actor Groups, Including Black Basta, are Exploiting Recent ScreenConnect Vulnerabilities

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

FTI Cybersecurity Global Offices

AMERICAS

Atlanta
Boston
Chicago
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
San Francisco
São Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Düsseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm. ©2025 FTI Consulting, Inc. All rights reserved. www.fticonsulting.com

FTI CONSULTING