TRAVELERS

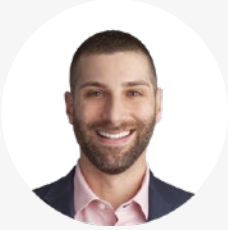
Q4 CYBER THREAT REPORT

Ransomware Goes Full Scale

2024

Table of Contents

Authors



Jason Rebholz
VP, Cyber Risk Officer
Travelers

Ryan Bell
Director, Threat Intel Cyber Risk Services
Travelers

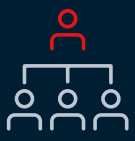
©2025 The Travelers Indemnity Company. All rights reserved.

Executive Summary

The fourth quarter of 2024 marked a pivotal period in the ransomware landscape. We saw operators continuing to move beyond their past reliance on opportunistic exploits and instead turning to a playbook (quite literally, as we cover in this report) that involves repeatable methods for their attacks, such as seeking out Virtual Private Network (VPN) accounts with weak credentials. Add into the mix that certain nation-states were actively supporting ransomware groups, and it's no surprise that attack volumes continued to surge in Q4 — in spite of the fact that major zero-day vulnerabilities were not responsible for the bulk of ransomware activity. Read on for more insights into this ever-evolving landscape.

Ransomware **leak site activity reached a new quarterly peak** with 1,663 victims posted—breaking a record that had held since Q3 2023

In 2024, 55 new ransomware groups emerged — **a 67% increase in group formation** from the previous year

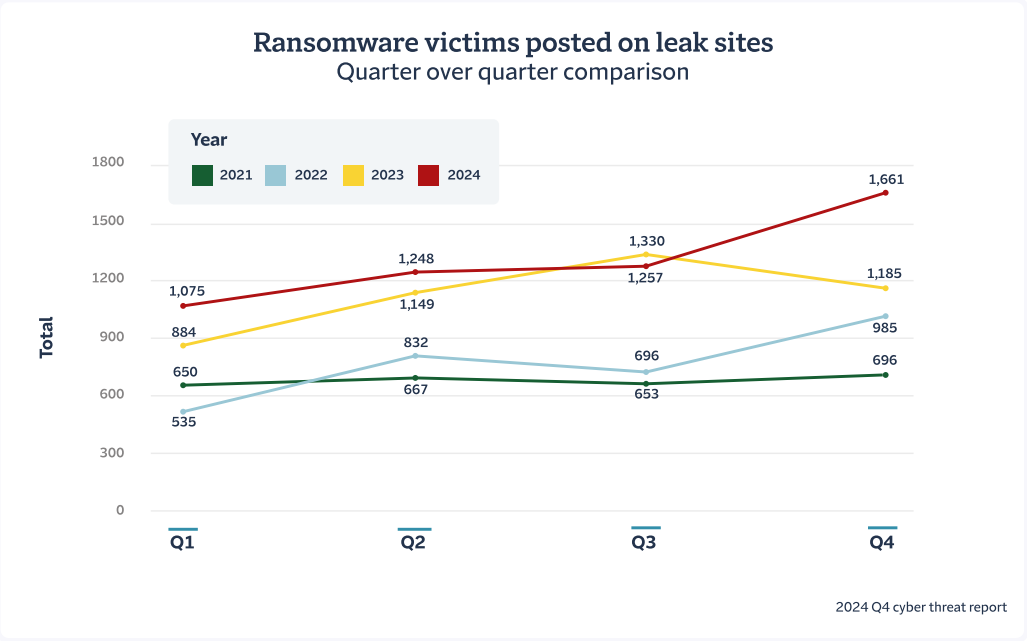


Q4 data continued to show a shift away from mass-scale vulnerability exploits and toward more repeatable methods of identifying targets, confirming 2024 as **a year of "scalability"** for ransomware groups

©2025 The Travelers Indemnity Company. All rights reserved.

Overview of Global Ransomware Activity

According to threat intelligence research conducted by Travelers, the fourth quarter of 2024 experienced the highest level of ransomware activity recorded in any single quarter to date, with a total of 1,663 known victims posted on leak sites. This represents a significant 32% increase from Q3. November was particularly notable, with 629 attacks, followed by a relative decline to 516 in December. This pattern aligns with historical trends of increased activity in the early holiday season, followed by a later decrease going into the new year. But this didn't stop Q4 from shattering prior records.



Looking at 2024 as a whole, the number of ransomware attack victims posted on leak sites reached 5,243, a 15% increase from the 4,548 incidents recorded in 2023. Globally, these attacks exposed over 195 million records according to one study, while other research estimated the total payments to ransomware groups at $813 million for the year.

©2025 The Travelers Indemnity Company. All rights reserved.

While the dollar figure is eye-popping, it actually marks a 35% decrease in revenue for ransomware from the prior year, per Chainalysis. A reasonable conclusion from the simultaneous increase in attacks and drop in revenue is that more organizations are better equipped to stand up to attackers by refusing to pay and accepting the consequences. While this marks progress of a sort in blunting financial losses from ransomware, it unfortunately does not mean an end to the costs of business disruption, IT system restoration, litigation, and regulatory fines for exposed records (in a review of 2024 claims received by Travelers, we found that attackers stole data in 87.6% of those claims, a similar rate to 2023).

These costs, and the many other ways that ransomware can menace an organization, mean that rising attack volumes point to the continued need for vigilance by all businesses. A ransomware attack is still impactful whether a ransom is paid or not.

The Year of Scalability

Clearly, with its record-breaking victim totals, 2024 was a big year for ransomware groups. Yet if you ask someone who follows cybersecurity to name a marquee vulnerability that was discovered in 2024 — something like Eternal Blue or ProxyShell — they might be hard-pressed. There simply wasn't one major discovery that drove a rash of exploits. That marks a shift.

Looking back to the previous peak of ransomware activity, the third quarter of 2023, much of the increase in ransomware leak site activity was attributed to opportunistic exploits of vulnerabilities found in common networking and software products. At that time we saw several ransomware groups pounce on major vulnerabilities and exploit as many victims as possible in a short period of time.

Contrast that style of activity with that of 2024, when we saw ransomware actors instead find reliable and repeatable methods to gain access to victim networks, such as targeting weak credentials on VPN and gateway accounts that weren't protected by multifactor authentication.

©2025 The Travelers Indemnity Company. All rights reserved.

> Rather than focusing on discovering the next zero-day vulnerability, [the leaked training playbook] advocated targeting widely-used VPNs with weak credentials to uncover opportunities

This shift had been months in the making. In the summer of 2023, a ransomware training playbook was leaked. Written by an "initial access broker" — a threat actor who specializes in gaining and selling illicit access to business systems — the manual laid out a surprising strategy. Rather than focusing on discovering the next zero-day vulnerability, it advocated targeting widely-used VPNs with weak credentials to uncover opportunities. The author instructed attackers to use a variety of tools to look for default usernames like "admin" or "test" and try combinations of common passwords. The approach has worked surprisingly well.

We started seeing claims resulting from this type of activity throughout the second half of 2023, beginning with one popular brand of VPN but expanding to include other VPNs and even other remote access technologies. Evidence suggests that in 2024 the methodology spread among initial access brokers and ransomware operators and permitted them to proactively hunt for profitable targets at an impressive scale. Gone are the days when threat actors had to play the role of scavenger, waiting for someone else to find the prey.

Nation-State Activity

When you hear "nation-state threat", you think sophisticated threat actors targeting government entities and the defense industrial base for espionage purposes. You don't think "ransomware enabler." That line is getting blurry. Security researchers have uncovered increasing connections between nation-state threat actors and criminal ransomware groups.

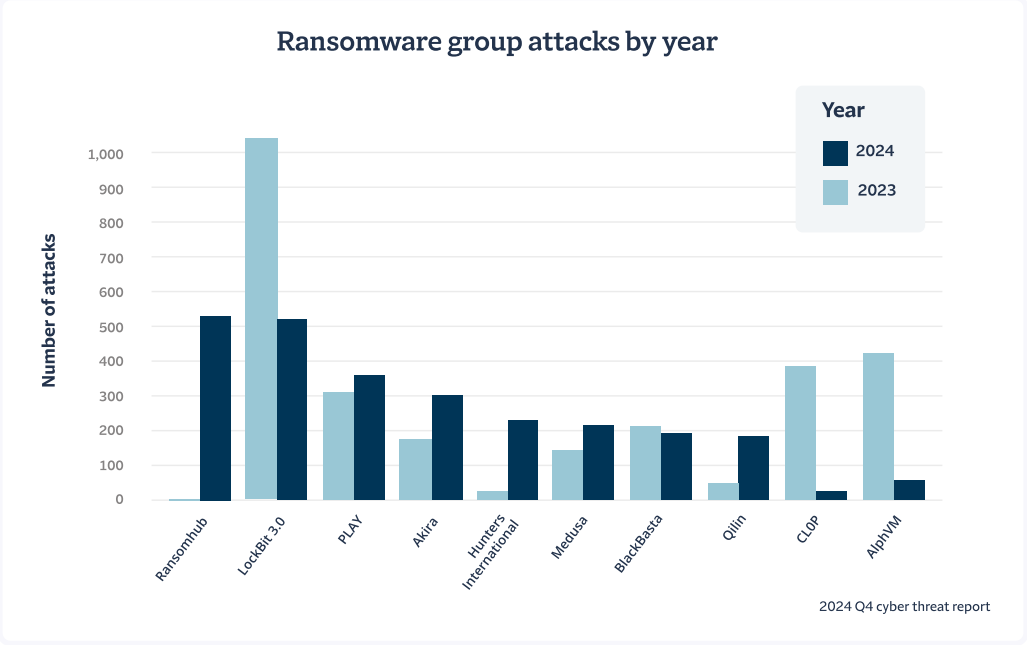
Notably, per CISA, cyber actors such as Pioneer Kitten have continued to coordinate efforts with groups like ALPHV by selling access to compromised networks or helping to carry out the encryption efforts. Additionally, recent connections have been identified between the threat actor tracked as Jumpy Pisces and the Play ransomware group. According to Unit42 researchers, Jumpy Pisces has been identified as either "acting as an initial access broker (IAB) or an affiliate of the Play ransomware group."

©2025 The Travelers Indemnity Company. All rights reserved.

These are generally well-resourced and can bring a new level of sophistication to attacks. One example of this effect is the use of AI, which has seen relatively slow adoption in ransomware attacks. Recent reports from the Google Threat Intelligence Group and from OpenAI identified numerous state-sponsored groups as users of those companies' AI tools for a variety of tasks including research, reconnaissance, and content development (such as in creating phishing campaigns).

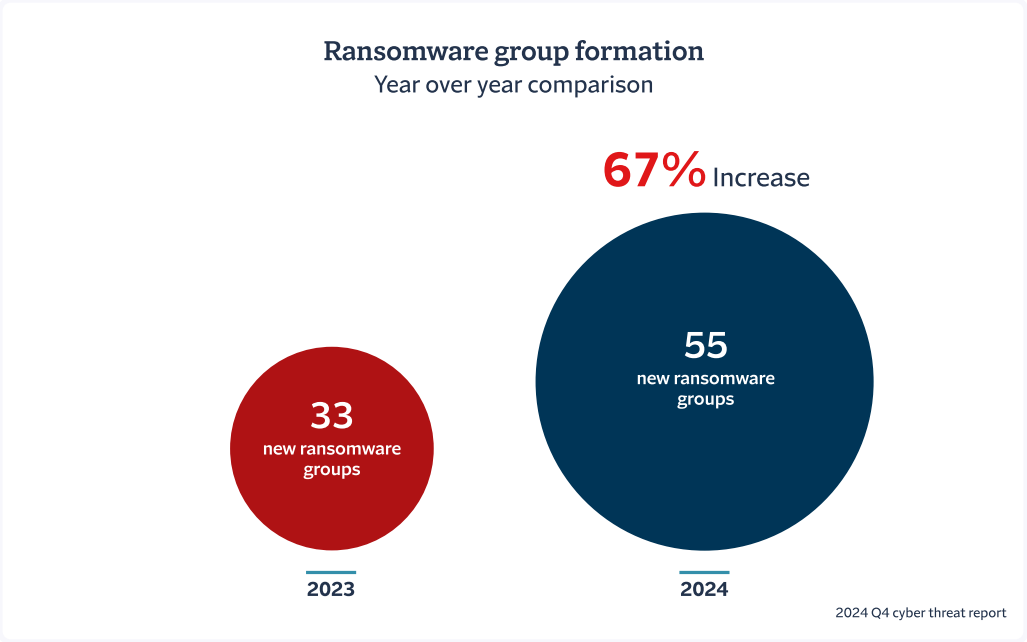
Ransomware Group Activity

Just as we had seen throughout 2024, the fourth quarter was marked by new players emerging and established groups adjusting their strategies. RansomHub continued to be a major threat, accounting for 238 attacks, or just over 14% of the quarter's total. Well-established groups like Akira and PLAY maintained a consistent presence, contributing 133 and 95 attacks, respectively, while newer threat actors like Kill Security and Fog contributed to the share of the quarter's activity.



©2025 The Travelers Indemnity Company. All rights reserved.

It's worth noting that this set of ransomware groups would have been unrecognizable to an observer from 2023. That year the leading groups were LockBit 3.0, AlphVM and CL0P. This total turnover of the primary ransomware groups can be attributed, in large part, to law enforcement disruption of several well-established Ransomware-as-a-Service (RaaS) platforms like LockBit and AlphVM, which opened the door for new operators. In 2024 alone, 55 new ransomware groups emerged — a 67% increase in group formation from the previous year — indicating a rapid proliferation of smaller, more agile players in the cybercrime ecosystem.



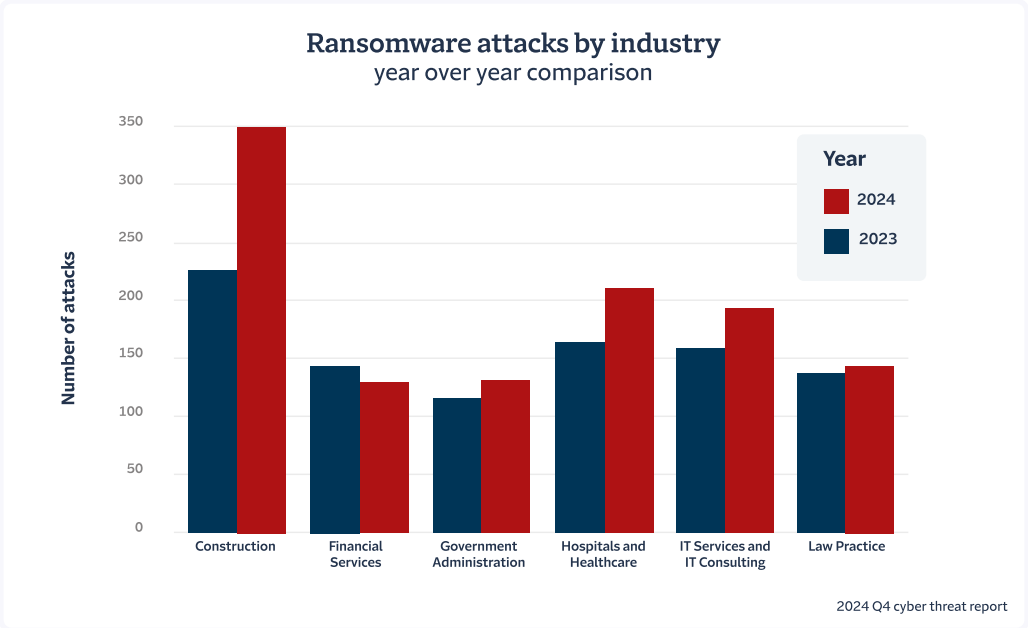
One intriguing development in Q4 was the emergence of FunkSec, a puzzling new ransomware group. Despite their aggressive presence, FunkSec has drawn attention for unusual reasons. Security researchers have raised questions about their credibility, particularly after reports suggested that FunkSec lacks the technical expertise typically seen in advanced ransomware operations. Moreover, FunkSec's claims of association with defunct hacktivist groups and their suspiciously recycled data on leak sites have led to further scrutiny. These factors have raised doubts about the group's true capabilities and objectives. Some analysts believe FunkSec may be overstating its achievements to gain notoriety or manipulate public perception, as detailed in recent research. Instead, the group appears to be relying heavily on AI tools to develop its code, a move that, somewhat surprisingly, has not been observed more often by established groups in the ransomware ecosystem.

©2025 The Travelers Indemnity Company. All rights reserved.

Industry Analysis

A trend worth noting from 2024 is the increased targeting of IT services and consulting firms. These entities often act as intermediaries for other industries, amplifying the impact of an attack through their connections to multiple clients. Government administration, while not as dominant as other sectors, experienced a surge in late 2024.

In addition to IT services and consulting firms, the construction sector remained a primary target in 2024, with 129 attacks recorded in Q4 alone, and a 56% increase in attacks year-over-year. Hospitals and healthcare organizations also faced persistent threats, with attacks rising from 166 in 2023 to 210 in 2024. Other notable targets included law practices and financial services, underscoring the broad spectrum of industries vulnerable to ransomware activity.



©2025 The Travelers Indemnity Company. All rights reserved.

Conclusion

The fourth quarter of 2024 saw an escalation in ransomware activity driven by groups that employ repeatable methods, such as targeting VPN accounts with weak credentials. This trend, coupled with the continued support of some groups by nation states, means that organizations should anticipate a future with more, not fewer, groups and attacks — in spite of some successful law enforcement activity.

Cyber Risk Control Recommendations

To mitigate these risks, organizations should adopt a strong cyber prevention program, including our Cyber Risk Control recommendations detailing the top security investments with the greatest return on investment.

These recommendations will help increase the bar required for ransomware actors to successfully carry out an attack on an organization.

They include:

- Implement phishing-resistant MFA for all remote access and email.
- Run an effective vulnerability management program to quickly patch critical vulnerabilities in edge devices, such as VPNs.
- Ensure you have reliable backups and have a resilient disaster recovery and business continuity plan
- Run EDR solutions with 24x7 active monitoring

Built for cyber.

With always-on threat intelligence, we're able to help brokers and policyholders outpace cyber attacks.

Learn More

©2025 The Travelers Indemnity Company. All rights reserved.

travelers.com

One Tower Square
Hartford, CT 06183

Travelers analysis was made possible with supporting data from eCrime.ch.

Travelers Excess and Surplus Lines Company and its property casualty insurance subsidiaries and affiliates, Hartford CT 06183

This material is for general informational purposes only and is not legal advice. It is not designed to be comprehensive and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or other professional advisor. This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

CyberRisk customers may receive certain services through external vendors and, if using these services, must agree to the vendors' terms of use and privacy policies. Travelers makes no warranty, guarantee or representation as to the accuracy or sufficiency of any such services. The use of such services and the implementation of any product or practices suggested by such vendors is at the customer's sole discretion. Travelers disclaims all warranties, express or implied. In no event will Travelers be liable in contract or in tort for any loss arising out of the use of such services or any vendor products.

© 2025 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. CP-9781 New 1-25

©2025 The Travelers Indemnity Company. All rights reserved.