# Extortion and Ransomware Trends January-March 2025

## Executive Summary

Unit 42 regularly monitors the cyberthreat landscape, including trends in extortion and ransomware. Ransomware actors continue to evolve to increase the effectiveness of their attacks and the likelihood that organizations will pay what is demanded. In our 2025 Unit 42 Global Incident Response Report, we found that 86% of incidents involved business disruption, spanning operational downtime, reputational damage or both.

In this survey of recent trends, we share qualitative observations based on incident response cases and the broader threat landscape. These include:

- Threat actors claiming compromises that can't be substantiated
- Nation-state actors working with ransomware actors
- Use of tools to disable endpoint security sensors
- Attacks on more types of systems, including cloud
- Insider threats leading to extortion

We also share insights about public reports of ransomware compromises posted on threat actors' leak sites. This includes:

- The most active ransomware leak sites
- Activity by month
- Activity by country
- Industries most affected by ransomware

Palo Alto Networks customers are better protected from ransomware threats through our Network Security solutions and Cortex line of products.

Unit 42 can help organizations proactively prepare to mitigate the threat of ransomware through our Ransomware Readiness Assessment.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

| | |
|---|---|
| **Related Unit 42 Topics** | **Ransomware**, **Cybercrime** |

# Incident Response Trends: Ransomware and Extortion Highlights

Unit 42 responds to many ransomware and extortion incidents every year.

As organizations are becoming more security-savvy, they are catching attacks in the early stages. This means we have seen a rise in investigations that stop at network intrusion, before attackers have a chance to succeed at their other objectives. However, we still see a large number of successful ransomware and extortion attacks. We have also seen threat actors becoming more aggressive to gain victims' attention and command consistent and higher payments. For more details about these observations, please see our 2025 Global Incident Response Report.

Here are some of our key recent observations of ransomware and extortion campaigns.

## Attackers Lie

Unit 42 has tracked various extortion campaigns where the attackers exaggerated threats of leaking data (often using old or fake data) to pressure victims into making payments.

In a March 2025 campaign, scammers physically mailed threatening letters to executives claiming to be a known ransomware group preparing to leak sensitive data. An example of one of the letters used in the campaign is in Figure 1.

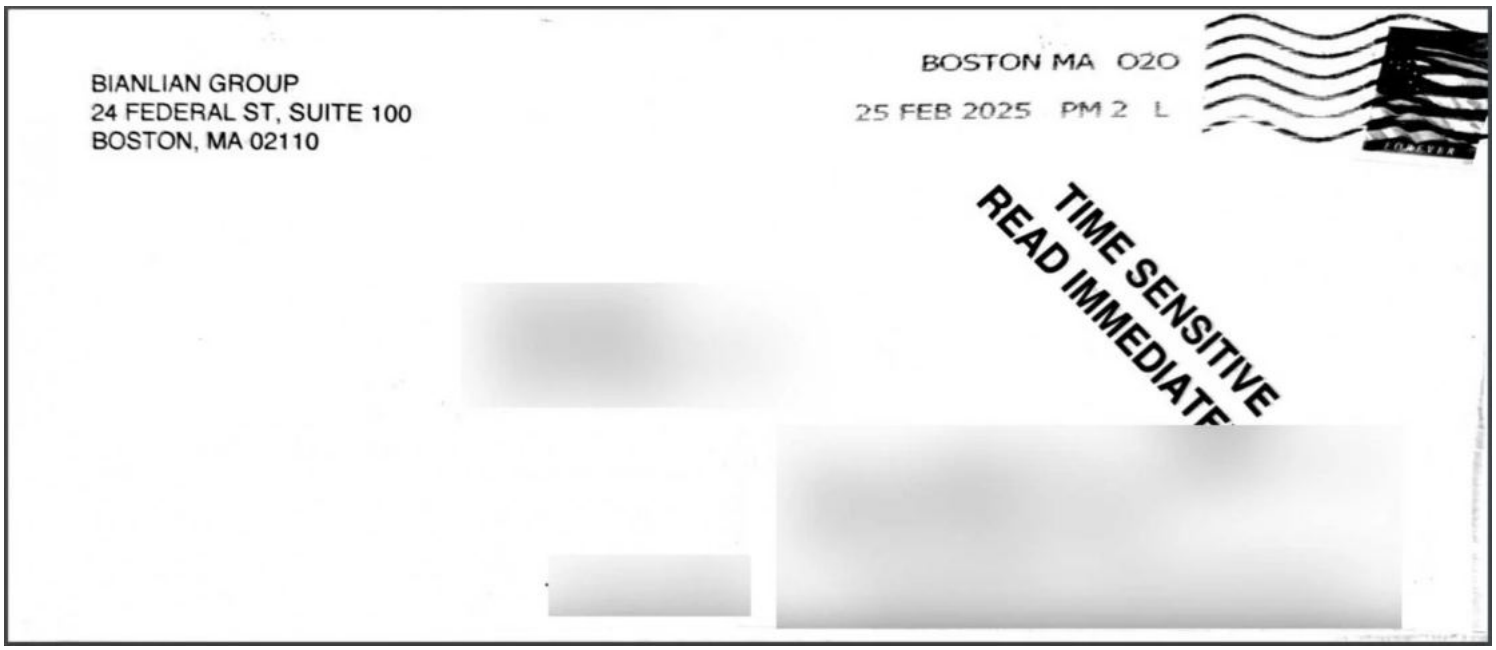

Figure 1. Envelope for fake BianLian ransom note. Source: Bleeping Computer.

However, the letters' recipients had no other evidence of a breach. These letters claimed to be the threat actor we track as Bitter Scorpius, publicly known as BianLian. However, we currently have no evidence confirming this is actually BianLian (moreover, the FBI assessed this to be a scam).

We also saw multiple cases of a threat actor posing as a rebrand of the notorious Babuk group. This threat actor used data from older, already resolved extortion campaigns to attempt to re-extort more than 60 victims.

## Nation-state Actors Are Working With Ransomware Actors

In October 2024, Unit 42 published observations of a nation-state actor directly collaborating with a ransomware group. We identified Jumpy Pisces, a North Korean state-sponsored threat group associated with the Reconnaissance General Bureau of the Korean People's Army, as a key player in a ransomware incident. This change marked our first observed instance of the group using existing ransomware infrastructure. It was potentially acting as an initial access broker (IAB) or an affiliate of Fiddling Scorpius, which distributes Play ransomware.

Since that time, we have seen additional artifacts of North Korean actors (already notorious for large money theft) continuing to cooperate with ransomware groups, signaling a new trend in the

cybercriminal threat landscape.

In March 2025, a North Korean hacking group tracked as Moonstone Sleet reportedly deployed Qilin ransomware payloads in a limited number of attacks.

## Ransomware Actors Are Using Tools to Disable Endpoint Security Sensors

Ransomware actors continue to evolve their capabilities, and we've recently observed them using tools known as "EDR killers." These tools are designed specifically to terminate defensive software, making it easier for attackers to encrypt vast amounts of data before anyone notices.

Their success has sparked interest in the affiliate community, leading to rapid adoption. The integration of these tools has become more common, making them a favored asset in an affiliate's toolkit.

In one extortion incident that Unit 42 investigated, we observed an attacker unsuccessfully attempt to use an AV/EDR bypass tool to get around Cortex XDR. In this particular case, our incident responders were able to turn the tables by using the threat actors' attempts to gain a certain level of access to their rogue systems. In the process, we gained visibility into the threat actor's tooling, targeting and persona. The attack chain from this incident is presented in Figure 2.

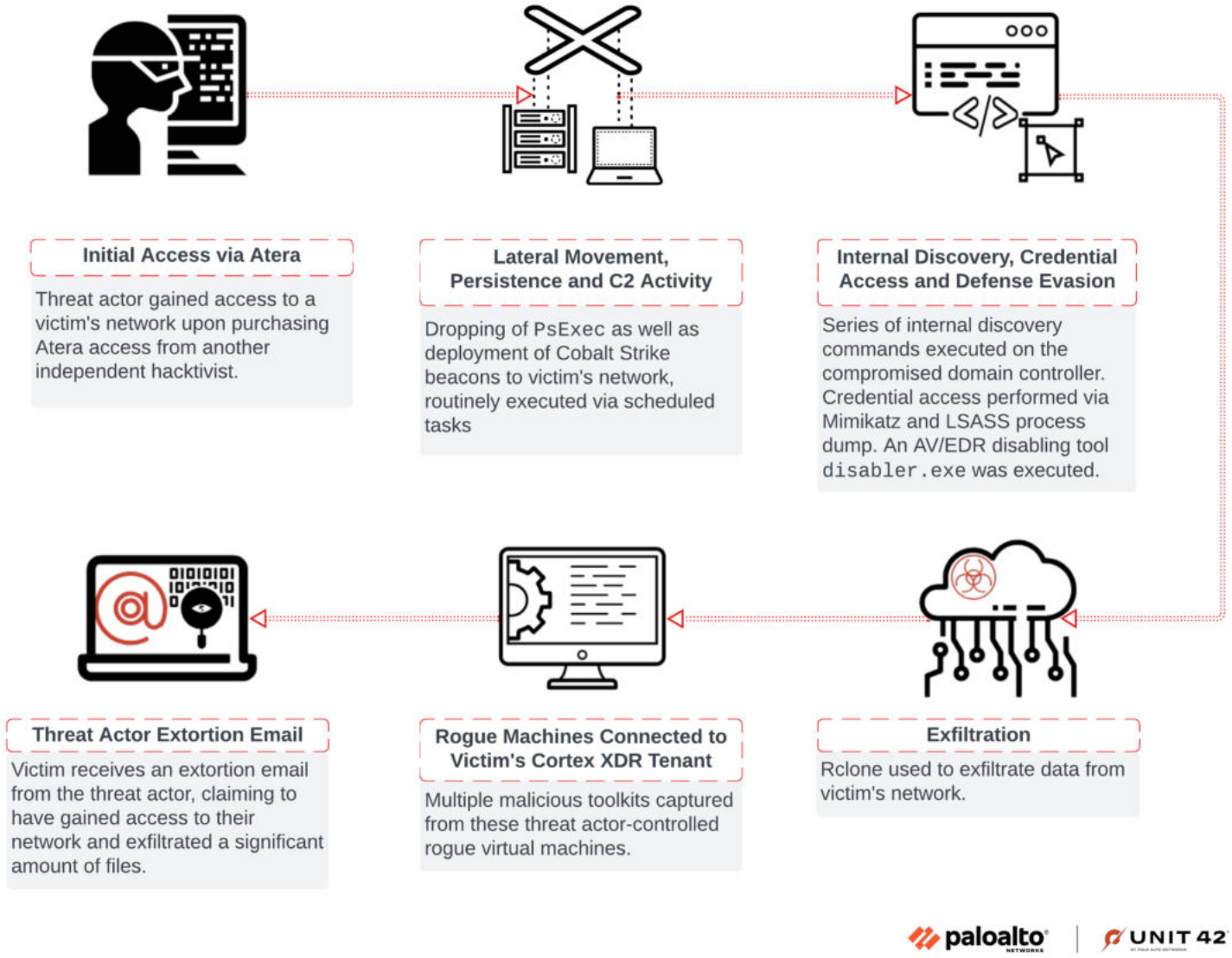


Figure 2. High-level chain of events in the attack investigated by Unit 42.

Outside of this ideal outcome, organizations should be on the lookout for EDR killers.

## Ransomware Actors Are Attacking More Types of Systems, Including Cloud

Extortion attacks continue to evolve to impact more data in victim networks. Actors are now targeting critical servers and applications, including those running on virtualized infrastructure and in the cloud.

We are also seeing more ransomware payloads that can be ported to run on more than just Windows – Linux, hypervisors (ESXi) and even macOS.

Cybercriminals such as Bling Libra (distributors of ShinyHunters ransomware) and Muddled Libra gain access to cloud environments by exploiting misconfigurations and finding exposed credentials.

## Insider Threats Can Lead to Extortion

Since 2023, Unit 42 has tracked North Korea state-sponsored threat actors who gain unauthorized remote employment with worldwide organizations. These actors often use fake AI-enhanced identities to infiltrate organizations.

Circumventing sanctions to work and gain money is one part of the scheme. Alongside that are security and legal risks, including the possibility of extortion [PDF].

After being discovered on company networks, North Korean IT workers have extorted victims by holding stolen proprietary data and code hostage until the companies meet ransom demands. In some instances, North Korean IT workers have publicly released victim companies' proprietary code. North Korean IT workers have copied company code repositories, such as GitHub, to their own user profiles and personal cloud accounts. While not uncommon among software developers, this activity represents a large-scale risk of theft of company code.

In multiple instances, the conspirators supplemented their employment earnings by stealing sensitive company information, such as proprietary source code, and then threatening to leak such information unless the employer made an extortion payment.

# Reported Ransomware Compromises: Charts and Stats

Unit 42 monitors public reports of ransomware compromises posted on threat actors' leak sites. The charts and insights below are based on our observations from January-March 2025. They cover the ransomware groups that created the highest numbers of public posts about compromises, as well as information on reported compromises by month, country and industry.

However, no collection of publicly reported compromises ever reflects all compromises. In addition, the data shared below does not reflect all leak site posts. We've included only data that has been vetted according to established analytic standards. It's also always important to note that threat actor groups may not report compromises honestly.

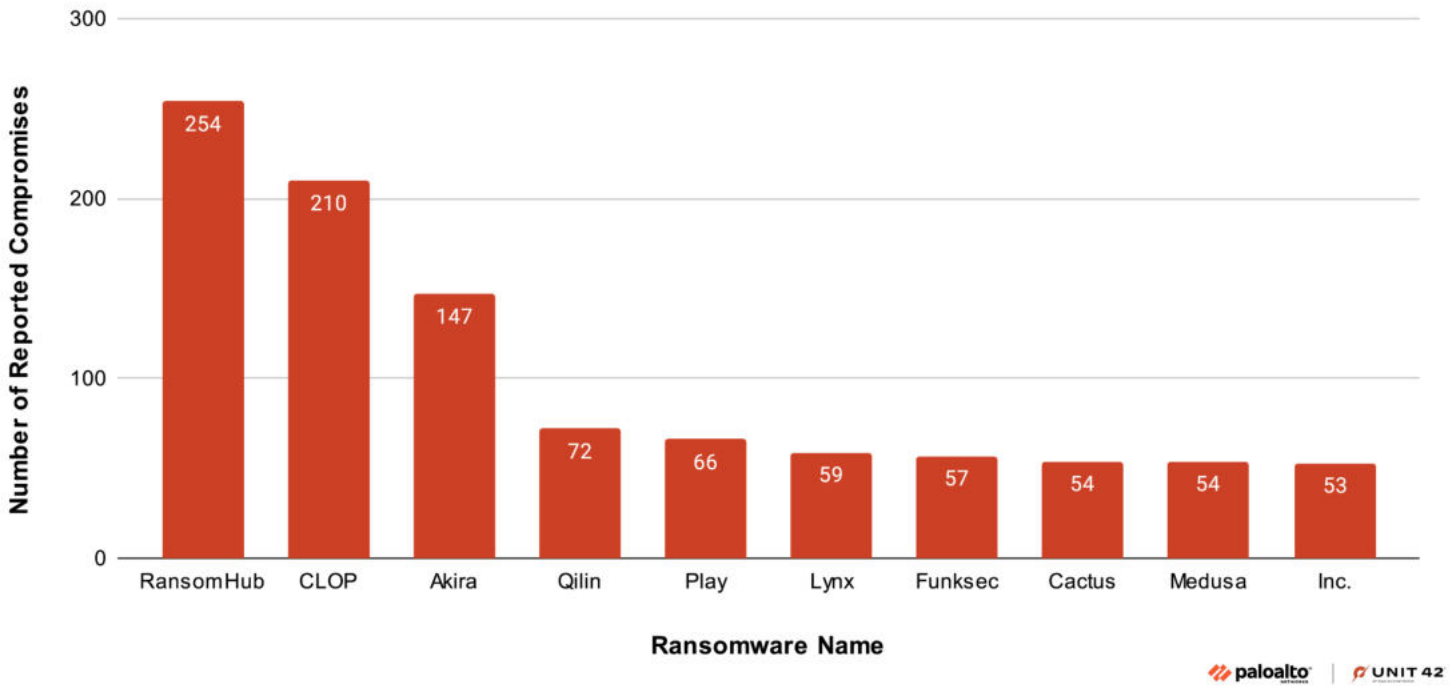


Figure 3. Most active ransomware leak sites from January-March 2025.

RansomHub is the most prolific type of ransomware among public reports on leak sites from January-March 2025, as seen in Figure 3. Unit 42 tracks the group that distributes RansomHub as Spoiled Scorpius. In our ransomware retrospective published in August 2024, we listed RansomHub as an emerging ransomware to watch. While extremely active since it started in 2024, we expect a drop in RansomHub activity during the next quarter due to operational issues this group has endured in April 2025

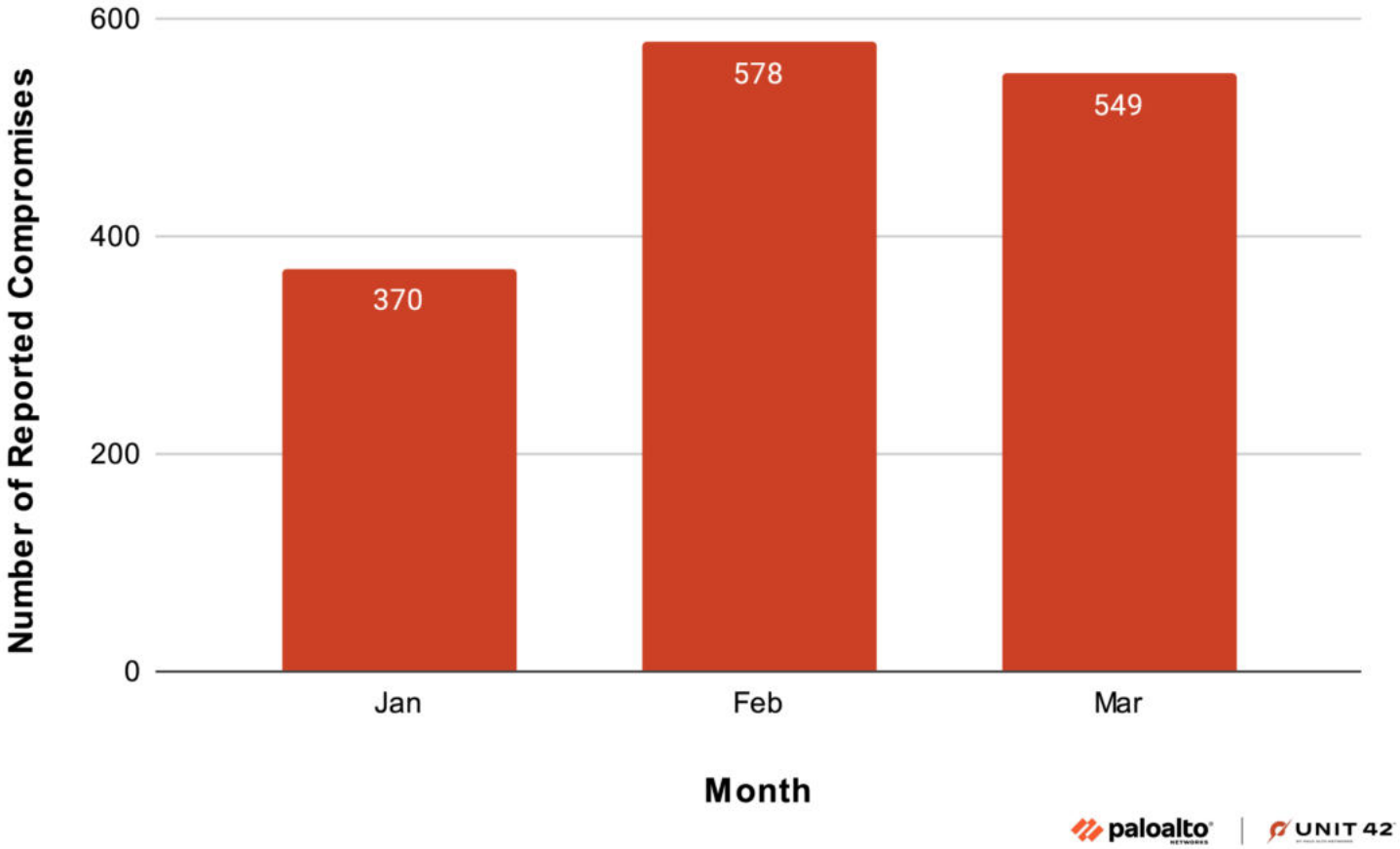


Figure 4. Leak site posts from all ransomware families per month.

Ransomware activity tends to fluctuate seasonally, making it important, for example, to compare activity to the same quarter of the previous year, rather than the most recent quarter. This helps account for changes that can occur due to travel seasons, annual holidays and other recurring events.

Following this pattern, we observed similar fluctuations in leak site data in 2025, as seen in Figure 4, compared to leak site data during the previous period of January-March 2024. In particular, in both 2024 and 2025, we saw a rise of activity from January to February, followed by a slight dip in March.

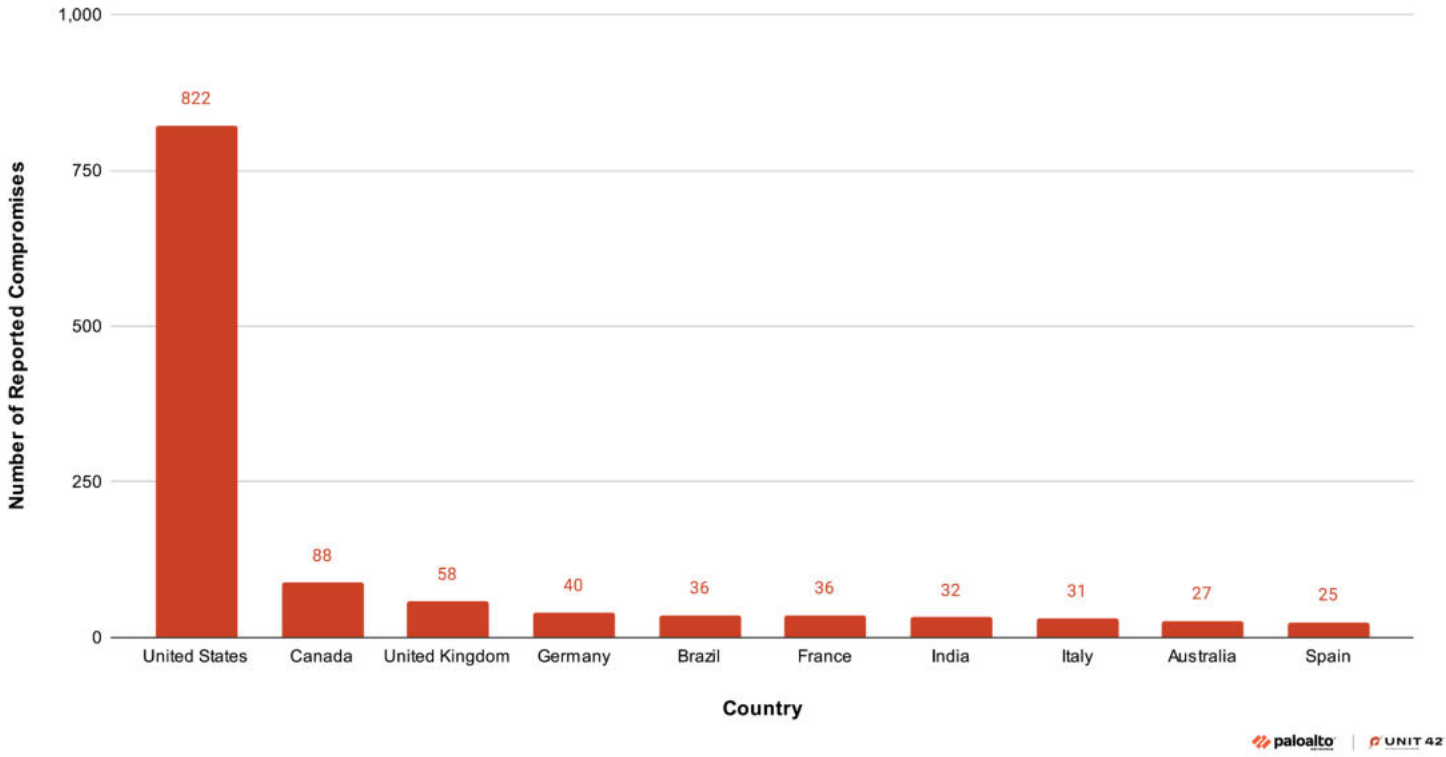


Figure 5. Ransomware activity categorized by the country in which the victim organization is headquartered.

While the vast majority of organizations publicly impacted by ransomware in January-March 2025 are headquartered in the United States, as seen in Figure 5, this may not paint the full picture of the impact of ransomware attacks. Since many large organizations have offices in countries besides where they are headquartered, a ransomware attack could affect organizations, employees or customers in multiple parts of the world.

With that caveat, we have consistently seen the United States at the top of this list for the years we've tracked leak sites. After the United States, commonly impacted organizations are headquartered in Canada, the United Kingdom and Germany, though the specific order can change.

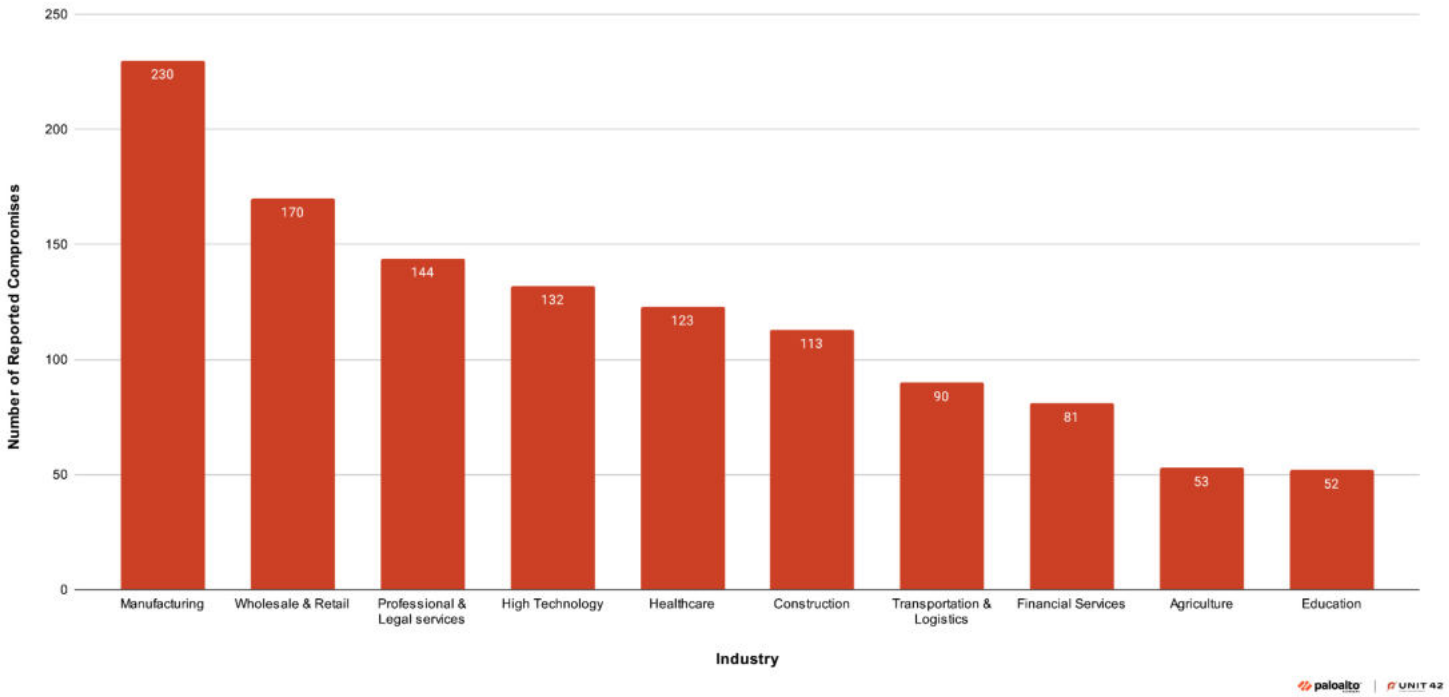


Figure 6. Leak site posts January-March 2025 per industry.

Many ransomware attacks are opportunistic, with threat actors focusing on organizations they can compromise and where they will make the most money. That said, interesting patterns can emerge in affected industries.

For example, in the first half of 2024, the healthcare industry was the second most impacted, driven in part by prominent compromises of organizations in that vertical. However, when looking at data over the past several years, healthcare more commonly occupies the fifth or sixth most impacted spot, as seen above in Figure 6.

For the past several years, manufacturing has topped the list of most impacted industries. This may be in part due to features of the industry, such as the common use of specialized software that is difficult to update, combined with the immediate financial impact of downtime.

# Conclusion

Unit 42 continues to monitor ransomware threats, through incident response cases, observation of dark web leak sites and other sources of telemetry. Ransomware remains a significant and evolving threat,

especially as threat actors continue to evolve more ways of gaining access. The involvement of nation-state groups, combined with low barriers to entry for ransomware affiliates, means that cybercriminals at all skill levels may get involved with ransomware.

Organizations should stay aware of trends in ransomware and employ a defense-in-depth strategy for protection. While it is important to maintain backups, organizations should be prepared for ransomware actors to apply other forms of pressure (such as reputational pressure) to force a ransom payment even if the organization has not lost access to data. For more about Unit 42's recent observations of ransomware trends, please read the 2025 Global Incident Response Report.

## Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from ransomware threats through Network Security solutions and the Cortex line of products.

The Next-Generation Firewall with Cloud-Delivered Security Services includes the following capabilities:

- Advanced URL Filtering and Advanced DNS Security can block malicious URLs and domains associated with ransomware.
- Advanced Threat Prevention can block ransomware threats at both the network and application layers, including port scans, buffer overflows and remote code execution.

Our Cortex protections include Cortex Xpanse, which detects vulnerable services exposed directly to the internet that might be exploitable and infected by ransomware.

Through Cortex XDR and XSIAM, all known ransomware samples are prevented by the XDR agent out of the box using the following endpoint protection modules:

- The Anti-Ransomware module helps prevent encryption behaviors on systems running Microsoft Windows or macOS.
- The Local Analysis module helps detect ransomware binaries on Windows, macOS and Linux.
- XDR also includes protection capabilities like Behavioral Threat Protection (BTP) which helps prevent ransomware activity on Windows, macOS and Linux.

- Palo Alto Networks' Cloud Security Agent (CSA) leverages XSIAM to provide cloud based detection and monitoring capabilities to both Cortex and Prisma Cloud cloud agents.

Our cloud-based security solutions also help protect virtual machines running in cloud environments.

We frequently update machine learning models and analysis techniques in Advanced WildFire with information discovered from our day-to-day research on ransomware.

Unit 42 can help organizations proactively prepare to mitigate the threat of ransomware through our Ransomware Readiness Assessment.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

# Additional Resources

- 2025 Unit 42 Global Incident Response Report – Unit 42, Palo Alto Networks
- Ransomware Review: First Half of 2024 – Unit 42, Palo Alto Networks