The 2024 Ransomware Landscape: Looking back on another painful year

By Christiaan Beek, Senior Director, Threat Analytics, Rapid7

The ransomware landscape in 2024 continued to evolve at a rapid pace, outgrowing many of the trends we saw in 2023. Threat actors remained relentless and innovative, targeting organisations of all sizes and sectors. In this article, we'll examine the latest data points, discuss notable groups, and estimate the potential impact on victims — helping security teams plan their defences for the months ahead.

2024 by the Numbers

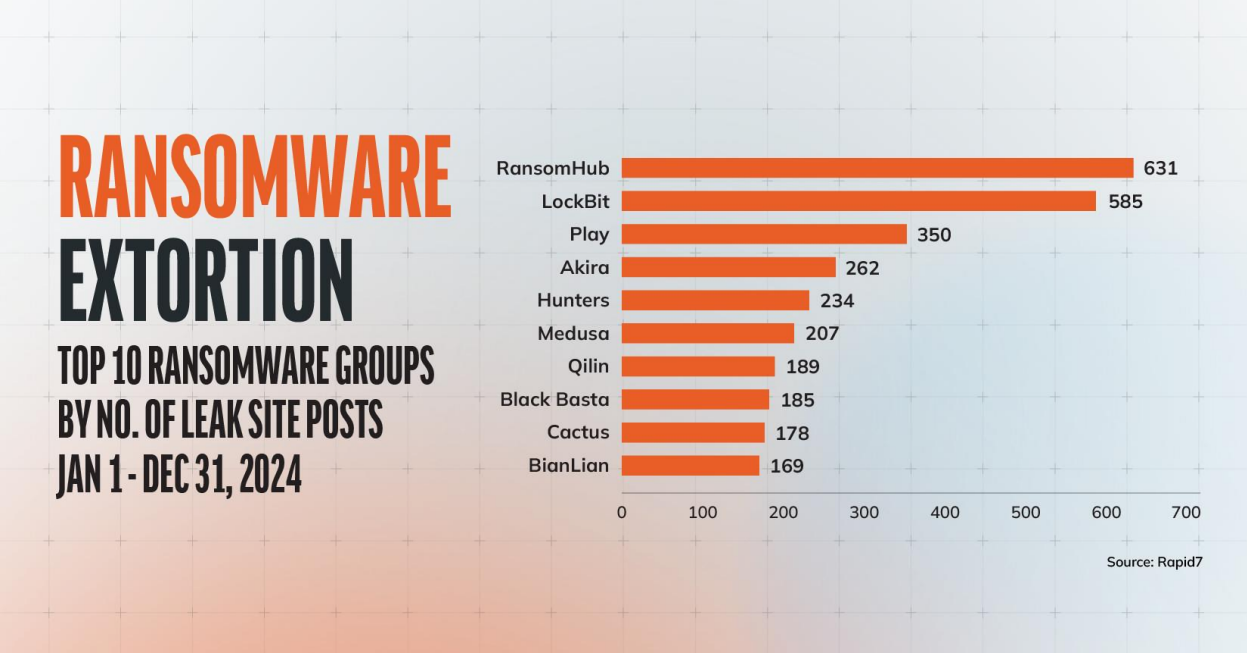
Mid last year, Rapid7 Labs released our Ransomware Radar Report highlighting key stats for the first half of 2024. Here is how 2024 played out as a whole:

- Total number of leak site posts: 5,939
- Number of active ransomware groups: 75
- Average number of active groups per month: 45
- Average ransom payment in Q3 2024: USD $479,237 (Source: Coveware)
- Median ransom payment in Q3 2024: USD $200,000 (Source: Coveware)
- Median percentage of companies that pay: 32% (Source: Coveware)

These numbers offer insight into just how expansive ransomware activity has become. While the overall figures are alarming, it's the variety of actors and their ability to adapt that pose the greatest challenge for defenders.

Top 10 Ransomware Groups

Below are the 10 most prolific ransomware groups in 2024, ranked by the number of posts on leak sites:



While these numbers reflect public disclosures, many victims choose to negotiate privately, meaning the true scope could be significantly higher.

The Cl0p group recently disclosed exploiting a vulnerability in Cleo file transfer software, further illustrating how threat actors can pivot between high-profile platform vulnerabilities with minimal downtime. While the group avoids using conventional ransomware payloads, they still rely on a leak site to extort payment from victims. Because Cl0p's business model isn't driven by fully encrypting victims' data, the ransom amounts they demand, and ultimately receive, remain opaque, making it difficult to quantify their financial impact within the broader ransomware ecosystem.

Estimated Financial Impact

Based on the median payment amount of USD $200,000 cited above and the stat that about 32% of companies choose to pay, we can make **rough** estimates of total potential revenue generated by these groups.

Note that this calculation assumes:

1. Each post represents one victim.
2. 32% of those victims pay.
3. Ransom is always USD $200,000.

These assumptions likely understate the actual impact, as some victims pay more (the average is USD $479,237). Even so, the total in 2024 could easily exceed USD $380 million in ransom paid.

Group	Posts	32% of Posts (Paying Victims)	Hypothetical Revenue (USD)
RansomHub	631	201.92	$40,384,000
LockBit	585	187.20	$37,440,000
Play	350	112	$22,400,000
Akira	262	83.84	$16,768,000
Hunters	234	74.88	$14,976,000
Medusa	207	66.24	$13,248,000
Qilin	189	60.48	$12,096,000
Black Basta	185	59.20	$11,840,000
Cactus	178	56.96	$11,392,000
BianLian	169	54.08	$10,816,000

Table Note: These calculations are illustrative only; actual outcomes will differ.

Trends and Observations

Following are four trends we're seeing in Rapid7 Labs, based on the global threat intelligence we gather, as well as input from our internal research and open source communities.

1. **Proliferation of Groups:** With over 75 active groups, it's clear that the barrier to entry for launching ransomware campaigns remains relatively low. In addition, fragmented groups are splintering and rebranding, making it more difficult to track and mitigate.
2. **Persistent Dominance:** Teams like RansomHub, Akira, and Fog continue to reign at the top, demonstrating sophisticated extortion strategies and steady affiliate growth.
3. **Increased Transparency on the Victim Side:** More organisations are disclosing breaches to comply with emerging regulations as well as to maintain customer trust. These self-reports, combined with the data ransomware actors post as a form of extortion, can give us a view of the threat. Still, not all attacks become public, obfuscating the true scale of the ransomware problem.
4. **Rise of Double and Triple Extortion:** Threat actors often demand multiple payments for data release, encryption keys, and in some cases, to prevent DDoS attacks or direct contact with partners and clients.

An additional observation: LockBit remained active throughout 2024, even as it became the focus of significant law enforcement attention. In a recent case, a dual Russian-Israeli national was charged for allegedly serving as a LockBit developer — an accusation that centres on crafting malicious code, overseeing affiliate activities, and orchestrating ransomware attacks worldwide. The indictments underscore intensified global cooperation, with agencies from the United States and the United Kingdom coordinating to disrupt LockBit's infrastructure and hold key figures accountable. While LockBit continues to operate, these collective enforcement actions have highlighted the value of cross-border partnerships in mitigating ransomware threats

Building Resilience

Now that we've looked at the numbers and trends, let's examine how we can use these learnings to inform decision-making and enable conversations at the executive level:

- **Prepare for Multiple Vectors:** Ransomware attacks often begin with credential compromise, phishing campaigns, or exploitation of unpatched vulnerabilities. Build layered security defences accordingly.
- **Secure Collaborations:** Ensure robust security protocols with third parties, given the reliance on supply chains and outsourced IT services.
- **Incident Response Readiness:** Create clear IR plans that include legal and public relations strategies. In addition, we highly recommend that companies hold twice-annual tabletop exercises to test the efficacy of their ransomware IR plans. Rapid containment and a well-managed response can help minimise financial and reputational damage.
- **Ongoing Risk Assessment:** Regularly revisit threat models, especially as top-tier groups (like RansomHub or Cl0p) adopt new tactics and expand their affiliate networks.

Planning Ahead

Looking at the big picture, the financial incentives for cybercriminals are undeniable. Even if only one-third of victims pay a median of USD $200,000, the potential revenue surpasses USD $380 million — and that's likely just the tip of the iceberg. This underscores three critical points for defenders:

1. **Defence in Depth:** Organisations must invest in proactive measures, from user awareness training and robust patching to strict access control and secure backups.

2. **Threat Intelligence:** Regularly monitor emerging ransomware groups and tactics to tailor defences. Knowing who is targeting your industry and their methods is essential.
3. **Commanding Your Attack Surface:** In line with Rapid7's emphasis on complete visibility and proactive security, it's essential that organisations maintain a continuous view of their external footprint. This includes:

    - Regular Scanning: With automated tools that identify internet-facing assets and highlight newly exposed services or vulnerabilities.
    - Real-time Monitoring: For detecting changes in cloud environments, development pipelines, and system deployments.
    - Holistic Patch Management: To prioritise fixes based on known exploits and potential impact to reduce windows of opportunity for attackers.

    By commanding your attack surface, you can reduce the likelihood of unpatched systems and publicly exposed services becoming easy entry points for ransomware groups.

Conclusion

The 2024 ransomware landscape signals an ongoing escalation in the volume, variety, and financial impact of attacks. Groups like RansomHub, Akira and Cl0p demonstrate how quickly affiliates can scale, while many new entrants take advantage of commoditised ransomware-as-a-service models. For organisations of all sizes, building resilience, staying informed, and preparing a strong response plan are critical steps in countering this persistent and evolving threat.

Disclaimer: The statistics and financial estimates shared in this blog are based on public data and should be considered general indicators rather than exact figures. Real-world incidents often involve factors that deviate from these simplified calculations.