CORVUS

Q1 RANSOMWARE REPORT

Ransomware Groups Don't Die, They Multiply

2024

Table of Contents

Authors

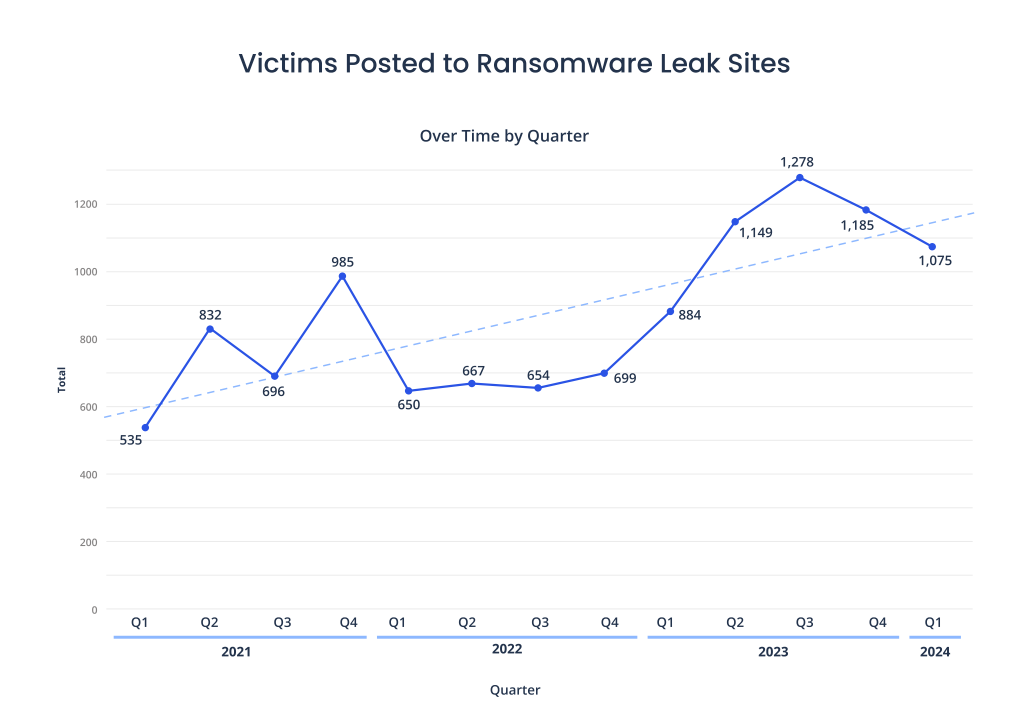
Jason Rebholz
Chief Information Security Officer
Corvus Insurance

Ryan Bell
Head of Threat Intelligence
Corvus Insurance

Introduction

Despite a record-breaking and tumultuous 2023, the early months of 2024 have not brought respite. With 1,075 leak site victims reported in Q1, this quarter has seen a 21% increase over the same period last year and is the most active first quarter ever recorded on ransomware leak sites. This rise is particularly notable given the expected seasonal downturn and the recent high-profile disruptions of leading groups such as LockBit and BlackCat. Our analysis demonstrates that while the public brands of ransomware groups may change in the face of crackdowns, the threat, like the mythical Hydra with its multiplying heads, only redistributes and continues to grow. Our Hercules has yet to appear.

The report also delves into the impact across various industries, with tech, healthcare, industrial, and legal sectors facing significant challenges as the frequent target of ransomware threat actors. Additionally, we will examine the continued role of vulnerabilities in Internet-facing tools, like ScreenConnect, in facilitating high-impact ransomware attacks, highlighting the importance of robust cybersecurity measures in mitigating these risks.

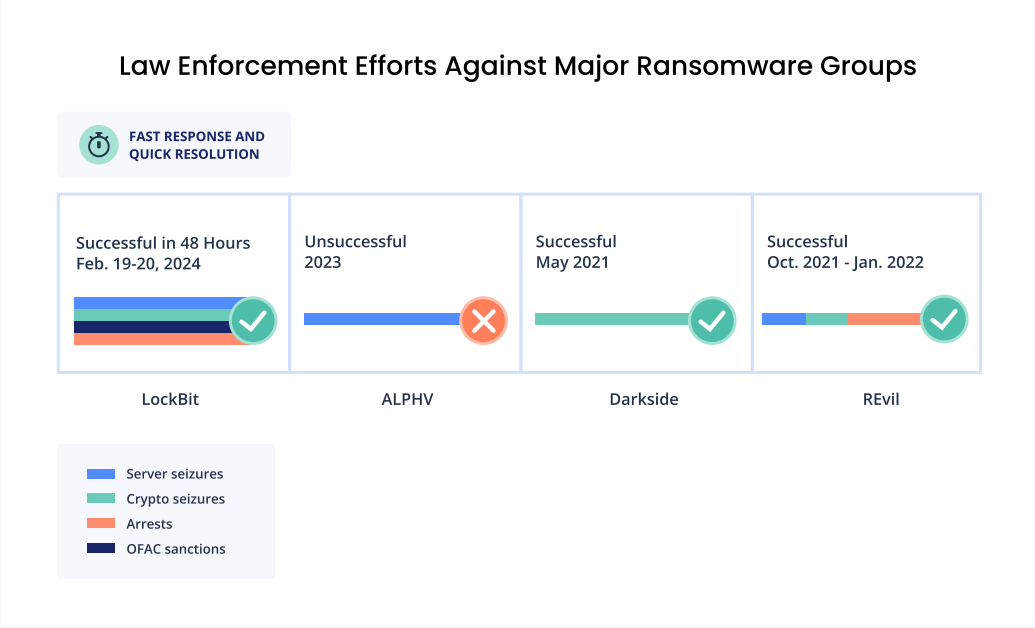


Lockbit takedown: the ransomware monster is headless (for now)

Two significant changes occurred among major ransomware groups in the first quarter. The first involved an international law enforcement action, while the other was a self-imposed disruption.

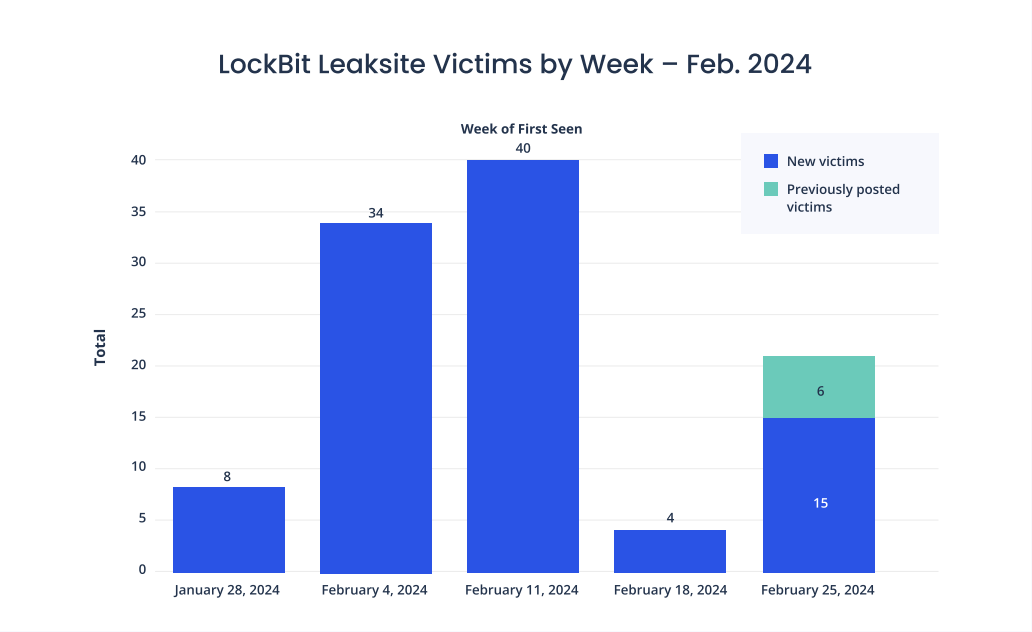
On February 20, 2024, an international operation involving ten countries targeted the LockBit group's infrastruct ure to disrupt their operations. This joint action led to the confiscation of 34 servers and the immobilization of 200 cryptocurrency accounts associated with the group, along with two arrests made in Poland and Ukraine. Additionally, the United States Office of Foreign Assets Control (OFAC) imposed sanctions on two other individuals, and authorities succeeded in dismantling software accounts related to LockBit's data theft capabilities, dealing a substantial blow to the group.

The thoroughness of these law enforcement actions represents a considerable advancement in global efforts to prevent cybercrime. As shown in the table below, the speed and comprehensiveness of the LockBit takedown exceeds every other notable attempt in the recent past.



Lockbit's dark web leak site, which had been bustling with an average of 76 new victims per month, suddenly took on a different shape. Law enforcement seized the servers hosting the leak sites and posted details of the operation and information on Lockbit's infrastructure. This seems to have been an attempt to not only take out the infrastructure but also cause reputational harm to the group.

A few days later, on February 25, the LockBit administrator established a new leak site and resumed posting data. Since then, however, around 40% of the activity on the new leak site has consisted of information from organizations that had already been compromised prior to the law enforcement operation. The group may be attempting to project an image of resilience, but it does not seem like the group is anywhere near its former strength in launching new attacks. LockBit's operations have significantly declined from their status a year ago (a 49% decrease) and two years prior (a 61% decrease).



Disruption from the Inside: Alphv/BlackCat Shuts Down

The second major upheaval in the ransomware domain involved the ALPHV/BlackCat ransomware group, one of the most active groups throughout 2023 and the subject of an attempted takedown by law enforcement in December (which ultimately only slowed, but did not halt, the group's operations). By late January 2024, the group had largely bounced back.

On March 6th, 2024, ALPHV/BlackCat conducted an exit scam following the high-profile attack on Change Healthcare, which had affected thousands of medical practices and pharmacies across the United States. Normally, a ransomware group would distribute profits among its members, with BlackCat typically claiming a 20-25% share of the ransom payments leaving the remaining 75-80% for its affiliates. In this case, however, BlackCat's leaders kept all the funds and abruptly terminated operations. The affected affiliates quickly aired their frustrations on dark web forums, upset that they didn't receive their share of the purported $20 million dollar ransom.

Subsequently, numerous victims previously listed by BlackCat (ALPHV) were found on new LockBit leak sites. This is perhaps yet another indication of LockBit grasping for relevance in their post-takedown world.

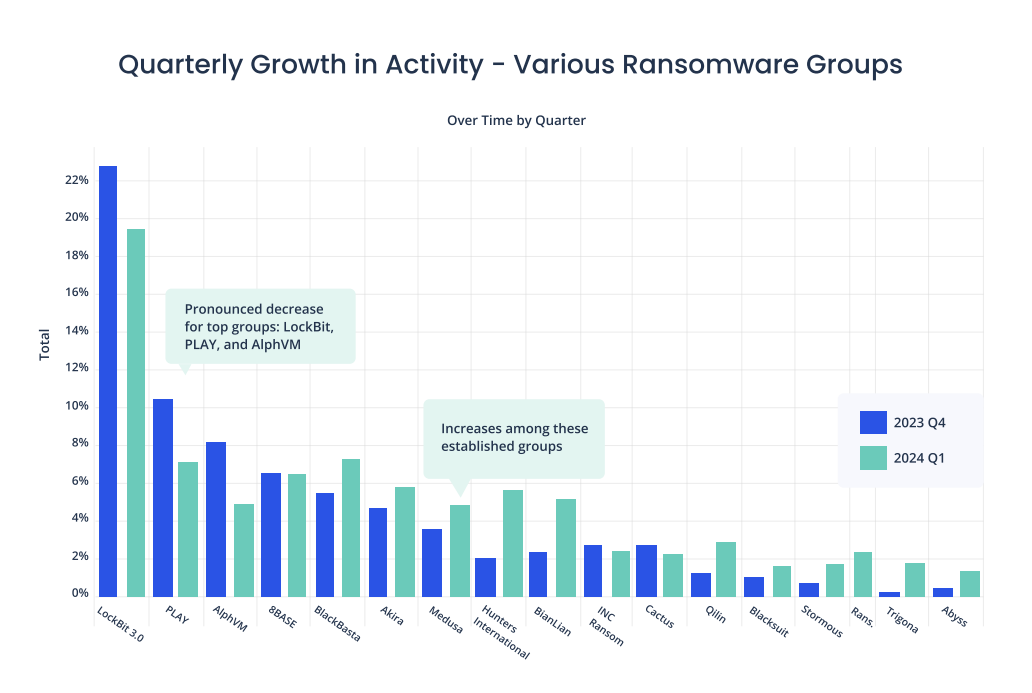
The Hydra Rears its Head(s): The dispersion of ransomware affiliates

Considering that LockBit and BlackCat were responsible for a combined 30% of leak site victims in Q4 2023, one might have anticipated an overall reduction in ransomware activity when both groups essentially ceased operations in the past quarter (see previous section).

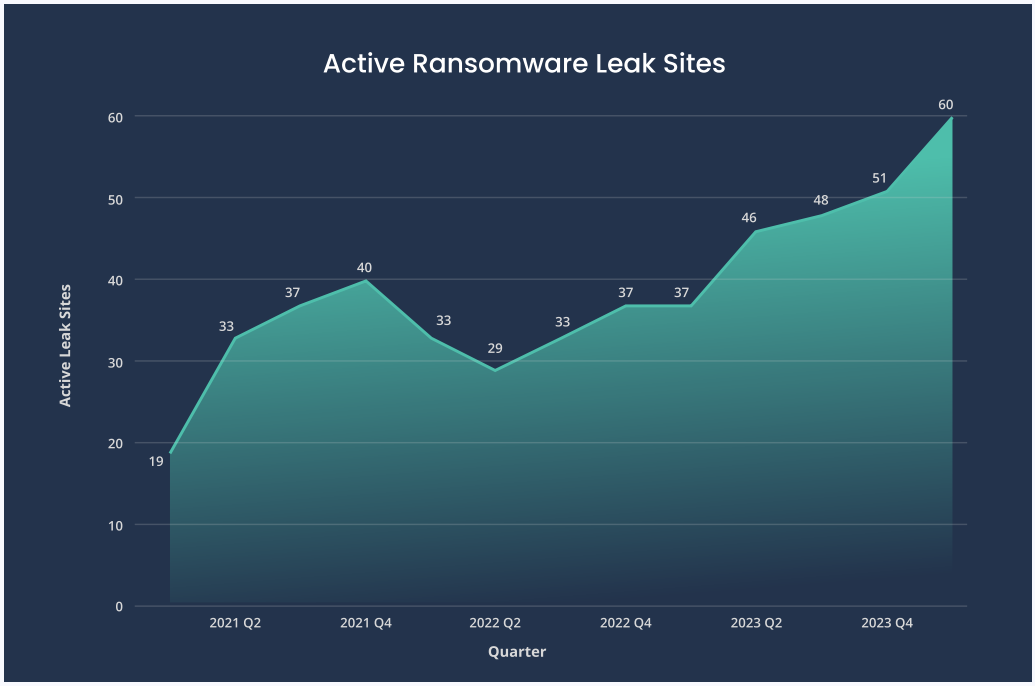
On the contrary, overall ransomware figures remain higher than in any previous year's first quarter and have even risen from February to March in the aftermath of the takedowns we discussed. Why? To get an answer, we first have to understand a bit more about how the affiliate system works.

Ransomware affiliates are independent operators who conduct the attacks that lead to extortion events. Affiliates use the infrastructure of Ransomware-as-a-Service (RaaS) groups, such as Lockbit, to gain access to encryptors and leak site infrastructure. The profits of paid ransoms are split between the two. It's a symbiotic relationship, but due to the availability of many RaaS groups, the success of any individual RaaS largely depends on the affiliates' trust in its stability and efficacy. When a group like LockBit is compromised, affiliates might question its reliability and shift their allegiance to more secure criminal networks, undermining the original group's strength.

So when we observe growth in ransomware activity even after two major groups shut down, we can look to where an affiliated individual or group might naturally go to continue their enterprise. Indeed, our data shows recent upticks in activity from other ransomware groups, such as Black Basta, Akira, Hunters International and BianLian. This trend supports the notion that affiliates are likely shifting their operations to alternative groups.



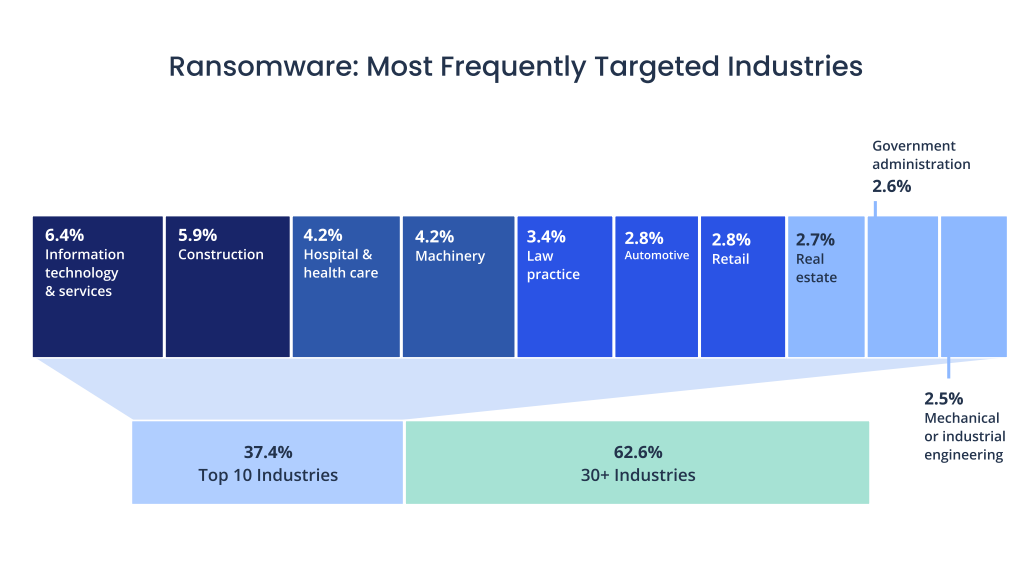
Another way to see how these affiliate relationships can quickly shift and manifest in new places is to look at the number of unique active leak sites and the number of newly added leak sites. These figures can serve as indicators for the splintering of the ransomware economy, since affiliates will seek new partners in the absence of a reliable "market leader". We've observed that the number of active leak sites reached an unprecedented high, totaling 60 in the first quarter of this year. In addition, 18 newly discovered leak sites emerged at the same time. That figure is higher than in any prior quarter.



Collectively, these indicators suggest an intensification of activity within established groups coupled with a surge in new entrants, with all parties seeking to capitalize on the power vacuum created by the dissolution of the two most prominent ransomware groups. The disconcerting conclusion is that, rather than experiencing a decline followed by stabilization, the ransomware ecosystem has swiftly adjusted to significant disturbances with minimal disruption to its overall activity. The hydra simply grew new heads.

Ransomware Targets by Industry

In Q1, 2024, the distribution of the impact among various industries remained relatively stable, with Information Technology & Services, Construction, Health Care, and Legal consistently ranking among the top five most-targeted industries for several quarters.



Despite the anticipated seasonal decline from Q4, most industries experienced only a marginal reduction in incidents compared to the previous quarter, with one prominent exception: medical practices, which we'll discuss in the following section. The year-over-year analysis of industry changes shows a significant change across various sectors, including Architecture, education, and medical practices.

Medical practices increasingly targeted by ransomware groups

Medical practices, such as specialists or family clinics, saw concentrated activity by a few ransomware groups. In 2023, BlackCat alone accounted for almost 17% of the total number of leak site victims, second only to BianLian, which had a share of 20%. LockBit was also a significant player, with a share of 15%. In 2024, BlackCat remains near the top with 12%, behind BianLian at 20% and LockBit at 16%.

Interestingly, we see the same primary groups responsible for cyberattacks against hospitals and healthcare facilities more generally: BianLian, ALPHV, LockBit, and INC. Among these, ALPHV has emerged as a significant threat, accounting for 9% of the total number of victims in hospitals and healthcare in 2023. In the first quarter of 2024, ALPHV's share increased to almost 12%, and one attack in particular against Change Healthcare

was reminiscent of the Colonial Pipeline ransomware attack three years ago. BlackCat carried out an attack against UnitedHealth subsidiary, Change Healthcare, causing outages to healthcare billing and payment systems, impacting nearly every part of the healthcare system, and prompting their exit scam.

Lifecycle of ScreenConnect

In our previous quarterly report [link], we highlighted the intensified efforts of ransomware groups to exploit vulnerabilities for initial access. This trend has persisted unabated into Q1 2024, with threat actors swiftly capitalizing on these weaknesses. Consider the following incident as an illustration of the rapid exploitation of vulnerabilities and the critical role of patch management.

On February 19th, ConnectWise released an advisory regarding two security flaws in its ScreenConnect remote management software. Corvus had already dispatched a comprehensive alert with remediation steps to its policyholders well in advance of the publication of a CVE for these vulnerabilities. As details of an exploit became public knowledge through security researchers, hackers promptly began exploiting the vulnerability in the days after the disclosure.

Corvus monitored the situation, observing both policyholders and non-policyholders using ScreenConnect. As the Corvus Threat Intel team monitored patch rates, we noticed that a plateau in patching activity was reached around seven days after the vulnerability was announced. At that point organizations with strong patch management programs had responded to the threat, leaving a long tail of activity from other organizations that may eventually discover they are vulnerable over the course of weeks, months, or years.

Meanwhile, the Corvus Risk Advisory team maintained consistent communication with our policyholders and brokers, following up and providing guidance on patching vulnerable systems. Ultimately, the proportion of Corvus policyholders who applied patches to rectify the flaw was 15% higher than that of other ScreenConnect users after 13 days, and it continues to climb.

Rapid action in response to vulnerabilities is the best defense. Many organizations, however, aren't able to reach an optimal level of patching frequency and speed. That's where advisors like our team at Corvus can help. The difference in this case was having the capacity to meet policyholders and their brokers where they were to increase patch rates far above the plateau seen in the general population.

Conclusion

Despite unprecedented disruptions to the dominant ransomware groups, the first quarter of 2024 has not seen the expected downturn in ransomware activity. With a 21% increase in leak site victims over the previous year and the highest activity level for the first quarter on record, it is clear that the threat landscape remains dynamic and resilient. While the role of law enforcement disruption is vital in the long term, it's clear that the short-term impacts have yet to take hold and cybercriminals remain resilient in the face of the challenge.

The persistence of vulnerabilities in Internet-facing tools and services underscores the necessity for vigilant cybersecurity practices, particularly timely patch management and the resolution to find and patch all vulnerable assets in your environment. As ransomware groups continue to exploit these weaknesses, the importance of proactive defense measures cannot be overstated. The industry-specific data reveals that no sector is immune, with technology, healthcare, industrial, and legal sectors continuing to be prime targets.

This report reaffirms the adaptability of the ransomware ecosystem, which seems to stabilize rapidly after significant events without substantial interruption to operations. It is a stark reminder that the fight against cyber threats is ongoing, requiring constant vigilance and collaboration to protect vulnerable systems and data.

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