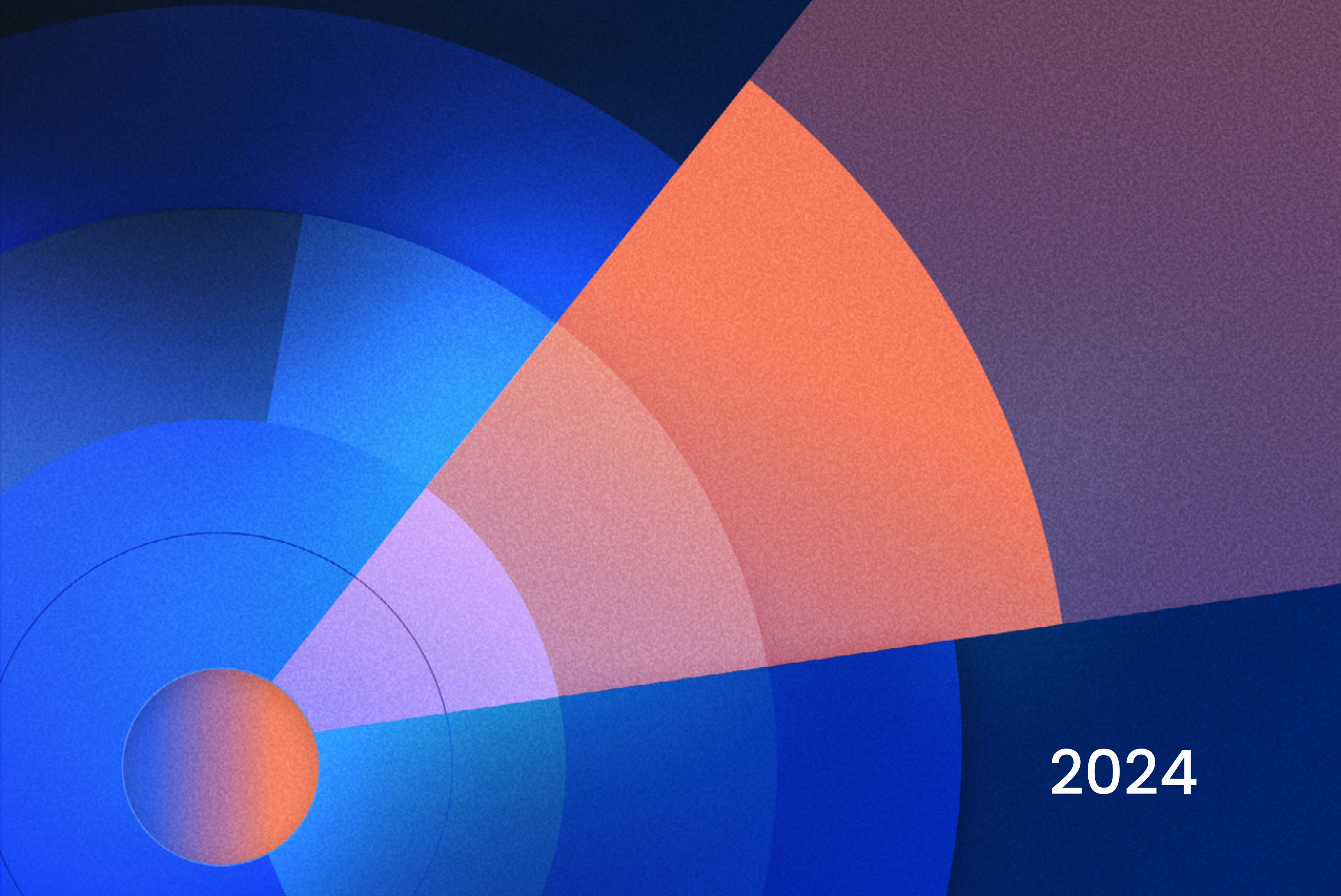
CORVUS
BY TRAVELERS

Q3 CYBER THREAT REPORT

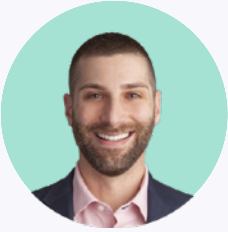
The Ransomware Ecosystem is Increasingly Distributed



2024

Table of Contents

Authors

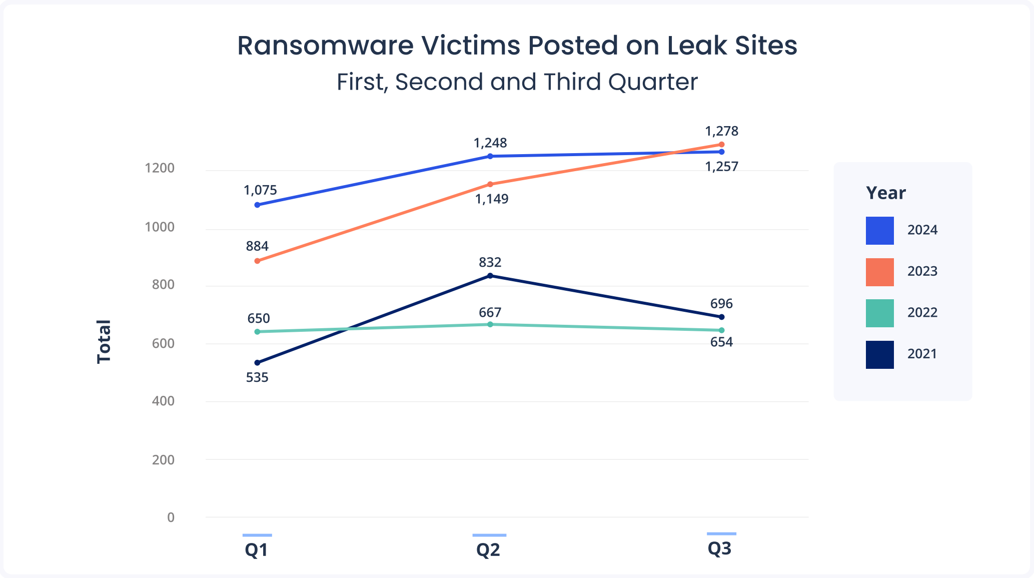


Jason Rebholz
Chief Information Security Officer
Corvus Insurance

Ryan Bell
Head of Threat Intelligence
Corvus Insurance

Introduction

In Q3 2024, the ransomware threat level remained elevated. While the increase in attacks quarter-over-quarter was marginal, a continuously high volume of attacks over an extended period points to a more enduring insight about the ransomware ecosystem today: unlike previous periods, where high levels of activity were clearly linked to the discovery of a particular vulnerability, current activity appears to be driven by a broad-based, “organic” increase in ransomware attacks. Groups are honing their methods of gaining initial access through infostealers or brute force attacks, creating their own opportunities rather than waiting for a mass-exploit event. And this heightened environment has been sustained by a wide array of small ransomware groups, rather than a few prolific ones. Read on to hear more about these trends, and more.



Ransomware Victims Posted on Leak Sites

First, Second and Third Quarter

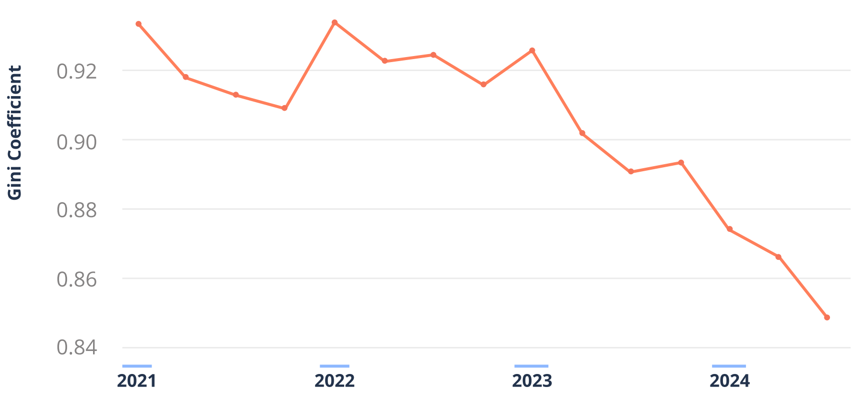
Typically, the third quarter sees heightened activity as attackers return from a summer hiatus. This year was no different, except the increase was less pronounced. This quarter saw 1,257 victims posted to leak sites, marking a 0.7% rise from Q2’s total of 1,248 victims.

Activity Across Ransomware Groups: Shifting Dominance

The ransomware ecosystem has long been dominated by a few players. Indeed, three groups — RansomHub, PLAY, and LockBit 3.0 — drove the majority of attacks in the last quarter. And yet the extent of those large players' dominance is consistently diminishing. The overall number of active ransomware groups across the world rose to reach 59, reflecting an increasingly complex threat landscape and one that's more competitive than ever before. Law enforcement campaigns in late 2023 and early 2024 against LockBit and ALPHV may be transforming the ransomware ecosystem, resulting in more small-scale operations than before.

To examine this increasingly distributed landscape, we employed the Gini coefficient, a statistical metric that represents the inequality within a distribution — here, the distribution of ransomware attacks among different groups. The Gini coefficient has been decreasing since late 2023, meaning ransomware attacks are becoming more evenly distributed among a larger number of groups, rather than being dominated by just a few actors.

Ransomware Attacks Dispersed Across More Ransomware Groups



This rise reflects the emergence of newer or lesser-known groups, even as major players like **AlphVM** cease operations. Affiliates of LockBit, which was hampered by law enforcement actions, and of AlphVM have been observed jumping to other variants or starting their own.

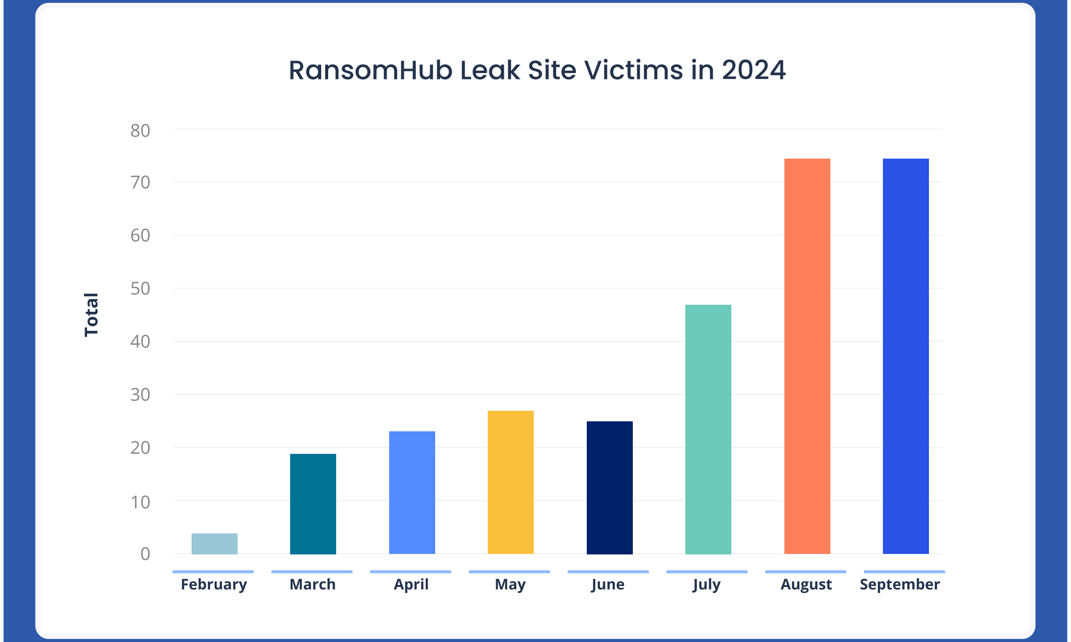
Still, the shift is not total. A few major groups that have avoided law enforcement continue to contribute heavily to the picture of overall ransomware activity. We noted some shifts in dominance among these key ransomware groups:

- **RansomHub** cemented itself as the most active group, with a **160% increase** in victims posted compared to Q2. Its 195 reported victims reflect an increased focus on sectors like **Construction** and **IT Services**. (See the next section for more on this group).
- **PLAY** maintained its strong presence by posting 93 victims, showcasing consistent activity across multiple industries, including **Healthcare**.
- **LockBit 3.0's** activity fell sharply from 208 in Q2 to 91 victims in Q3, likely signaling a response to law enforcement pressure.
- **Medusa** and **Akira** both continued to impact the landscape with around 40-50 victims each, reflecting steady activity.

Together, the decreasing Gini coefficient and the uptick in the number of active groups suggest even though the most powerful groups dominate the victim count, the ransomware ecosystem is getting more competitive. For a prime example of this, look no further than one of Q3's most active and also one of 2024's newest groups, RansomHub.

Who is RansomHub?

RansomHub, a ransomware-as-a-service (RaaS) operation that started in February 2024, has rapidly become one of the most prolific and dangerous cybercriminal groups. Previously known as Cyclops and Knight, RansomHub has drawn high-profile affiliates from other notable variants like LockBit and ALPHV by providing favorable payment terms and a range of appealing technological capabilities. Since its inception in February 2024, the group has claimed over 290 victims across various sectors.

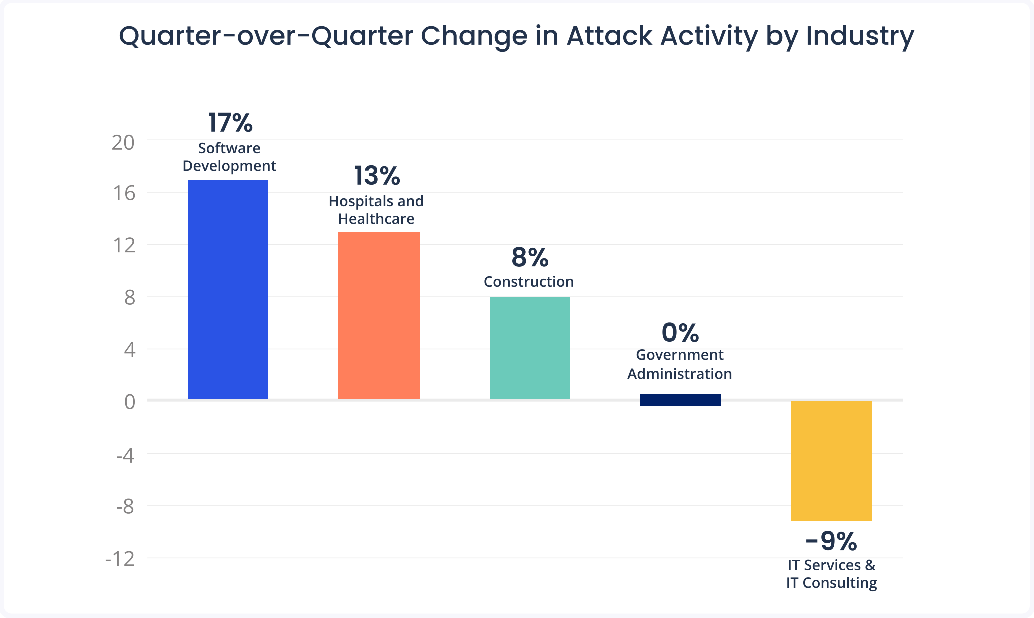


The group's success can be attributed to its tried-and-true tactics and tools. RansomHub employs a double-extortion model, encrypting systems and exfiltrating data to maximize pressure on victims. They've also integrated advanced tools like EDRKillShifter, which can disable endpoint detection and response (EDR) solutions and antivirus protections, allowing them to evade detection and persist in compromised environments.

RansomHub's rapid rise highlights just how quickly the ransomware ecosystem can shift while remaining much the same. Their ability to attract skilled affiliates, coupled with their use of cutting-edge evasion techniques, has made them a formidable adversary for organizations worldwide.

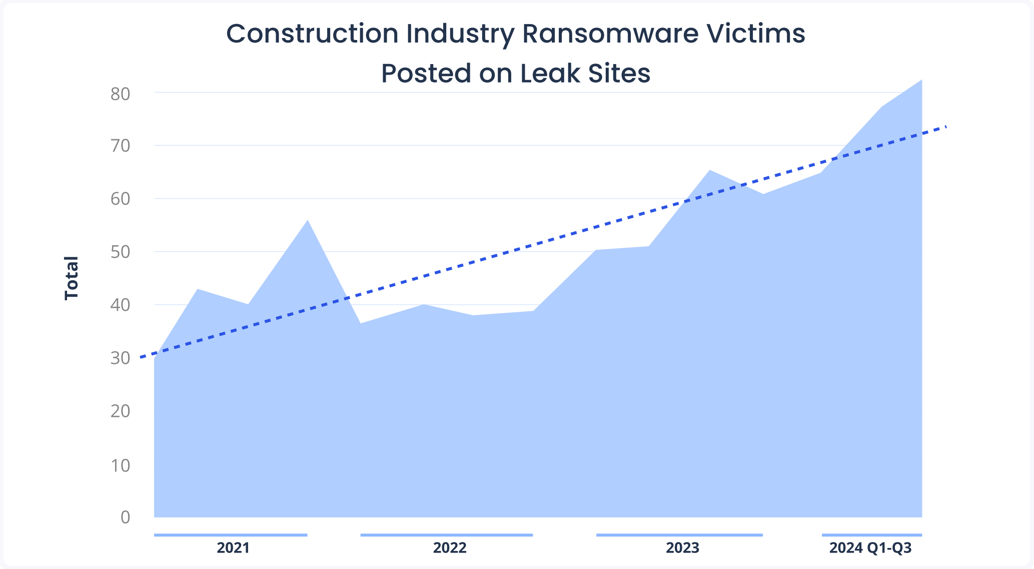
Industry Insights: Construction and Healthcare in the Crosshairs

The top targeted sectors in Q3 remained largely consistent with Q2, but some experienced notable increases in victim counts.



Construction

The Construction industry remained the most targeted sector in Q3, with 83 victims, a 7.8% increase over Q2's 77 victims. This focus on construction reflects sustained interest from ransomware groups, particularly those like RansomHub that continue to target infrastructure and related sectors.



Healthcare

Healthcare organizations saw a 12.8% increase in attacks, with 53 victims in Q3 compared to 47 in Q2. This rise highlights persistent vulnerabilities in legacy technologies within the sector, driven by the critical nature of healthcare data and the high likelihood of ransom payments. Ransomware groups like PLAY and Medusa remain active in targeting this sector.

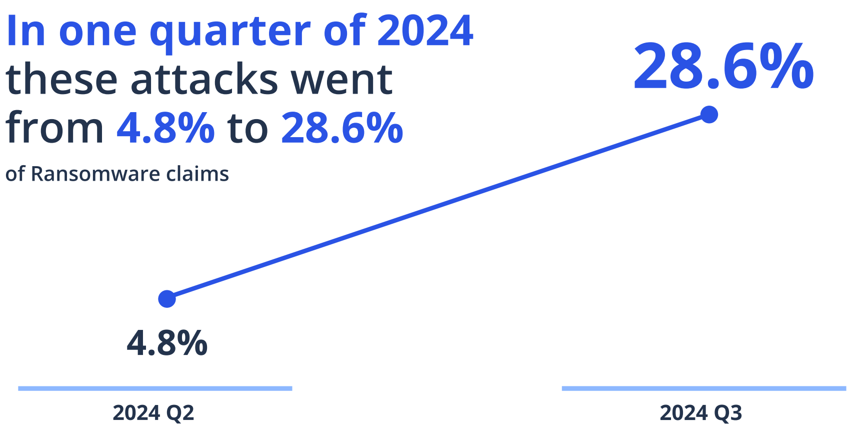
IT Services and Consulting

The IT Services sector saw a slight decline in Q3, with 49 victims compared to 54 in Q2. However, given the systemic risks associated with attacks on IT providers, in that an attack against one IT provider can impact many customer environments, this sector remains a priority for a number of ransomware groups.

A surge in VPNs for initial attack access

One pressing question for cybersecurity professionals is the method behind these ransomware breaches. Q3 data highlights a surge in attackers leveraging VPNs for initial access, contributing to 28.7% of ransomware claims. Many incidents were traced to outdated software or VPN gateways with default or weakly protected accounts. Common usernames like “admin” or “user” and a lack of multi-factor authentication (MFA) make these accounts vulnerable to automated brute-force attacks. Attackers exploit publicly accessible systems by testing combinations of these weak credentials, frequently achieving network access with minimal effort.

Percentage of Ransomware Attacks Where VPN Was the Point of Initial Access



In one quarter of 2024 these attacks went from 4.8% to 28.6%

of Ransomware claims

Notably, a lack of MFA for remote access was a common factor in ransomware claims, with roughly 75% of policyholders either not using MFA, implementing it only partially, or their coverage was unable to be determined. This leaves organizations open to attackers who rely on weak or default credentials to gain entry, omitting a crucial safety net in case a threat actor does get access to credentials through brute force attacks or other means.

Conclusion

Ransomware activity remained persistently high in Q3 2024, with a slight increase in victims and a continued reliance on VPN-based initial access by attackers. The growing number of active ransomware groups, up to 59 this quarter, underscores the increasing competitiveness of the ransomware ecosystem, which now includes a mix of prominent players like RansomHub, PLAY, and LockBit 3.0, alongside other emerging groups exploiting security gaps.

Sectors like Construction and Healthcare face sustained targeting, driven by the appeal of vulnerable systems and the perceived likelihood of ransom payments. The persistence of weak credentials and lack of multi-factor authentication on VPN gateways has facilitated these attacks, making secure access controls crucial for mitigating threats. As we approach the end of 2024, organizations, especially in high-risk industries, must strengthen defenses against a persistent and increasingly crowded ransomware landscape.

Corvus analysis was made possible with supporting data from eCrime.ch. This report is intended for general guidance and informational purposes only. This report is under no circumstances intended to be used or considered as specific insurance or information security advice. This report is not to be considered an objective or independent explanation of the matters contained herein.

CORVUS
BY TRAVELERS

Corvus Insurance, a wholly owned subsidiary of The Travelers Companies, Inc., is building a safer world through insurance products and digital tools that reduce risk, increase transparency, and improve resilience for policyholders and program partners.

Our market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance® and Smart Tech E+O®.

This material is intended for general guidance and informational purposes only. All insurance products are governed by the terms, conditions, limitations, and exclusions set forth in the applicable insurance policies, as issued.