RAPID7

KEY TAKEAWAYS: THE RANSOMWARE RADAR REPORT

Ransomware is a global criminal enterprise that knows no borders, includes an ever-changing group of attackers, and can target nearly any business it chooses. It is also evolving…rapidly. In the first half of 2024, there has been a significant evolution in the ransomware ecosystem. It includes major shifts in attack methods, potential amalgamation and collaboration between attackers, victim identification, and overall cybercriminal tactics.

In the Ransomware Radar Report, Rapid7 Labs researchers, threat intelligence experts, and those on the front lines of detection and response have taken a deep dive into the first six months of 2024 as they compare to 2023, and emerged with some startling discoveries about the current state of ransomware and where it may be heading.

This report represents a comprehensive analysis of ransomware incidents over the course of 18 months ending in June 2024. It offers insights into trends, attacker profiles, ransomware insights, and the implications for cybersecurity defenses.

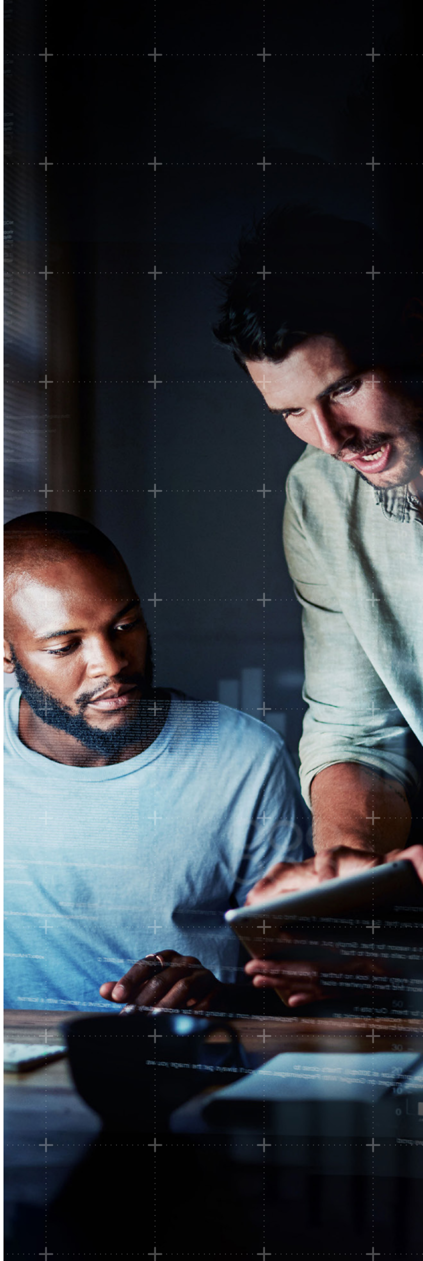
Let's take a look at some of the major takeaways from the Ransomware Radar Report.

KEY TAKEAWAY 1: THE CAST OF CHARACTERS IS EVER-CHANGING

During the first half of 2024, Rapid7 identified no fewer than 21 new ransomware groups taking the stage. Some of these are net new, while others are rebranding under different names, potentially as a response to law enforcement actions. Rapid7 identified a total of 68 unique groups posting extortion attempts to their leak sites during this time.

KEY TAKEAWAY 2: BUSINESS IS BOOMING

Rapid7 used the number of posts to each ransomware group's leak site to gauge roughly how much business they were doing. We found a 23% increase in these posts — and thus successful infiltrations — in the first half of 2024 over the same time period in 2023. RansomHub, one of the newer groups, has quickly established itself as a prolific attacker with 181 posts on their leak site. However, their total pales in comparison to LockBit's attempted extortion numbers with 474 posts on their site.



21 NEW

ransomware groups taking the stage

474

data leaks published by LockBit in H1 2024

KEY TAKEAWAY 3: THE SWEET SPOT IS $5 MILLION

It may be easy to assume that the bigger the fish, the more likely they are going to be the subject of attacks from ransomware actors. However, our data show that organizations with $5 million in annual revenue are being targeted as much as five times as often as their larger cousins. The hypothesis for this is that while larger companies are more lucrative, those with $5 million in revenue tend to have the data attackers look for when seeking to extort a company, but often have less mature ransomware prevention tools and tactics in place.

KEY TAKEAWAY 4: FEWER NET NEW RANSOMWARE FAMILIES

It may seem counterintuitive, but the number of unique ransomware families observed in the wild has actually gone down since 2022. In 2023 there were fewer than half the number observed the year prior. The trend appears to have continued in 2024. The possible reason for this is that ransomware groups are focusing their efforts in more specialized ways and with more effective ransomware variants than in years past. Essentially, they are going for quality over quantity.

KEY TAKEAWAY 5: DEJA VU ALL OVER AGAIN

One of the most unique methodologies the Ransomware Radar Report used to study the ransomware ecosystem involved the use of the Machoc Hash to determine what similarities exist between different kinds of ransomware strains. What we found was that there are three major clusters of similar ransomware variants indicating the potential for reuse of source code, use of common builders, and perhaps even code exchanges between groups.

Ultimately, one of the biggest takeaways from the Ransomware Radar Report is one of framing. These aren’t (just) a collection of individuals in hoodies operating in the shadows. These ransomware groups are fully-fledged and globalized criminal enterprises with their own marketplaces, business models, 24X7 support/help desks, and an ecosystem of collaboration and consolidation. It is important for security operators at organizations large and small to understand the level of sophistication that currently exists in the ransomware industry.

Businesses with

$5 MM

in annual revenue are targeted

3 MAJOR CLUSTERS

of ransomware with source code similarities

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact