2024 YEAR IN REVIEW

Ransomware

This summary highlights Cisco Talos' findings on the most targeted industries for ransomware attacks, the most prolific ransomware groups, and how actors are disabling security solutions and hiding in plain sight. For the full analysis, download the full 2024 Year in Review report.

Higher education hit hardest in 2024

Ransomware actors targeted education entities more than any other sector in 2024. This is in line with trends from previous years, where education was also the most targeted in 2022, and the second most targeted in 2023. Ransomware attacks were also high against public administration, manufacturing, and healthcare entities, suggesting ransomware actors focused their operations against large organizations that traditionally have a low downtime tolerance and/or limited security budgets.

Actors prioritize disabling security solutions frequently and early on in their operations

Ransomware operators endeavored to disable targets' security solutions in most of the Talos Incident Response (IR) cases we observed, almost always succeeding (see figure 2). They also modified certain solutions that could allow remote access and removed evidence of their activity.

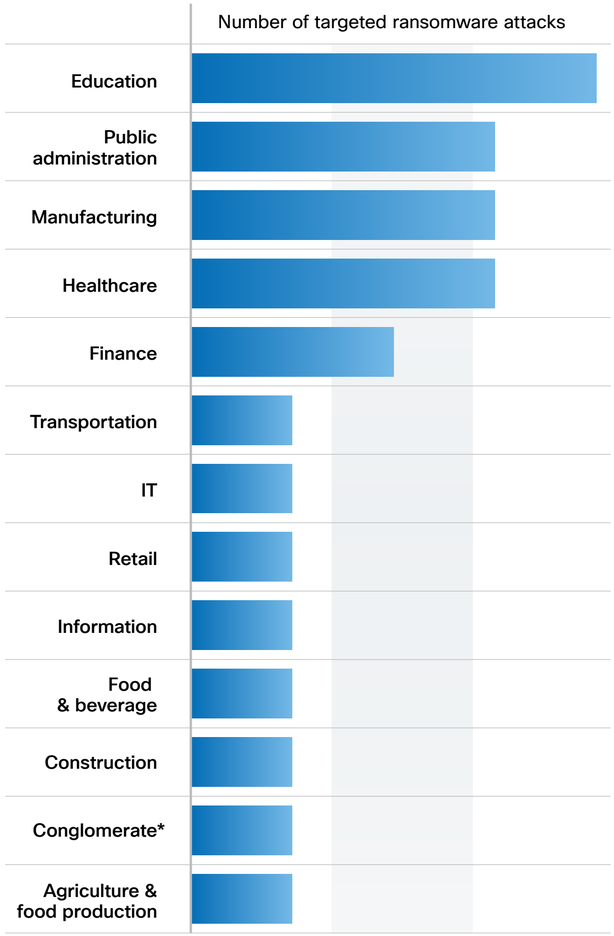
Separately, we also saw ransomware actors abuse poorly configured security solutions. Many out-of-the-box security products come with baseline/default policies enabled, but organizations often fail to configure these products specifically for their own network's needs. Therefore, we saw many cases where ransomware operations were successful in environments where security policies were set to "audit-only" mode, meaning that the product only alerted an administrator to malicious activity but did not automatically block it.

Initial access largely achieved via valid accounts

Ransomware actors overwhelmingly leveraged valid accounts for initial access in 2024, with this tactic appearing in almost 70 percent of related cases (see figure 3). This tactic is facilitated in large part by the sale of compromised credentials on dark web forums.

Figure 1

Targeted sectors



**Conglomerate organizations and their subsidiaries are not included in any other verticals.*

Figure 2

Disablement of security solutions

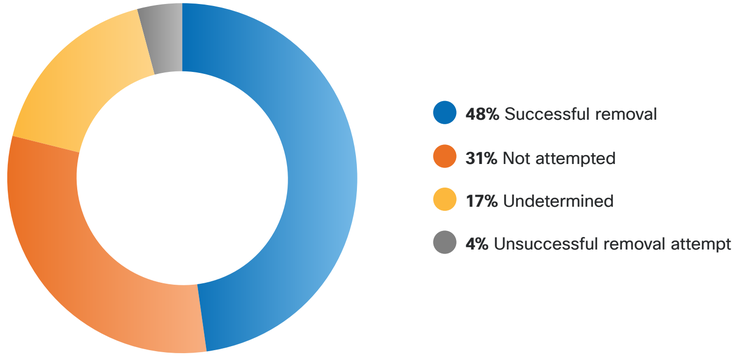
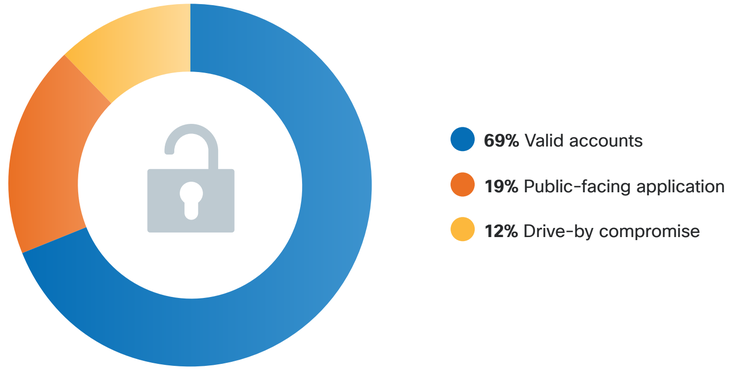


Figure 3

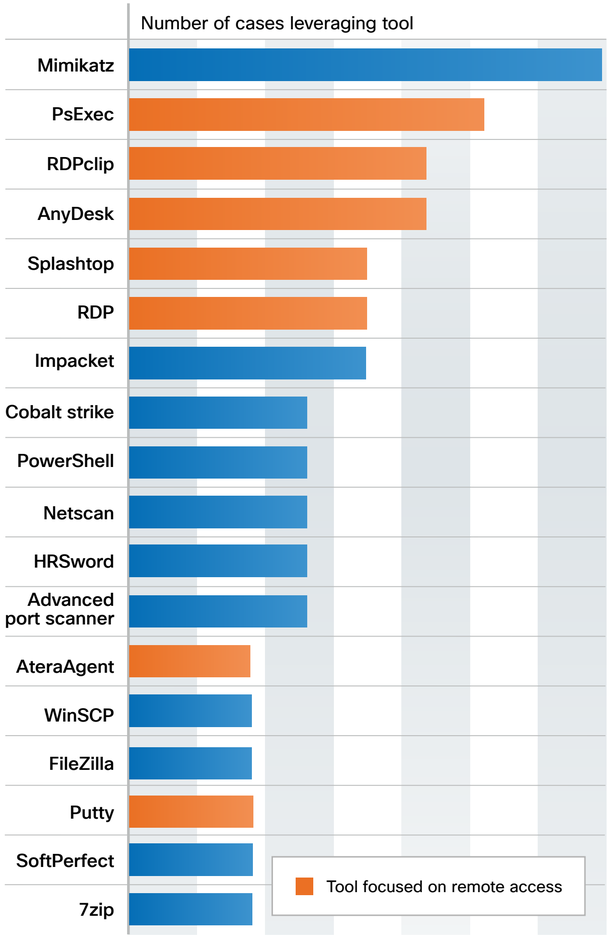
Initial access



CISCO TALOS

Figure 4

Top tools seen in Talos IR ransomware engagements



Actors rely heavily on remote access tools, commercial products, and LoLBins

Actors leveraged commercial products and living-off-the-land binaries (LoLBins) for command and control in their 2024 campaigns. Many organizations rely on legitimate remote access applications (such as AnyDesk and Splashtop) for daily operations, making detecting or blocking malicious use of these tools more challenging.

LockBit remained top player while newcomer RansomHub quickly ascended to the No. 2 spot

For the third year in a row, LockBit was the most active ransomware-as-a-service (RaaS) group. In a dynamic space defined by constant change and the rise and fall of new ransomware groups, this type of longevity is unexpected.

Newcomer RansomHub – a suspected successor of the Knight ransomware group that was first seen in February 2024 – followed close behind and has come to play a significant role in the ransomware landscape. RansomHub typically targets large organizations, likely in pursuit of hefty payouts. The average employee count of organizations targeted in RansomHub incidents Talos responded to this year was over 18,000 employees.

Akira, Hunter's International, INC Ransom, Qilin, and BlackSuit ranked in the top ten for most active RaaS groups this year but not last year, demonstrating how dominance shifts quickly in this threat landscape.

Release of decryptor is the game-changer in disrupting ransomware gangs

Ransomware actors are far less likely to fully rebound from a takedown if associated decryption tools are made publicly available. ALPHV's dominance plummeted after an FBI disruption at the end of 2023, which included law enforcement offering a decryption tool to affected victims that enabled them to restore their systems. This group was ranked second in our 2023 report and dropped to 22nd this year.

By contrast, LockBit was also targeted in a major takedown, but this operation did not include the release of a decryptor.

Figure 5

2024 volume of posts made to data leak sites by ransomware groups

- **16%** LockBit 3.0
- **11%** RansomHub
- **8.5%** Akira
- **7%** Play
- **5%** Hunters International
- **4%** INC Ransom
- **4%** Black Basta
- **4%** Qilin
- **3%** BianLian
- **3%** BlackSuit
- **3%** 8Base
- **2%** Cactus
- **2%** Everest
- **2%** FOG
- **2%** Rhysida
- **25%** Other

**Percentages do not add up to 100 due to rounding*