

M-Trends

2024 Special Report

Today's cybersecurity trends, developments, and impactful attacker operations revealed through frontline Mandiant incident response investigations and threat intelligence findings from January 1, 2023 to December 31, 2023.

Who Attackers Are

Mandiant experts currently track over 4,000 threat groups and activity clusters, which includes 719 newly tracked groups for this M-Trends reporting period.

In 2023, the active threat groups found across investigations included 4 financial threat groups (FIN), 2 advanced persistent threat groups (APT), and 310 uncategorized threat groups (UNC).



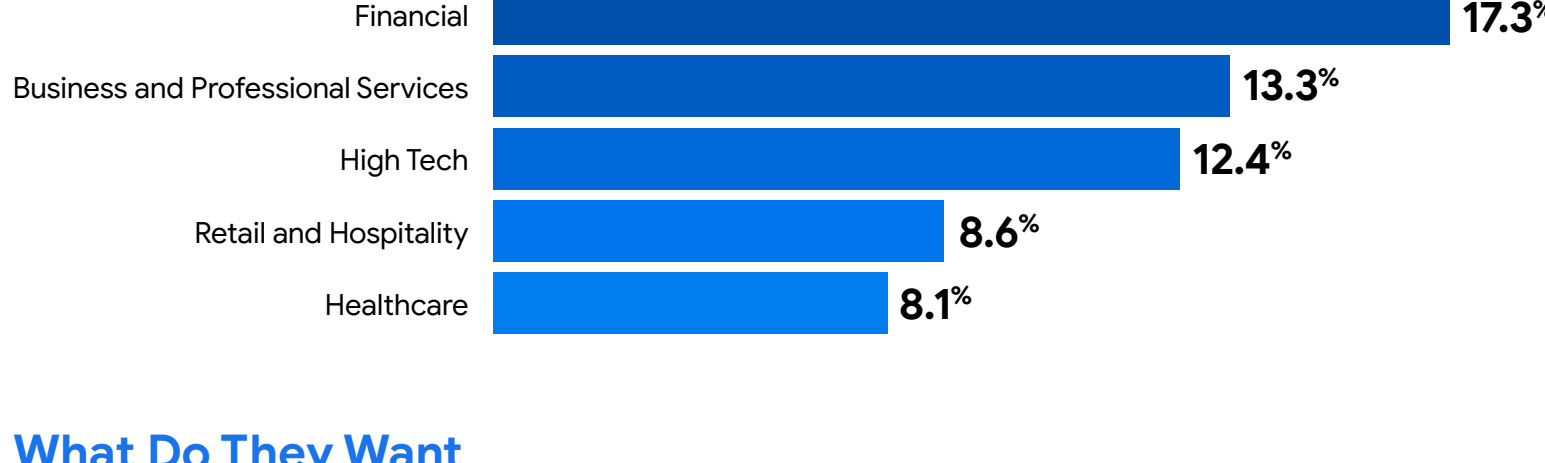
Threat Group Spotlight

APT43 is a prolific cyber operator that supports the interests of the North Korean government. This group possesses moderately sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and U.S. government organizations, academics, and think tanks focused on geopolitical issues surrounding the Korean Peninsula.

What Do They Target

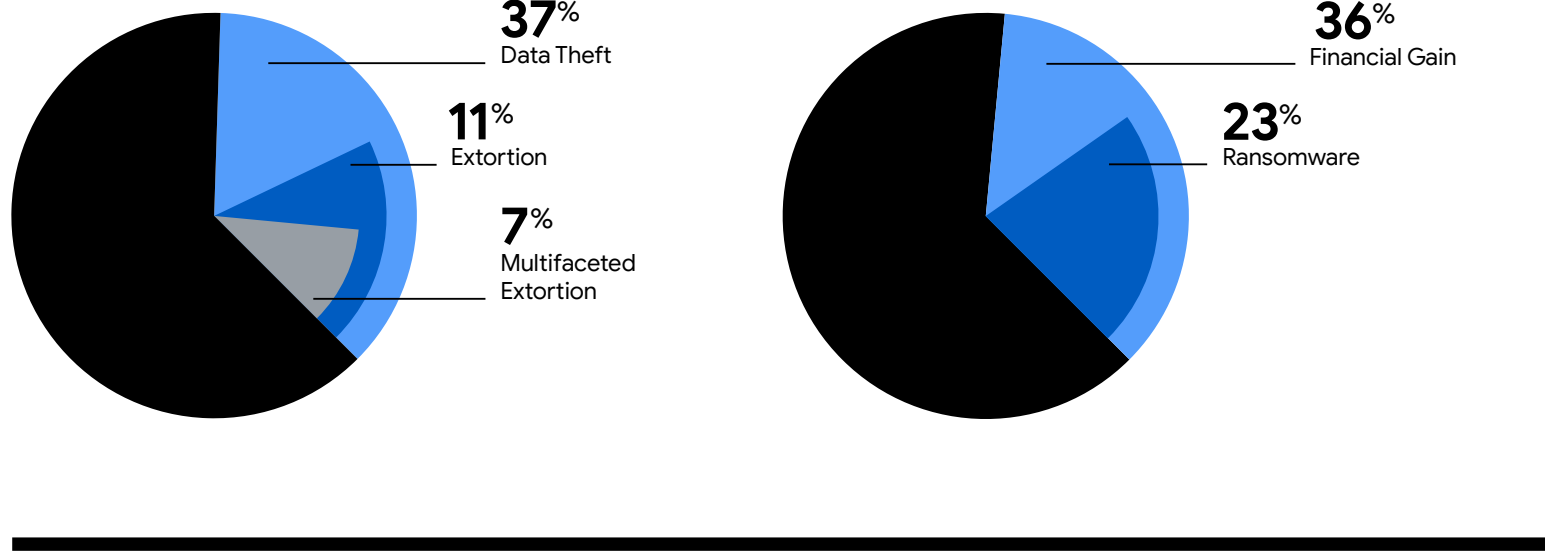
Top Industries Under Attack

Response efforts for financial services organizations captured nearly a fifth of investigations. The next four most targeted industries are consistent with Mandiant's observations over the last two M-Trends reporting periods.

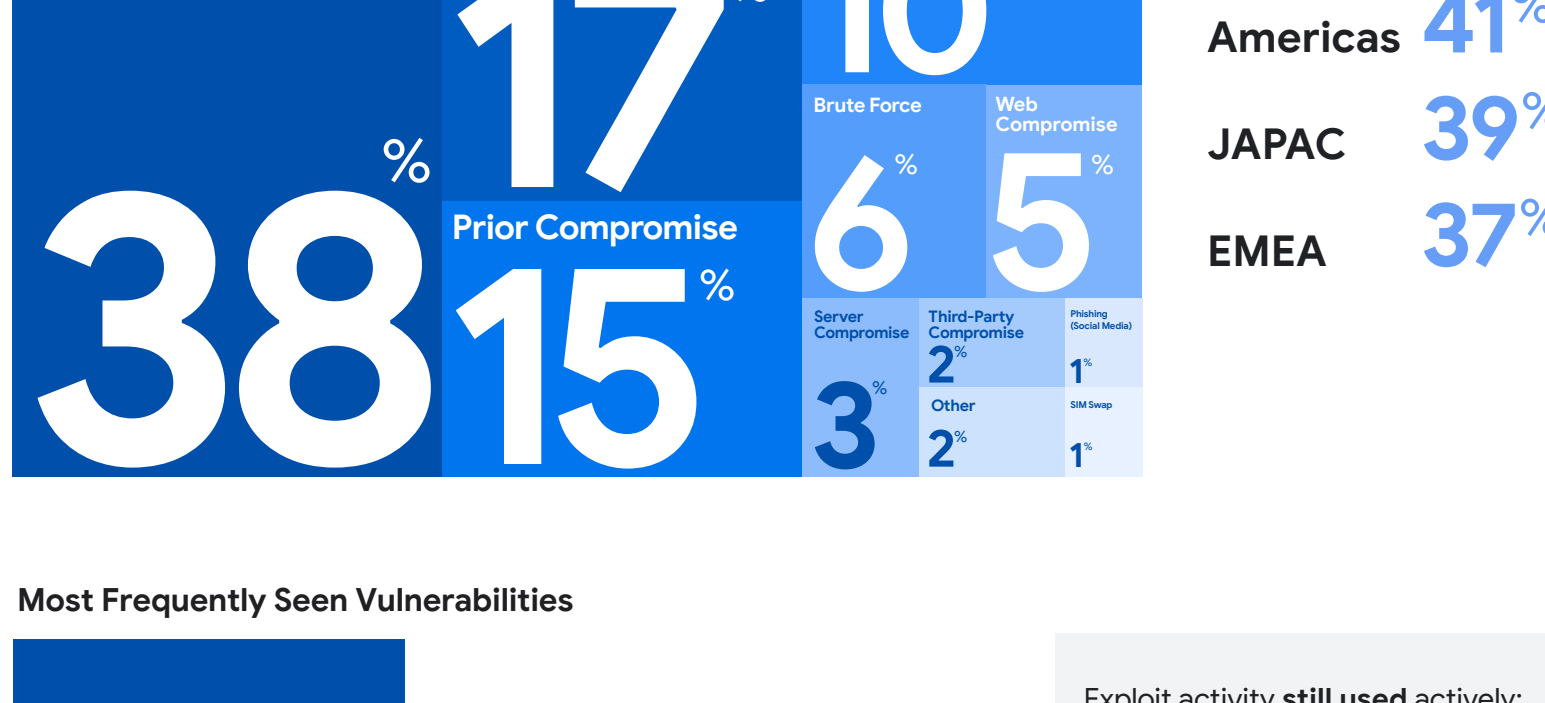


What Do They Want

Mandiant identified data theft in 37% of 2023 intrusions, which is slightly lower than the 40% of intrusions reported in 2022. The proportion of intrusions Mandiant responded to that served financially motivated objectives increased from more than a quarter of all investigations in 2022 to more than a third in 2023 at 36%.



Where Do They Attack



Most Frequently Seen Vulnerabilities

MOVEit Transfer
CVE-2023-34362

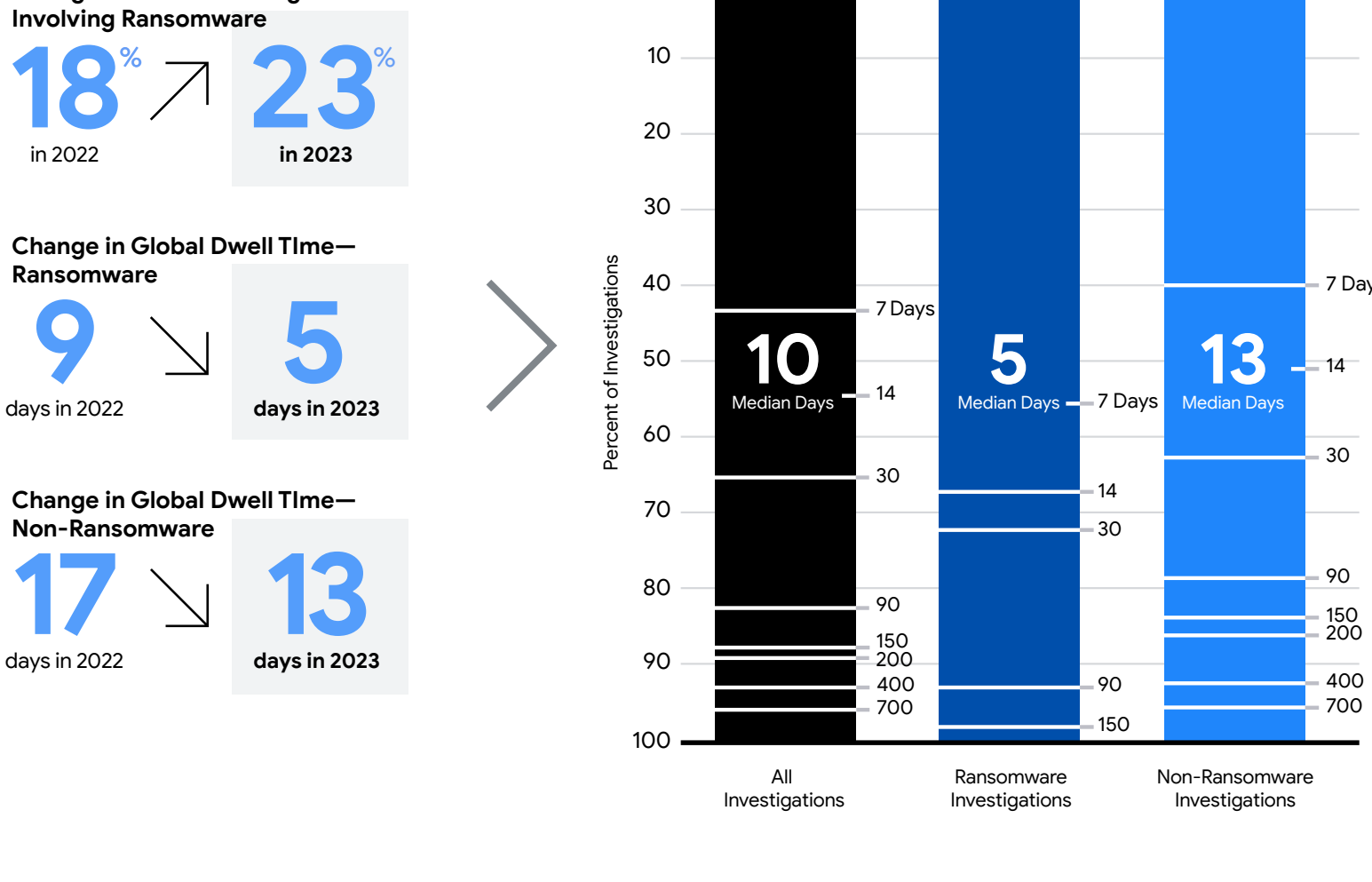
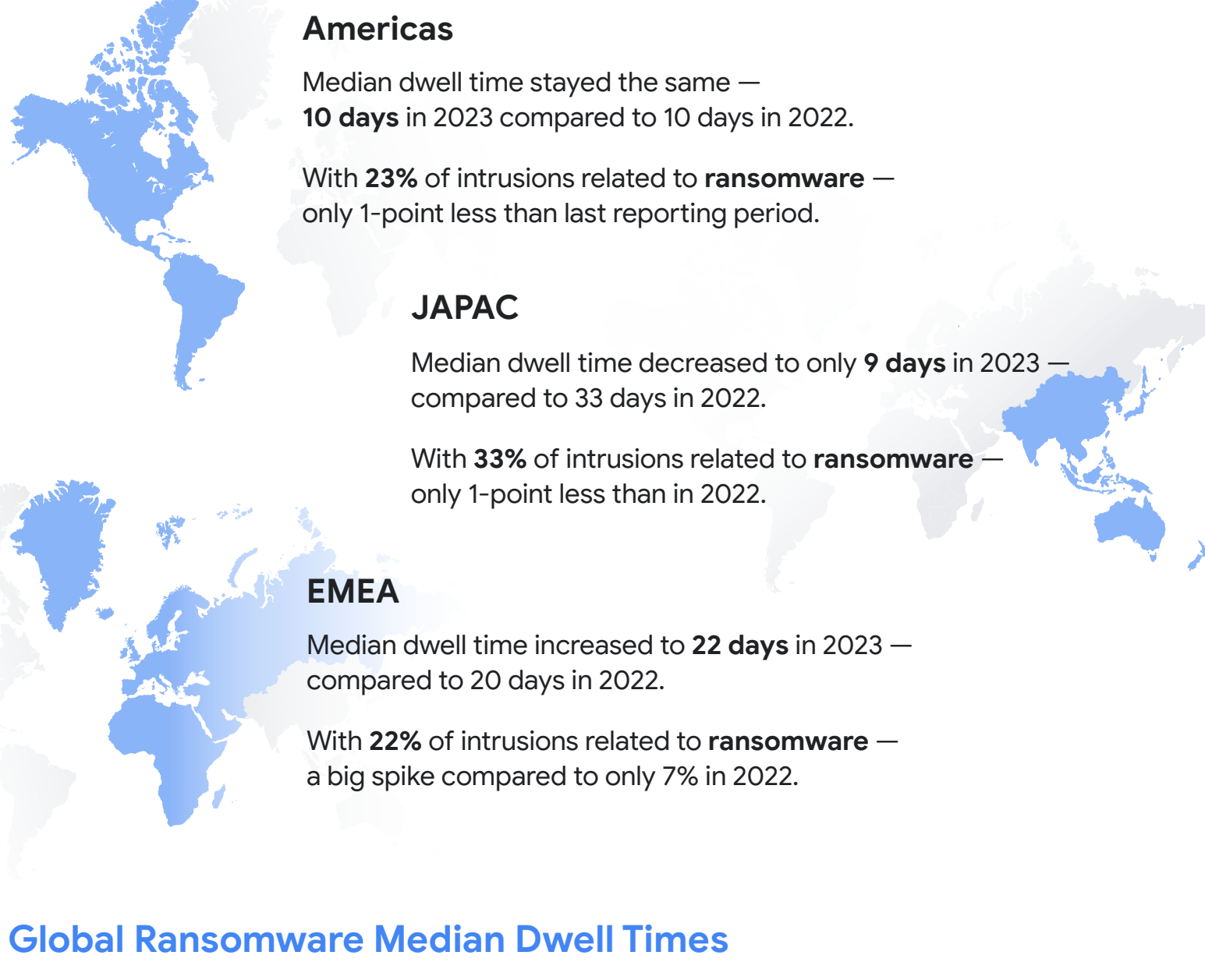
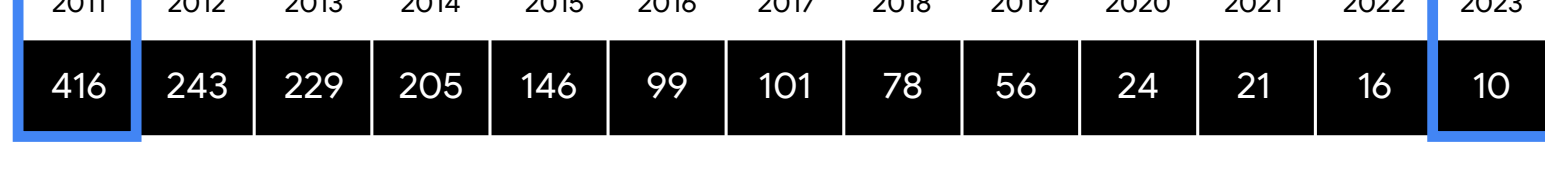
Oracle Web Applications Desktop Integrator
CVE-2022-21587

Barracuda Email Security Gateways
CVE-2023-2868

Exploit activity **still used** actively:

- Microsoft Access 2003
CVE-2008-2463
- Windows Server 2016
CVE-2017-0144
- Telerik
CVE-2019-18935

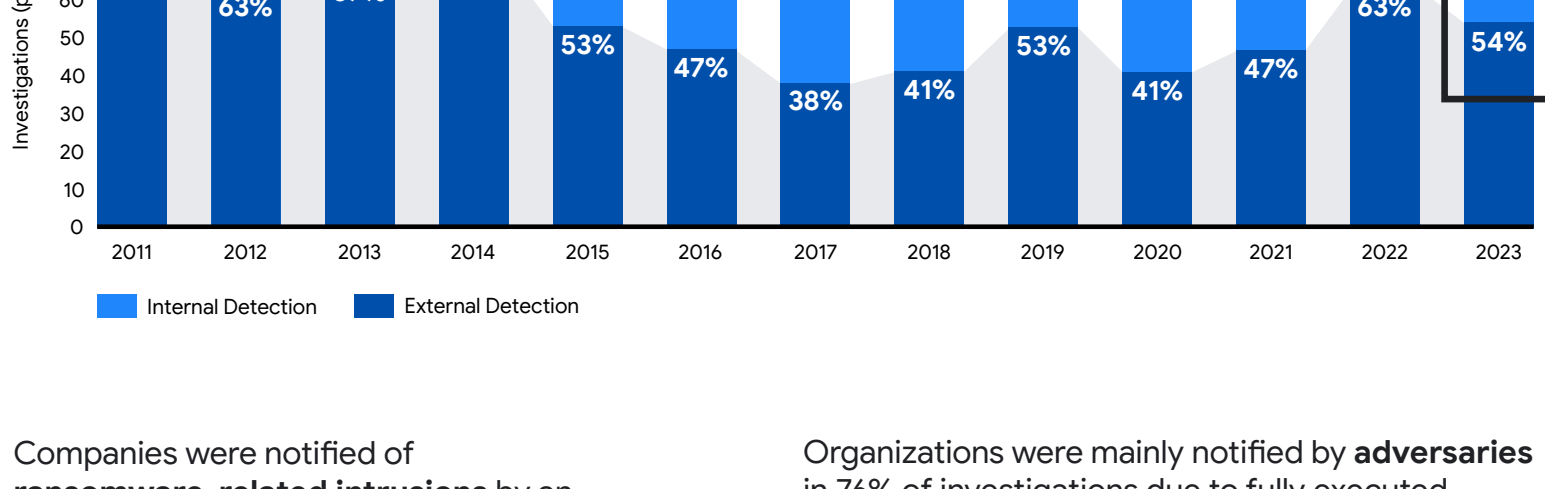
When Are Attackers Found



How Are Attackers Found

Internal detection is when an organization independently discovers it has been compromised.

External notification is when an outside entity informs an organization it has been compromised.



Companies were notified of ransomware-related intrusions by an external entity 70% of the time. Organizations were mainly notified by adversaries in 76% of investigations due to fully executed ransomware attacks detected by ransomware notes.

External partners make up the remaining 24% of ransomware investigations.

