2024 YEAR IN REVIEW & 2025 THREAT LANDSCAPE OUTLOOK

The Modern Threat Actors' Playbook: How Initial Access and Ransomware Deployment Trends are Shifting in 2025

eSENTIRE
THREAT RESPONSE UNIT

Executive Summary

The ever-growing complexity of cyber threats demands a deep understanding of the Tactics, Techniques, and Procedures (TTPs) used by malicious threat actors to infiltrate, persist, and ultimately fulfill their objectives within an organization.

These insights are essential for mitigating cyber risks, minimizing downtime, and establishing a robust security posture that can withstand even the most sophisticated cyber threats.

Latest research conducted by the eSentire Threat Response Unit (TRU) highlights the most pressing threats impacting global organizations. These threats include business email compromise (BEC) attacks, signed malware (e.g., Lumma, NetSupportManager RAT, etc.), and ransomware.

When it comes to malware gaining access into organizations, TRU continues to see an increase in valid credential abuse and browser-sourced threats. While malware sourced from emails has declined, email remains the second most common initial access technique for malware deployments.

As we step into 2025, we project an increase in politically motivated cyberattacks, with adversaries disrupting the physical infrastructure of the Internet to disrupt internet access. We will also see continued growth in ransomware attacks against all industries, abuse of certificate authority, and an increase in browser-based threats to deploy malware.

In this report, we highlight the trend of ransomware attacks originating from out-of-scope endpoints and the subtle shifts in attacker behavior, particularly in pivoting from email to browser-based threats.

Our research highlights the pressing need for a multi-faceted cybersecurity strategy that integrates 24/7 real-time threat detection and response, actionable threat intelligence to develop novel detections, comprehensive endpoint protection, and proactive measures against advanced emerging cyber threats.

Initial Access: How Malware Enters Corporate Environments

All attacks start by gaining an initial foothold in the target environment. Most often, this occurs by tricking employees into downloading malware onto their machines or compromising third-party vendor accounts with access to your network or cloud resources.

These initial access methods usually exploit existing vulnerabilities or compromised credentials to remote access services like Virtual Private Networks (VPNs) or Remote Desktop Protocols (RDPs).

Failure to identify and disrupt these initial footholds in a timely manner can lead to severe consequences, such as ransomware deployment and the resulting financial, and legal, costs of incident response.

Therefore, it is vital for security professionals to understand how cybercriminals gain unauthorized initial access and the most common TTPs used by attackers.

As seen in Figure 1, based on the attack volume observed by TRU, the top initial access vectors are valid credentials, browsers, email, removeable media, and remote exploits.

The use of valid credentials dominated as an initial access vector in 2024. This vector captures cases where compromised credentials were used to access network

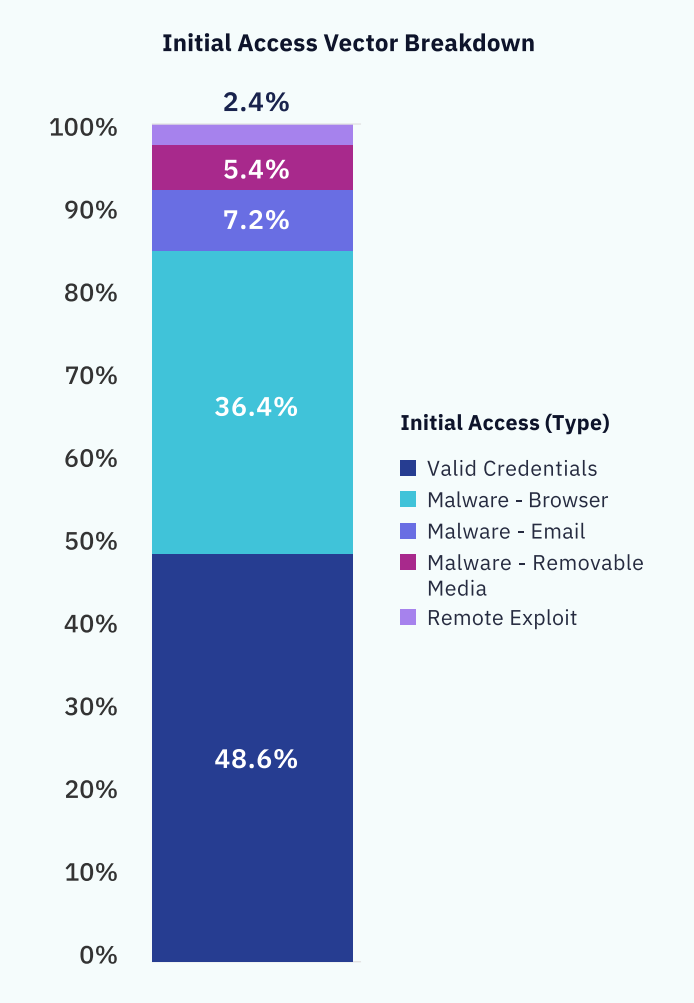


Figure 1: Breakdown of Initial Access techniques observed by TRU in 2024.

resources and further the attacker's objectives. This can include configuring email forwarding rules for BEC attacks or remotely accessing the network via VPN or RDP.

Much of the reliance on credentials is unsurprising given how widely available user credentials are across the Dark Web. In fact, fraud shops particularly offer a one-stop-shop for locating high-value credentials for network access, often for as little as $10 USD.

Based on TRU's observations, compromised credentials were most often detected at the email layer, which accounted for a significant percentage of incidents in 2024. A subset of these detections was traced to Adversary-in-the-Middle (AiTM) Phishing-as-a-Service (PhaaS) operations.

Like Malware-as-a-Service (MaaS) operations, PhaaS arms low-skilled threat actors with advanced capabilities and even a "phishing kit" to launch attacks. Often, these "phishing kits" include email templates, fake website templates, list of potential targets, detailed instructions, and even customer support.

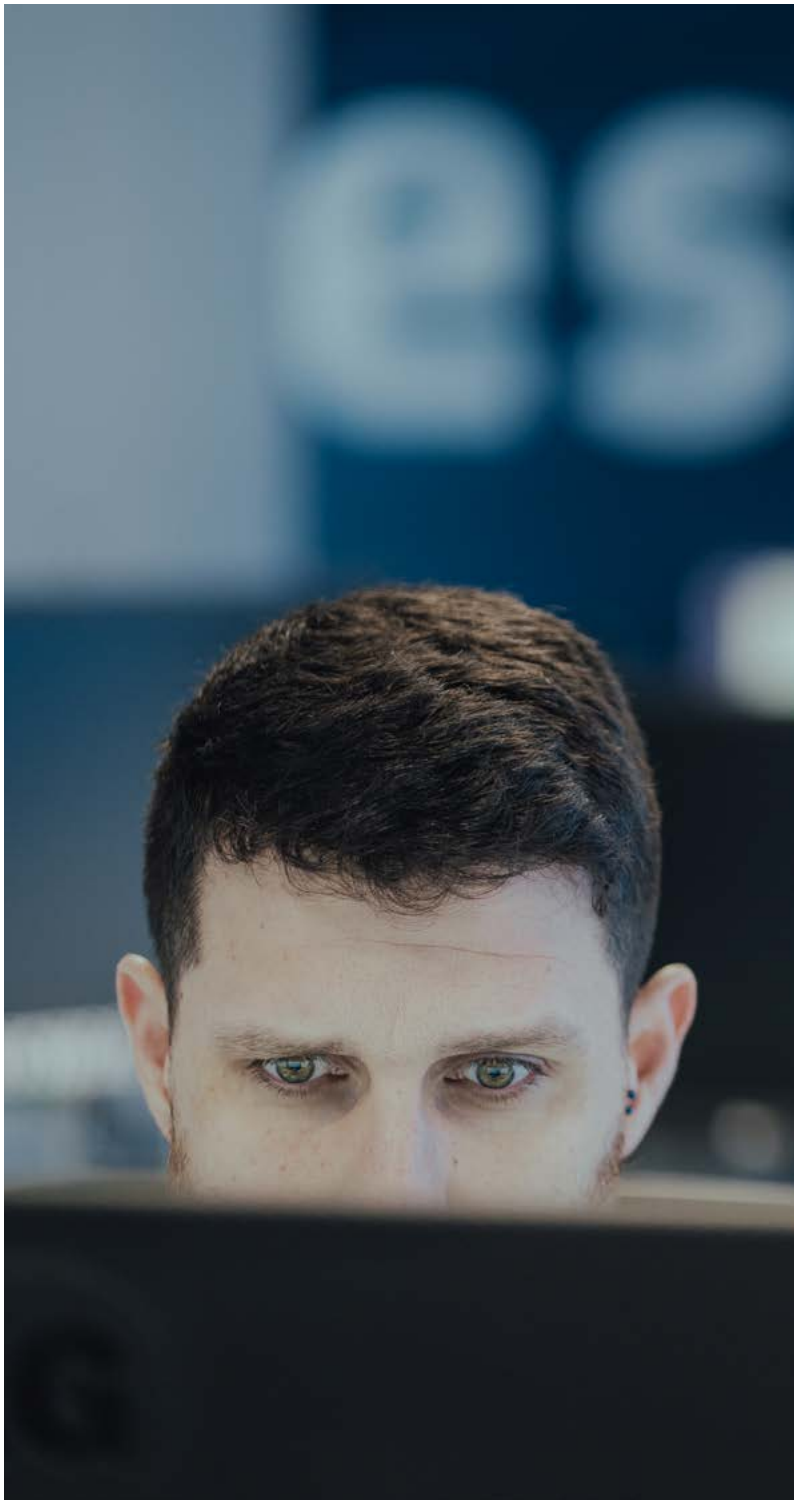
In comparison to email, the use of compromised credentials for remote access services remained uncommon, but impactful. While email access is motivated by Business Email Compromise (BEC) and other fraud, remote access services like VPN or RDP can offer direct access to a target's internal network and resources.

This VPN access allows the threat actor to bring their own unmonitored device onto the network using stolen credentials. In most cases, these accounts were not protected by Multi-Factor Authentication (MFA), specifically phish-resistant MFA.

However, organizations that have already implemented traditional security measures against credential compromise (e.g., MFA, MDM, etc.) should consider a **Dark Web Monitoring** service that alerts when credentials are offered for sale.

Threat actors continue to deploy malware successfully by using drive-by download techniques, noted as Malware – Browser in Figure 1, over email. They have driven innovation in browser-based threats to craft convincing web lures and increase resistance against takedowns from law enforcement agencies.

The Lumma Stealer Malware-as-a-Service (MaaS) contributed a large portion of malware cases in 2024 and was seen employing various initial access techniques throughout the year.



Most Impactful Initial Access Vectors

While browser-sourced malware and compromised email credentials were the most common threats observed in 2024, they were also some of the most impactful. To measure the impact, we rely on the intrusion ratio, which measures the fraction of incidents where the attack moved beyond the initial access phase and intrusion actions were identified (Figure 2).

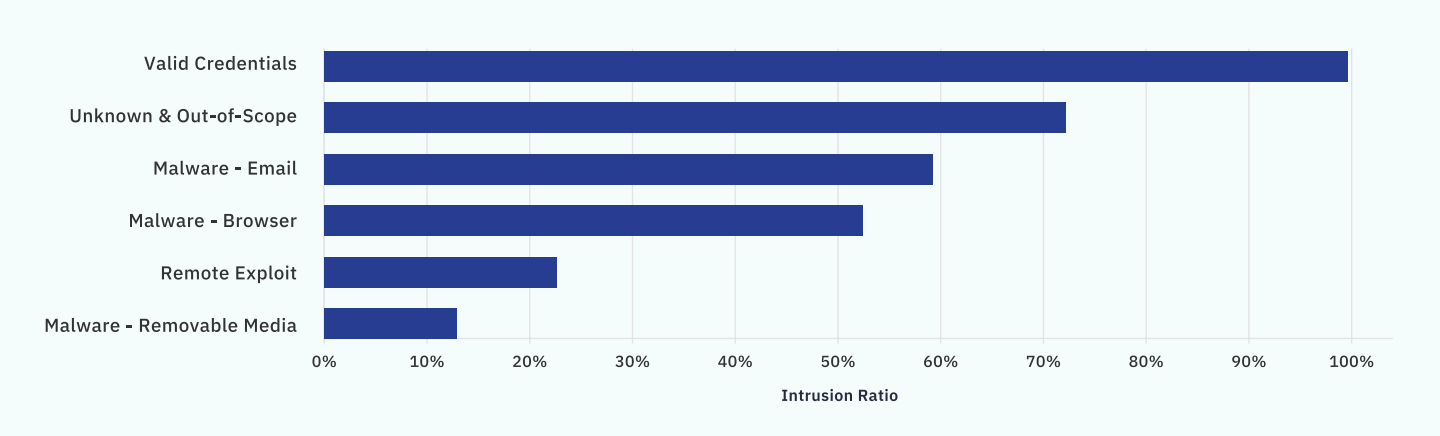


Figure 2: Intrusion ratios by initial access vectors.

Moreover, when combined with initial access vector, the intrusion ratio can reveal possible blind spots in security monitoring and controls, particularly when the threat is detected post-initial access.

For example, consider a scenario where a threat actor gains access to the network using stolen VPN credentials. Due to a lack of controls (i.e., MFA on the VPN Gateway) and/or 24/7 security event monitoring (i.e., VPN logs not captured or monitored), the attacker can begin scanning and exploiting internal hosts, enabling them to move farther along the kill chain. It's not until the threat actor is detected by endpoint telemetry on monitored systems that the organization is alerted to the malicious activity.

This was a common scenario TRU observed in 2024, particularly for impactful incidents such as hands-on-keyboard ransomware attacks.

With intrusion ratios of 100% and 54% respectively, valid credentials and browser-sourced malware being two of the most common, and impactful initial access vectors is particularly concerning.

This is because it suggests that attackers leveraging email and valid credentials frequently succeed in escalating their attacks beyond initial access, enabling them to achieve more advanced stages of intrusion.

'Unknown' and Out-of-Scope Access Vectors

Much like in last year, blind spots due to a lack of monitoring on devices continue to be a problem for organizations and security defenders alike. Figure 2 shows the intrusion ratio of these blind spots, denoted as Unknown & Out-of-Scope, wherein the intrusion was identified but traced to unmanaged systems.

This is both a configuration issue and a purposeful tactic on the part of adversaries. Unfortunately, security teams cannot protect systems they cannot see, and adversaries continue to exploit these blind spots by bringing their own systems

onto a network using VPN or by exploiting out-of-scope endpoints such as personal devices.

Out-of-scope endpoints are particularly a growing concern for businesses who rely on third-party vendors. Incident response teams have discovered that a subset of compromised credentials belonged to contractor accounts, where their unmanaged devices were infected with infostealer malware.

This is further supported by **Microsoft's Digital Defense Report 2024**, which stated that 90% of cases where attacks progressed to the ransomware deployment stage originated through unmanaged devices.

Valid Credentials Stolen from Personal Devices

QR Code phishing has emerged as a popular technique, aimed at pushing malicious content to personal devices instead of monitored systems.

The technique, which is employed heavily by **Phishing-as-a-Service** (PhaaS) operations, requests the victim scan an image with their phone, then input their authentication information using their device.

Security teams may not detect the account has been compromised until days or weeks later when an adversary attempts to exploit the account for fraud. In 2024, **TRU upped their efforts** to protect eSentire's customers from PhaaS operations and detect compromises even when the compromise occurs out-of-scope.

MSP's Remote Management and Monitoring (RMM) Application Exploited by Bl00dy Ransomware

In early 2024, eSentire's team of 24/7 SOC Cyber Analysts investigated attempts to execute ransomware binaries and scripts in several customer environments. These attempts, which were prevented by eSentire MDR for Endpoint, were traced to ScreenConnect's remote access clients.

Further investigation revealed these customers employed the same managed service provider, who's ScreenConnect instance was vulnerable to several **high severity vulnerabilities**.

eSentire's Threat Response Unit (TRU) continues to work hand-in-hand with our team of 24/7 SOC Cyber Analysts to focus on early threat detection and disruption across our customer base. We continuously process and analyze security incidents to assess the efficacy of detection and response playbooks.

Initial Access Vectors by Industry

When examining the breakdown of initial access methods by industry, TRU's data shows certain industries are more susceptible to particular initial access vectors over others (Figure 3).

For example, the Construction and Transportation industries saw a greater share of valid credential abuse, primarily in phishing and BEC incidents. This is likely due to increased reliance on remote workforces and job sites within these industries where unmanaged devices (e.g., a construction worker's personal phone) are more common.

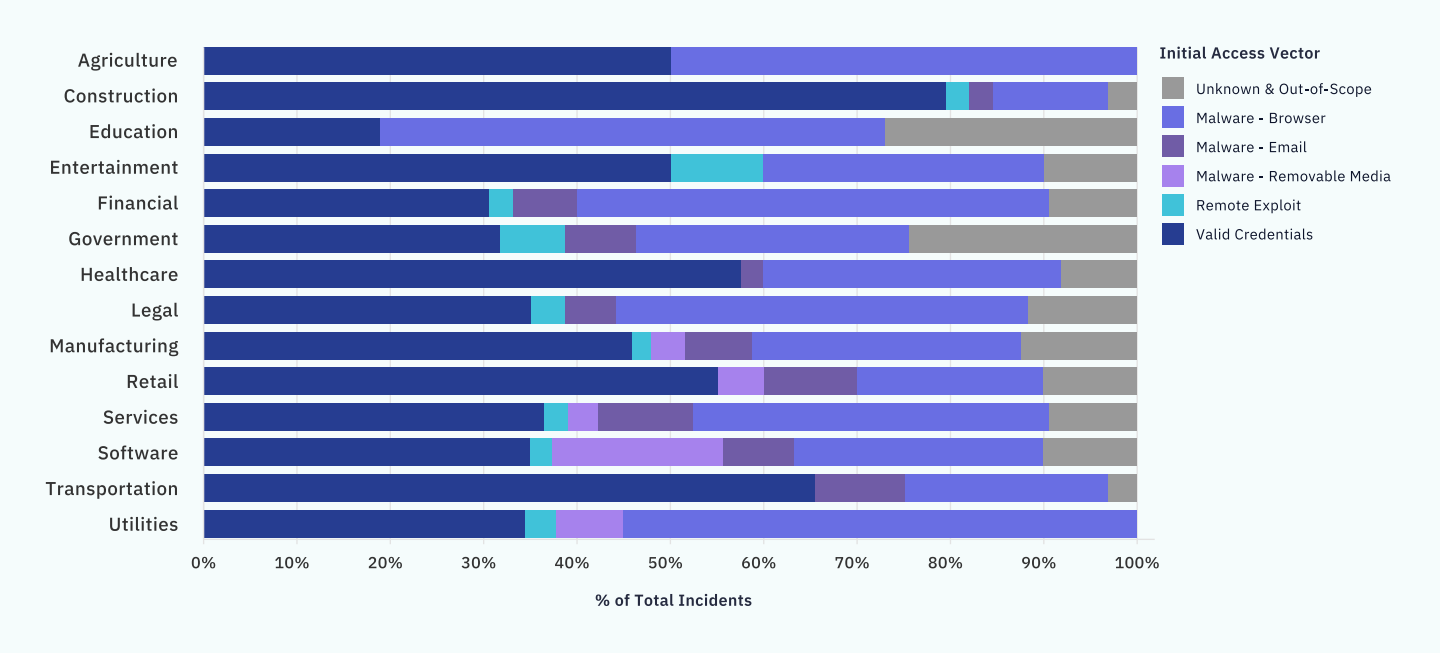


Figure 3: Industry breakdown of initial access vectors.

On the other hand, the Education industry saw the greatest proportion of browser-sourced malware and 'unknown' initial access vectors, which can be attributed to several factors.

First, employees in this sector are made up of educators, administrative staff, and students often sharing segmented but linked networks. The 'unknown' vector often points to out-of-scope endpoints or network segments as the origin for intrusions; in this case, student WiFi networks provide one such possibility.

Second, educators often use search engines to find documents such as lesson templates, exposing them to malware distributed via search advertisements or SEO poisoning.

Agriculture and Utilities industries were also heavily impacted by browser-based malware. The past year has seen an **increase** in the targeting of the **Agricultural** sector from cyberattacks. This may be due to the Agriculture industry presenting as a 'soft target' for threat actors since these organizations have been slower to adopt controls to mitigate the risk of cyberattacks.

On the other hand, the Utilities sector has continued to be a top target for threat actors. Although Utilities organizations generally have more mature cybersecurity operations, they likely focus on educating their employees specifically on phishing emails.

As threat actors continue to shift their initial access techniques to focus on techniques like search engine optimization (SEO) poisoning, organizations in the Utilities sector will have to update their PSAT training to include this returning technique for initial access.

Another industry that continues to standout with respect to browser-sourced malware is the Legal industry, which saw the greatest percentage of GootLoader malware cases in 2024 relative to their observed threats. GootLoader is distributed through poisoned search results (tracked as Search Engine Optimization Poisoning) for document templates commonly in the form of contracts and other legal agreements.

Key Recommendations to Defend Against Initial Access Vectors

Initial access represents the most critical stage of a cyberattack, one in which the threat actor's success depends on exploiting vulnerabilities to enter your network and establish a foothold.

- Therefore, we recommend focusing on proactive cyber defense strategies to reduce risk and better anticipate the initial access vectors that threat actors rely on:
- Conduct regular **phishing and security awareness training exercises**, especially those that train against browser-based attacks, including current social engineering tactics. The training should include exposure to real-world malware campaigns, such as:
    - **Pikabot**, which uses malvertising, especially with **Google Ads**
    - **Lumma Stealer** and **FakeBat**, which uses fake browser updates
    - **RATS and Infostealers**, which use free software or software bundles
    - **Advanced Persistent Threats**, which rely on fake job postings
- Protect your endpoints with comprehensive endpoint coverage to catch User Execution tactics before initial access malware evolves into an intrusion foothold. Implement an **endpoint detection and response (EDR)** tools to detect and contain threats, and ensure all endpoints are covered to remove any blind spots.
- Implement a network detection and response (NDR) tool and log monitoring solution to protect against **remote exploitation** and the exploitation of services that run on http servers (like Windows IIS and SSL VPNs), which can only be detected with proper logging of the relevant server software.
- Know your asset inventory and prioritize actively exploited vulnerabilities that overlap with your tech stack.
- Use phish-resistant multi-factor authentication (MFA) to increase resilience against intrusions that use stolen credentials to get past VPN gateways.
- Deploy a Mobile Device Management (MDM) solution to restrict network from non-compliant devices can also greatly reduce risk.
- Use a **Dark Web Monitoring service** to protect your organization with early detection of compromised user credentials on the Dark Web and minimize unauthorized access.

Understanding How Malware Trends Have Shifted

Building on the broader discussion of initial access trends, it's important to focus on how these methods are specifically leveraged for malware delivery.

Building on the broader discussion of initial access trends, it's important to focus on how these methods are specifically leveraged for malware delivery.

TRU's research highlights the tactics most frequently used by threat actors to deploy malware within corporate environments, and how these tactics have shifted between 2023 and 2024 (Figure 4).

Browser-based delivery, which includes techniques such as malicious advertisements (malvertising), search engine optimization (SEO) poisoning, and fake browser updates continues to trend upwards.

Browser-based initial access methods accounted for 70% of malware cases analyzed by TRU.

On the other hand, malware delivery via email continues to trend downwards from 22% in 2023 to 15% in 2024, which may be due to increasing implementation of Phishing and Security Awareness Training (PSAT) programs by organizations.

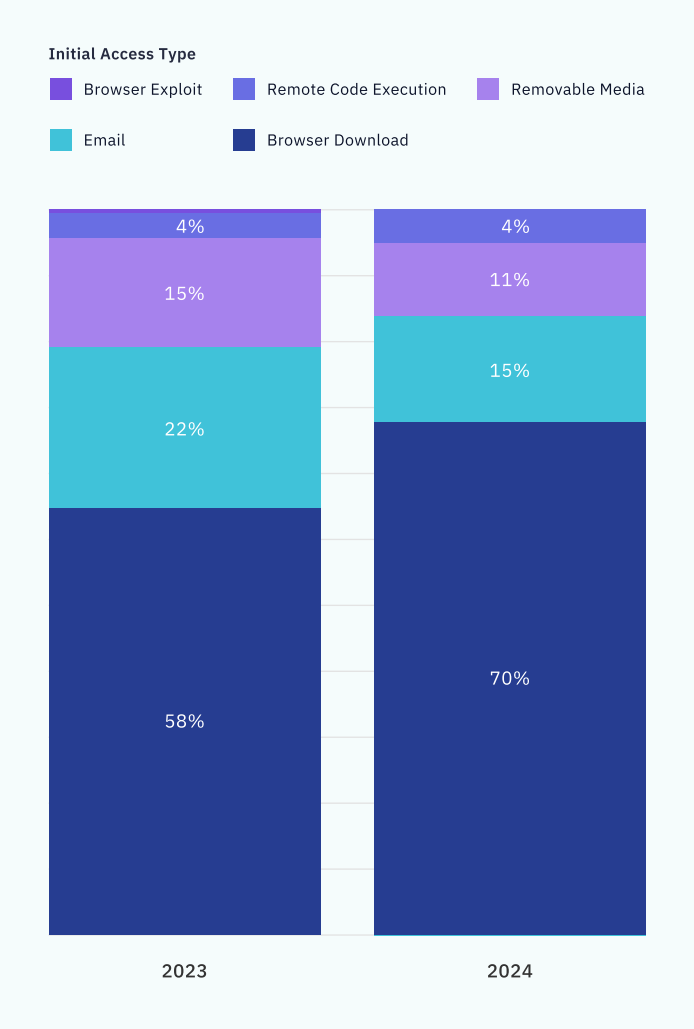


Figure 4: Initial access types as a percentage of malware cases by year.

ClickFix: Emergence of a New Malware Delivery Method

When examining malware delivery methods throughout 2024, a new method emerges – the "ClickFix" method.

Although it initially appears in Q2 2024, it takes flight in Q3, before accelerating in Q4 2024 (Figure 5).

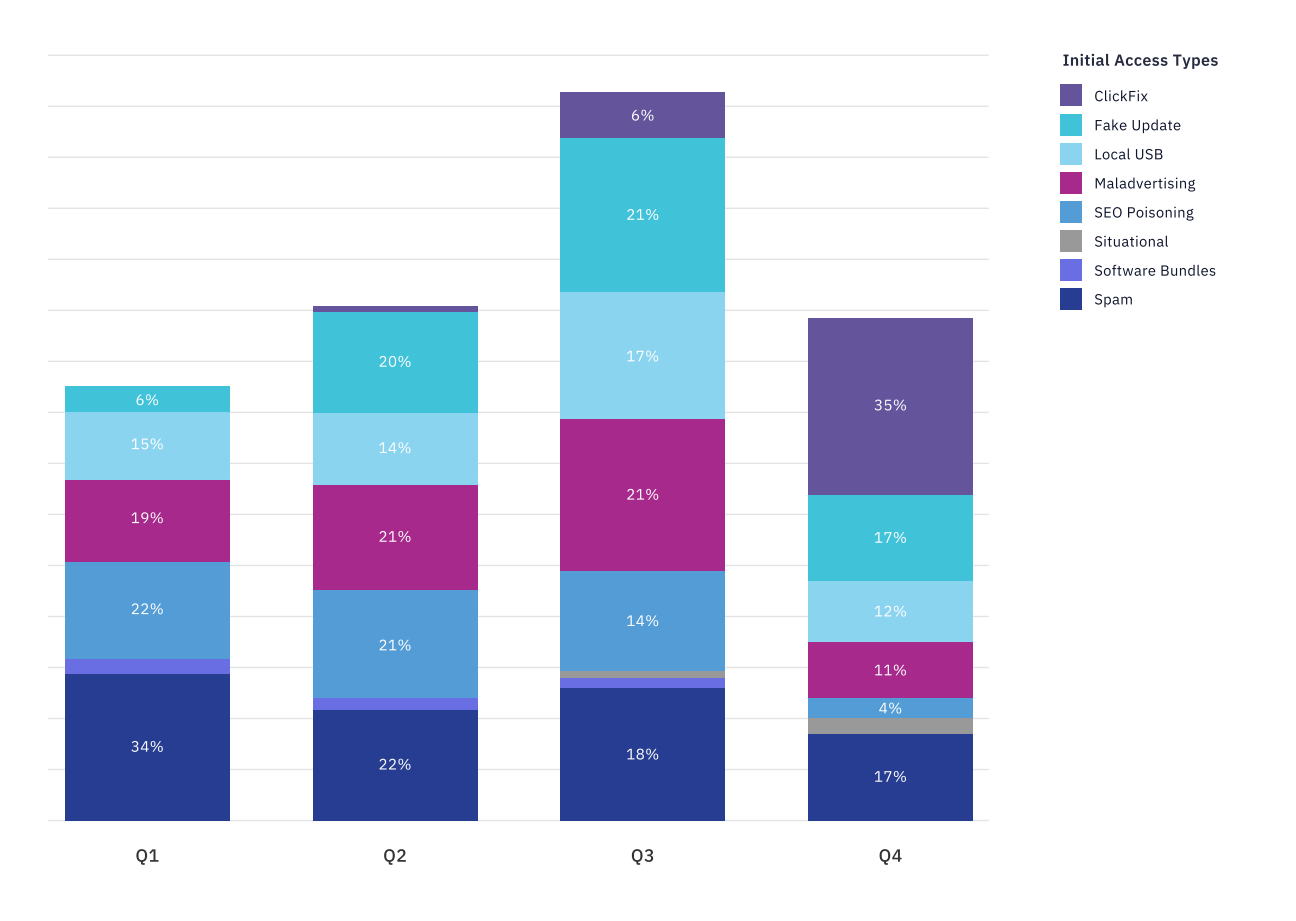


Figure 5: Malware delivery trends throughout 2024.

Initially discussed by TRU in the **November Threat Intelligence Briefing**, ClickFix is a social engineering technique which involves manipulating victims into running malicious commands, typically PowerShell, via a copy-paste prompt posing as CAPTCHA challenges.

Infostealers and RATs Remain a Popular Choice for Cybercriminals

Infostealers and remote access trojans (RATs) remain favored by cybercriminals with the goal of monetizing user credentials as well as data and network access as quickly as possible (Figure 6).

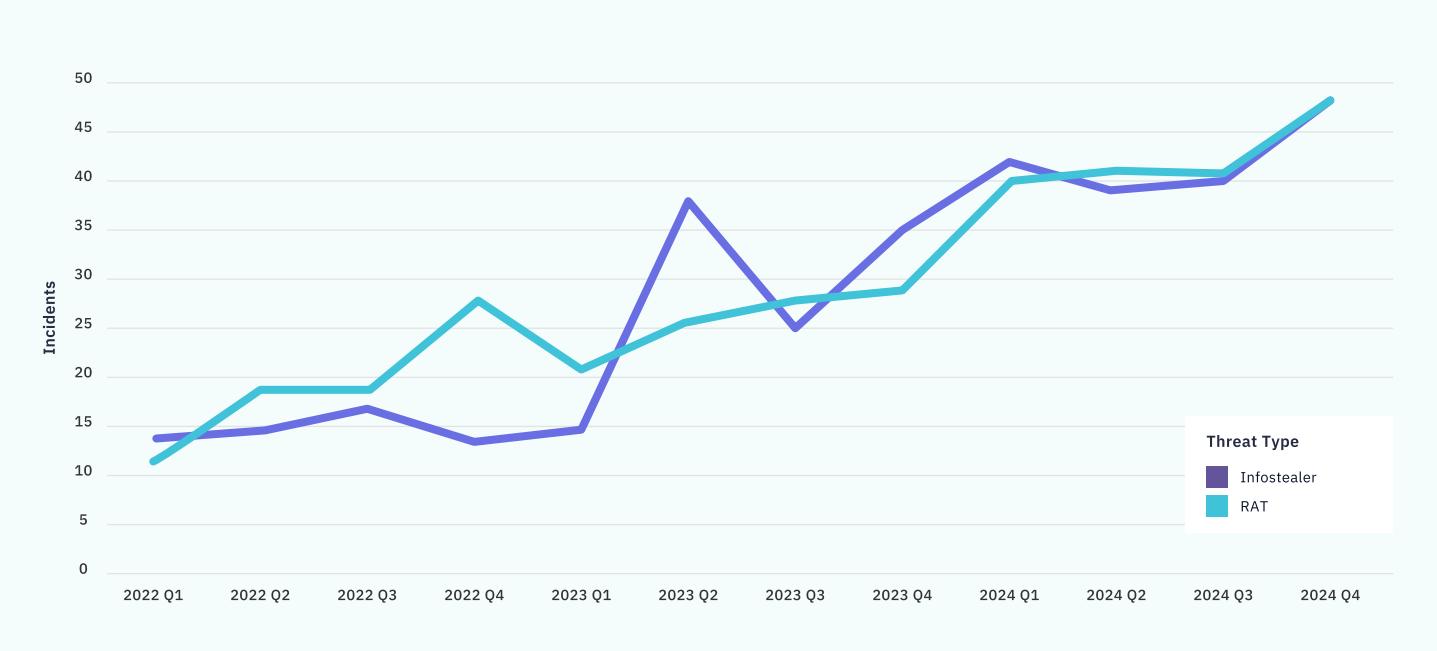


Figure 6: Incidents involving infostealers and RATs since 2022.

TRU observed a 31% increase year-over-year in the number of infostealers cases, largely due to the popularity of the **Lumma Stealer malware**. There was also an increase in distinct infostealers used, with 35 detected in 2024 vs. 26 in 2023.

For example, infostealers such as **Koi Stealer**, **Poseidon**, Purelogs, **Invisible Ferret** were among some of the newly detected threats in 2024. Invisible Ferret in particular is notable for its connection to North Korean threat actors and OS-agnostic approach which uses pre-packaged Python libraries and scripts to steal data from Windows, Mac and Linux users.

On the other hand, RATs such as NetSupportManager and ConnectWise are used to gain an initial foothold or maintain access by hands-on-keyboard operators. In fact, NetSupportManager was identified in 6.2% of cases in 2024, commonly arriving via installer packages disguised as popular software or browser updates.

CASE STUDY

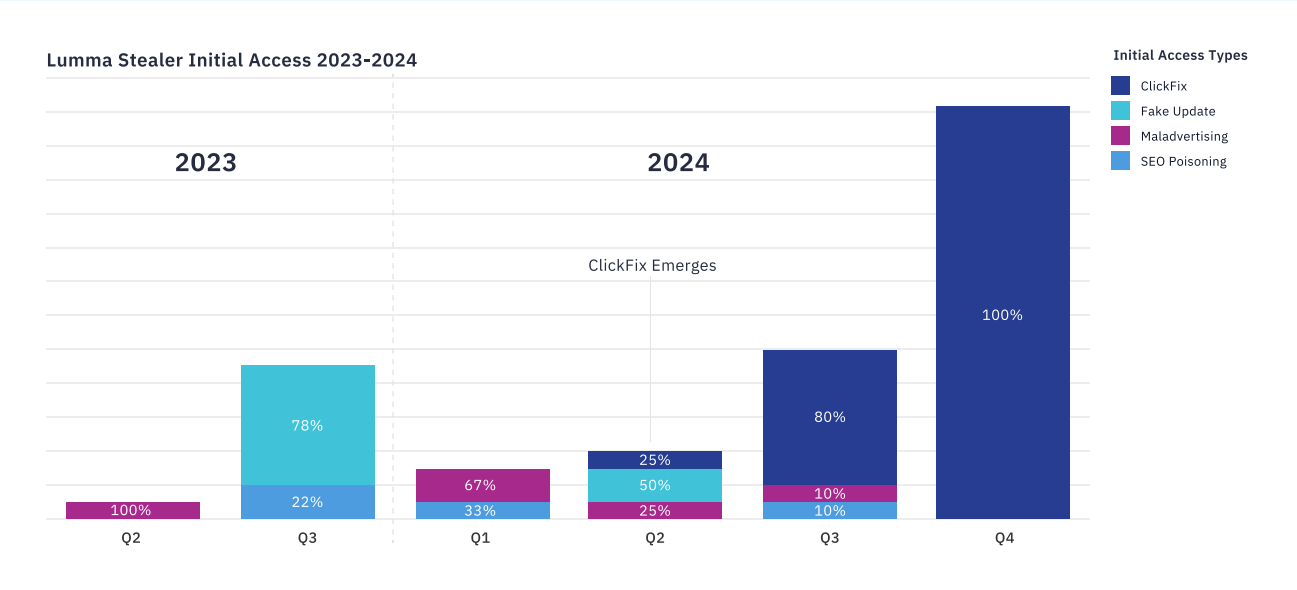
A Rise in Lumma Stealer (aka LummaC2) Malware

Emerging in 2022, Lumma is a popular malware-as-a-service offering that targets data belonging to crypto applications, financial institutions, and remote access services. Lumma monetizes logs as effective as possible by using stolen account credentials to drain accounts and/or sell stolen credentials on underground marketplaces such as Russian Market.

One likely factor for Lumma's popularity is its success rate, claimed to be between 75-85%, and its capability to filter and highlight high-value logs/credentials for rapid monetization.

Regardless, Lumma offers a flexible foothold for monetizing a compromised asset and pushes these capabilities down to low-skilled actors while allowing others to focus and improve on other phases of their operations.

As a MaaS offering, customers are free to use the best available methods or services to deploy the malware. In fact, Lumma even offers reporting on which channels are most effective. The figure below shows the different initial access methods used by Lumma in throughout 2023 and 2024.



Initial Access percentage breakdown by quarter, Lumma cases.

The data indicates Lumma's success rate with the ClickFix technique surged in Q3 and Q4 2024, driving nearly all infections in the second half of the year.

Good ideas are usually copied among cybercriminals and given the popularity of this malware-as-a-service, it can almost be seen as a bellwether for initial access techniques employed by other threats. More iterations on the ClickFix technique are likely to continue into 2025.

User Account Compromise and Business Email Compromise Enabled by AiTM and Phishing Services

Business Email Compromise (BEC) continues to be a concern, with billions of dollars and hundreds of thousands of **reported victims**. Accounting for customer growth, 2024 saw a 70% increase in detected user account compromises and BEC cases compared to 2023.

TRU's research highlights that the availability of Adversary-in-the-Middle (AiTM) and phishing services have greatly increased opportunities for low-skilled actors to conduct credential phishing attacks.

As seen in the figure below, BEC attacks are broken down into several phases:

1. Compromise accounts through phishing or credential stealing malware.
2. Access the email account.
3. Identify emails involving financial transactions.
4. Intercept and modify these transactions to reroute payments.

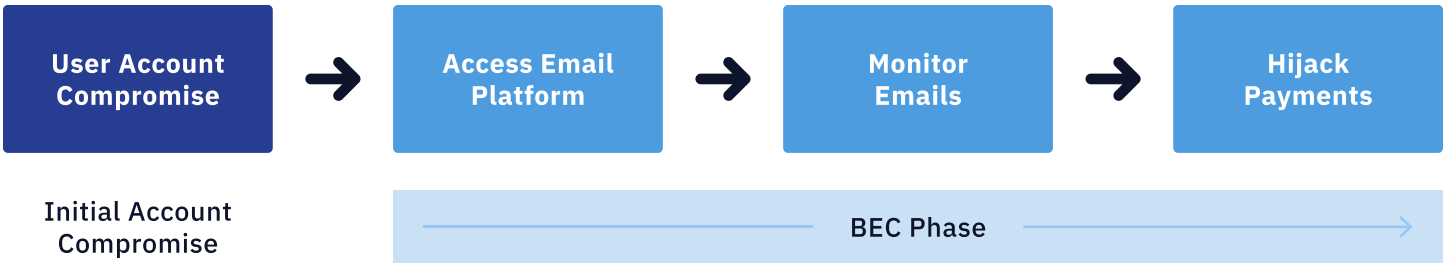


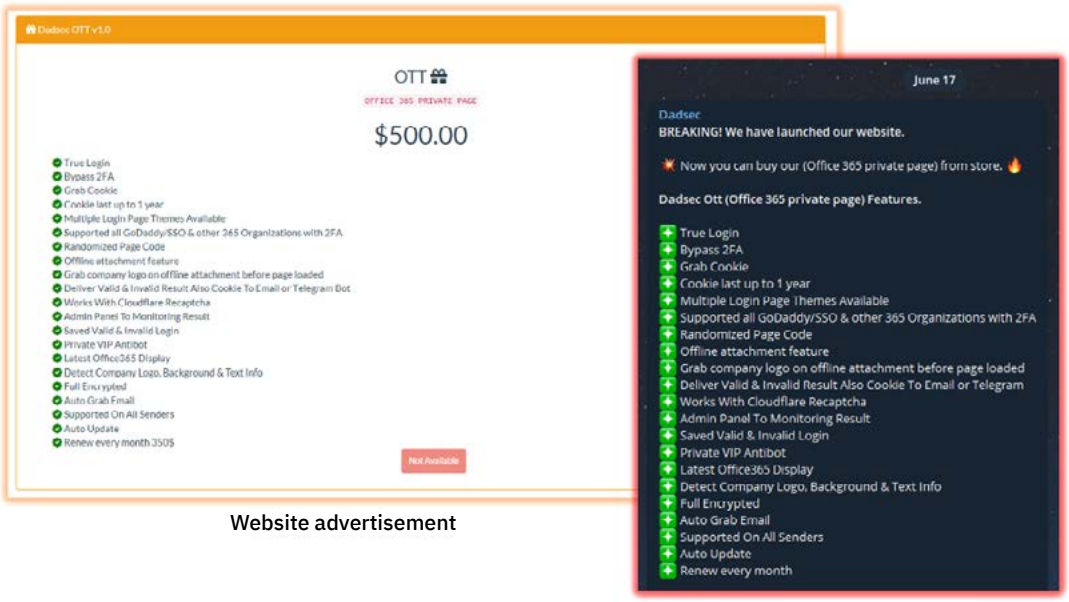
Figure 7: User account compromise / business email compromise kill chain.

The eSentire Threat Response Unit (TRU) targets each phase with detection content and investigation runbooks with the aim of detecting the compromise prior to the BEC phase. How quickly compromised accounts are accessed by threat actors varies on various factors, such as whether the account changes hands.

For example, in late 2024, TRU examined a BEC incident within a customer environment initially alerted by eSentire's SOC Cyber Analysts. In the incident, an unknown threat actor accessed the customer's email platform from a commercial VPN node geographically proximate to the customer and attempted to configure forwarding rules for payment-related messages.

The account compromise was traced to an authentication event nearly 30 days earlier. This event originated from an IP address tied to Global Connectivity Solutions, a UK-based hosting provider TRU associates with a myriad of malicious activity.

According to TRU, it's likely that this authentication event was tied to an Adversary-in-the-Middle phishing platform known as DadSec/Phoenix/Rockstar 2FA/Storm-1575 (Figure 8).



Website advertisement

Telegram advertisement

Figure 8: Dadsec Storefront, retrieved October 2023. [Source]

Therefore, early detection continues to be a focus with respect to BEC. In fact, the ratio between initial account compromise and BEC phase detection has improved in 2024.

In 2023, email account takeover detection occurred at the BEC stage 60% of the time. **In 2024 this number is down to 24%**. This would suggest overall detection of the initial account compromise has improved, limiting the opportunity window for exploiting email accounts.

Remote Monitoring and Management (RMM) Abuse

Whether for gaining a foothold or maintaining access, RMM tools have continued to be abused in 2024. Like Remote Access Tools (RATs), RMM tools provide remote access to systems and networks.

However, where they differ is in purpose and intent:

- RMM tools are intended to be used by authorized parties such as IT admins or service providers and are typically overtly installed on systems.
- RATs are typically covertly installed by malware or intrusion actors granting them unauthorized access to the environment.

The line between the two continues to gray as threat actors increasingly abuse legitimate RMM tools in their attacks to evade detection, providing an advantage over using RATs.

In fact, state-sponsored threat actors from North Korea have been known to **use remote desktop software** such as AnyDesk, TeamViewer, and RustDesk to get hired by target organizations and maintain the illusion of being a local employee to gain access into the organization's network.

Threat data from TRU has supported the increasing RMM abuse as well; throughout 2024, RMM tools such as NetSupport Manager, Remcos, and ConnectWise Screenconnect are overtaking malicious RATs in observed cases in 2024 (Figure 9).

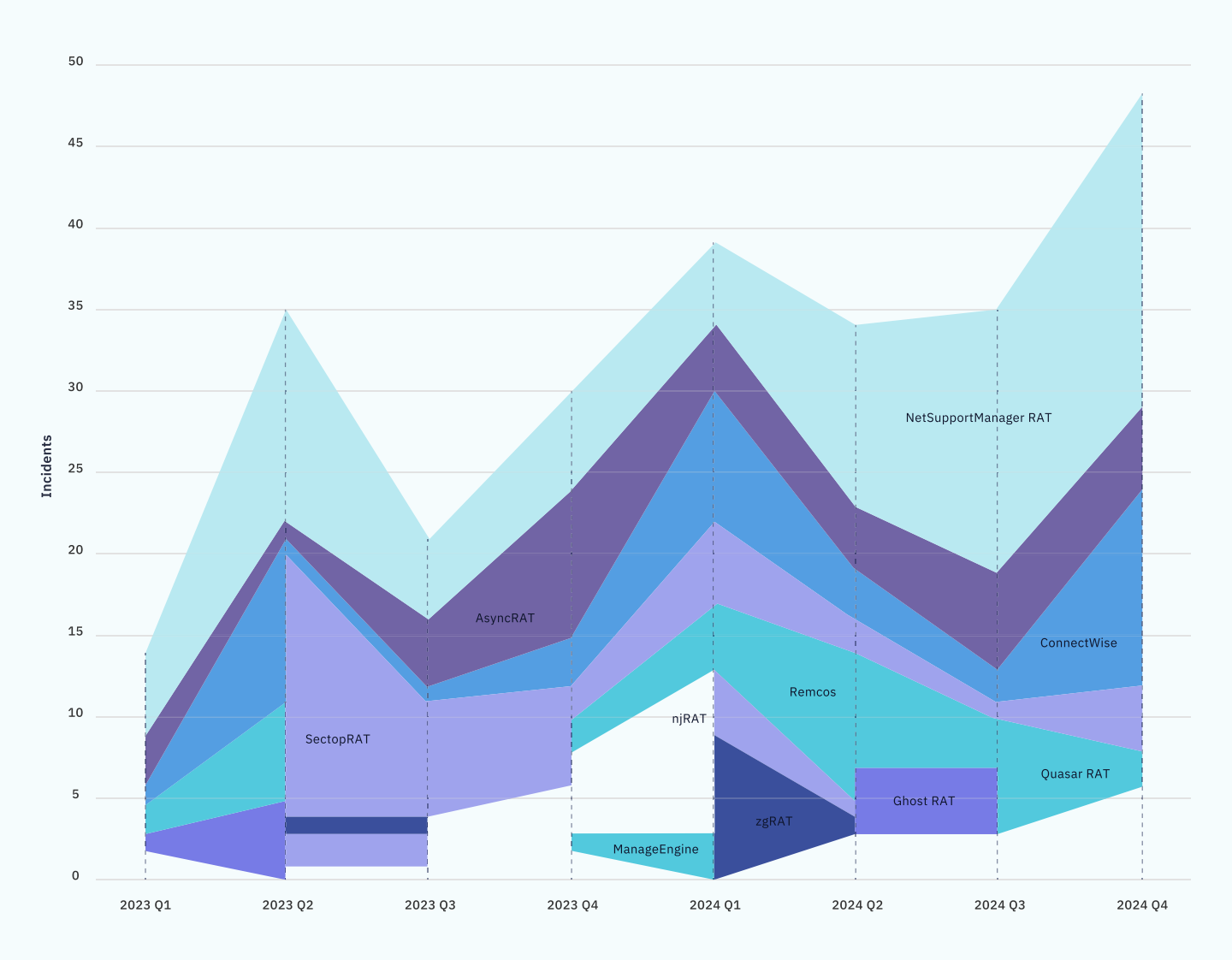


Figure 9: Dadsec Storefront, retrieved October 2023. ***https://www.esentire.com/blog/exploiting-qr-codes-aitm-phishing-with-dadsec-phaas***

Tactical Use of RMM Tools

NetSupport and ConnectWise are both commercial remote access products marketed to IT professionals as remote management solutions. Remcos is also a commercially sold tool albeit one less likely to be used legitimately as an RMM solution; Remcos offers key logging, password and cookie recovery, camera access, etc.

Throughout 2024, TRU observed threat actors abuse RMM tools such as NetSupport in attacks. Figure 10 shows a signed MSIX installer package disguised as 7-Zip which covertly deploys a preconfigured NetSupport client. These packages were widely distributed in malicious search advertisements and fake updates in 2024 by adversaries **such as FIN7**.

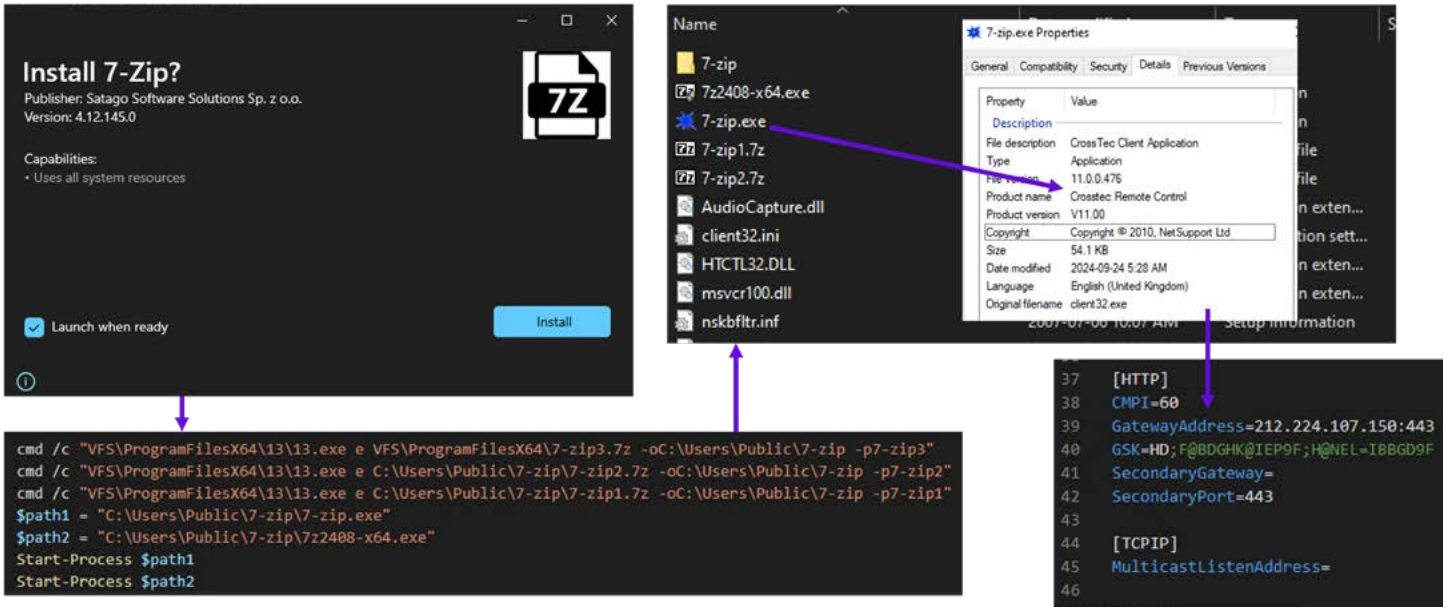


Figure 10: Netsupport Manager distributed with signed MSIX installers.

TRU also examined cases where email bombing and other tech support scams led to victims granting adversaries access to their systems using ScreenConnect, AnyDesk, Quick Assist, and others.

In one notable case from October 2024, a compromised account belonging to a customer's IT provider was used to contact victims over Microsoft Teams following a wave of spam emails (Figure 11).

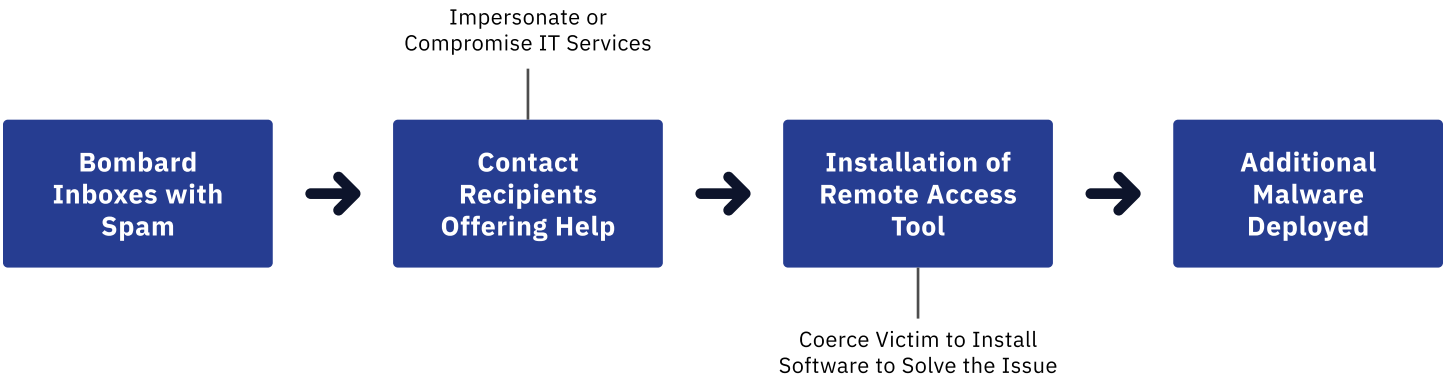


Figure 11: Typical email bombing scam.

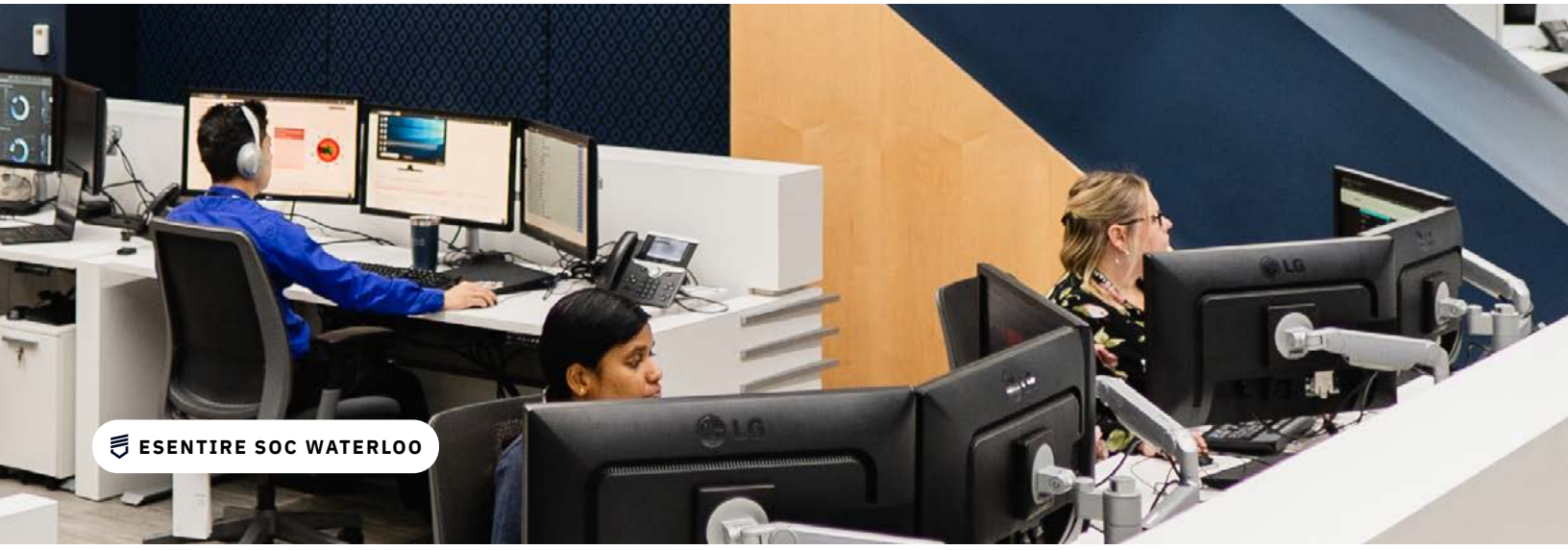
Using the IT provider's account, the adversary successfully convinced victims to grant access via Microsoft Quick Assist to remediate the spam issue. The adversary used this access to deploy a malicious RAT on the victim's machine.

Key Recommendations to Defend Against Intrusion Actions

The progression to the intrusion stage is characterized by lateral movement, privilege escalation, and evading detection. It is at this stage that threat actors seek to establish themselves within the network with the intent to compromise critical systems and data.

To prevent this, security leaders must leverage strategies that disrupt these tactics. Therefore, we recommend:

- Practice zero trust using an internal fire wall to deter **Lateral Movement**. To maintain productivity, make applying for and getting access opened between machines easy.
- To stop **Privilege Escalation**, use the Principle of Least Privilege to start all users with the lowest privileges and require access requests as needed. Ensure an expiration method for access and ensure old accounts are being cleaned up.
- To impair **Defense Evasion**, ensure you have comprehensive endpoint coverage on domain controllers, workstations, and servers – anything that can be used as a staging ground for hands-on intruders. Intruders will intentionally use out-of-scope endpoints as staging grounds.
- Ensure internal-to-internal traffic is monitored and configured to alert on signs of lateral movement, credential collection, and command & control beaconing.
- Attackers are more frequently practicing Bring Your Own Virtual Machine (BYOVM) in which they register their own machine on the network by using valid credentials and hiding in the VPN pool. Since VPN software does not support endpoint monitoring agents, detection and investigation requires VPN logging to identify their real IP address.



The State of Ransomware

Although multiple law enforcement agencies have taken down major threat actor groups like Lockbit and Scattered Spider affiliates, ransomware-as-a-service (RaaS) continue to remain resilient with new "franchises" emerging to fill the void left by key players.

At its core, the RaaS model provides the means for ransomware affiliates to monetize their intrusions. Moreover, affiliates are free to bring their extortion victims to the RaaS group that will guarantee a quick payout for the lowest fees.

In many cases, ransomware attacks can be traced to **opportunistic infections** or intrusions stemming from preventable security issues. Furthermore, TRU's research on **SMB ransomware readiness** highlighted that industries with greater exposure to crimeware (i.e., infostealers) and initial access brokers also had elevated exposure to ransomware.

By examining cases that involve both precursor threats to ransomware (e.g., infostealers, RATs, and loaders like GootLoader and SocGholish) and intrusion TTPs, we can identify which industries have increased exposure (Figure 12).

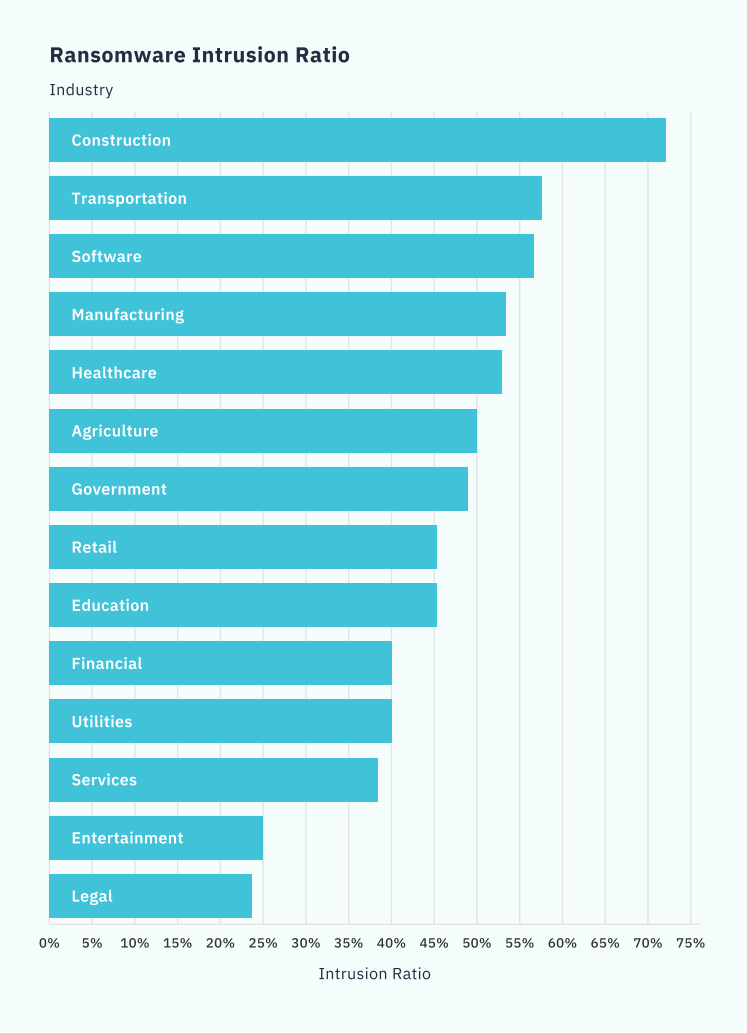


Figure 12: Ransomware intrusion ratio by industry.

Examining leak site activity by quarter in 2023 and 2024, TRU observed an increase in distinct groups by quarter in conjunction with an overall rise in victims (Figure 13). For example, in 2023 Q2, we saw nearly 900 victims across 24 groups, while 2024 Q2 had nearly 1,000 victims across 52 groups.

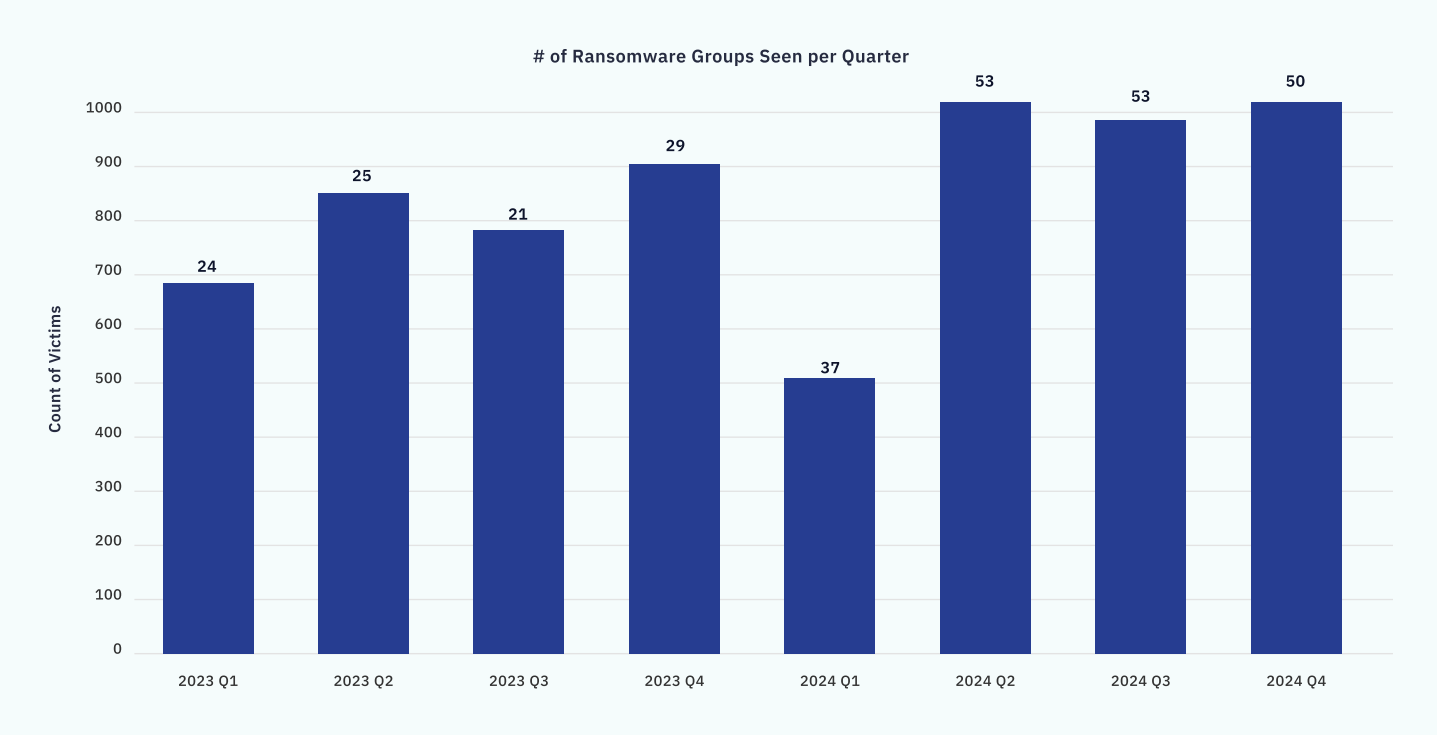


Figure 13: Count of victims listed on leak sites over time.

Expanding this back to 2020, unique ransomware groups operating leak sites remained more or less stable from 2021to 2023 before spiking in 2024 (Figure 14). When examining leak site data, TRU's research shows that the number of unique ransomware groups that reported a victim has risen from 41 unique groups (in 2023) to 77 unique groups (in 2024) – an increase of nearly 88%.

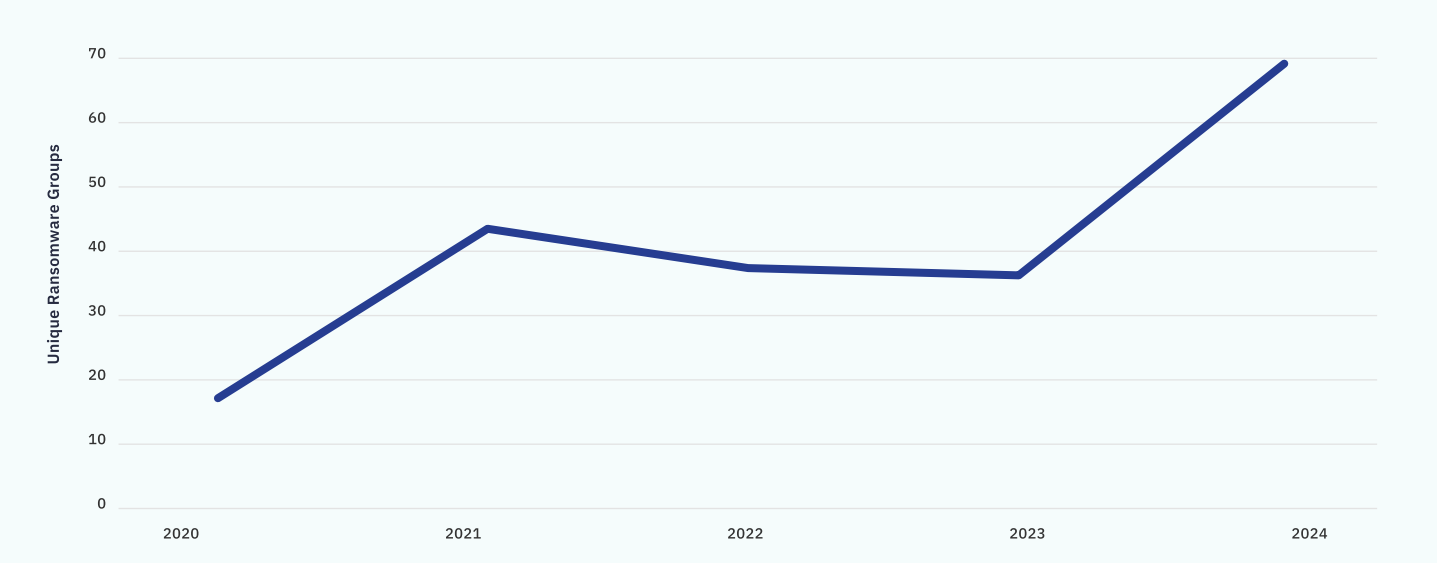


Figure 14: Number of unique ransomware groups over time.

This change is likely due to affiliates and ransomware operators seeking new ventures following law enforcement actions against Lockbit (**Operation Cronos**) and **ALPHV/Blackcat**, which was speculated to be involved in an exit scam around the **Optum attack**.

For example, Ransomhub emerged in March 2024 following Lockbit's takedown and has listed 300+ victims so far. Other new groups also emerged or rose in prominence; DragonForce and BrainCipher even took advantage of leaked Lockbit 3.0 source code to forge their own ransomware operation

This is a cycle that has been seen before, one that mirrors the corporate world. When one business shuts down, the employees join another venture or may even start their own business. The Ransomware-as-a-Service model at its core provides the market and means for affiliates to monetize their intrusions. Affiliates are free to bring their extortion victims to the RaaS group that will guarantee a quick payout for the lowest fees.

SMBs and Manufacturing Sector Remain Most Victimized

According to public leak data, the majority of victim businesses are small-medium businesses (SMBs) that had less than $50 million in revenue (Figure 15). The businesses that were the most impacted fell in the $1-5 million revenue range, followed by the $10-25 million revenue range.

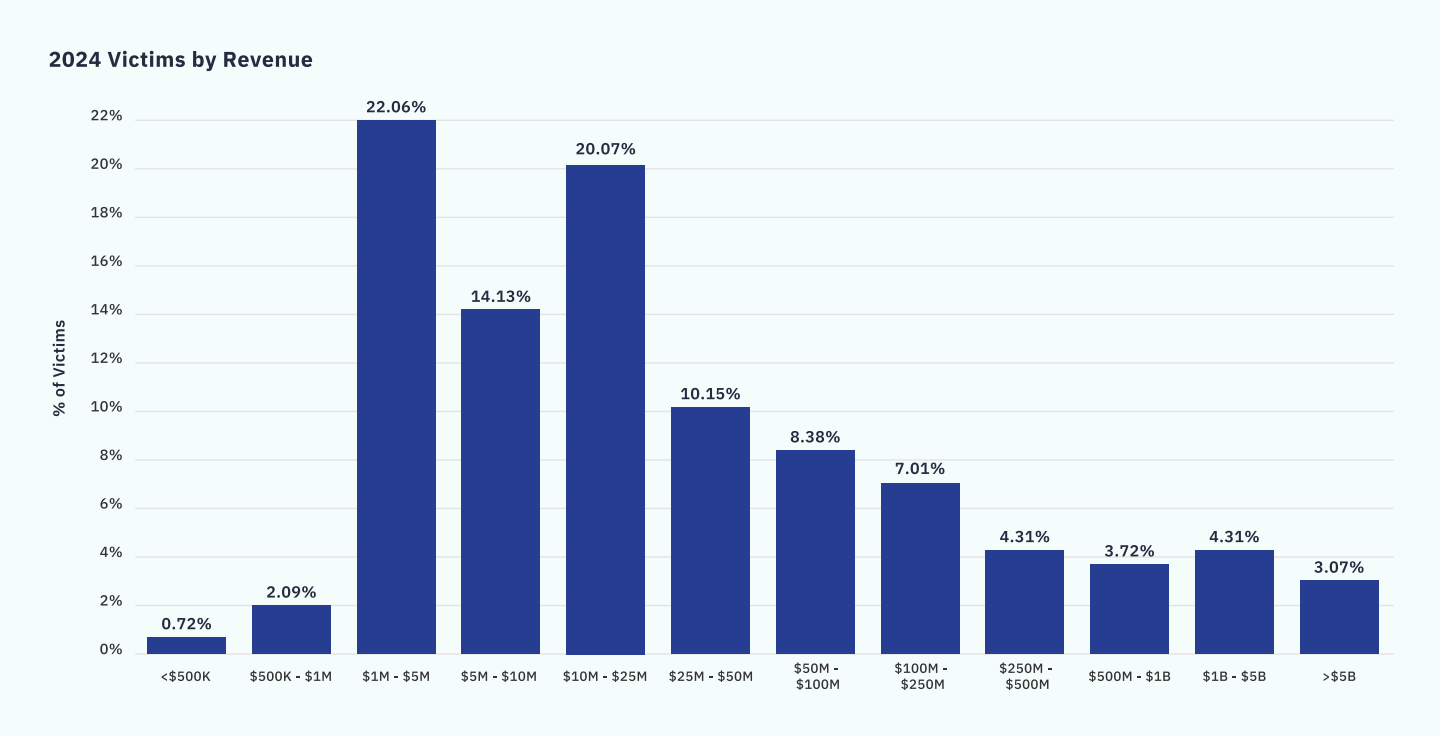


Figure 15: Victims by their revenue in 2024.

Comparing victim industries, Manufacturing remains at the top spot, followed by Business Services and Construction (Figure 16). Notably, Construction was the top concern in customer cases based on ransomware precursors and intrusion rates as indicated in Figure 12 above.

2023 Industries	
Manufacturing	558
Business Services	296
Retail	269
Construction	241
Education	174
Finance	138
Law Firms & Legal Services	119
Hospitality	117
Transportation	109
Software	98
Hospitals & Physicians Clinic	97
Consumer Services	83
Government	80
Organizations	65
Insurance	61
Energy, Utilities & Waste	61
Real Estate	58
Media & Internet	56
Telecommunications	46
Healthcare Services	32
Holding Companies & Conglomerates	27
Agriculture	20
Minerals & Mining	15

2024 Industries	
Manufacturing	633
Business Services	373
Construction	300
Retail	266
Education	154
Hospitals & Physicians Clinic	135
Hospitality	129
Law Firms & Legal Services	124
Finance	115
Consumer Services	115
Transportation	100
Software	91
Government	82
Energy, Utilities & Waste	72
Insurance	65
Organizations	61
Real Estate	58
Media & Internet	53
Telecommunications	50
Healthcare Services	38
Minerals & Mining	20
Agriculture	18
Holding Companies & Conglomerates	13

Figure 16: Top victim industries 2023 and 2024, based on public leak site data victims.

Key Recommendations to Build Resilience Against Ransomware

To build resilience against ransomware, and even prevent ransomware deployment, it's critical for security leaders to build a cybersecurity strategy targeted towards anticipating, withstanding, and recovering from these attacks. Therefore, we recommend:

- Anticipating threats by continuously assessing, and understanding, your risk exposure and remaining vigilant against sophisticated ransomware threats.
- Prioritizing 24/7 threat detection and response capabilities to withstand ransomware attacks and using real-time security telemetry to identify data breaches, mitigate damage, and maintain operational continuity.
- Remediating malware infections as quickly as possible by:
    - Isolating systems and locking out accounts during threat investigations.
    - Investigating account activity on other systems during the compromise window.
    - Returning the system to a known good state by revoking active sessions and resetting compromised credentials post-cleanup.
- Creating, maintaining, and exercising a strong incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.

Looking Ahead: The Outlook for the 2025 Threat Landscape

As we head into 2025, cybersecurity experts, including CISOs, need to be prepared for a constantly shifting threat environment.

Despite growing technological advancements and proven business strategies, the complexity and flexibility of cyber threats are not decreasing. Here are some things to be mindful of in 2025:

Continuation of Hybrid Attacks Globally Targeting Critical Infrastructure

Over the past decade, there has been a steady escalation globally by state sponsored threat actors engaging in a variety of cyber and information operations. The nation states implicated in these attacks include **China** and **Russia**.

These attacks have impacted organizations in a variety of **industries and sectors including critical infrastructure**. As hybrid conflicts continue globally, it's probable that we will see the continued targeting of critical infrastructure.

Organizations in the critical infrastructure sectors, namely Manufacturing, Energy & Utilities, Transportation, and Government, should ensure they have 24/7 threat detection, investigation, and response capabilities with real-time security monitoring and proactive threat intelligence to minimize business disruption against sophisticated cyber threats.

Physical Disruption of the Internet Infrastructure

As hybrid conflicts continue globally, it's probable that we will see the continued physical disruption of the internet through the tampering of its **physical infrastructure**. As a result of this disruption, there may be a shift to adopting satellite internet to minimize the impact, and risk, of a physical disruption to the internet infrastructure.

It's also probable that more European nations will pursue adoption of satellite internet as a measure of redundancy and to minimize the impact and risk of an internet blackout.

However, this presents its own **potential risks** as well. For instance, Ukraine adopted satellite internet prior to the nation's most recent invasion and during the invasion, satellite internet was targeted, resulting in a **partial disruption** of services.

As organizations shift to satellite internet, it's probable that state-sponsored threat actors will target satellites to degrade, disrupt, and deny communications.

Continued Ransomware Attacks Against all Industries

Although law enforcement agencies had moderate success dismantling ransomware groups, ransomware operations continue to impact organizations **globally** and continues to disrupt **critical infrastructure**.

Ransomware gangs will continue to operate in 2025, and they will continue to target revenue-rich organizations to pay a ransom.

Increased Extortion Attacks Against Cloud Services

Information stealing malware was among the most observed threats in 2024 and one of the quickest methods of monetizing network access by selling credentials on fraud shops such as Russian Market.

Fraud shops have made locating high value accounts tied to unmanaged devices and cloud services trivial. The extortion of SnowFlake customers through infostealer-sourced creds surfaced what has been a lucrative methodology for some time.

It's probable other enterprising threat actors will use fraud shops in 2025 for high-value credentials to cloud services.

Continued Abuse of Certificate Authority

The Threat Response Unit (TRU) conducted in-depth research this year on the rise of signed malware, which was a tactic leveraged only by Advanced Persistent Threat (APT) groups historically. However, this approach has become more common for commodity malware.

Until controls are increased for validating a business, certificate authorities will likely continue to issue certificates for fraudulent businesses allowing for the continued adoption of signed malware through 2025.

Browsers as the Main Initial Access Method for Malware Deployments

Given that email defenses have hardened, threat actors are finding more success in gaining initial access to organizations through the abuse of the broader internet. Specifically, this has come in the form of using **fake job lures**, **fake browser updates**, Search Engine Optimization (SEO) poisoning, and **malvertising**.

As threat actors continue to find success with these methods, it's probable that the risk of employees falling victim to these schemes will continue in 2025.

Continued Abuse of Valid Credentials

Acquiring valid credentials to gain access to organizations' environments continues to be an initial access method that provides threat actors with stealth and opportunity.

By leveraging valid credentials, a threat actor minimizes the likelihood of being detected in an environment and affords them the opportunity to leverage that access to create the most value for the threat actor; either by enabling BEC attacks or deploying ransomware.

Threat actors will almost certainly continue to abuse valid credentials in 2025 and beyond.

Recommendations: Staying Ahead of the 2025 Threat Landscape

As threat actors shift away from email-based initial access vectors to those that use browsers and stolen credentials, security leaders must understand the importance of adopting a multi-layered defense strategy to prevent ransomware deployment and minimize business disruption.

TRU's research underscores the importance of understanding the most impactful initial access vectors (i.e., those that enable attackers to move beyond the initial breach into full-scale intrusion). This is further compounded by the strategic use of Remote Access Trojans (RATs) and the abuse of legitimate remote access tools.

Given that many security teams continue to face budget constraints and are asked to consolidate their tools, it becomes imperative to prioritize the right security investments that will address the most impactful initial access vectors relevant to their specific industry.

To truly stay ahead of the threat curve, we recommend that security leaders must:

- **Have up-to-date knowledge about the threat landscape.**
  This involves staying informed about the latest threats, trends, and TTPs that adversaries are employing. Organizations should invest in conducting proactive threat hunts and operationalizing threat intelligence to anticipate potential threats.

- **Know your users, your endpoints, and your existing technology stack and understand where they intersect with the threat landscape.**
  Analyze how specific threats could target specific users or leverage vulnerabilities in specific endpoints or software. By identifying these intersections, you can implement targeted defenses and equip users with the knowledge to recognize and avoid such threats.

  A critical step in this process is maintaining a detailed inventory of all users, their roles and access privileges, a comprehensive mapping of endpoints, and a thorough understanding of the technology stack. This visibility

not only reduces the risk of shadow IT but also empowers your team to create customized security policies and respond swiftly to suspicious activity.

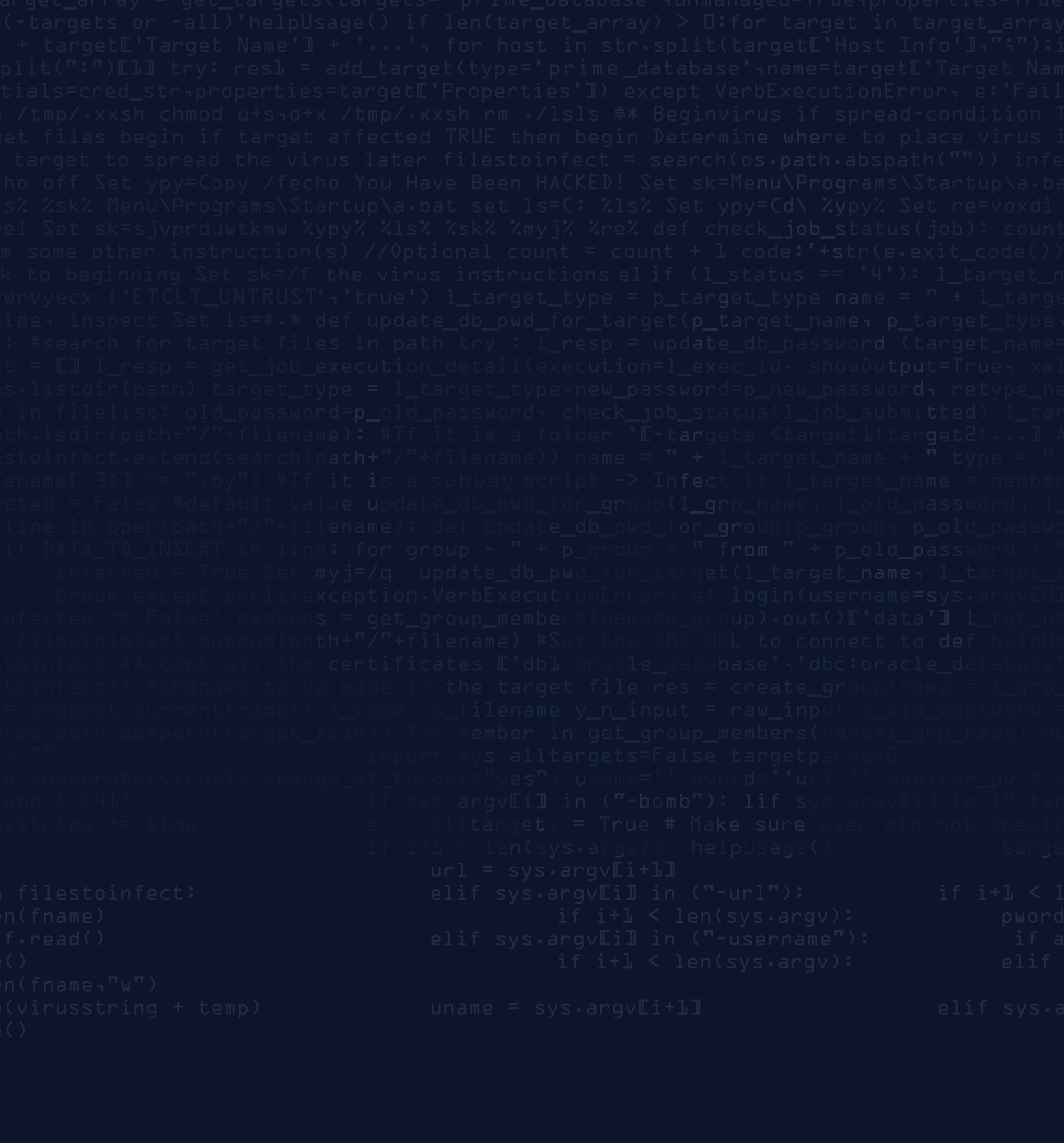
- **Minimize unnecessary access (and thus, activity) between users, endpoints, and software.**
  Apply the principle of least privilege rigorously to make sure that users only have the access necessary to perform their roles. This means restricting unnecessary interactions between users, endpoints, and software and reducing the opportunities for threat actors to exploit excess permissions or conduct lateral movement within the network.

- **Detect suspicious activity between users, endpoints, and software with 24/7 threat detection and response capabilities.**
  To be able to detect threats and reduce the risk of out-of-scope endpoints leading to ransomware incident, it's important to implement advanced monitoring solutions that can detect anomalies and potential security incidents in real-time.

  Partner with a **24/7 multi-signal Managed Detection and Response (MDR)** provider that offers continuous protection from 2**4/7 SOC Cyber Analysts** and **Elite Threat Hunters** who rapidly investigate, contain, and manually shut down threats before they disrupt your business.

- **Take immediate response actions to contain and isolate any suspicious behavior.**
  Containing and responding to threats in a timely manner will be integral to make sure threat actors don't progress past the initial access stage. However, not all security teams have the capabilities needed to disrupt malicious behavior. Therefore, when evaluating an MDR provider, we recommend partnering with one that will respond to threats on your behalf, not just drown your team in alerts.

Lastly, we also recommend conducting post-incident reviews to extract lessons learned, refine response strategies, and strengthen defenses against future attacks.



eSentire

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.