2023 YEAR IN REVIEW & 2024 THREAT LANDSCAPE OUTLOOK

From Initial Access to Ransomware Deployment: A Deep Dive into the Modern Threat Actors' Playbook

eSENTIRE
Threat Response Unit

Executive Summary

As cyber threats evolve with alarming sophistication, understanding the tactics, techniques, and procedures (TTPs) that threat actors rely on to not only gain initial access, but achieve intrusion actions and achieve actions on objectives is critical to reducing your organization's cyber risks, avoid downtime, and build a resilient security operation.

When it comes to gaining initial access, threat research analyzed by our Threat Response Unit (TRU) reveals that there has been a sharp rise in 'unknown' vectors tied to out-of-scope endpoints, which are effectively blind spots within an organization's network that are not covered by endpoint monitoring or EDR tools. We also identify the most impactful initial access vectors to be valid credentials, supply chain compromises, and system misconfigurations.

Furthermore, TRU's research also highlights a rise in intrusion ratios, now nearing a 50% threshold, which signifies that nearly half of all initial breaches culminate in serious intrusions.

This is compounded by the increased deployment of Remote Access Trojans (RATs) and sophisticated abuse of legitimate remote access tools, which not only advance intrusions but also blur the lines between various stages of the attack lifecycle.

Industry-specific insights reveal sectors with expansive and interconnected networks—such as healthcare, education, and government—are particularly susceptible to 'unknown' vectors. Conversely, industries with smaller network footprints face their own unique challenges, exacerbated by mergers or government affiliations.

As we step into 2024, we project an increase in politically motivated cyberattacks, with adversaries leveraging advanced TTPs to target critical infrastructure sectors and cause civil unrest.

Plus, the evolution of Ransomware-as-a-Service into a consulting-like model signifies a future where cybercriminal operations continue to mirror legitimate corporate structures and possibly cooperate with government agencies to deploy nation-state attacks.

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 findings underscore the urgency for a multi-layered defense approach to cybersecurity that combines 24/7 threat detection and response capabilities, robust threat intelligence, comprehensive endpoint coverage, and proactive defense against the exploitation of zero-day vulnerabilities.

Initial Access: Understanding How Malware Enters Corporate Environments

One of the main challenges within cybersecurity is to anticipate threats and prevent the various tactics, techniques, and procedures (TTPs) that cybercriminals can use to infiltrate corporate networks, compromise sensitive data, and deploy ransomware.

The first step in any successful attack is to gain initial access to a target system, often by exploiting vulnerabilities or tricking users into executing malicious code. This initial access is the entry point for further malicious actions, such as lateral movement, privilege escalation, or data exfiltration.

Moreover, the initial breach – where a threat actor first establishes a foothold in a system – often sets the stage for the potential damage that can unfold.

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, the top five initial access vectors based on attack volume, as observed by TRU, are browsers, email, removeable media, 'unknown' vectors, and remote exploits.

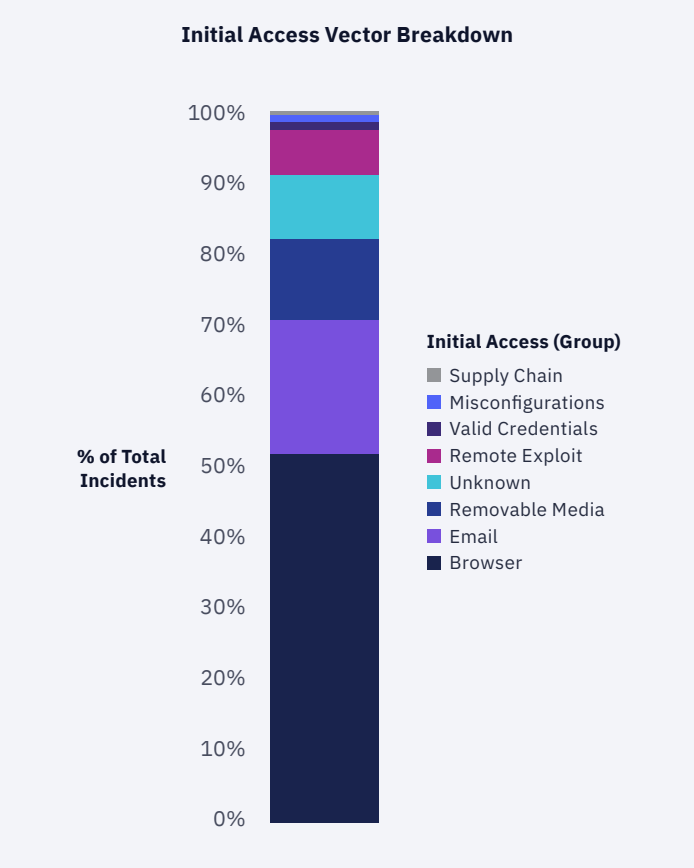

Figure 1: Breakdown of observed initial access vectors.

The Rise of Browser-based Threats

Over the past year, threat actors have largely pivoted from using email-based threats to browser-based threats. This is likely due to the adoption of rigorous phishing and security awareness training programs focusing on email threats (e.g., phishing and business email compromise attacks), leading attackers to adapt and become more sophisticated in how they gain initial access.

Specifically, there are four primary methods threat actors have been using to socially engineer employees into downloading malware:

1. **Malvertising:** Threat actors use Google Ads to publish fake advertisements for webpages that host malware claiming to be legitimate software.
2. **Search Engine Optimization (SEO) Poisoning:** Threat actors predict keyword search terms that users might search for and get their attacker-controlled webpages to appear in the first page of results for search engines like Google and Bing.
3. **Watering Hole:** Threat actors compromise pages that their targets are already visiting, plant malware, and trick users into downloading and executing it.
4. **Freeware:** When users download "free software" or "cracked software" from third-party software repositories found online, they can sometimes get "software bundles" that include adware, RATs, and infostealers in addition to the legitimate file they were intending to download.

'Unknown' Access Resulting from Out-of-Scope Endpoints

Prior to engaging an endpoint detection and response (EDR) solution, if an organization hasn't adequately scoped all endpoints for monitoring or if they lack maturity in inventory discovery and management, there may be endpoints that haven't been properly covered by the EDR solution; these are called 'out-of-scope' endpoints. These blind spots are even more dangerous than known threats.

When "patient zero" (i.e., the first endpoint to get compromised in a network) is out-of-scope, the telemetry surrounding initial access is not captured, making it difficult to detect the presence of threat actors within the environment and respond immediately.

This means threat actors have a longer time to establish foothold and spread laterally to infect other endpoints. Moreover, in using these out-of-scope endpoints, threat actors can easily use them as stealthy staging grounds to launch ransomware attacks and exfiltrate highly valuable data.

In fact, TRU's research has shown that ransomware attacks make it further down the kill-chain when they begin on out-of-scope endpoints.

While there are a small handful of cases where only log or network monitoring can resolve investigations into initial access methods, particularly in the case where attackers are hiding in the organization's VPN pool. However, it's important to note that although some evidence of compromise may appear through log and network monitoring, initial access typically cannot be investigated without endpoint telemetry.

Therefore, if your organization chooses to implement endpoint monitoring or an EDR solution to detect malicious execution when social engineering attacks bypass user scrutiny, it's critical to make sure that endpoint coverage is fully comprehensive.

Most Impactful Initial Access Vectors

When considering how to prioritize defending against initial access vectors, it's important to look at the most impactful vectors, as opposed to the most common. This is largely because impact is measured by the fraction of attacks that make it to the intrusion actions phase of the attack kill chain (Figure 2).

In other words, the most impactful vectors are those that enable cybercriminals to establish persistence, gather user credentials, move laterally in the environment, etc. with a success rate of 100%.

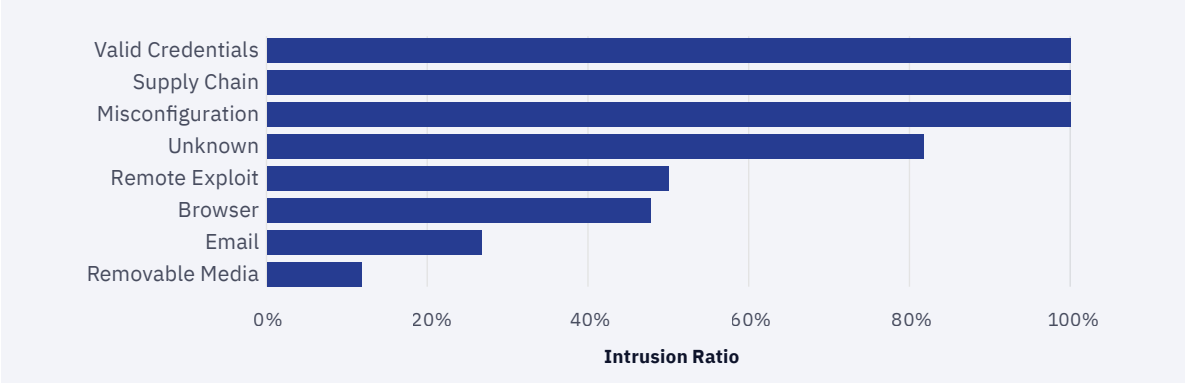

Figure 2: Intrusion ratios of different initial access vectors.

Interestingly, initial access vectors with the highest impact are those that are the least commonly used: valid credentials, supply chain, and misconfigurations:

- **Valid Credentials:** Threat actors use stolen user credentials to mask themselves as legitimate users and gain access to an organization's network. Once inside, they can perform unauthorized activities, such as moving laterally and escalating privileges.

  Based on TRU's observations, the use of valid credentials often intersected with out-of-scope endpoints. In other words, cybercriminals were more likely to use valid credentials to access out-of-scope endpoints to ensure their presence is undetected by EDR and endpoint monitoring solutions. This in turn leads to higher likelihood that the attackers will achieve intrusion and go undetected, when compared to the use of remote exploitation and browser-based malware to gain access.

- **Supply Chain:** Supply chain attacks occur when a threat actor infiltrates the network using a third-party/supply chain vendor that has access to your systems. This type of attack can happen at any stage of the supply chain and can be challenging to detect because it can bypass typical security controls, especially if they exploit trusted software applications.

  Furthermore, ransomware actors can compromise these supply chains for extortion, especially when they contain sensitive information about customers. This method was observed by Cl0p ransomware and the **MOVEIt** supply chain attack.

- **Misconfigurations:** Whether its within hardware, software applications, or within the cloud, misconfigurations provide an easy entry point for attackers, as they can exploit these vulnerabilities to gain unauthorized access or escalate privileges within a system.

Valid credentials and misconfigurations don't explicitly need out-of-scope endpoints; in many cases, ransomware actors will simply register their own remote machine on the network, automatically creating an out-of-scope endpoint that connects to the target organization. This technique has been largely enabled by the work-from-home era of COVID, in which organizations were forced to accept a distributed network topology.

Breakdown of Initial Access Vectors by Industry

When we drill down to consider initial access vectors from an industry perspective, TRU's data shows that most industries are susceptible to browser-based attacks, although email-based attacks are still prevalent (Figure 3).

However, there is also an increased presence of 'unknown' initial access vectors, specifically with respect to the Healthcare, Education, Utilities, and Government sectors.

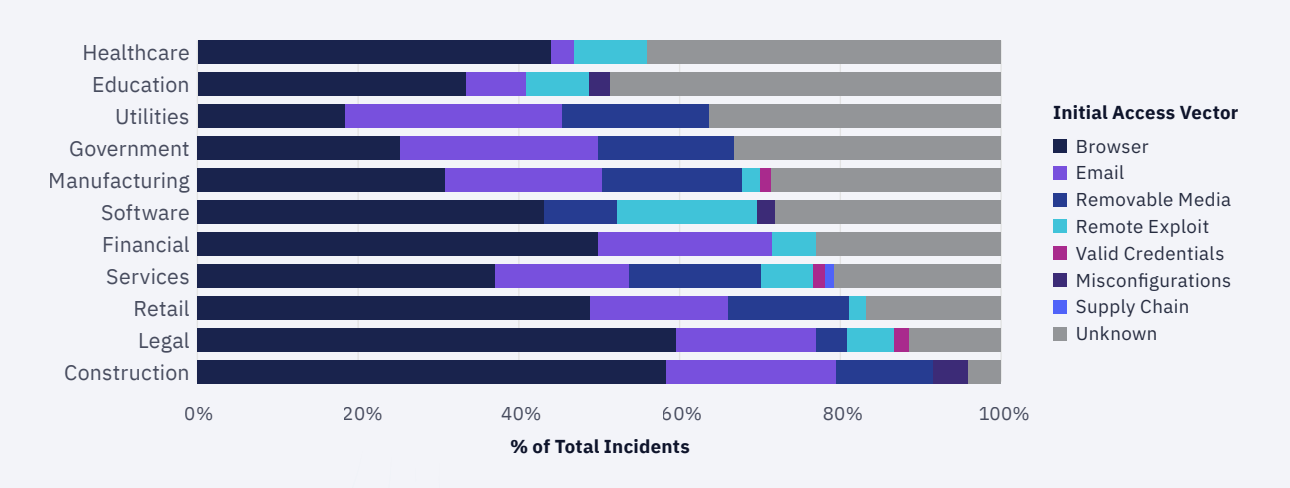

Figure 3: Industry breakdown of initial access vectors.

Unsurprisingly, Healthcare, Education, Utilities, and Government sectors tend to be most impacted by the 'unknown' initial access vectors. This may be because organizations within these sectors tend to have larger networks that are integrated with other, larger networks and have strict regulations limiting where and when monitoring devices can be installed.

On the other hand, organizations with a smaller, less integrated network footprint – like Construction, Legal, and Retail – tend to have an easier time defining the boundaries of their network. However, this premise may not hold when two or more of an organization's entities are merging or have government ties, especially within the Legal sector.

Key Recommendations to Defend Against Initial Access Vectors

Initial access represents the most critical stage of a cyberattack's kill chain, during which an adversary's success hinges on exploiting vulnerabilities to enter your network.

Therefore, we recommend that security leaders focus on proactive cyber defense strategies to reduce risk and better anticipate the initial access vectors that today's threat actors rely on:

- Implement robust **phishing and security awareness training** to educate your users to identify and report potentially malicious content and specifically include exercises that expose your users to real-world scenarios like social engineering tactics (e.g., browser-based attacks and email threats).
- Protect your endpoints with comprehensive coverage to intercept User Execution tactics before adversaries can establish a foothold and progress to further stages of intrusion. It's critical to use an **endpoint detection and response (EDR)** tool to detect and contain threats. Ensure that all endpoints are properly covered to remove any blind spots.
- Implement 24/7 network and log coverage to protect against remote exploitation and secure all remote access services by placing them behind a VPN and/or restricting access.
- To reduce the impact of compromised user credentials, enable multi-factor authentication (MFA) use on all accounts, limiting access to managed and compliant systems, and deactivating authentication sessions in the event of account compromise.

Intrusion Actions: Understanding How RATs Lead to Increased Intrusion Ratios

The second stage in an attack workflow is intrusion actions, during which the threat actors engage in intermediate actions (e.g., establish persistence, find critical systems, exfiltrate data, spread laterally, etc.) that will help them progress into the next stage – ransomware deployment, run coinminers, or steal data.

To determine how adept threat actors are becoming at avoiding detection by traditional security tools, we look at the intrusion ratio, which helps measure the percentage of incidents that proceeded past initial access.

Over the past three years, TRU's threat research shows a steady increase in intrusion ratios across our global customer base; since 2021, intrusion ratios have jumped to nearly 50%.

As of 2023, nearly half of all initial breaches have led to serious intrusions, indicating that once attackers get in, there's a high chance they can execute their malicious objectives (Figure 4).

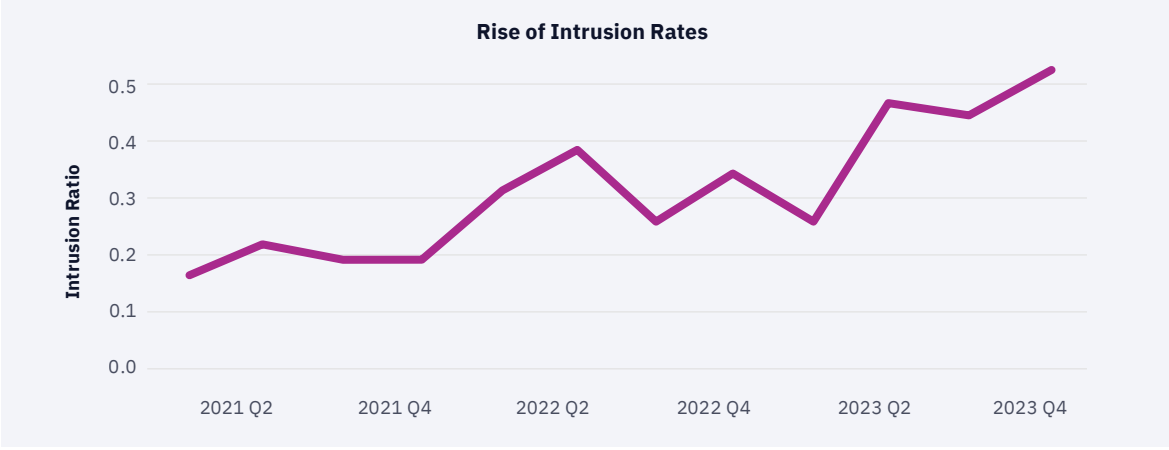

Figure 4: Intrusion ratios have been rising steadily from 2021–2023.

The Rise of RATs

As seen in Figure 5, when understanding why intrusion ratios have increased so significantly since 2021, TRU's research showed a correlation with the increased presence of RATs (both remote access trojans and remote access tools):

- **Remote Access Trojans:** These are commodity malware variants that function as infostealers and limited backdoors and tend to arrive via browser-based vectors. When users attempt to install free or cracked software, they unknowingly download and execute RATs instead.
- **Remote Access Tools:** These are remote management tools (e.g., ConnectWise, AnyDesk, NetSupport RAT) that threat actors use to spread laterally across the target organization's environment. These tools are often **deployed manually** by hands-on-keyboard attackers during ransomware intrusions.

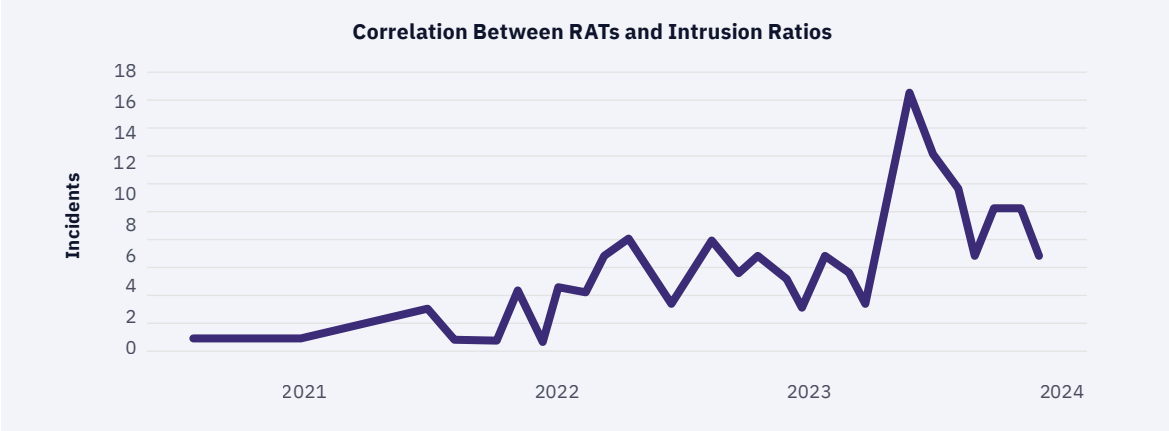

Figure 5: Volume of incidents involving RATs between 2021–2024.

Shift in Intrusion Tactics

While the number of intrusions has risen overall, TRU's research indicates that there has been a notable decline in the use of Cobalt Strike for intrusions, a tool that was once popular amongst attackers. Instead, cybercriminals have pivoted towards using RATs to steal information, such as NetSupport RAT, AsyncRAT, Remcos, and Sectop RAT (Figure 6).

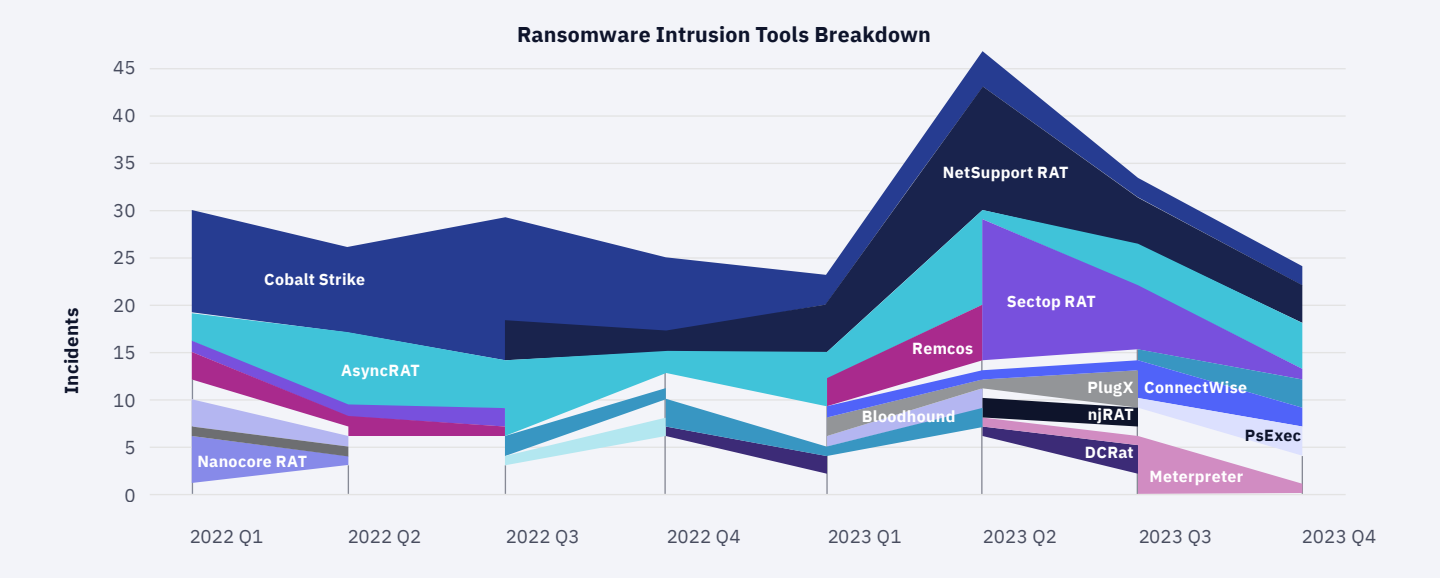

Figure 6: Breakdown of intrusion tools in the last two years.

Adapting New Tools for Ransomware Intrusions

Originally designed for legitimate use by red and blue security teams, remote access tools like ConnectWise, AnyDesk, Bloodhound, and PsExec are now being adopted by threat actors to take control of multiple systems in a network and deploy ransomware (Figure 7).

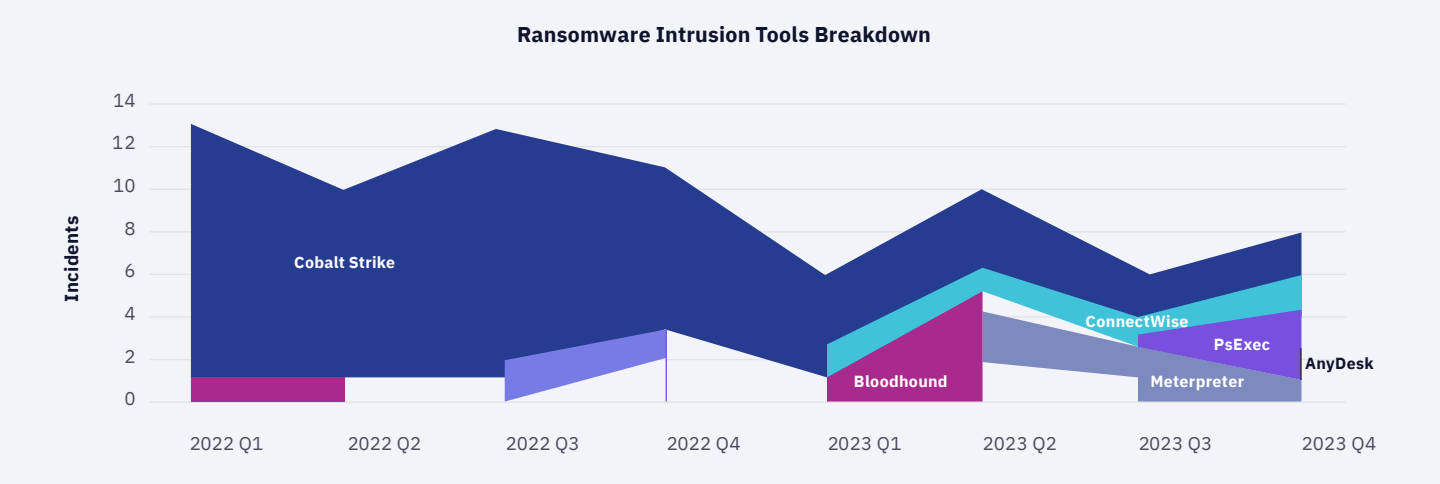

Figure 7: Intrusion tools associated with ransomware incidents.

Threat actors infiltrate networks using browser-based threats like GootLoader, Nitrogen, and SocGholish before attempting to deploy ransomware to as many endpoints as possible.

Based on TRU's data, this has been more prevalent across the Retail, Utilities, Software, Government, and Healthcare industries (Figure 8).

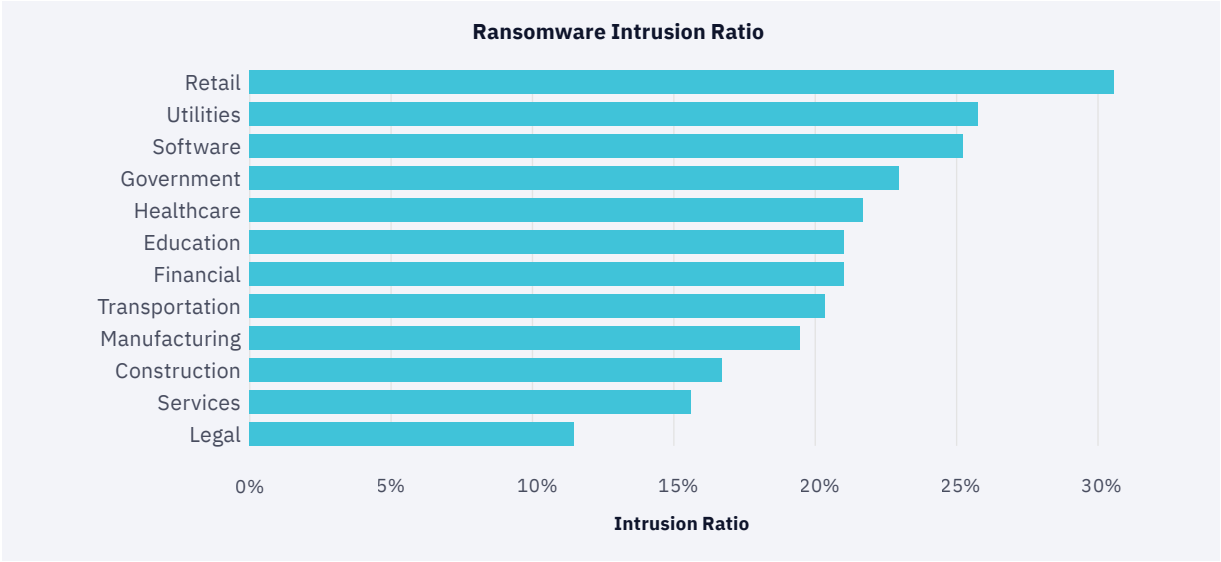

Figure 8: Breakdown of intrusion ratios for different industries.

Key Recommendations to Prevent Progression into the Intrusion Stage

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:

- Practicing zero trust using an internal fire wall to deter **Lateral Movement**. To maintain productivity, make applying for and getting access opened between machines easy.
- Impairing **Privilege Escalation** by starting all users with the lowest privileges and requiring access requests as needed. Ensure an expiration method for access and ensure old accounts are being cleaned up.
- Limiting **Defense Evasion** by ensuring you have comprehensive endpoint coverage on domain controllers, workstations, and servers – anything that can be used as a staging ground for hands-on intruders. Remember, intruders will intentionally use out-of-scope endpoints as staging grounds.
- Monitoring and configuring internal-to-internal **network traffic** to alert on signs of lateral movement, credential collection, and command & control beaconing.
- Implement a **log monitoring solution** since VPN logs and domain controller logs can help to track intruder movements from endpoint to endpoint, to identify initial access, and to help determine when the attacker has obtained domain administrator privileges.
  - In recent attacks, intruders have been observed registering their own virtual machine in the VPN pool; when attackers do this, their IP cannot be differentiated from other IPs in the VPN pool and VPN logs are required to identify their true IP.

Actions on Objectives: Achieving the Final Outcome of a Cyberattack

The last stage of the attack workflow – actions on objectives – is achieved once threat actors perform the activity that's directly tied to fulfilling their intended objectives, such as encrypting files, exfiltrating data, or disabling systems, by deploying specific malware and tools designed for this purpose.

While the presence of these tools in a network doesn't necessarily mean the attack was successful, it does indicate what the attackers' aims may be and how far the attack already progressed.

Ransomware Deployment

The highest impact objective is deploying ransomware so threat actors can extort their victims for money. According to TRU, ransomware attacks surge in the latter half of the year, which may be attributed to threat actors waiting for more opportune moments when the organization's defenses might be lower (Figure 9). Their data also shows that valid credentials were the most likely initial access vector that led to ransomware.

Additionally, in our **2024 SMB Ransomware Readiness Report**, TRU's research also highlights that most ransomware victims tend to be small and medium-sized businesses (SMBs) within the Manufacturing, Business Services, and Retail industries.

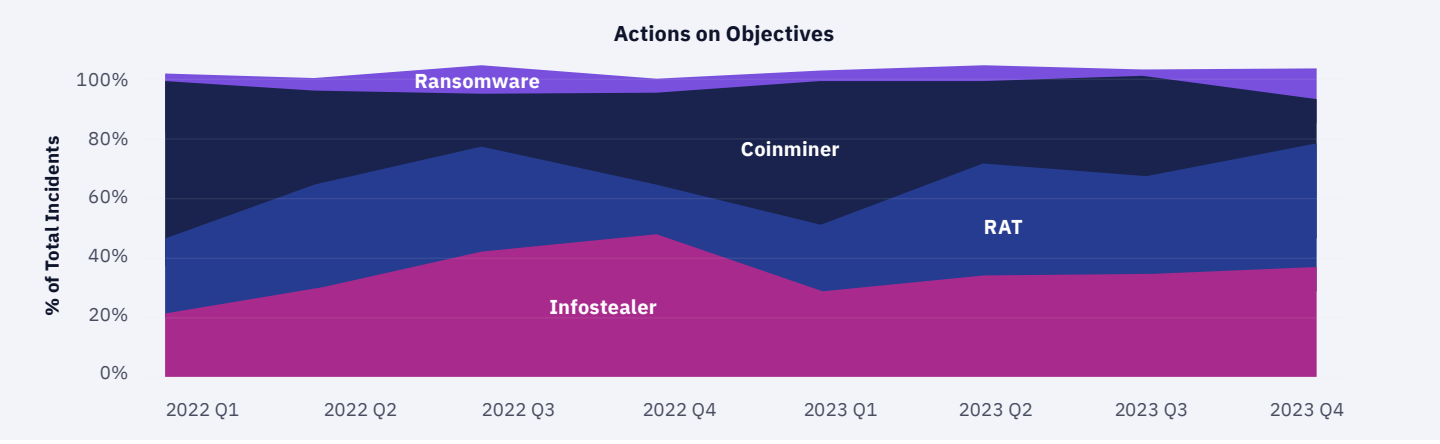

Figure 9: Percentage of incidents falling under particular actions-on-objectives.

Coinminers

Although the use of coinminers is also financially motivated, they tend to have a lower impact compared to ransomware. However, successful running coinminers signals that attackers have the capability to execute code within the organization's environment.

Threat actors typically use unknown initial access vectors and remote exploitation to deploy coinminers and tend to target public-facing servers that have limited network privileges.

RATs and Infostealers

Since RATs can double as infostealers to exfiltrate high-value data, they are included in the actions on objective stage of the attack workflow. However, there are edge cases of RATs being used as malware loaders or lateral movement tools. They commonly infiltrate systems through employee internet use, such as when downloading software or searching for document templates, especially legal documents.

It's important to note that the danger of infostealers lies in their ability to facilitate further attacks. Stolen user credentials can lead to subsequent unauthorized access and obtain single sign-on (SSO) credentials to deploy ransomware, email credentials to conduct BEC attacks, cryptocurrency wallets for theft, or steal targeted information for espionage.

This makes it challenging for security leaders to understand where one cyberattack ends and another begins, as one attack can seamlessly transition into another without clear demarcation, particularly when stolen credentials are sold or repurposed.

Key Recommendations to Build Resilience Against Cyberattacks

In the final stage of the cyberattack, the attackers are focused on achieving their end goals, which may include data exfiltration, asset compromise, or persistent access establishment. The ability to stop an attacker's final objectives not only requires proactive strategies but also demands robust, immediate responses to ongoing threats.

Security leaders, in turn, should focus on not only withstanding these threats, but also effectively counteracting and neutralizing the adversary's actions to maintain organizational integrity and prevent business disruption. Therefore, we recommend:

- Anticipating future threats by continuously assessing, and understanding, your risk exposure and remaining vigilant against sophisticated cyber threats.
- Being able to withstand cyberattacks by prioritizing **24/7 threat detection and response** capabilities. Leverage real-time security telemetry to identify data breaches, mitigate damage, and maintain operational continuity. Also, have redundant processes in place should critical systems be compromised.
- Remediating malware infections as quickly as possible by:
  - Isolating systems and locking out accounts while threat investigations take place.
  - 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.
- Create, maintain, and exercise a strong **incident response** plan and associated communications plan that includes response and notification procedures for a ransomware incident.

Looking Ahead: A 2024 Outlook for Cyber Threats

As we move towards 2024, a pivotal year marked by significant elections across the globe, security leaders and Chief Information Security Officers (CISOs) must brace for an evolving cyber threat landscape.

The sophistication and adaptability of threat actors are not diminishing; instead, they are expected to harness technological advancements and proven business frameworks to escalate their activities.

Increase in Hacktivism and Political Disruption

It's likely that hacktivists and nation state-sponsored threat actors will use sophisticated TTPs to interfere with, and sway, crucial electoral processes around the world in 2024 – especially given that the United States, Ireland, Moldova, Georgia, and the European Union are all entering election seasons this year.

Moreover, threat actors may use AI-generated misinformation to launch campaigns that will make it challenging for legacy and new media entities to discern fact from fiction, further eroding public trust and exacerbating social divisions.

The Next Evolution of Ransomware-as-a-Service

With the widespread adoption of Ransomware-as-a-Service (RaaS), ransomware operations are expected to continue mimicking legitimate corporate structures. It's possible that this level of professionalism and reliability will set the foundation for ransomware groups to **partner with government entities**, blurring the lines between financially motivated **cybercrime and nation state-sponsored attacks**.

However, RaaS-as-a-Service is poised to be the next evolution of RaaS, wherein experienced RaaS operators will help new ransomware start-up operations flourish by taking on a 'consultant' role and providing services like **brand management**, human resources, and money laundering (Figure 10).

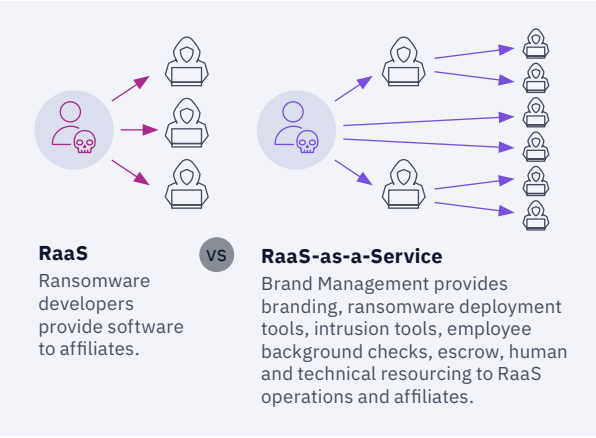

Figure 10: Ransomware Consulting as a Service.

This evolution will also include providing strategic **reputation management**, so new operators know when to promote their brands and when to retire them in response to law enforcement actions and sanctions.

In addition, it's likely that cybercriminals will continue to specialize in particular roles along the kill-chain to signify becoming more dependent on a diverse cybercrime ecosystem. Operators will also invest in research and development towards enabling more sophisticated attacks, including zero-day exploits and supply chain attacks.

Expansion of the Attack Surface Due to AI Integration

The use of Large Language Models (LLMs) and AI technologies will continue to skyrocket as more organizations adopt Generative AI tools. However, this will greatly expand the attack surface that organizations will have to maintain visibility. Plus, the integration of Gen AI with internal data sets will present new points of vulnerabilities, particularly through prompt and malicious code injections.

Moreover, threat actors will also develop and train their own AI models to streamline ransomware operations, conduct personalized **social engineering** and spear-phishing attacks at scale, and **orchestrate intrusions** more efficiently to overcome security and network defense measures.

Critical Infrastructure Targeting by State-Sponsored and State-Aligned Groups

Critical infrastructure sectors (e.g., energy, water, transportation, healthcare, etc.) will continue to be targeted by state-sponsored and state-aligned cyber groups. These actors may use sophisticated cyber espionage tools, disrupt operations through destructive malware, or lay dormant within networks for future strategic operations.

Therefore, security leaders in these sectors must prioritize proactive threat intelligence, 24/7 threat detection and response capabilities with round-the-clock security operations coverage and enforce robust incident response protocols to mitigate the risk of disruption of critical services.

Exploitation of Zero-Days in Edge Devices

Edge devices, which serve as the entry points to network environments, are increasingly integral to business operations. This includes IoT devices, routers, and smart sensors – all of which can be potential gateways for attackers. Zero-day vulnerabilities in these devices are particularly valued by threat actors for initial access, as they can provide stealthy entry points to otherwise secure networks.

In the coming year, the exploitation of these vulnerabilities is expected to rise, as attackers aim to leverage the often less stringent security measures in place for edge devices compared to traditional IT infrastructure.

Organizations must be vigilant in applying security patches, conducting regular security audits on edge devices, and employing advanced threat detection solutions to identify and respond to such exploitative attempts.

Abuse of Remote Monitoring and Management (RMM) Tools

While RMM tools are essential for managing and monitoring IT systems remotely, it's highly probable that cybercriminals will continue to exploit them for malicious purposes. Following a significant uptick in abuse in 2023, it is projected that threat actors will continue to leverage RMM tools for widespread attacks in the next year.

To counteract this trend, it is essential for security teams to implement stringent access controls, monitor the use of RMM tools continuously, and apply behavioral analytics to detect anomalous activities indicative of misuse. Additionally, employing multi-factor authentication and ensuring RMM solutions are up-to-date will be critical in safeguarding against such abuse.

Recommendations to Stay Ahead of the 2024 Threat Landscape

The cybersecurity landscape is in constant flux, presenting a multifaceted matrix of threats that continue to challenge even the most robust security postures.

As threat actors pivot from traditional email vectors to more sophisticated browser-based and 'unknown' vectors exploiting out-of-scope endpoints, for initial access, security leaders must understand that these methods are precursors to deeper, more damaging intrusions that will undoubtedly lead to costly ransomware attacks and extensive network compromise.

Our research also highlights the most impactful initial access vectors that nearly always enable the threat actor to progress past the initial access stage and into intrusion.

The rise in intrusion ratios, which now affect nearly half of all initial breaches, signifies a stark increase in the efficiency with which cybercriminals can exploit initial footholds. This is further exacerbated by the strategic use of RATs and the manipulation of legitimate remote access tools.

Security leaders should pay special attention to how often and how severely different attack vectors are used, especially as we see malicious actors taking advantage of valid user credentials, supply chain weaknesses, and misconfigurations to deploy ransomware, run coinminers, and execute infostealer malware to exfiltrate data.

Given that security teams are also underfunded and asked to consolidate their security spend, it's important that security leaders prioritize their investment by focusing on the most impactful initial access vectors for their industry.

In addition, we also recommend that security leaders become more forward-leaning in their defense strategy by examining the cyber risks that Generative AI, zero-day exploits, ransomware attacks, and nation-state actors pose.

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.**

  Emerging threats can potentially exploit the unique combinations of users, their devices, and the software they use within your organization. Therefore, your team must analyze how specific threats might target certain users or exploit vulnerabilities in particular endpoints or software. By understanding these intersections, you can implement targeted defenses and train users to recognize and avoid specific threats.

  Moreover, you should have a detailed inventory of all users, including their roles and access privileges, along with a comprehensive mapping of endpoints – be it mobile devices, workstations, servers, or IoT devices – and a thorough understanding of the technology stack in use across the organization to limit the presence of shadow IT. This granularity enables your team to develop tailored security policies and take response action rapidly when suspicious behaviour is detected.

- **Minimize unnecessary access (and thus, activity) between users, endpoints, and software.**

  To make sure that users only have the access necessary to perform their roles, it's critical to apply the principle of least privilege rigorously. Start by restricting unnecessary interactions between users, endpoints, and software to minimize the attack surface and reduce 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 eliminate the presence of out-of-scope endpoints, it's important to leverage advanced monitoring solutions that can detect anomalies (e.g., unusual user behavior, unexpected network traffic) and potential security incidents in real-time.

  Engage a multi-signal **Managed Detection and Response (MDR)** provider that offers continuous protection from 24/7 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, given the lack of skilled in-house cybersecurity experts, not all security teams have the capabilities needed to disrupt malicious behavior. Therefore, we recommend engaging a trusted MDR provider that will actually 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.

How eSentire Protects Organizations Against Sophisticated Cyber Threats and Ransomware Attacks

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry—financial services.

Over the last two decades, with two 24/7 Security Operations Centers (SOCs) and hundreds of cyber experts, we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale.

With eSentire in your corner, you can anticipate, withstand, and recover from even the most sophisticated cyber threats before they disrupt your business. Here's why 2000+ enterprises across 80+ countries choose eSentire:

- 24/7 threat detection and security operations to stop ransomware attacks before they deploy across your organization
- Battle-tested Elite Threat Hunters and security experts who manually hunt, contain, and respond to ransomware attacks on your behalf
- Our eSentire XDR Cloud Platform provides Security Network Effects so your defenses are hardened with every ransomware detection across our global customer base
- Industry-leading threat research and detection model development from our Threat Response Unit (TRU) to create encryption keys and new detection methodologies for lateral movement and cyber gang activities
- Industry-leading SLAs – 15 minute mean time to contain with eSentire MDR, and 4-hour remote threat suppression with our IR Retainer

Ready to get started?

Connect with an eSentire Security Specialist to learn how eSentire Multi-Signal MDR, powered by our XDR Cloud Platform, can help you reduce cyber risk and prevent ransomware attacks from disrupting your business.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSentire