expel

Annual Threat Report 2025

Cybersecurity insights, resilience recommendations, and predictions

“Regardless of your org’s security maturity, there’s something here for everyone.”

Dave Merkel
CEO, Expel

Letter from the CEO

Expel’s customer base runs the gamut, spanning organizations across almost every industry. This diversity grants our operators unique access to a wealth of data, which is crucial for staying ahead of threat actors and driving innovation.

This access also comes with serious responsibility. Namely, in protecting and maintaining the trust of our customers, but also in how we use our access and insights to share our learnings to continue fighting cybercriminals together as defenders.

As we delve into trends from 2024—ranging from cloud to phishing and everything in between—we’ll share what the data told us, how to detect (and protect yourself) against similar threats, and what that might look like in the coming year. Additionally, we’ll share thoughts and predictions for 2025 from our Expel experts, based on both their personal experiences and what they’re seeing throughout the industry.

Regardless of your org’s security maturity, there’s something here for everyone. Whether you’re strengthening your cloud environment, working to identify specific threats, or just exploring the data, we hope this report helps you start 2025 more informed and better equipped as we face the looming challenges ahead together.

“Cybersecurity is a team sport, and it’s a game of inches—not yards. Slow, continuous progress is the key to creating a sustainable security strategy that scales with your business.”

Greg Notch
CSO, Expel

Letter from the CSO

In an industry that’s oversaturated with digital content, I want to thank you for carving out some time from your likely overbooked schedule to review our Expel Annual Threat Report. Cybersecurity isn’t a slow industry, and, again, we know your spare time is limited. Your day-to-day consists of nothing but complex, nonstop problem-solving, so hopefully this report makes your day job a little bit easier.

While the data presented here is based on technology, it’s colored by the experiences, challenges, and successes our analysts saw throughout 2024. This team of experts works 24x7, every day of the year to keep us and our customers safe. In this report, you’ll see the threats they encountered and how they overcame them, so we can all learn together as we work towards a more secure future.

Cybersecurity is a team sport, and it’s a game of inches—not yards. Slow, continuous progress is the key to creating a sustainable security strategy that scales with your business. Our goal is to translate our data into strategic guidelines you can use to better protect your business, while, in the process, sharing information and contributing to the betterment of our cybersecurity community.

Contents

Executive summary

Key insights and takeaways

For the last four years, we've published this report detailing the attack trends our security operations center (SOC) analysts protect against every day. This is an analysis of the incidents, email submissions, vulnerability tracking, and threat hunting leads that our team investigated from January 1 to December 31, 2024.

We break down the trends into four essential threat categories: identity, cloud infrastructure, computer-based, and phishing. We do this to keep the report easy to digest and take action on, but keep in mind these threats are often tightly related. For example, attackers using **endpoint phishing** to deploy **malware** can lead to **compromised user identities**, impacting an organization's **cloud assets**. We'll highlight this interconnectivity throughout the report. But first, let's review what we saw as the top trends in each threat category.

OUR TOP TAKEAWAYS:

Identity trends continue to dominate incident investigations

Identity-based incidents made up 68% of all incidents among Expel customers, up four percentage points from 2023. While attempting to access email accounts is the most classic form of account abuse, successful identity attacks can be used to modify payroll settings, access cloud environments, or connect new (and malicious) devices to a network. Identity-based threats are highly lucrative for attackers, and should continue to be a high priority for defense.

Leaked and stolen credentials cause most cloud incidents

Attackers abusing leaked or stolen secrets caused the most cloud incidents this year, continuing previous years' trends. It's easy for users to expose keys inadvertently, and these keys typically provide high levels of access to attackers, making them attractive targets.

New malware scams drive most endpoint threats

Infostealing malware—which is malware that targets user credentials—made up the highest number of endpoint incidents. Stolen information often ends up on the dark market, where adversaries can buy and leverage it for new attacks. If credentials don't change or accounts aren't disabled, attackers can abuse them *years* after the original malware execution.

A popular means to deploy malware is a tactic tricking users into executing malicious scripts on their own machines (like presenting the user with a fake CAPTCHA). This tactic has become the most frequent means of installing malware onto a device because it bypasses the need for a user to download and run a program.

Vulnerability trends

The newest and most severe vulnerabilities in 2024 were in firewall and VPN appliances. Firewall and VPN appliances normally gate access to an environment, but can provide a springboard for attackers when compromised. However, despite these new and powerful vulnerabilities, we also observed attackers frequently leveraging vulnerabilities from years past. Older vulnerabilities still being leveraged include Log4j (CVE-2021-44228), Oracle WebLogic remote code execution (CVE-2020-14882), and Microsoft Office Outlook privilege escalation (CVE-2023-23397).

Credential harvesting has become the most prominent form of phishing

Of the phishing trends our SOC saw in 2024, about 41% of malicious phishing submissions were attempts to deploy credential harvesters, and about 34% of submissions were other forms of social engineering. These rates were consistent across industries.

In addition to hearty amounts of credential harvesters and social engineering attempts, we also saw extortion attempts across several industries. This tactic typically involves a phishing email sent to a user's corporate email account, which includes pieces of personal information in an attempt to scare the targeted user into completing a desired action for the attacker. The activity appears to be a steady campaign with no signs of diminishing any time soon.

Spotlight: Microsoft Teams setting allows malicious external messages

A default setting in Microsoft Teams allows users to receive messages from external organizations, and attackers abused this tactic throughout 2024 to gain unauthorized network access. These attacks abuse a built-in remote access tool—Quick Assist—and leverage other commercial remote access tools to gain and keep access to target systems.

2024 by the numbers

Incident types detected by Expel's SOC

This year's incident data compared to last year

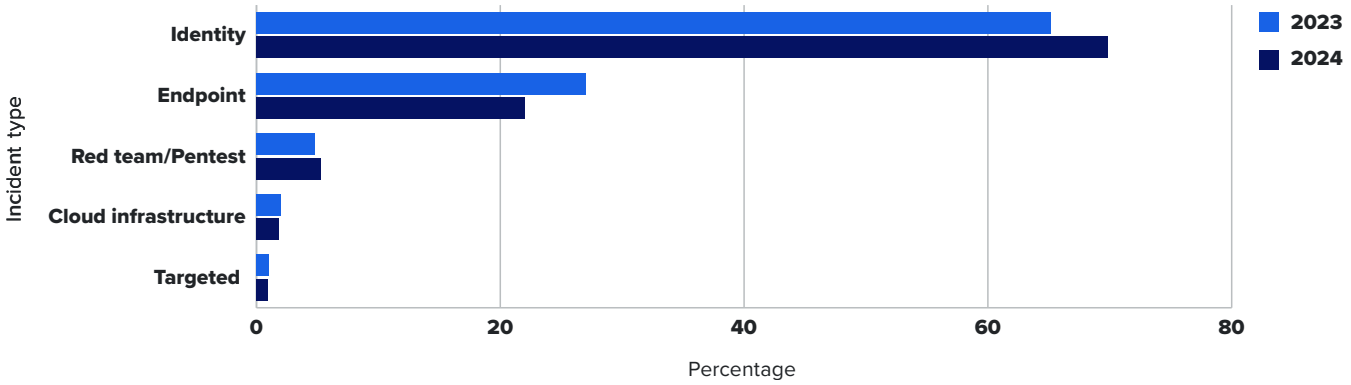
- **Identity-based incidents** dominated again this year, making up 68% of all incidents in 2024—four percentage points higher than in 2023.
  - In the context of this report, we define identity-based attacks as attempts by cybercriminals to gain access to a user's identity to perpetuate fraud.
- **Endpoint-based incidents** accounted for 22% of threats, likely only decreasing from 2023 due to the increase in identity threats.
  - The highest subcategory was malware, driven up by a tactic called ClickFix, which we'll discuss in depth on page 16.
- **Attacks specifically targeting cloud infrastructure** accounted for approximately 2% of threats, which was identical to 2023. While a few actors are specializing in targeting these assets, this category doesn't have the volume of incidents that other categories have.
  - The highest volume of cloud infrastructure incidents are the result of leaked or stolen cloud secrets.
- **Targeted threats** account for 1% of incidents. These attacks involve a bad actor who has their eyes set on a very specific organization or goal.

Why measure a category that's only 1% of incidents?

Even though targeted attacks make up a small percentage of incidents, these attacks deserve special attention in detection and response. Most incidents are opportunistic, and cast a wide net to identify *any* vulnerable target. With targeted attacks, they're incredibly persistent because attackers have their sights set on a specific target, and this persistence makes them a bit more dangerous.

Targeted attacks are tailored to a specific organization and may rely on open source intelligence collected about employees. Attackers are likely to make several attempts if one fails, using any learnings from failed attacks to adapt and improve. Although they make up a small number of incidents, this determination to succeed means analysts should be extra vigilant when a targeted attack is spotted.

Chart 1: Breakdown of incidents detected by the Expel SOC in 2023 and 2024

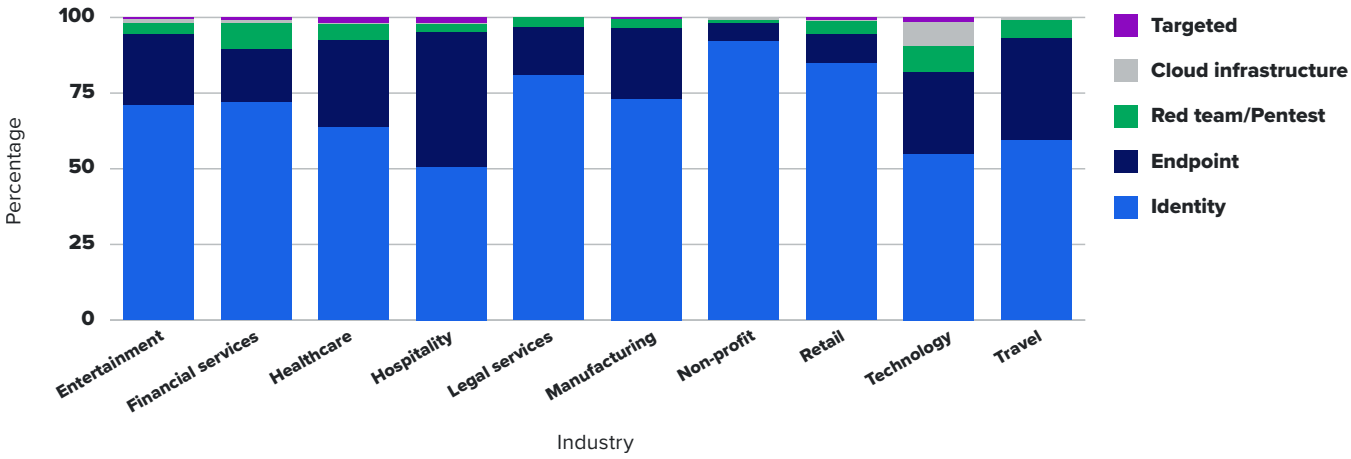


Incidents across industries

Identity compromise, most often the result of phishing, is a threat seen across all industries. While some sectors face higher volumes, no industry is immune. This is a major reason that identity incidents feature prominently in this report.

The following graph depicts the volume of incidents across the top ten industries that our customers represent. Within our customer base, we tracked the highest number of identity incidents for non-profits, retail, and legal services. But it's important to note these industries lead all others only by a small margin, as identity threats continue to dominate the threat landscape, regardless of industry, size, or security maturity.

Chart 2: Incidents across top 10 industries

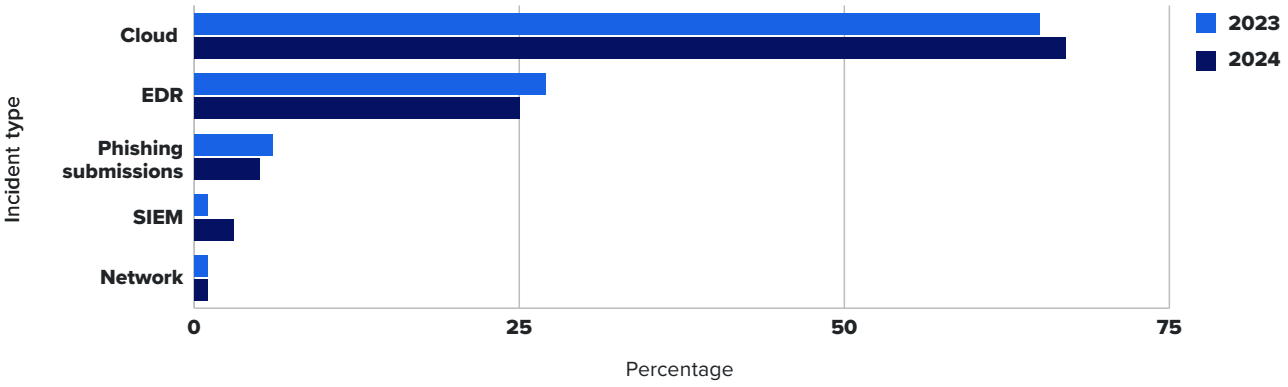


Initial alert sources in 2023 and 2024

Cloud resources managing identity, data, and infrastructure provided the highest number of leads to identify malicious activity, with identity being the foremost. This is consistent with identity being the most common entry point for cyber attacks, and it trended the same in both 2023 and 2024.

Endpoint detection and response (EDR) systems continued to be the primary source of monitoring and means of finding threats within networks in 2024. EDR systems identified 25% of all incidents, while SIEM and network monitoring systems provided alert leads for 3% and 1%, respectively.

Chart 3: Initial alert sources identifying incidents



Identity threats

Stealing and abusing credentials

Year-over-year, identity-based attacks continue to be the most common attack type we see across our customer base, with increasing volume. Barring major changes in cybercrime, we expect this trend to continue into 2025. Threat actors will continue to innovate, finding new ways to iterate on tried-and-true methods to steal and abuse credentials.

How are credentials stolen?

This year, we observed three primary contributors to the theft and abuse of credentials: phishing-as-a-service (PhaaS) platforms, traditional phishing, and infostealing malware. PhaaS platforms are a fairly recent innovation to phishing that arose out of attackers' needs to bypass multi-factor authentication (MFA). Unlike traditional phishing, PhaaS platforms create attachments and emails, and maintain infrastructure on behalf of attackers. Despite this convenience, PhaaS platforms haven't fully replaced traditional phishing—yet.

Unlike credential harvesters, which target one type of login, infostealing malware targets a wide array of sensitive data on a computer, whether it's stored by the browser or in files. Infostealing malware has been around for decades, but has become a much more common threat in the last few years. The computer-based threats section of this report delves into infostealing malware, but for now, let's focus on the rising popularity of PhaaS platforms as an identity threat.

PhaaS platforms

PhaaS platforms provide an aspiring criminal with an easy introduction into cybercrime. Just like platform-as-a-service (PaaS) software products used by legitimate businesses, PhaaS offers access to a service without requiring the buyer to set up their own infrastructure. These platforms offer many of the necessary components for running a phishing campaign, such as templates, infrastructure, and victim tracking. The buyer is only responsible for providing a target list and then acting on any stolen credentials.

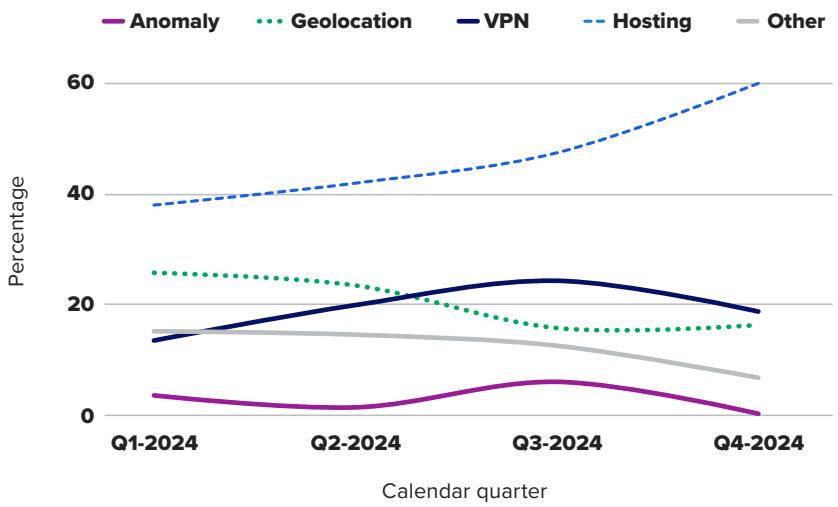
PhaaS platforms work by creating a webpage that can proxy information to and from the legitimate login domain. This type of proxying is classified as an adversary-in-the-middle (AiTM) tactic, since it allows an attacker to intercept traffic.

Since the webpage is proxying traffic, it's often configured to load the same graphics as the legitimate login page. If the target organization has a specific background or logo, the malicious page will also use this information to make it look legitimate. The fake page then submits any information supplied by the user and returns any results provided by the real login

page. So if the real login page requests a MFA token or a one-time pass (OTP), the fake one will request this information too. The proxying page intercepts session cookies, which can then be used by an attacker to access the account and bypass MFA. We most frequently see this attempt to access the account occur from a hosting provider.

Over 2024, we've continued to see a growth in the use of PhaaS platforms by observing login attempts from hosting providers. This trend in authentication sources is detailed in the graph below.

Chart 4: Authentication sources over time



Attackers can change user agents for malicious logins easily, but they often don't. Identifying and triggering alerts with suspicious user agents is a valuable way to identify many malicious logins.

Based on our tracking and analysis of the data, logins from hosting providers were consistently the result of users interacting with phishing distributed from a PhaaS platform. The logins often exhibit signs of automation, such as user agents that are part of automation systems. Examples include axios and node-fetch. This combination of automation and hosting infrastructure is a high-confidence indicator of malicious activity.

Understanding the data

As an authentication source, **hosting** is defined as infrastructure offered from a data center. This may consist of physical or virtual private servers consumers can spin up.

The **VPN** category tracks malicious logins identified from sources associated with consumer VPN providers and logins using The Onion Router (TOR).

Geolocation tracks instances where a login was flagged as a suspicious location—either from miles away, or on the other side of the planet.

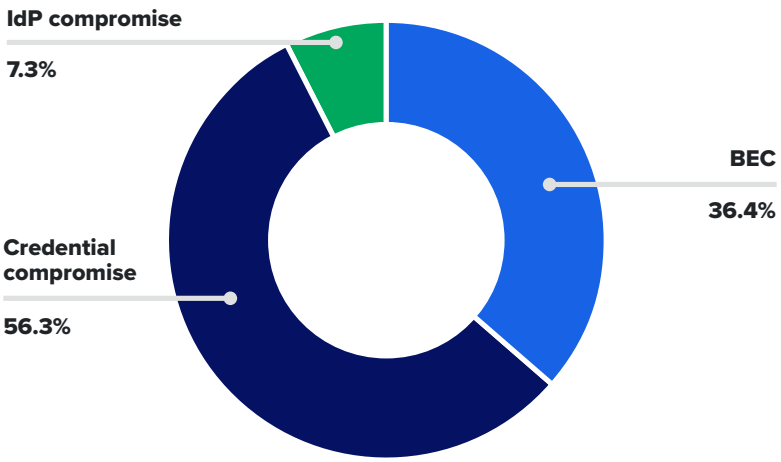
The **anomaly** category is used for tracking malicious logins that were eerily close to the user's expected geolocation. These logins may have been identified as malicious for reasons other than geolocation, but the login source often suggests an attacker is using a proxy.

How are stolen credentials leveraged?

For credentials to be leveraged, they first must be stolen. The graph below represents incidents where credentials have been successfully compromised. In most identity incidents we observed this year (56%), the bad actor was blocked from accessing the account via customer security controls *after* the credentials were compromised. The other 44% of the time, attackers most often used stolen credentials to access email accounts and single-sign-on (SSO) applications.

It's important to note that even though credentials were compromised 56% of the time but not leveraged for additional actions like identity portal compromise (IdP) or business email compromise (BEC), that doesn't mean it isn't a security concern. Credentials should always be updated when compromised, regardless of whether an attacker's first attempt to apply them was successful or not, because they will try again.

Chart 5: Type of identity compromise tracked in 2024



Understanding the data

At Expel, we track three main types of identity incidents:

BEC: This is an unauthorized party authenticated to an active email account. When this happens, abuse of the account is a matter of when—not if—and requires action from automation or security teams to kill sessions and investigate activity.

Identity portal compromise (IdP compromise): This is when an unauthorized party authenticates to an identity portal, where they can then access SSO applications

Credential compromise: This occurs when an unauthorized party attempts account access and is denied. This indicates an attacker successfully intercepted a user's credentials, but access was restricted (likely due to access policies). In future attempts, this could be circumvented with retries using VPNs or proxies. Credential compromise introduces additional risk because one blocked login attempt doesn't mean the attacker won't try to access other services with the same password.

Protecting your organization from PhaaS platforms

PhaaS platforms make session token theft easier for adversaries, so it's important organizations reset passwords *and* terminate sessions for compromised users immediately after a successful attack. Otherwise, the attacker can (and will) continue to access the account for as long as the session is valid.

For any accounts accessed by an attacker, it's important for security teams to investigate and identify any newly added MFA devices. In many situations, attackers will attempt to add MFA devices to maintain an account connection even after the session has ended.

It's also important to create detections for each stage of an attack to ensure an attack is detected even if another control fails. Examples include:

- Triggering alerts for newly added MFA devices
  - Give special attention to MFA devices added after passwords resets, and MFA devices added while connected to a proxy or VPN.
- Triggering alerts for the creation of new inbox rules
  - Attackers commonly use simple names for inbox rules. Many attacker-created rules can be caught by looking for rules consisting of two to three characters or only containing a single repeating character.
  - Monitor for rules created containing keywords like "payroll", "malware", or "virus". Rules with these keywords often indicate malicious activity.
- Advising employees to know their payroll information and report any abnormal or suspicious activity to the security team. Changes resulting in unexplained variances in paychecks are evidence of an identity compromise.
  - Some HR management systems allow administrators to require approval for sensitive information updates (such as direct deposit details). Consider implementing this type of control for your own organization.

Creative uses of credentials

In last year's Annual Threat Report, we reported the highest volume of targeted attacks among our customers were the result of the hacking group known as **The Com**, a group including actors such as Scattered Spider. This year, that trend continued. During 2024, **some individual arrests were made within the group**, but we anticipate these tactics will continue into 2025.

Actors within this group share a primary tactic. Specializing in SMS message abuse, they perform **SIM swaps**, assigning a victim's phone number to a device they control to target a user's identity. This allows attackers to receive SMS messages intended for the recipient. In this case, these are SMS messages allowing the user to complete authentication for an account. The attacker uses credential harvesting or self-service password resets to bypass their need for the user's password.

A subgroup known as Atlas Lion (and as **Storm-0539**) conducted one of the incidents we observed this year. In an attempt to gain access to a target network, the threat actor created a virtual machine within Azure. During the installation of Windows 10, the threat actor used stolen credentials to register the device to the target domain. This registration behaved as a newly enrolled device, and connected with the AzureID to install designated software for corporate devices. Expel's SOC detected this activity because the automation downloaded the corporate EDR agent and triggered an alert due to the user's abnormal location.

Service credentials

A high-profile news story in 2024 also highlighted a creative use of credentials. **A large number of Snowflake data stores were compromised**, and during the investigation, analysts discovered the attacker purposefully purchased credentials specific to Snowflake data lake instances. Additionally, the attacker developed a custom tool targeting this specific platform.

The main reason this incident was possible was because Snowflake didn't require MFA for accounts at the time. As a result, accounts that weren't secured with MFA were easy targets for the attacker, who specifically sought out the Snowflake data lake credentials.

The credentials purchased had been stolen by infostealing malware and were sold on the dark market. **As we've discussed on our blog**, the purchase of credentials to steal data isn't limited to any particular platform (like Snowflake). When exposed credentials are sold to attackers, this type of incident can happen on other platforms, too.

Ransomware gangs love stolen credentials

We noted this trend in 2023, have seen it continue through 2024, and expect it to continue in 2025. Ransomware gangs are also keen on using stolen credentials to gain network access, and will often collaborate with other criminals who sell credentials or access to infected computers.

In tracking tactics from multiple ransomware gangs, we've observed several gangs buy credentials and leverage them against corporate VPN accounts. If they're not protected with MFA, these purchased credentials give an attacker easy access to corporate systems.

Cloud platform threats

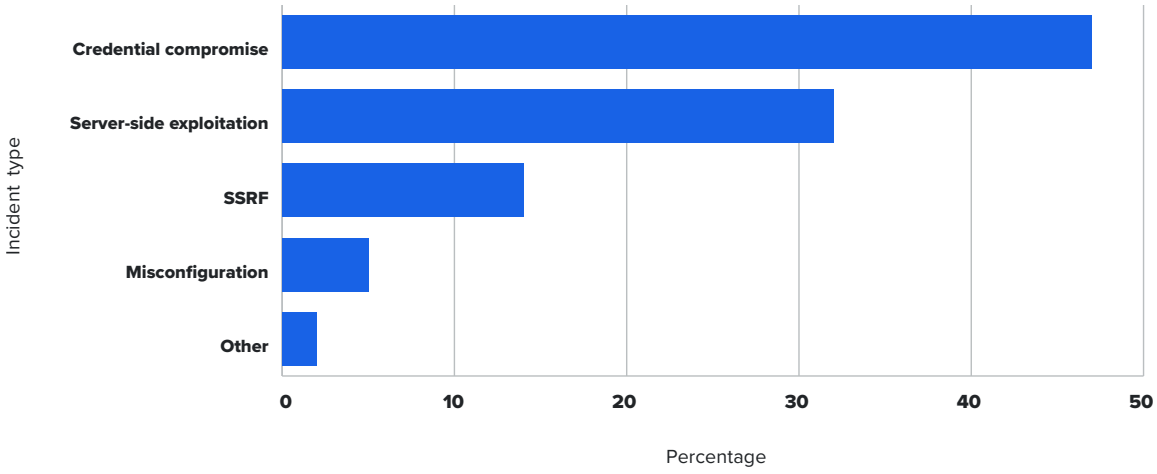
Increased cloud adoption leads to increased cloud threats

Cloud infrastructure incidents in 2024

Cloud infrastructure attacks target assets hosted on cloud platforms such as Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes. The techniques and frequency of these attacks continue to evolve, reflecting the growing adoption of cloud environments and the expanding attack surface that comes with them.

Expel defines cloud infrastructure activity as an incident where an attacker can gain access to the control plane or data plane of a cloud platform. In 2024, **86%** of our cloud infrastructure incidents impacted assets in AWS, while only **9%** impacted assets in Google Cloud and Azure.

Chart 6: Cloud infrastructure incident types in 2024



Just like previous years, credential compromise continued to be the top cause of cloud infrastructure incidents in 2024. Stolen or leaked cloud credentials (also known as secrets) provide attackers with access to the cloud control plane through an attack framework or a command line utility. These secrets can be exposed through accidental uploads to repositories, vulnerability exploitation, or infostealing malware.

The second leading cause of cloud incidents in 2024 was server-side exploitation. In these incidents, an attacker identified and exploited a vulnerability in a web application to deploy a web shell or malware. While we couldn't identify a leading cause for these types of incidents (due to a lack of successful compromise), we do know the most common payload deployed was cryptomining malware.

The third-highest cause of incidents were server-side request forgeries (SSRF), where an attacker tricks a public-facing web application into exposing sensitive information. Specifically, it tricks an Amazon Elastic Compute Cloud (Amazon EC2) instance into exposing secrets by requesting information from the instance's own metadata. To protect against this type of attack, it's important to review the security of the application in the instance you're using. Ensure the instance is using **AWS's Instance Metadata Service version 2 (IMDSv2)**. AWS originally released IMDSv1 to mitigate the issue, but version 2 should be used instead to best protect sensitive information.

From identity to infrastructure: Scattered Spider targets compromised AWS accounts

Scattered Spider has adapted its tactics to include data theft from cloud storage objects. Some individuals in the group have also shifted their primary goal to exfiltration-based extortion.

During a 2024 phishing/smishing campaign, Expel confirmed Scattered Spider actors accessed multiple applications via compromised user accounts while using Okta SSO. One compromised account was then used to authenticate access to the organization's AWS console and assume an engineering role. The attacker attempted AWS discovery before being locked out of the account.

A key portion of Scattered Spider's campaigns involve gathering intelligence and data. Had the attackers been more successful in their attempts to understand the organization's environment configuration for the next stages of their attack, they may have been able to successfully iterate through AWS resources to locate the most valuable data for their attack or extortion.

Protecting your organization from cloud infrastructure threats

Just like with other technologies, it's important to ensure your cloud infrastructure is monitored with a defense-in-depth strategy. That is, build your detections to spot suspicious activity at multiple stages of the attack lifecycle.

Secrets are most often exposed accidentally. We recommend using secret scanning to prevent key exposure. This process can identify accidentally exposed access keys in code repositories during development, or after publishing. Secret scanning can also be performed through paid services, or can be configured with open source tools. These can identify hundreds of secret types from a wide range of sources to keep you secure.

For AWS specifically, you can create detections around long-term and short-term access keys (beginning with AKIA and ASIA, respectively) to detect early stages of unauthorized access to your environment.

Computer-based threats

Trending malware and popular vulnerabilities

In the neverending game of cat-and-mouse, both attackers and defenders study each other to understand what tactics might outwit their opponent. Just like defenders, successful cybercriminals learn from one another and adopt effective techniques. Throughout the year, we monitor those trending techniques to improve our detection capabilities. We're sharing our observations here to alert others to trends in malware and vulnerabilities.

Malware trends

Malware is any software that's used to harm networks, computers, or users. This includes custom and off-the-shelf software repurposed for cyberattacks. As defenders, we're responsible for defending against *both* types of malware.

At Expel, we break malware into two major categories based on risk: high-risk malware and latent-risk malware. High-risk malware can take off fast and cause a lot of damage. This category includes remote access tools (RATs), initial access tools (IATs), and USB initial access tools. Latent-risk malware is all about the long game: the cybercriminals deploying malware aren't acting immediately on their objectives. This category includes infostealers, cryptocurrency miners, and banking trojans.

Commonly observed malware types

IATs: Also called loaders or droppers, IATs attempt to circumvent defenses to get onto a system, so they can download or load additional malware.

RATs: Aptly named, RATs enable remote access to computers. RATs can include abuse of legitimate commercial tools like remote management and monitoring (RMM) tools or custom attacker-built tools.

USB initial access tools: This is malware that runs from infected USB drives. When the infected drive is plugged into a computer, the malware attempts to connect to pull down additional tools to give bad actors access to the device.

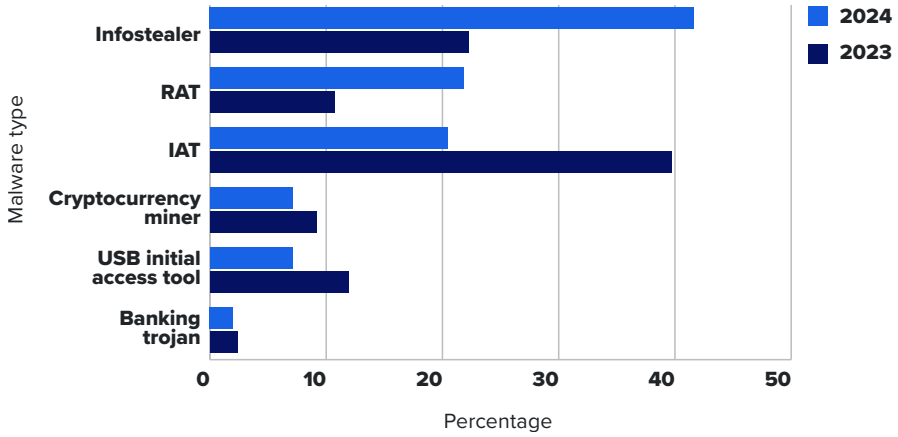
Infostealers: Infostealers are malware that access sensitive data on a device and then send it to an attacker. They most frequently target passwords stored in the browser, cryptocurrency wallets, or files stored in common places.

Cryptocurrency miner: This is malware that uses the resources of a computer or server to generate cryptocurrency on behalf of the attacker.

Banking trojan: This type of malware steals or intercepts financial information as the victim is using this information.

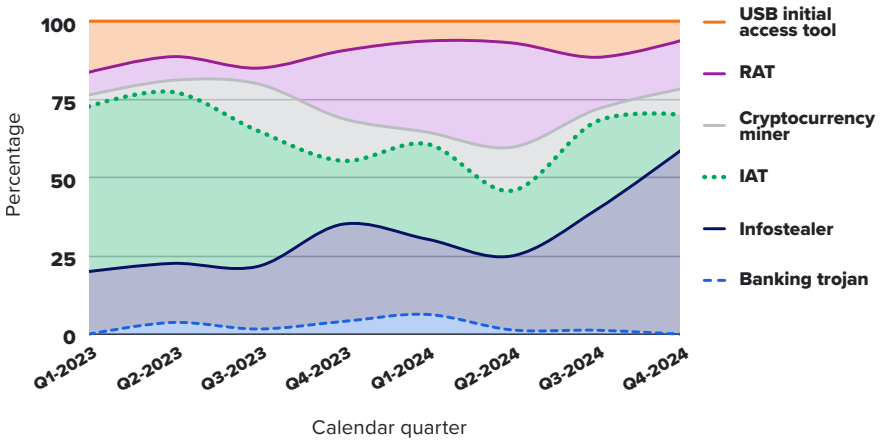
The following graph compares the prevalence of these subcategories in 2024 and compares them to our data from the prior year. The biggest difference between the years was a shift in prevalence from IATs to infostealers.

Chart 7: Malware type prevalence 2024 vs. 2023



The following graph depicts the change in malware types over the last two years.

Chart 8: 2023 and 2024 malware types



Understanding the data

Of all the malware incidents we investigated in 2023 and 2024, Chart 8 highlights the frequency of each malware type throughout the year.

The graph is always at 100%, representing all the malware types we saw in each quarter from 2023–2024, with the quarters as follows:

- Q1: January–March
- Q2: April–June
- Q3: July–September
- Q4: October–December

Q1 of 2023, for example, would be read as about 50% of malware occurring during that time was IAT. About 20% were infostealers, and no banking trojan malware was encountered. However, by Q4 of 2024, IATs were only about 10% of the malware encountered, and infostealer malware was over 50% of the malware encountered by our SOC.

It's important to note that percentages on the y axis represent the portion of 100%, and not all start at zero. It requires a little bit of mental math to determine exact percentages, but provides a helpful visual guide to malware trends.

As depicted in the graph above, the largest volume of malware in the first quarter of 2023 were IATs. These were largely attributed to the Qakbot botnet and Gootloader malware. Qakbot was virtually eliminated as a threat after the 2023 takedown of the botnet. Additionally, Gootloader's activity also significantly decreased in the second half of 2023, and declined even further in the second half of 2024. This decline largely seems to be the result of threat actors changing tactics from SEO poisoning to using PDF-to-doc converter websites. These changes resulted in RATs and infostealers taking a larger share of observed malware activity in 2024.

PDF-to-doc converter websites

It's critical to make sure your employees have the tools they need to do their job, including authorized PDF editing tools. With Gootloader, a victim uploads (sometimes sensitive) documents to convert the files from PDFs to Microsoft documents (.doc), but instead installs malware that can lead to ransomware if unmitigated.

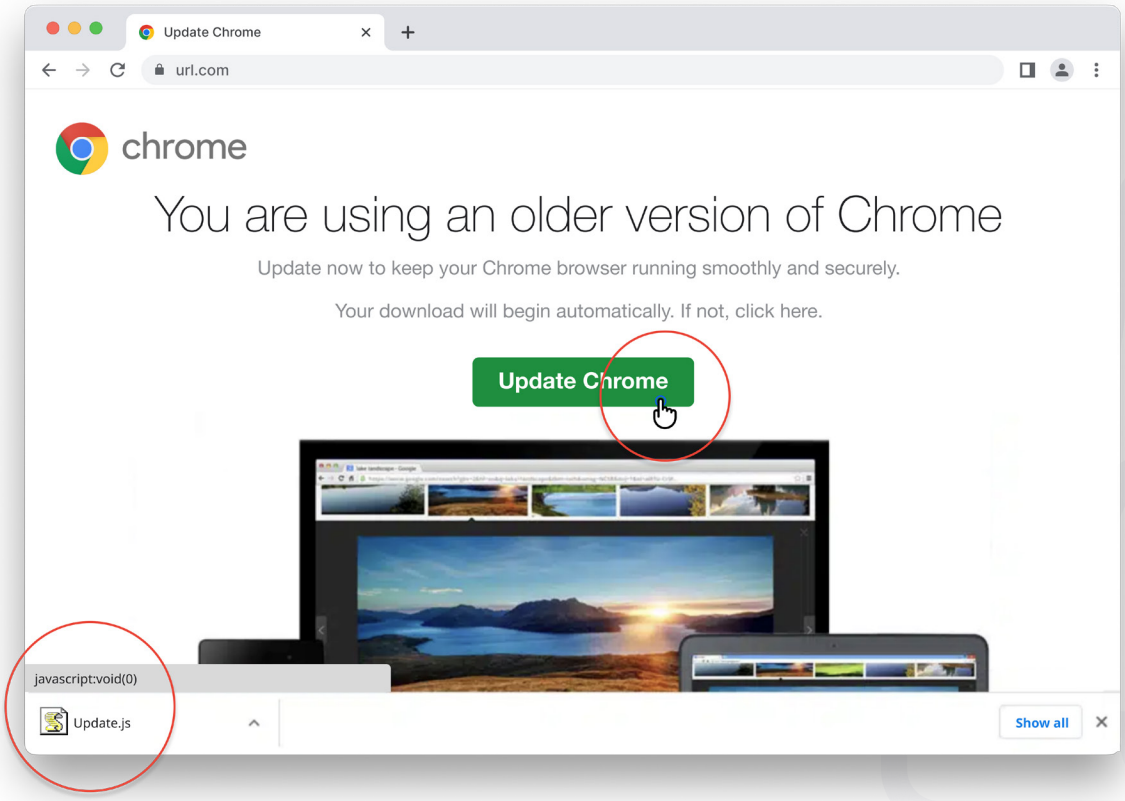
Our SOC also observed a massive increase in infostealers beginning in the third quarter of 2024. This was driven by the decrease in the Qakbot and Gootloader malware, and the rise of the ClickFix tactic.

Development and growth of the ClickFix tactic

With the decline of Qakbot and Gootloader malware, the most consistent IAT threat is SocGholish malware. The criminal group maintaining the malware consistently relies on infected websites to deliver it, and many other aspiring cybercrime groups are looking to follow in their digital footsteps.

In this approach, the infected website displays a message instructing the user to download and run malware disguised as a browser update. If the user attempts to download the fake update, they'll receive a JavaScript file which, when executed, loads malware onto their system. The actor running this malware often hands off infected computers to ransomware gangs.

Image 1: Example of SocGholish phishing designed to execute JavaScript and deploy IAT malware



Preventing malicious JavaScript execution

JavaScript files are often difficult for EDR agents or browsers to adequately block. This is because it's formatted as a text file and is usually heavily obfuscated.

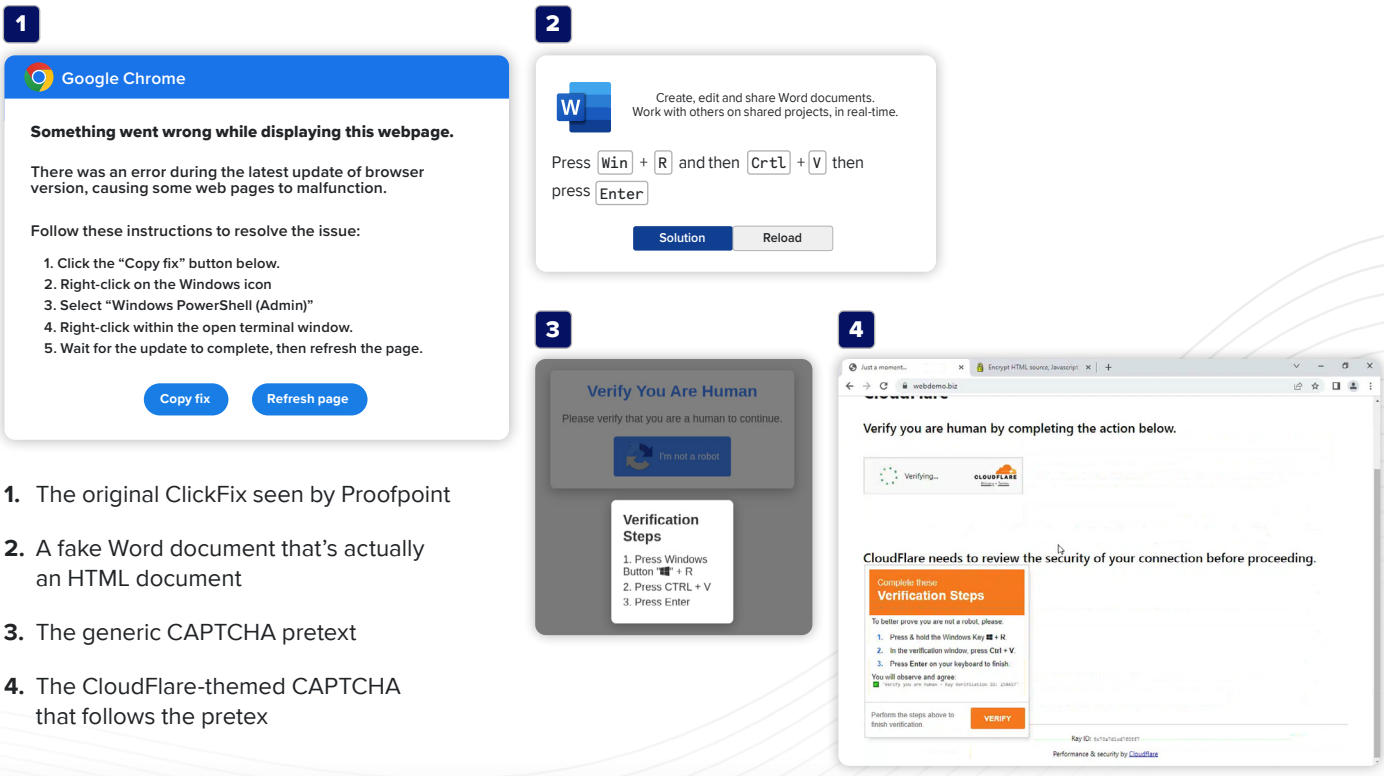
By default, Windows will execute JavaScript when double-clicked by a user; however, the default can be easily changed to open the file with Notepad instead using Group Policy. This simple setting change prevents this common tactic from threatening your organization.

In 2023, multiple threat actors hopped on the "fake update pop-up" bandwagon to trick users into downloading malicious files. In 2024, a new variation on this tactic started to appear. Users were instructed to run code to fix a supposed problem by following instructions that would complete an action on behalf of the bad actors instead. Thus, the ClickFix attack was born. Proofpoint has documented and explained some of the earliest examples of this tactic. In the second half of 2024, this tactic increased in popularity.

In some early iterations, infected websites provided the user with code and instructions. It required users to open PowerShell as administrators and willingly copy and paste content given to them into the terminal.

Attackers continued to innovate on this tactic throughout 2024. New versions simplified the instructions and started to use other scenarios such as fake CAPTCHAs, documents, and system errors. These versions automatically modified the user's clipboard and instructed them to run the code using the Windows Run application (launched with the Windows + R key combination). This was easier for the user and streamlined the attack.

Image 2: Examples of the ClickFix tactic

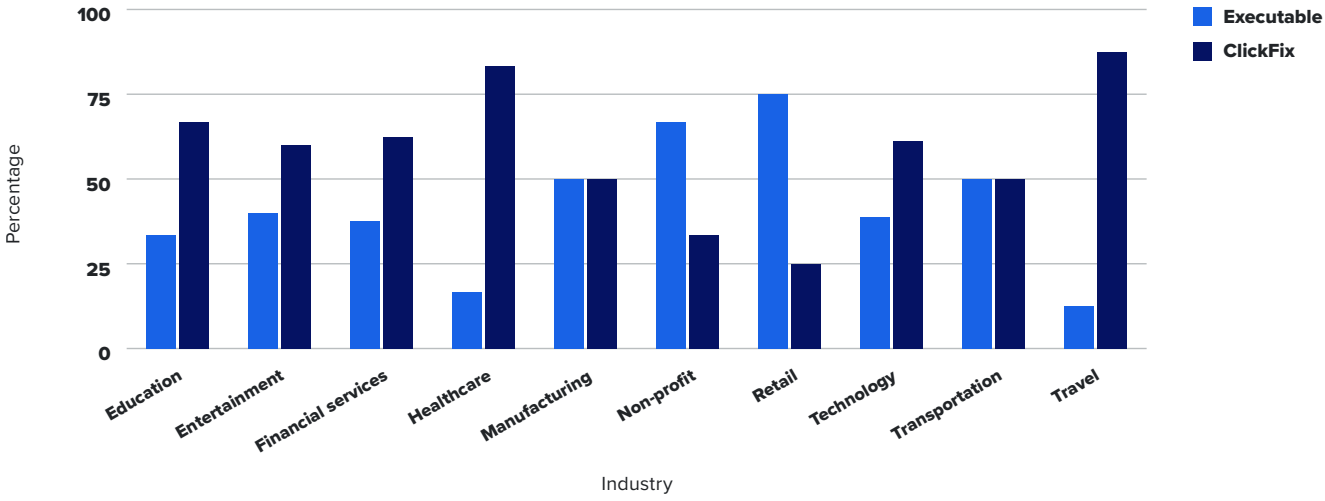


1. The original ClickFix seen by Proofpoint
2. A fake Word document that's actually an HTML document
3. The generic CAPTCHA pretext
4. The CloudFlare-themed CAPTCHA that follows the pretex

It's important to understand this tactic is popular because of its ability to bypass common download defenses. Based on our 2024 data, the tactic is most commonly used to deploy infostealers; however, we've also seen attackers use it to deploy RATs. We know nation-state actors are leveraging it, too.

In most industries, it's more likely a user will be tricked into executing malicious code than downloading a malicious file. This is because interrupting a user fits into a wider range of phishing scenarios than downloading a file (which is also more work). This tactic also bypasses the ability of the browser or operating system to block the download because there is no download—instead, the user executes code that retrieves the malicious script to run. These scripts often decrypt and load a file into memory without ever writing the file to disk, reducing opportunities to detect a file and block the activity.

Chart 9: Prevalence of executable vs. ClickFix execution



Protecting your organization against the ClickFix tactic

- Use secure web gateways to block traffic from attacker-controlled domains.
  - Secure web gateways provide a means to block websites based on reputation, policy, or other factors. In this instance, secure web gateway policies will block very new domains (or those with bad reputations), which often completely blocks the display of malicious pop-ups or connections to attacker-controlled websites.
- Ensure hosts are monitored with EDR *and* have the EDR in blocking mode. Blocking mode gives the EDR the best chance at blocking the script execution when—not if—it happens.
- Consider disabling the Windows Run program for users who don't need it using the Group Policy Editor.
  - Most attackers use the Windows Run program to run malicious code. Disabling the feature can cause friction, preventing a user from executing the code.

Lumma infostealer prominence

Of all the infostealers out there, we noticed one rise in prominence this year: Lumma infostealer. Infostealers typically fall into a category of malware we call commodity malware. That is, the malware is readily available for criminals to purchase—they just have to find their own delivery method. As a result, it can be delivered in a variety of ways, but the ClickFix tactic is the most popular method we're seeing right now.

We observed usage of Lumma malware trending upward in the third quarter of 2024, and it continued into the end of the year (also confirmed with other public reporting). The popularity of this infostealer highlights the importance of understanding—and protecting against—its specific behavior.

Lumma infostealer relies on three different domain types for its command and control (C2) functionality:

1. **Multiple uncommon domains**

   Lumma is configured to rely on a dozen or so low-prevalence domains. They rotate these domains weekly to avoid giving them a bad reputation. These generally leverage inexpensive top-level domains (TLDs), such as .xyz, .site, and .shop.

   In organizations where it's possible, we recommend blocking TLDs known for high amounts of abuse, temporarily blocking newly registered websites, or temporarily blocking a website the first time the organization network sees it.

2. **A dead drop resolver**

   If the infostealer isn't able to reach any top-level domains, it will reach out to a dead drop resolver. This uses a legitimate website to host information directing malware to another C2 infrastructure. With Lumma specifically, it uses steamcommunity.com. This site hosts profiles for Steam accounts, and attackers use player names to hold the dead drop resolver text.

3. **Exfiltration via Telegram**

   Lumma infostealer—and many other infostealing malwares—use Telegram's messaging functionality for credential exfiltration. This allows attackers to use common domains to receive stolen information. It also instantly notifies the attacker via SMS message once data is successfully stolen.

   If Telegram isn't required or authorized in your organization, we recommend blocking it on the corporate network due to the high volume of abuse via infostealers.

Vulnerability trends

When attackers want to gain access to a network, they leverage vulnerabilities. When assessing vulnerabilities, we review incidents within our customer environment alongside broader industry data—such as data from vendors, social media, CISA, and other sources—to understand what vulnerabilities are of interest to attackers and to confirm trends we're seeing.

Vulnerability landscape

In 2024, we tracked over 250 high severity vulnerabilities and prioritized tracking the vulnerabilities with the highest likelihood of attracting attackers. This included vulnerabilities known to be exploited, that had the potential to cause a lot of damage, or that were easily available through publicly available code.

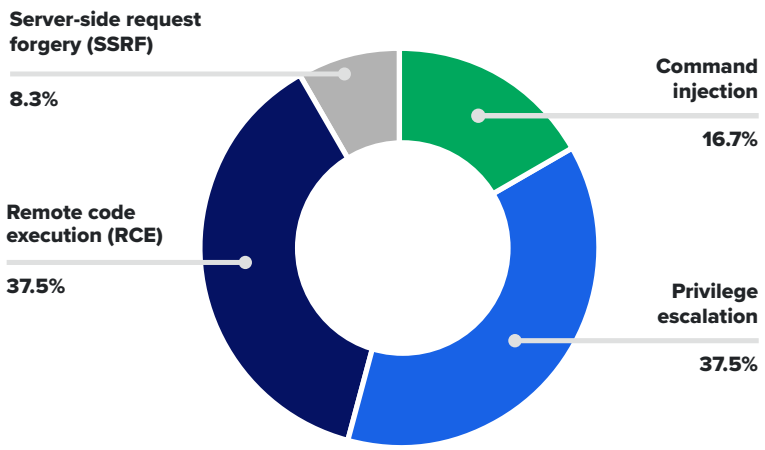
The most severe vulnerabilities we tracked were in internet-facing network appliances—primarily firewalls and VPN appliances. These appliances normally provide a barrier to keep bad actors out. When they're compromised, attackers can use them to gain access to a corporate network, bypassing the device or even leveraging the device itself. Last year, we observed several threat actors prioritizing these vulnerabilities, and that trend continued into this year. We don't expect that to slow down in 2025.

Protecting your organization against stolen credentials

- Prepare a playbook for resetting credentials if an infostealing malware is executed on a device.
  - Most infostealers prioritize stealing credentials from the victims' browsers. Credentials saved in the browser should be changed any time malware is encountered to prevent abuse.
  - Some infostealer malware intentionally target AWS, Azure, and Google Cloud credentials saved on a host. Be sure to build a plan in your playbook to reset these if they're stored on an impacted host.
- Implement a password manager within your organization.
  - Password managers encrypt stored passwords until they are needed, preventing credential theft.
  - Ensure contractors have access to secure password storage, too. They're also at risk of downloading infostealers, and their device could also give attackers access to your organization.
- Ensure unused accounts are deactivated and monitored for compliance with the NIST800–53B policy.
  - NIST800–53B no longer recommends periodic password rotation, and this policy is in place to prevent the atrophy of passwords over time. However, one unintended consequence of the policy is that compromised and exposed passwords remain at risk as long as the account is active.

Out of the vulnerabilities we observed, we identified threat actors frequently exploiting 56 different common vulnerabilities and exposures (CVEs) within our customer base. This is consistent with the 50 CVEs identified in 2023. This number—compared to the average number of CVEs published throughout the year—is low, but is helpful because it both validates the work our SOC is doing, and confirms customers are properly patching and addressing common vulnerabilities we escalate to them throughout the year.

Chart 10: MDR repeated vulnerabilities



Double trouble: old and exposed vulnerabilities in external-facing assets

Throughout 2024, our SOC observed exploitations in various types of assets exposed to the internet. Our data shows half (56%) of incidents involving externally-exposed assets impacted servers. In *all* of these server incidents, the Microsoft Windows server operating system was beyond the standard end of life (EOL). So, in addition to the risk introduced by the externally-facing vulnerabilities, these assets were also at risk for further exploitation due to vulnerabilities in their operating systems.

We recommend security practitioners evaluate their high-risk externally-facing servers and take at least one of the following actions to limit external server risk:

1. Develop processes to upgrade Microsoft server operating systems regularly
2. Develop a high-availability server patch rotation scheme to limit downtime and increase patch frequency
3. Develop a robust patching program with scheduled downtime

External server exploitation risk continues to rise, especially for older operating systems. Developing and implementing these plans can reduce risk and limit operational impact, while maintaining—or even enhancing—server security.

Most commonly exploited asset types

Asset type exploited	Incident frequency
Server	56%
Endpoint	26%
Firewall	10%
Cloud (EC2s)	8%

Most commonly exploited server operating system (OS) versions

Exploited server asset OS versions	Incident frequency
Windows Server 2008	7%
Windows Server 2012	14%
Windows Server 2016	14%
Windows Server 2019	65%

Endpoint risk

In 2024, we attributed 50% of endpoint incidents to CVE-2023-23397, a Microsoft Outlook elevation of privilege vulnerability. Attackers exploited this vulnerability by sending malware through phishing emails. Since the vulnerability was present in specific versions of Outlook, it gave attackers a foothold on both Windows 10 and 11 systems. The risk of attackers gaining access through unpatched applications highlights the need for patch management to ensure endpoint operation systems are up-to-date, too. In October of 2025, we'll see the EOL for Windows 10, so we recommend ensuring you have a plan to have endpoints upgraded before then to minimize risk.

Most commonly exploited server operating system (OS) versions

Exploited server asset OS versions	Incident frequency
Windows 10	57%
Windows 11	43%

Repeated vulnerabilities

We observed 24 additional vulnerabilities repeatedly leveraged against our customer base. The table below highlights the four most common CVE targets we saw in 2024. Note that older vulnerabilities are still being leveraged regularly as a means of targeting specific environments. Attackers will continue to abuse vulnerabilities even after a patch is released as long as those vulnerabilities work.

Frequently exploited 2024 vulnerabilities			
Vulnerability	**Targeted asset(s)**	**Attack vector(s)**	**Threat actor tactics**
CVE-2023-23397	Microsoft Office Outlook **Privilege Escalation** Vulnerability	Phishing campaigns	▪ OS: Windows ▪ Email link ▪ Malware
CVE-2020-14882	Oracle WebLogic Server **Remote Code Execution** Vulnerability	Public-facing servers	▪ OS: Oracle Linux, RHEL, & Windows Server ▪ Multiple RDP tools deployed
CVE-2021-44228	Apache Log4j2 **Remote Code Execution** Vulnerability	Public-facing servers	▪ OS: Windows Server ▪ Malware ▪ Webshell file deployed ▪ Cryptocurrency miner deployed
CVE-2024-21887	Ivanti Connect Secure and Policy Secure **Command Injection** Vulnerability	Public-facing servers	▪ VPN compromised ▪ JavaScript backdoor ▪ Credentials posted to attacker-controlled domain ▪ Outbound network connection

Protecting your organization against vulnerabilities

Have a clear patching plan and policy in place.

- This policy should include regular vulnerability scans to identify what vulnerabilities exist within the network *and* have a clear prioritization strategy for mitigation.
- Ensure your plan includes clear guidelines on how your team should address different severities.
  - Many critical vulnerabilities have a high rate of abuse. When identified, attackers are quick to leverage the vulnerability (assuming they haven't already). In these situations, your team may need to plan to work extra hours to patch and review known indicators of compromise. Having plans helps set expectations for your team and keeps these rare events from being surprises.
- Ensure that critical vulnerabilities remain a high priority.
  - Vulnerabilities like Log4j remain interesting to attackers, so their patching priority should never decline. Constantly monitor for vulnerabilities that are continuously abused by attackers.

Allocate (and utilize) resources for identifying and prioritizing vulnerability patching.

- Resources may include network scanners, personnel to plan and patch, or outside vendors to help with these tasks.

Have clear plans to maintain up-to-date operating systems.

- Outdated servers introduce additional risk into an environment if exposed to the internet.

Have clear plans for managing the Windows 10 EOL.

- As of October 2025, Windows 10 will no longer receive regular maintenance and security updates. Due to the trusted platform module (TPM) hardware requirements for Windows 11, additional planning may be required to ensure systems can be migrated to the new operating system.
- Ensure web applications hosted in cloud applications are part of the vulnerability scanning and patch management plan.

Phishing threats

Credential harvesters and social engineering

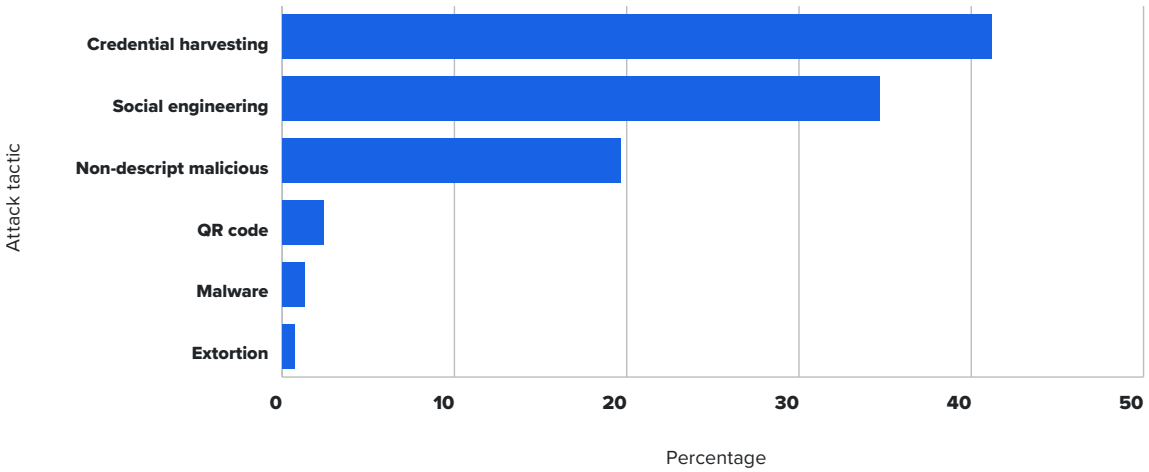
The following section is based on our phishing analysis of email submissions throughout 2024.

Throughout the year, credential harvesters made up, on average, 41% of malicious submissions. Another 34% of submissions were other forms of social engineering, such as fake invoices aiming to get targets on the phone to then install RATs on their computers, CEO impersonations asking for gift cards, or emails requesting sensitive information under the guise of a government organization. These rates are consistent across industries.

Expel® Phishing takes complete ownership of a customer's phishing inboxes and provides remediation and guidance when threats enter via this critical attack vector. Unique data from customer security technology helps Expel monitor and remove phishing emails from their inboxes as well as protecting the entire environment from these attacks.

For example, if a user sends a marketing email to our team, we can detect it as such with machine learning and treat it appropriately—without manual analysis. For malicious emails, our team reviews and investigates to ensure no users in the customer's environment have engaged with the same or similar phishing email.

Chart 11: Percentage of malicious submissions



One notable phishing category in 2024 was attempted extortion phishing emails. While it's normal to see some extortion attempts throughout the year (usually less than 1% of all emails), we began seeing these attempts increase in September (1.15% to 2.5% of all emails each month). They continued at this increased level through the end of the year.

The attempts appeared to be part of a campaign where the extorter sends an email to the user's corporate inbox. The subject and body of the email only contain the recipient's name but have a PDF or text file attached to it with an incriminating claim and subsequent demand (usually a bitcoin payment). The attacker often includes the user's phone number or home address to legitimize the threat.

We observed this campaign across multiple industries, but it focused heavily on employees in hospitality and healthcare. This is likely due to these industries experiencing **the largest theft of employee data** from third-party providers.

Lower phishing malware rates

Within our customer base, we observed a low rate of user submissions with malware attached or linked compared to last year, largely due to a few reasons:

1. Within our customer base, many organizations filter out a large number of emails with other security tools before they reach the end-user. This is a positive thing, but it results in our team analyzing fewer malware-infested emails.
2. The threat actors responsible for the large malware campaigns observed in 2023 are no longer active. In past years, this would have been Emotet or Qakbot, but those botnets and actors are no longer sending spam campaigns.
3. One cybercrime group targeting the hospitality industry shifted their tactics. As we reported last year, threat actors sent large volumes of links containing infostealing malware. However, instead of using broader infostealing malware, the threat actor shifted to using credential harvesters targeting online travel management platforms. In December of 2024, this actor shifted back to using malware, leveraging the ever-popular ClickFix tactic discussed in the computer-based threats section of this report (see page 16).

Understanding the data

In 2024, we saw (and stopped) various types of malicious phishing submissions.

Credential harvesting (41%): This is an attempt to compromise a user's credentials by directing them to a login page controlled by an attacker.

Social engineering (34%): This category contains a broad range of tricks, from fake invoices attempting to gain access to victim computers to CEO impersonation scams requesting gift cards.

Non-descript malicious (19%): This category consists of emails our analysts determined were malicious but were unable to fully identify the attacker's end-game. In many of these situations, the attacker's infrastructure may have been inactive, preventing our analysis. However, our analysts observed enough to determine the activity was malicious.

QR code (2.4%): This is the malicious use of QR codes, most often used to lead the user to a credential harvester. We separated this category from credential harvesting, since this tactic requires special care to detect and prevent.

Malware (1.3%): This category involves emails sent to the user with malware attached as a direct link to a malware download.

Extortion (0.75%): This category identifies emails which threaten the recipient in an attempt to extort them for money.

Protecting your organization from phishing

- Ensure users rely on MFA wherever possible.
  - The most secure forms of MFA follow the Fast Identity Online 2 (FIDO2) standard. These often leverage biometrics, physical tokens, and cryptographic keys to ensure the user logging in is who they say they are, and the website is legitimate.
  - Most of the phishing attempts we observed targeted corporate credentials, but we also see attacks targeting individuals or specific web pages. As much as possible, it's important to teach a culture of security, so using MFA is easy and encouraged for every account.
- Use secure email gateways and similar products.
  - These products can filter out a substantial amount of phishing emails. This reduces the overall risk of users downloading and executing malicious files or accessing credential harvesters.
- Ensure users have training to identify and report suspicious emails.
  - When users report suspicious emails, it helps provide defense-in-depth. It can notify security teams to investigate, and help them identify if malicious activity occurred because of the phishing email (whether from the submitter's interaction with the email or others in the environment).

Annual spotlight

Microsoft Teams continues to be a phishing target

Throughout the year, threat actors leveraged Microsoft Teams to gain access to targeted networks. A campaign using this tactic—which was seen first in **April** and then throughout the year—performed social engineering under the guise of being helpful. The attacker would sign their target up to receive spam emails and then contact the user through a Teams message, offering support to resolve the spam. The invite usually came from an account disguised as a tech support team. If the victim accepted the invite, the attacker would request to connect to the user's computer using Microsoft's built-in remote access support tool, Quick Assist.

Upon launch, Quick Assist generates a code users can provide to grant someone remote access to their device. Once the attacker connects to the victim's device, they can run a script to install additional RATs, allowing them to maintain access for future malicious behavior. This activity was **primarily attributed** to cybercriminals working for the Black Basta ransomware gang.

Does this sound familiar? We previously reported on a similar tactic abusing Teams. In that scenario, attackers impersonated staff and sent messages containing an LNK attachment, which was configured to download and execute DarkGate malware. You can read more about it in our **Q3 2023 Quarterly Threat Report**.

Protecting your organization when using Microsoft Teams

By default, Microsoft Teams allows for external organizations to send invites. But this setting is being abused in both of the above campaigns. This setting should be set to restrict unauthorized invitations.

This will require an "Allow List" in order to allow external organizations to connect with your organization. While authorizing partner organizations is extra work, it protects your team against these types of attacks.

Looking ahead to 2025

Thoughts from Expel experts

David Merkel

Chief Executive Officer

"We've seen a steady increase in geopolitical tensions (a massive understatement, considering a land war in Europe and large-scale Middle East conflict are just the tip of the iceberg). There's no simple solution here, and, unfortunately, I think these situations will become more intense—the next geopolitical hotbed to emerge is anyone's guess. Whether these activities will increase the likelihood of cyber threat activity is a given...and not just from nation states. Activist groups advocating for either side of a conflict are also a factor, as are criminal actors looking to take advantage of the chaos. This year will be interesting, to say the absolute least."

Cat Starkey

Chief Technology Officer

"The use of common data schemas is a foundational element of scalable technology. They allow your platform to support a vast number of use cases without a lot of specialized code, making technology far less brittle and new features far easier to build. As cybersecurity technology evolves to cover more and more attack surfaces, defining a common data schema that's standard enough, and flexible enough, is a tricky exercise. You're not just working with apples and oranges—you're working with apples, oranges, apple carts, and giraffes.

"A community of folks from cybersecurity and technology companies are collaborating to standardize security data formats through the Open Cybersecurity Schema Framework (OCSF) project. As this schema matures to cover more and more data categories, we'd expect to see wider adoption across security lakes and security vendors, making it easier to integrate across technologies. This type of collaboration in the cybersecurity space demonstrates how cybersecurity is a unique market where competitors really do come together for the greater good. I expect this trend to continue as we see both the consolidation of existing cybersecurity solutions for normalization, storage, and integration, as well as the emergence of new solutions emerging focused on data analysis, governance, and applied AI."

Greg Notch

Chief Security Officer

"Protection against identity threats will remain the single most important part of most companies' security posture. Attacks will continue increasing in sophistication and speed, especially powered by artificial intelligence, which is aiding attackers to carry out tried and true methods more efficiently. This will only exacerbate onboarding and hiring fraud as a significant problem for most companies, especially those with large remote workforces. Validating and revalidating the identity of authorized users, especially for third- and fourth-party providers, will be a continued challenge. The rise of deepfakes and generated identities will also make identity adjacent security technologies critical."

Aaron Walton

Threat Intelligence Analyst

"Attacker implementation of AI and ML will have a heavy impact on small-to-medium businesses. These smaller businesses lack the resources of larger organizations and, thus, are slower to innovate, giving attackers the advantage. Attackers can easily scale and iterate on their attacks, and without equal innovation and acquisition of defenses, smaller businesses risk exposure."

Amy Rossi

Chief People Officer

"Where companies really need to prepare for change is in the rapid adoption of generative AI tools like ChatGPT, Claude, Gemini, DALL-E, and Sora. We're now in an era where most employees can benefit from GenAI to enhance how they work. They will use AI assistants for research, drafting documents, coding, business analysis, creative ideation, and more—whether their employers condone it for professional use or not. Think BYOD concerns from the early 2000s but multiplied a thousandfold by the power of generative AI.

"AI tools don't just store or transmit information—they learn from, transform, and reproduce it in ways that cascade beyond our ability to predict or control. This creates a security risk for companies, especially as most people will be 'dangerous novices,' not understanding the implications of their exploration of these tools. This is no longer a future hypothetical. Security and HR teams must work together to provide consistent education on how to safely use these tools to enhance work product and output—or risk major security consequences for their businesses."

Alex Glass

VP, Global Channel & Alliances

"As we move into 2025, partners will need to understand what risk generative AI poses within their customers and help them to define policies to best mitigate their risk. One of the major challenges they will face will be having to fight through all of the 'vendor noise' related to leveraging AI as a marketing buzz word, similar to the 'zero-trust' phrase seven to eight years ago. In reality, businesses shouldn't have to shell out more cash to security vendors just because they slapped an AI label on their solutions. AI should make security smarter and quicker, but that's a functionality upgrade, not a revolution. If a vendor claims AI is transforming their product and asks for more money to flip the switch, it's time to raise an eyebrow."

Matt Jastram

Senior Managed VM Analyst

"To meet financial goals, businesses must operationally maintain their externally-facing infrastructure. In 2025, we'll continue to see threat actor tactics evolve. Attackers will seek to advance their methods to actively leverage exploits, to ultimately create impactful outcomes on their targets. Only vigilant businesses who identify their whole attack surface, and comprehensively mitigate risk, will achieve outcomes that minimize cyber impacts."

2024 at Expel

Headlines, accolades, and research

AWARDS

- Expel clinches Gold at the 2024 Globee® Awards, named top cybersecurity vendor of the year
- Expel celebrates fourth consecutive ranking on the Deloitte Technology Fast 500™

INDUSTRY RECOGNITION

- Expel again recognized in the Gartner® Market Guide for Managed Detection and Response Services
- Expel's new partner program earns spot in 2024 CRN® Partner Program Guide
- IDC names Expel a Leader in 2024 MarketScape for worldwide emerging MDR services

RESEARCH

- From exhaustion to equilibrium: battling burnout in your SOC

NEWS

- Cybersecurity pioneer Kevin Mandia joins Expel's board of directors
- Expel announces expansion into Ireland with creation of 50 cybersecurity jobs

PRODUCT UPDATES & FEATURED LAUNCHES

- Expel unveils updated NIST CSF 2.0 getting started toolkit to help companies on their security maturity journey
- Expel unveils new, flexible offerings to allow organizations of any size and budget to benefit from leading MDR technology
- Expel MDR has new advanced identity threat detection & response

PARTNERSHIPS

- Expel and ivision partner to deliver industry-leading managed detection and response outcomes to ivision clients
- Expel and modePUSH forge strategic partnership to provide MDR and IR capabilities
- Expel double downs on cloud leadership with Wiz strategic partnership

EXPEL QUARTERLY THREAT REPORTS 2024

- Q1 QTR
- Q2 QTR
- Q3 QTR

WANT TO LEARN MORE ABOUT EXPEL?

- Subscribe to our blog
- Request a demo
- Contact us

Reference highlights

Sources consulted and our authors

Sources

- https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown
- https://gootloader.wordpress.com/2024/11/07/gootloaders-pivot-from-seo-poisoning-pdf-converters-become-the-new-infection-vector/
- https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/
- https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
- https://www.thewindowsclub.com/enable-or-disable-run-command-winr-box-in-windows-10
- https://spycloud.com/blog/lummac2-malware-stealthier-capabilities/

Report contributors

This report wouldn't be possible without Expletives dedicated to sharing this information with our community to empower practitioners creating safer cyber environments. Thank you!

Authors

Aaron Walton, Christine Billie, Matt Jastram

Technical reviewers

Joe Choi, Amar Rekic, Girish Mukhi

Editors

Andrew Rodger, Ben Baker, Brooke McClary, Scout Scholes

Designer

Mel Todas

ABOUT EXPEL

Expel is the leading managed detection and response (MDR) provider trusted by some of the world's most recognizable brands to expel their adversaries, minimize risk, and build security resilience. Expel's 24x7x365 coverage spans the widest breadth of attack surfaces, including cloud, with 100% transparency. We combine world-class security practitioners and our AI-driven platform, Expel Workbench™, to ingest billions of events monthly and still achieve a 20-minute critical alert MTTR. Expel augments existing programs to help customers maximize their security investments and focus on building trust—with their customers, partners, and employees. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn**.

01/30/25