expel



INDUSTRY SPOTLIGHT

Financial & banking services

Cybersecurity trends from
Expel's 2025 Annual Threat Report

Contents

Finance by the numbers 3

Credential compromise dominates identity risk 4

AWS cloud remains a big target 6

Shifts in malware trends apply to finance, too 7

Securing the industry: Expel & Visa 10

Our 2025 Annual Threat Report (ATR) covers all the incidents our security operations center (SOC) tracked throughout the year for our entire customer base. This summary is a zoomed-in version of that report focused on the finance industry, with specific takeaways for financial security strategies. **It includes statistics not released in our ATR exclusive to this industry segment.**

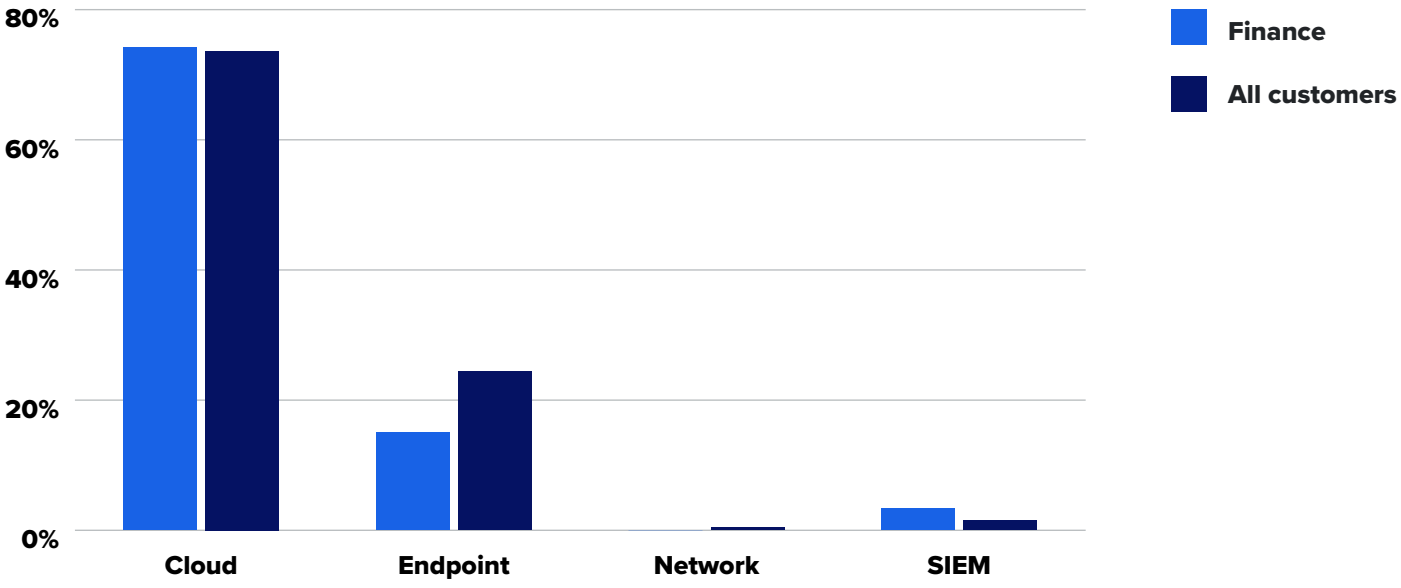
Finance by the numbers

Expel covers customers from every industry—of all shapes, sizes, and security maturity. In 2024, 12.62% of the incidents we investigated originated from our finance industry customers. While 12% may not sound like a large portion, it was the most targeted industry across our *entire* customer base.

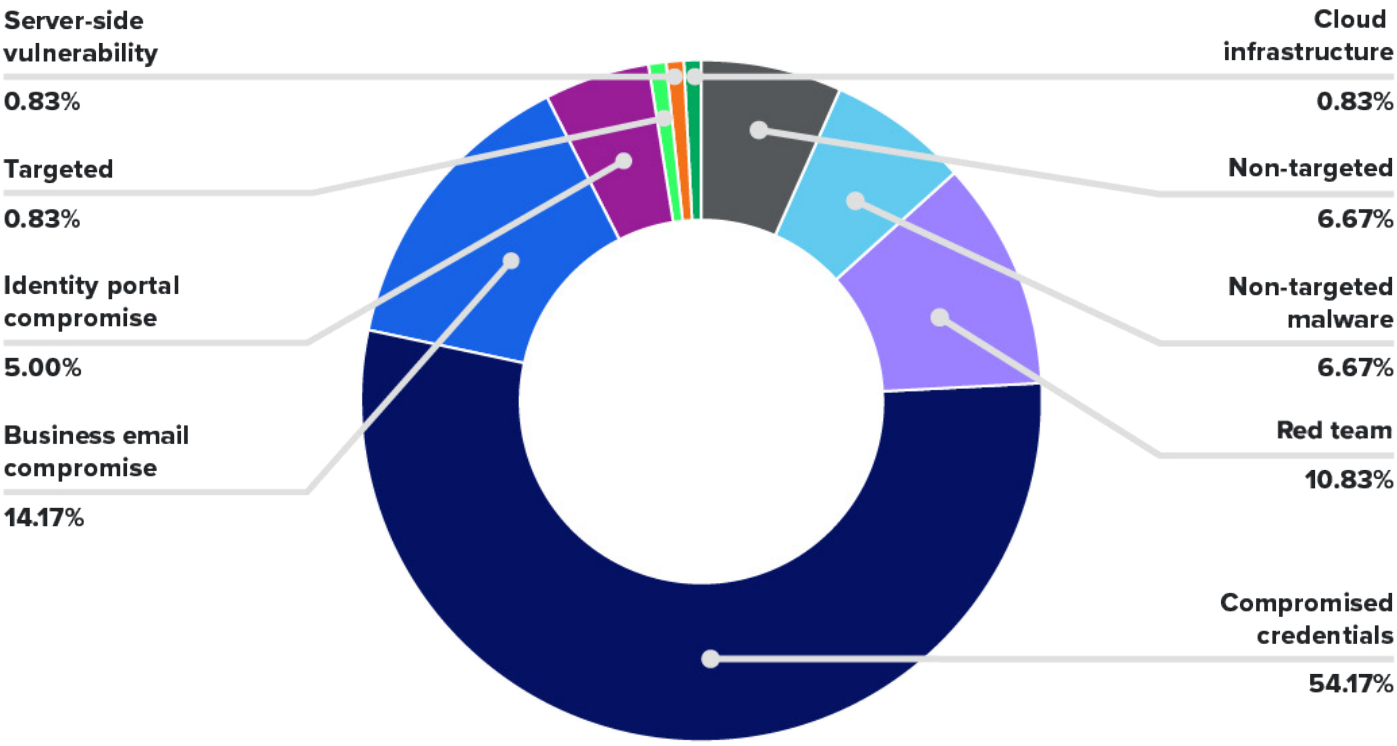
Here's an overview of incidents Expel protected its financial industry customers against in 2024:

- **54%** of all finance industry **incidents were a result of compromised credentials**
- Cloud incidents are the most common—**74% of all financial incidents were cloud-based attacks**
- **Endpoint incidents accounted for 22%** of observed issues in finance
- The finance industry recorded the **second-highest number of security incidents detected by SIEM systems** this past year

Finance customers vs. all Expel customer incidents in 2024



Incident types for financial services in 2024



Overall, the trends of the financial industry follow the larger trends in cyberattacks. However, financial industries often face a higher number of incidents overall, due to the sensitivity of their data. Attackers are financially motivated, so the incentive for targeting a financial organization doubles when that sensitive data can make it easier to steal the money they're ultimately after.

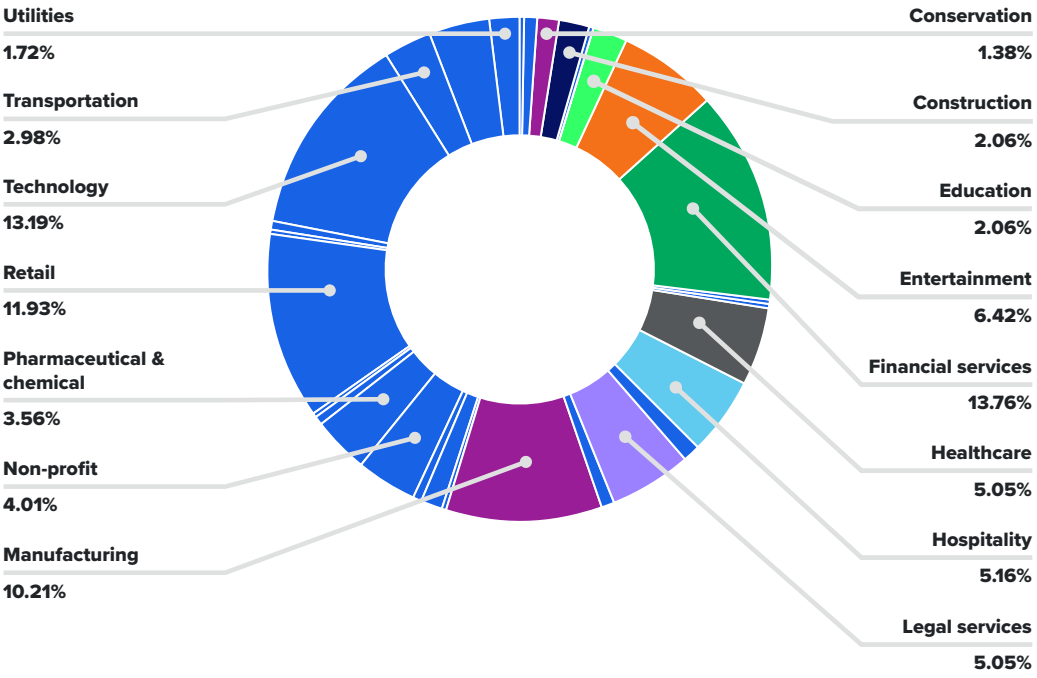
As an added pressure, financial institutions may take longer to change their policies, procedures, and technology because of regulatory concerns. However, this hasn't stopped them from investing in security in 2024. According to Jason Baker, Threat Analyst within the GuidePoint Research & Intelligence Team (GRIT) at GuidePoint Security, there has been a noticeable increase in investments in technology, tooling, and security personnel within large financial organizations, in an attempt to counter modern cybercrime.

Credential compromise dominates identity risk

The biggest identity threat in 2024 to all Expel customers, including financial services, was credential compromise.

In fact, credential compromise is a bigger threat to financial organizations than the average Expel customer. While 12% of Expel's customer base is made up of financial institutions, 17% of all compromised credential incidents came from this segment.

Compromised credential incidents by industry, 2024



The impact of credential compromise isn't always immediate, and that's part of what can make it so dangerous. It occurs when an unauthorized party attempts account access—whether they're successful or not. If they're successful, bad actors can inflict immediate damage. And even when attempts aren't initially successful, those same compromised credentials will be used until they're no longer active. If the login details aren't changed immediately after they are compromised, attackers can continue to use them to attempt to access additional platforms, or use VPNs or proxies next time to gain access successfully (if they didn't succeed on the first try). Some ransomware gangs will also sell these credentials to other cybercriminals, and the attacks can (and likely will) continue until someone succeeds or the account information is updated.

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.

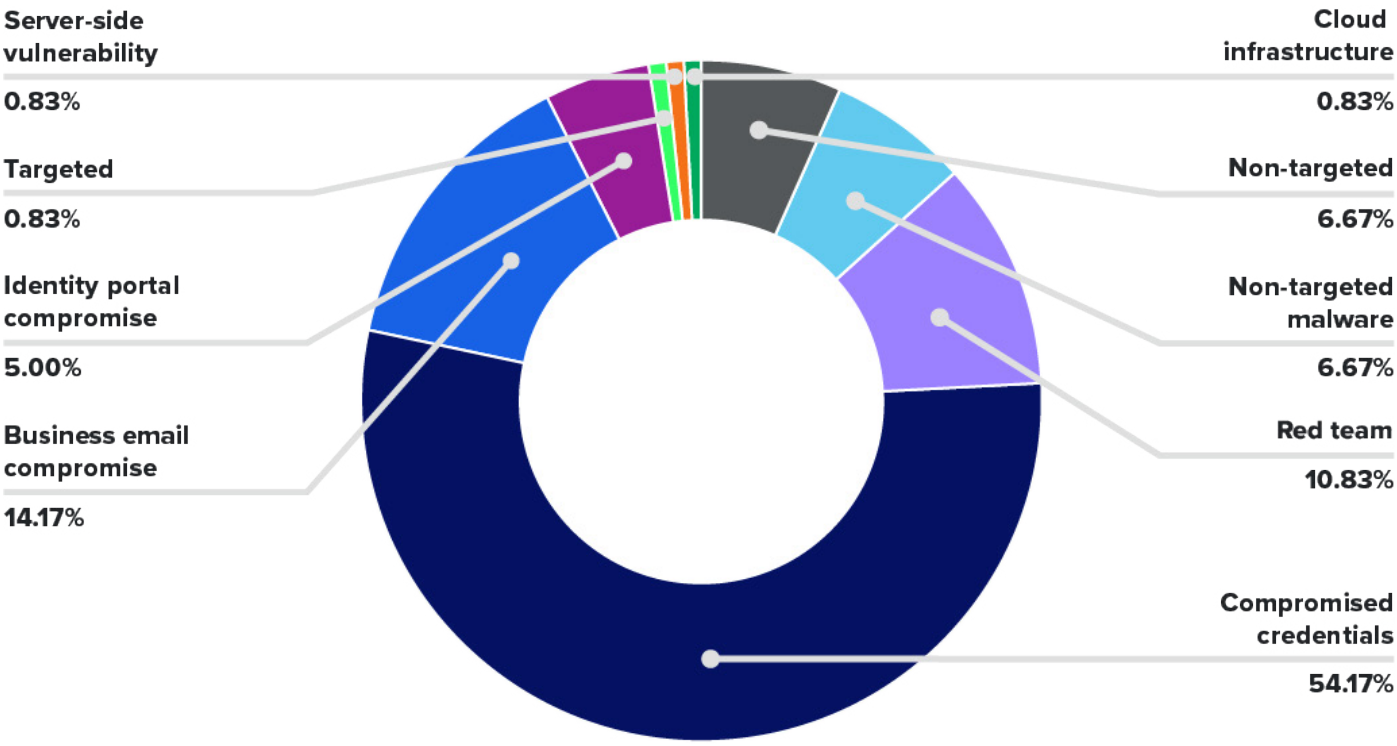
IdP compromise: This is when an unauthorized party authenticates to an identity portal, where they can then access SSO applications.

Credential compromise: This occurs when an unauthorized party illegally obtains user credentials. We are able to observe compromised credentials when an unauthorized party attempts account access and is denied. To us, this indicates that 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.

AWS cloud remains a big target

In 2024, all the cloud-based incidents Expel identified mostly targeted a specific cloud platform: AWS. 86% of cloud infrastructure incidents—regardless of industry—impacted AWS in 2024, and just under 50% of cloud infrastructure incidents were tied to credential compromise. For comparison, **almost half of the financial services organizations we secure use AWS** for their cloud. To understand the true depth of AWS targeting, let's revisit this chart:

Incident types for financial services in 2024



At a glance, you might be asking yourself why AWS cloud is really something to be concerned with, if cloud infrastructure incidents are only 0.8% of finance incidents. That's because attackers can target the cloud in multiple ways—they can go after AWS credentials, spoof login pages, and utilize any other tactic they can think of to gain AWS access, if that's their end goal. In this chart, you can point to every single incident type and identify an AWS alert.

Here's an example: 37.9% of cloud incidents targeted AWS GuardDuty specifically in 2024. Of those incidents, about 4% came from a cryptocurrency tool, 5% were red team tests, 1% were banking trojan malware, and 13.7% were from flagged unauthorized access—to four different endpoints. While all these incidents targeted AWS GuardDuty, they're all also classified as different incident types in our Annual Threat Report, meaning protecting your AWS cloud should be a *major* goal of your security strategy.

Take action

AWS is popular cloud target for cybercriminals, but there are specific actions you can take to help protect your AWS cloud, including:

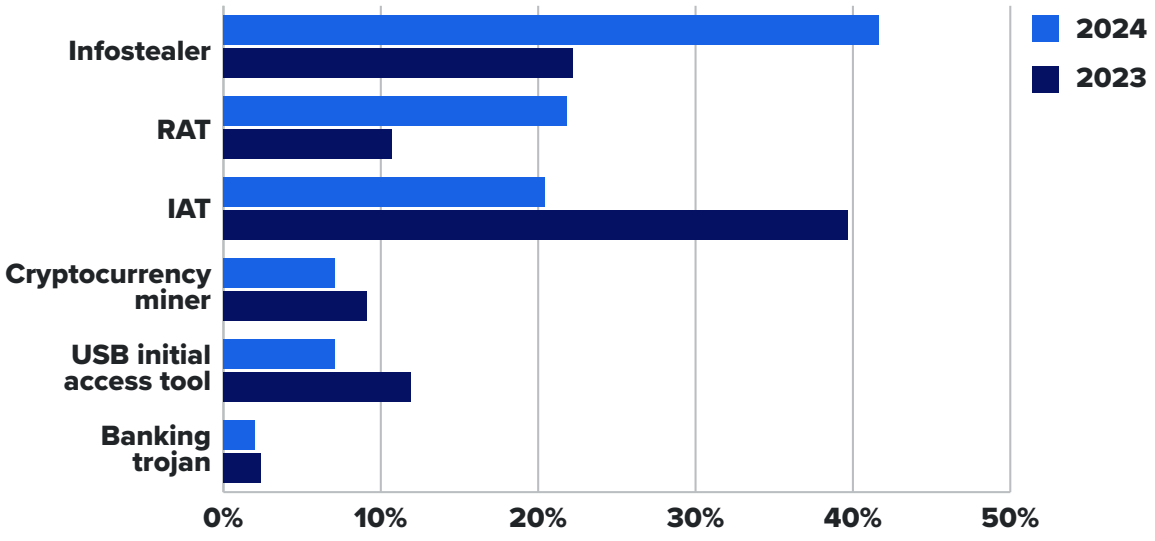
- Create detections around long-term and short-term access keys for AWS (AKIA and ASIA, respectively), to detect early stages of unauthorized access to your environment
- Confirm your org is using AWS's Instance Metadata Service version 2 (IMDSv2) to protect against server-side request forgeries (SSRF), where an attacker tricks a public-facing web app into exposing sensitive information
  - This type of attack tricks an Amazon Elastic Compute Cloud (Amazon EC2) into exposing secrets by requesting information from the instance's own metadata
  - Originally, AWS resolved the issue with IMDSv1, but v2 has since been released with more protective measures

Shifts in malware trends apply to finance, too

In 2024, we observed an overarching shift in the most common malware types bad actors were using to gain computer-based access to victims' machines. In 2023, initial access tools (IATs) were the most common malware. IATs are high-risk malware, meaning they can gain footholds fast, and cause lots of damage quickly.

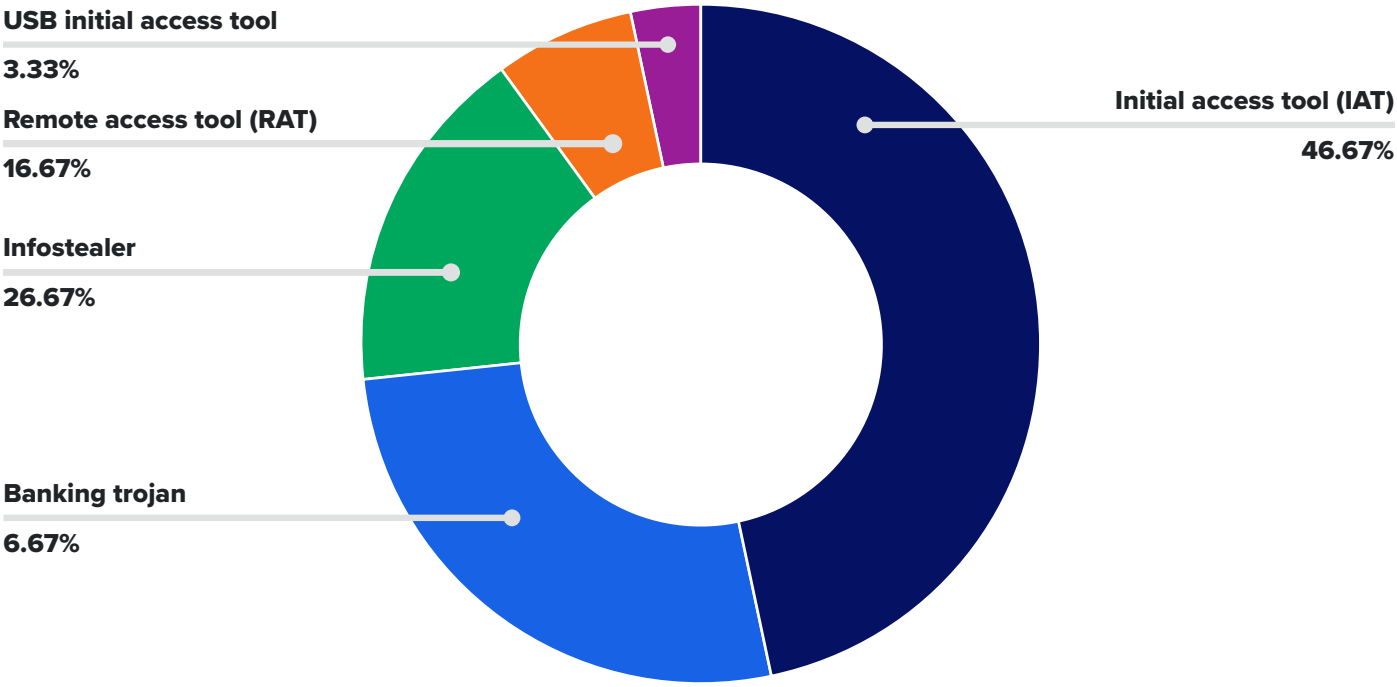
This past year, infostealer malware became more common overall than IATs. Infostealer malware is latent-risk, meaning the danger it presents isn't always immediate. The chart below showcases the shift in overall malware trends from 2023 to 2024.

Malware type prevalence in 2024 vs. 2023, across all industries



However, this decrease in IAT popularity was **not** a theme for financial industry customers. IATs remain the biggest threat to this industry segment based on our 2024 incident data.

Most common type of malware for finance customers in 2024



The biggest change to IAT malware for financial orgs to be aware of is the approach to deploying it. Part of the reason IAT malware's presence declined overall was due to major arrests in 2023. At the time, Qakbot botnet was a major IAT malware provider, and their presence decreased with this international takedown operation. Qakbot's decrease in popularity made room for SocGholish malware to take over the IAT space.

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.

Take action

SocGholish phishing tactics are designed to execute JavaScript and deploy IAT malware. These files are often difficult for endpoint detection and response (EDR) agents or browsers to block, because it's formatted as a text file, and 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.

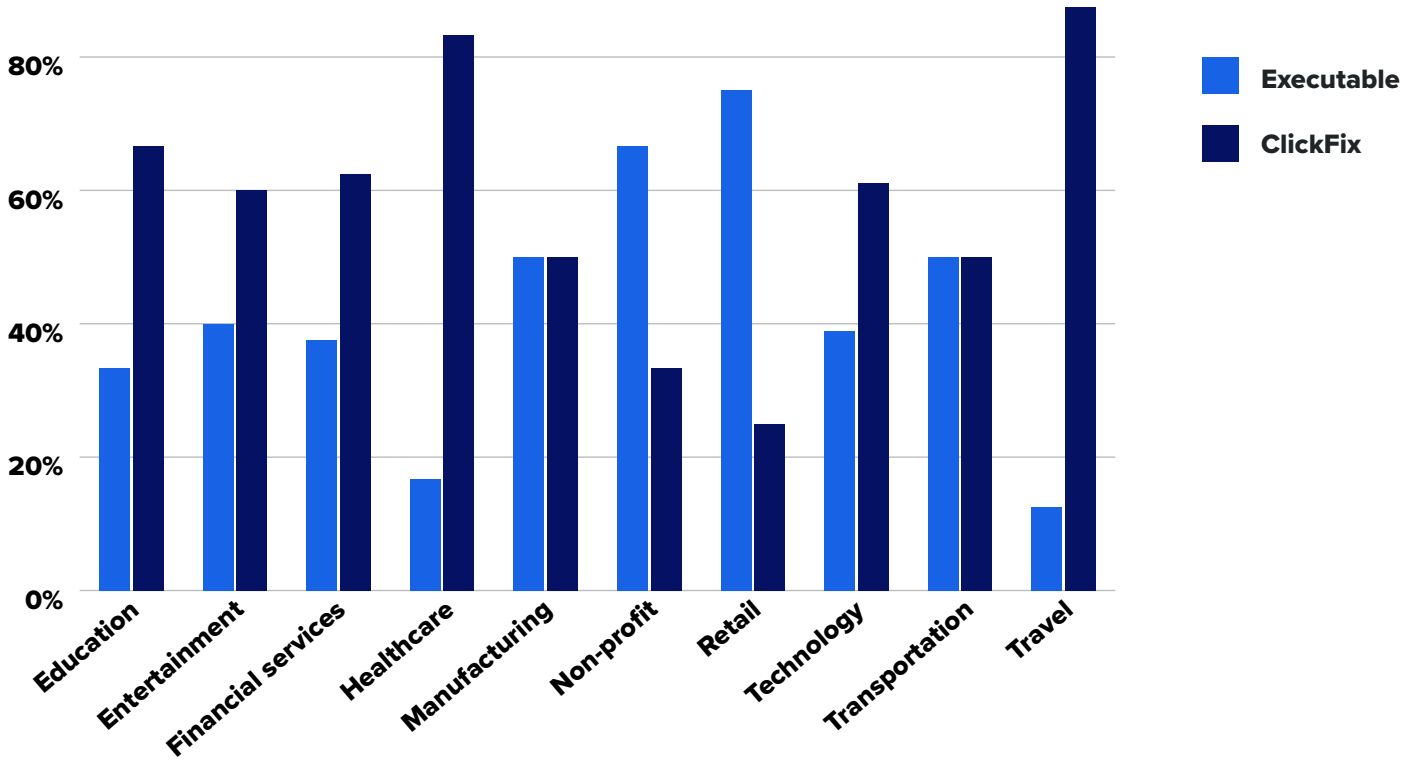
Keep an eye on infostealer malware

However, this doesn't mean infostealer malware isn't also a concerning threat to the finance industry. The seismic shift in its overall presence as a popular type of malware is large enough that anyone focused on cybersecurity should be familiar with infostealing malware—and how to protect against it.

The increase in infostealer malware is likely due to the popularity of the ClickFix tactic. In most types of IAT malware, a victim is tricked into running an executable file of malware, often disguised as a browser update. With infostealers and ClickFix, victims instead are prompted to run code instead. The benefit of this is twofold: victims have to take fewer steps (and are more likely) to successfully complete an action on behalf of an attacker, and running code bypasses most common download defenses that'd be triggered by an executable file download.

While IAT malware continues to dominate the financial services industry, infostealer malware is still a large threat, and will only continue to rise in popularity.

Prevalence of executable vs. ClickFix execution



Securing the industry: Expel & Visa

Visa chose Expel as their cybersecurity partner in managing the challenges associated with its approach to mergers and acquisitions (M&A). M&A involves complex security challenges at a company the size of Visa, including:

- 120 specialized security tools in their tech stack
- 1,300 security professionals
- A standard 18-month integration period for acquisitions

Visa needed a partner to maintain its high security standards across all operations while respecting the unique operational environments of its acquisitions without disrupting their business processes. That partner was Expel, and included benefits such as:

- Decreasing the onboarding period to 2–7 days, which was 99% less time than the previous process
- A 10–15% increase in efficiency through AI and improved tooling
- Comprehensive cloud support for major providers like AWS and Google Cloud

> **"By expanding our cybersecurity toolkit with Expel's solutions, we're enhancing Visa's security posture across the board."**
>
> —Ravi Soman, Vice President of Cybersecurity Governance Risk and Compliance

Securing financial services: the Expel advantage

- **Protect financial assets:** Prevent financial losses with 24x7 expert monitoring over sensitive transactions, customer data, and trading platforms, with rapid 16.4-minute response times.
- **Simplify regulatory compliance:** Utilize automated reporting and controls for GDPR, PCI DSS, and SOX requirements, with cost-effective data retention options to satisfy audit demands.
- **Cloud & identity protection:** Get comprehensive visibility across AWS, Azure, Google Cloud, and OCI data plane and control plane operations, plus identity platforms like Okta, protecting your infrastructure from misconfigurations and unauthorized access.
- **Identity fraud prevention:** Detect and prevent identity fraud before it affects your customers or reputation, with real-time monitoring of suspicious access patterns.
- **Boost operational efficiency:** Our expert analysts handle security monitoring so your financial teams can focus on core business operations while maintaining full audit control and transparency.

Want more on emerging threats in 2025? You can download the full Expel Annual Threat Report here.

Ready to secure your customers and capital 24x7? Contact us.

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 17-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**.

© **2025 Expel, Inc.**

03/13/25