expel®

# Quarterly Threat Report

## Q3 2023

www.expel.com

# Contents


## TL;DR 4

## Q3 by the numbers 5

Incident types . . . . . 5

Response speed . . . . . 6

## Key findings 7

Half of malware incidents presented immediate significant risk. . . . . 7

DarkGate: initial access malware for the masses. . . . . 9

Phishing with QR codes as the bait . . . . . 11

AiTM: the new attacker go-to . . . . . 12

## Quarterly spotlight 14

DarkGate through Microsoft Teams . . . . . 14

## Conclusion 15

## About Expel 16

About this report . . . . . 16

Want to learn more?. . . . . 16

# Welcome to our Expel Quarterly Threat Report

Welcome to the latest installment of the Expel Quarterly Threat Report (QTR). If you're new here, our QTRs provide data and insights on the attacks we're seeing, how to spot them, and ways you can protect your organization.

The format and content of this report distills the trends, notable new behaviors, and unusual attacks we saw over the past quarter. Where applicable, we also compare our findings to what we've seen over time to identify patterns.

The trends in our QTR are based on incidents our security operations center (SOC) identified through investigations into alerts, email submissions, or threat hunting leads in the third quarter (Q3) of 2023. We analyzed incidents across our customer base, which includes organizations of all sizes, in many industries, and with differing security maturity levels. In the process, we sought patterns and attacker tendencies to help guide strategic decision-making and operational processes for your team.

Our goal: by sharing how attackers got in, and how we stopped them, we'll translate the security events we detect and remediate into strategy for your organization.

# TL;DR

## Half of all malware incidents present immediate significant risk.

Roughly half of incidents involving malware involved pre-ransomware attempts or attacks that posed significant risk.

## QR code phishing is on the rise.

Attackers substantially increased the use of QR codes in phishing emails. Users scanning QR codes from their mobile devices unfortunately present challenges to defenders.

## Attackers increasingly use AiTM session cookie theft to successfully take over accounts.

Over the past year, we've seen adversary-in-the-middle (AiTM) session cookie theft skyrocket from being a non-factor in compromises to the primary way attackers successfully access victims' accounts.

## DarkGate malware becomes a prominent threat.

DarkGate, a malware recently available on the dark market, became a prominent threat. Multiple threat actors use this malware through various deployment methods, including compromised Microsoft Teams accounts.

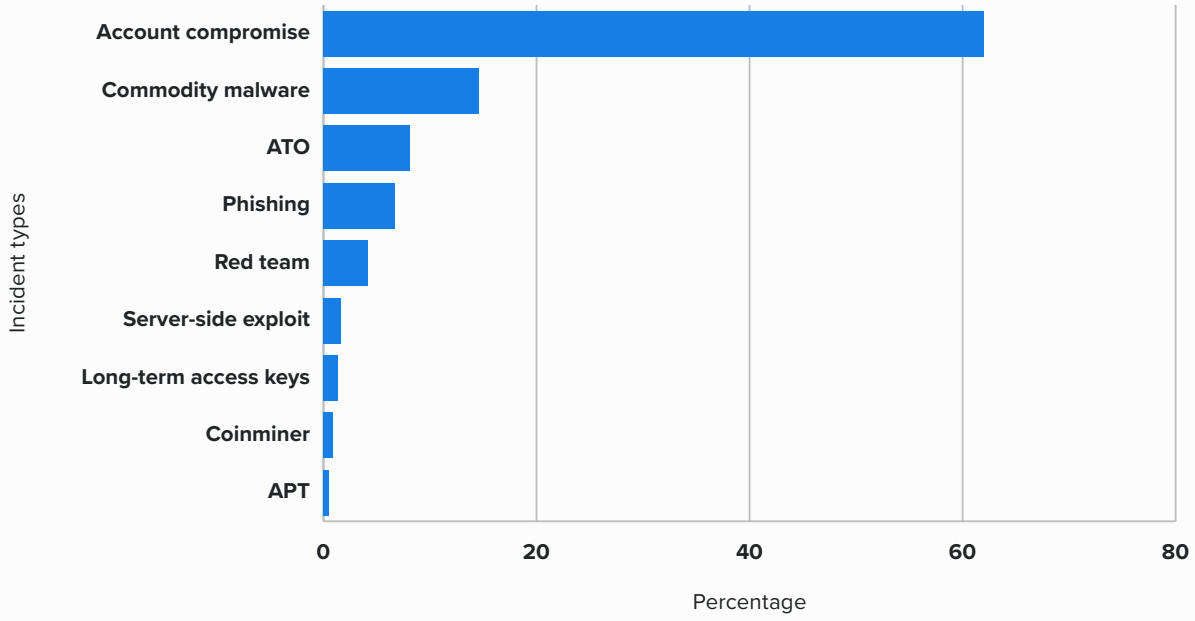
# Q3 by the numbers

## Incident types

- Identity-based attacks (account compromise, account takeover [ATO], and long-lived access key theft) accounted for 71% of all incidents identified by our SOC. This is an increase of seven percentage points for the second consecutive quarter.
  - Identity threats—which, in the context of this report, means attackers attempting to gain access to a user's identity to perpetuate fraud—are consistently the predominant threat our SOC sees. (Check out our 2023 Great eXpeltations annual threat report or our QTR from last quarter for more details.)
- Sixty-two percent of *all* incidents were Microsoft 365 (M365) account compromise or ATO. (For context, M365 accounts for 15% of all devices we monitor as of Q3.)
- The deployment of commodity malware and malware families linked to pre-ransomware operations accounted for 15% of incidents in Q3.
- Authorized penetration tests and red team/purple team exercises accounted for just over 4% of the incidents our SOC detected in Q3, down a percentage point from last quarter (and only half the 8% we saw in Q3 of 2022). While we can only speculate here, it could be that customers are running red teams half as often as last year because of macroeconomic conditions and reduced budgets for security teams.
- Long-lived access key theft in popular cloud environments like Amazon Web Services (AWS) and Google Cloud Platform (GCP) accounted for 1.5%—down slightly from last quarter's 2%.
- Activity associated with advanced persistent threats (APTs) accounted for 1% percent of incidents. APT groups are still active, but continue to comprise a small percentage of total incident volume—despite consistent coverage in the headlines.

**Sixty-two percent** of all incidents were Microsoft 365 (M365) account compromise or ATO.

**Chart 1: Incidents detected by the Expel SOC in Q3**




## Response speed

The median time-to-respond (MTTR) for all incidents our SOC handled in Q3 was 19 minutes—our fastest yet. For context, "time-to-respond" is the total time from when an alert lands in Expel Workbench™, our security operations platform, to when we assign the customer a remediation action. Our continual upgrades to Expel Workbench and our detection strategy allow us to keep improving that response speed for more immediate results for our customers.

The **median time-to-respond** (MTTR) for all incidents our SOC handled in Q3 was **19 minutes**—our fastest yet.

# Key findings

## Half of malware incidents presented immediate significant risk.

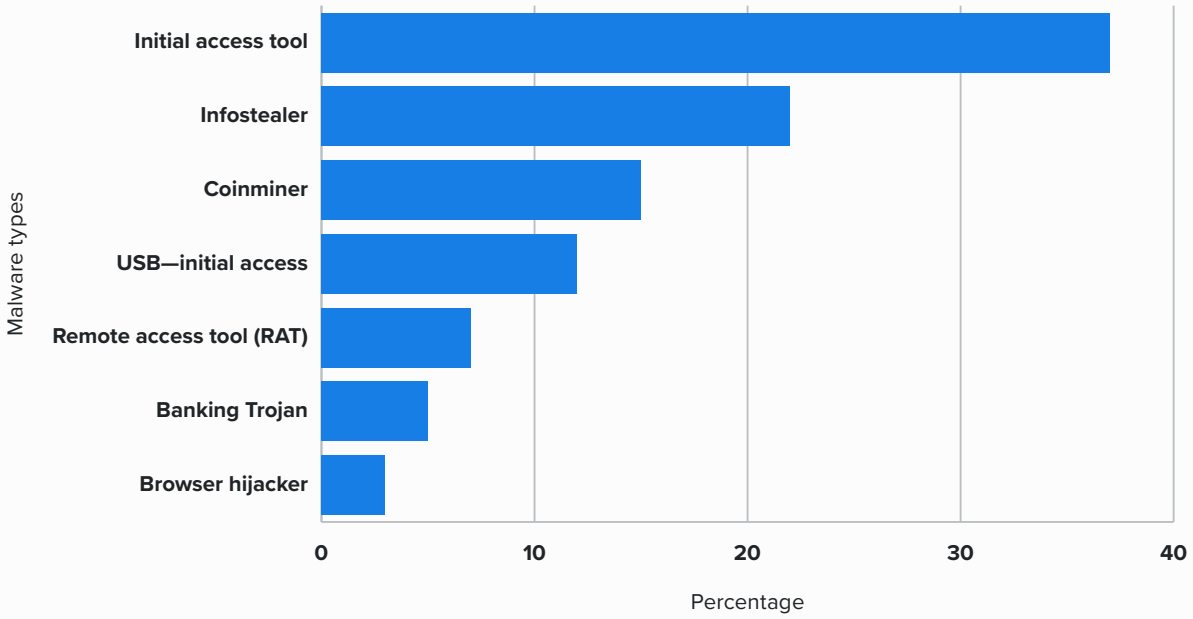
In half of the malware incidents we saw, the malware that attackers deployed presented an immediate and significant risk—including pre-ransomware or exfiltration. For reference, this number is consistent with previous quarters, *but* we're now calculating and presenting it differently. Previous reporting (think: our Q2 report) looked at malware families associated with ransomware gangs, but the lines of what is and is not pre-ransomware have always been a little blurry. We've changed the categories to better highlight and understand risk. We calculated the current numbers based on initial access malware and remote access tools (RAT) that attackers deployed. Here are some definitions:

- **Initial access malware:** also called "loaders" or "droppers," these attempt to circumvent defenses and download/load other tools or malware.
- **Remote access tools (RATs):** aptly named, RATs enable remote access. RATs can include abuse of legitimate commercial tools, custom attacker-built tools, or a mix of purpose-built tools with nasty and powerful features sold to attackers by an individual or group.

Both initial access malware and RATs provide an attacker access to an endpoint in the environment, introducing significant risk as the attacker is now loose in the system. We attribute many of these attacks to initial access brokers (IABs), who sell access to ransomware gangs or to other enterprising threat actors.

In half of the malware incidents we saw, the malware attackers deployed presented an immediate and significant risk—**including pre-ransomware or exfiltration.**

**Chart 2: Prevalence of malware types detected by the Expel SOC in Q3**




**The other half of incidents we observed fall into the following categories:**

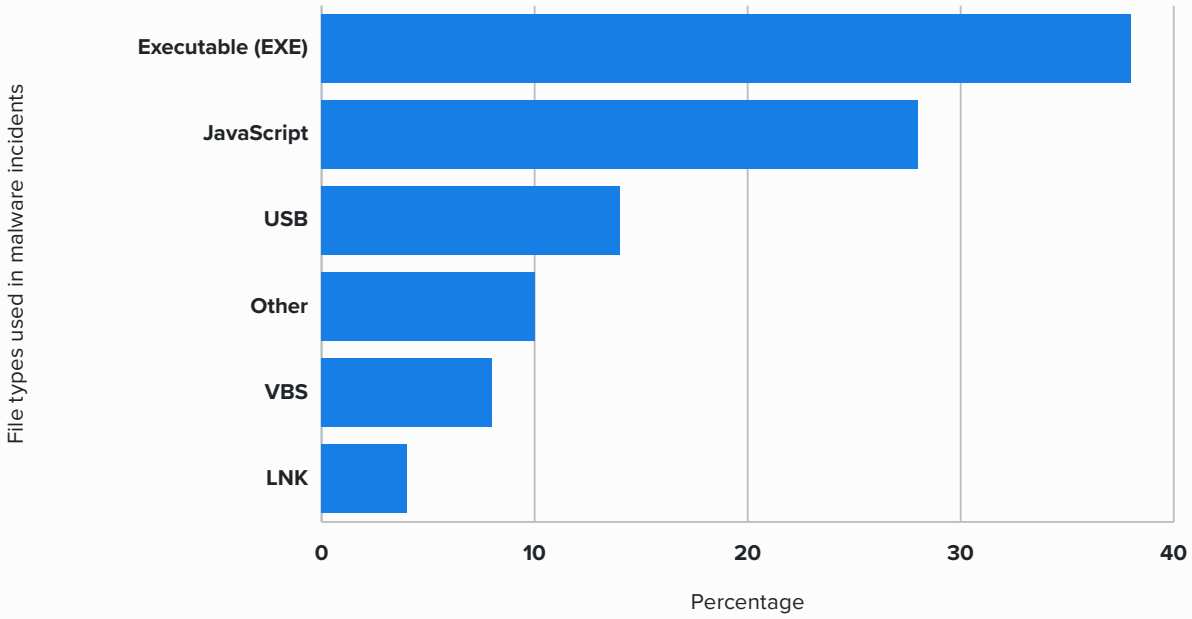
- **Infostealer** accesses sensitive data, like passwords, crypto-currency wallets, and other information stored in the user's browsers or devices.
- **Banking Trojan** steals or intercepts financial information from the user's browser.
- **Browser hijacker** redirects the user to advertisements or malicious websites.
- **Coinminer** uses the resources of a computer or server to generate cryptocurrency on behalf of the attacker.

### Popular types

We've tracked file types over several quarters and observed a wide variety of types used with the stealthier and more dangerous malware families. These families still favor scripts such as JavaScript, VBS, and LNK file types.

Part of the variety is due to a recent commodity malware, DarkGate, which allows attackers to use different file types and multiple methods to access a system. (We talk more about this below.)

**Chart 3: File types used in malware incidents detected by the Expel SOC in Q3**




**How to protect your organization:** Put playbooks in place for different malware types. While ransomware gets the most press, other threats, like Infostealers, can cause just as much damage. If an Infostealer executes successfully on a system, the credentials stored in the browser are likely compromised. While the risk isn't immediate, threat actors can (and will) sell these credentials to whoever wants them. We recommend using password managers to create and securely store strong passwords.

# DarkGate: initial access malware for the masses

This quarter, a malware known as DarkGate became very common among the incidents we saw. Using this malware, the attacker aims to gain initial access to an environment and then load additional malware.

DarkGate is commodity malware: it's sold to attackers for them to use when and where they see an opportunity. Multiple threat actors distribute the malware, including "TA577," the entity responsible for the Qakbot malware. (Note: Our SOC has ranked Qakbot as one of the most frequently observed malware files for several quarters.)

**We've observed DarkGate malware distributed via a few different means:**

- Google Ads
- LNK files downloaded from a link in an email
- LNK files via Microsoft Teams
- XLL files downloaded from a link in an email

**Let's talk about these methods:**

- **Google Ads**
  - With this approach, the attacker sets up a website that's identical to a legitimate website. Attackers often mimic websites offering productivity tools (such as note-taking apps) or administrative tools (like network scanners). The attacker then buys Google Ads which point to the fake website.
  - When a victim clicks the Google Ad, they're presented with the fake website and receive a malicious download. Often, to avoid suspicion, the malicious file downloads legitimate software that the user actually wants alongside the malware.
- **LNK via email**
  - LNK files are shortcuts that point to something else, usually an application or a game. However, an attacker can also use these files to execute programs. In the case of DarkGate, the LNK file executes the Windows Command Prompt (CMD) with commands to download and execute malware.
- **LNK via Teams**
  - In addition to email, attackers also send this malware via Microsoft Teams. An attacker gains access to an M365 account and sends ZIP archives containing an LNK file, which then attempts to download and execute malware.
- **XLL via email**
  - XLL files are made to be opened by Microsoft Excel. They contain compiled code that executes when run by Microsoft Excel. The XLL then reaches out to the internet to download and execute additional malware.

The common thread in these tactics? It's DarkGate malware that the user downloaded and executed each time. We highlighted each tactic because awareness goes a long way toward prevention.

**DarkGate is commodity malware:** it's sold to attackers for them to **use when and where they see an opportunity.**

**How to protect your organization:** Make sure your security and IT teams have visibility to these attack vectors: you cannot protect against what you cannot detect. When testing your security controls, ensure you have controls in place to detect action on endpoints (and ensure you're monitoring those detections). The security and IT teams should also have an up-to-date asset inventory with visibility into all your organization's assets.

Additionally, consider blocking ads for managed endpoints. Malicious Google Ads and Bing Ads are frequently used to deploy initial access tools and RATs. These attackers also target both Windows and MacOS. Think about ways tools (like Microsoft Teams) can be abused and test your detection and triaging capabilities. Attackers are always coming up with new ways to abuse these same tools.

## Phishing with QR codes as the bait

In Q3, our phishing team observed a significant increase in QR code abuse. Typically, when we think of a phishing email, we think of long-winded scams, or malicious attachments and links. When a phishing email contains an attachment or link, we can easily "detonate" it. However, security teams must analyze QR codes differently. What does this look like?

Essentially, a QR code is a link hidden within a picture. You're likely familiar with QR codes: you scan them like a barcode using your mobile phone's camera and it takes you to a website. In these phishing emails, attackers mention something along the lines of a security or benefits update, and then claim that the user can learn more from the link in the QR code. When users then visit the website, they're presented with a login page controlled by the attacker.

This poses an interesting challenge for security and IT teams: how do you know if a user scanned the QR code, thus successfully granting an attacker access to their account? With a URL, we can look for workstations that connected to the malicious domain, but a QR code takes the activity off of the workstation and moves it to the user's mobile device. This makes it more difficult for security teams to monitor, thus opening users and the organization up to increased risk.

**How to protect your organization:** It's important to remind users to treat QR codes with the same suspicion as they treat URLs. We recommend users never scan a code unless it's received through a trusted, verified source. Inform your employees what forms of communication you will and will not use. Should they expect QR codes from internal teams? Open-source decoding tools, such as zxing.org, also exist to help both end-users and security teams—these let you know where the QR code leads before you follow the link.

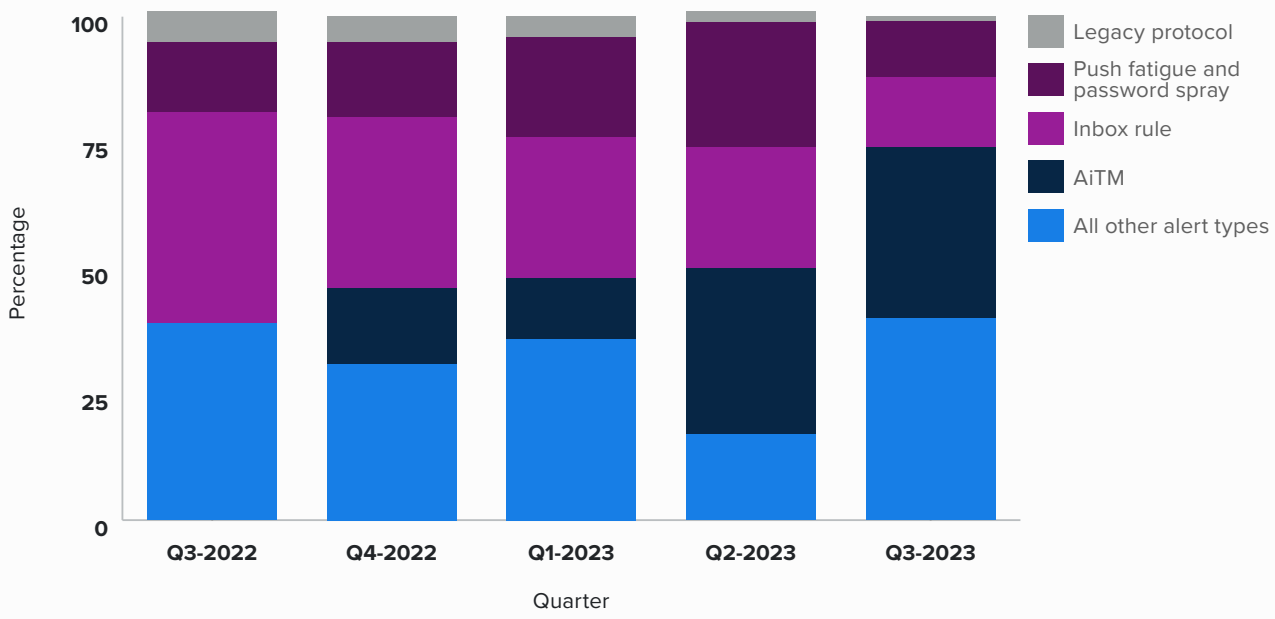
However, these attacks are best mitigated by security in depth, ensuring security controls exist in different stages. Not all users will accurately identify phish, so security or IT teams should review suspicious login activity for users. Malicious logins may go undetected, so security teams need to create and review suspicious activity associated with accounts, such as suspicious inbox rules. Security in depth provides multiple opportunities to detect suspicious activity.

# AiTM: the new attacker go-to

Over the past year, we've seen AiTM go from a rare problem to a regular staple of successful phishing attacks. Anomalous behavior, geolocation, or suspicious infrastructure accounted for roughly 90% of the account compromise alerts we actioned in the past year. These cast a broad net, and alert anytime the attacker has a legitimate password for a user but isn't able to actually get into the account and wreak havoc.

However, if we look at other source alerts, specifically those associated with incidents resulting in or indicative of account takeover, the activity we see has evolved. AiTM session cookie theft attacks rose from 0% in Q3 2022 to the single most common type of alert associated with successful account takeover today—more than 34%.

**Chart 4: The breakdown of ATO-related alerts by quarter**




AiTM session cookie theft allows attackers to circumvent multi-factor authentication (MFA), continuing a session and abusing their access.

These attacks generally begin with a phishing email. The email presents victims with an M365 login page which can be tailored to their organization dynamically. That is, attackers use automation to make the page look like the real deal using the victim company logo and branding. When victims enter their credentials and satisfy MFA, it allows both the victim and the attacker to log into the account simultaneously. (The attacker allows the user to log in to avoid raising suspicion.)

The authentications create a session cookie to keep the user and attacker logged in for a period of time. Once that session expires, the attacker theoretically loses access to the account.

That's why attackers often attempt to register a new MFA device, granting them indefinite access to the account. It's important for defenders to identify these authentications and zero in on the fraudulent device. Security teams must then revoke sessions and remove any newly added authentication devices to remediate successful attacks.

How did this attack vector evolve? Most likely, it's due to new security controls. Thanks to Microsoft's disabling of legacy authentication protocols in Q4 of 2022 and more organizations now enabling MFA, attackers have been forced to adapt. The most entrepreneurial attackers even took the opportunity to help other bad actors with software-as-a-service offerings for sale, making it easy for anyone to execute these attacks—for the right price.

That's why **attackers often attempt to register a new MFA device**, granting them indefinite access to the account.

**How to protect your organization:** As defenders, we must adapt, too. That includes using secure authentication methods (such as phish-resistant MFA), monitoring for suspicious activity, and remediating quickly once malicious activity is identified.

One very important note: session cookies can make it look like the malicious login is coming from a managed asset. This can throw off investigators and get tuned out by security teams. However, using conditional access policy and enabling the "require compliant device" setting can break the AiTM sequence and prevent compromise in the first place.

# Quarterly spotlight

## DarkGate through Microsoft Teams

Communication between teams within an organization is essential, particularly since the “new normal” of remote workplaces features now-ubiquitous communication applications, like Slack and Microsoft Teams, to facilitate interaction. But it’s also critically important to recognize that criminals want to use these same tools against you, and credential theft can help make that happen.

This quarter, we saw multiple incidents where an attacker leveraged Teams to deploy malware. In these incidents, the attackers appeared to exploit compromised M365 accounts for access to Teams. Threat actors can then use the Team’s account to target other organizations, as it allows organizations to submit chat requests to people at other companies.

In one of the incidents we saw this quarter, an attacker impersonated the CEO of the target organization. The impersonator sent a Teams chat invite to multiple team members on the pretense of discussing “upcoming changes to the organization.” The message included a link to a ZIP file hosted on Sharepoint that claimed to contain information about the upcoming changes.

However, the ZIP file didn’t contain updates. Instead, it held LNK files disguised as PDFs. When clicked, the files executed commands to retrieve and enact more malicious scripts, loading DarkGate malware on the victim’s device. The attacker then used the malware to load two remote access tools: a Netskope client and a GoToAssist client, providing remote access to the victim’s device.

By default, Microsoft Teams allows organizations to receive external chat invites. To combat this, we recommend disabling this setting and whitelisting external Teams organizations as they are needed. We also recommend reimaging hosts when malware is allowed to run. If all the actions performed by the malware aren’t seen, identified, and remediated, then there’s a significant risk to the computer and the entire environment.

# Conclusion

Everyone wants to do things faster, cheaper, and more effectively. Attackers are no different, and they're *highly* innovative on the whole. We consistently see new phishing behaviors, shorter attack lifecycles leading to faster return on investment (ROI) for bad actors, and a steady rise in the adoption of commodity malware (cybercrime-as-a-service).

Attackers even exploit common tools, like QR codes and Microsoft Teams, which were previously uncommon as attack vectors, catching users off guard.

Bad actors also continue to refine and master new behaviors after Microsoft made the cyber landscape a little more secure by default. Necessity is the mother of invention, and attackers continue to find a way—but so do we.

Necessity is the mother of invention, and **attackers continue to find a way—but so do we.**

# About Expel

Expel helps companies of all shapes and sizes minimize business risk. Our technology and people work together to make sense of security signals—with your business in mind—to detect, understand, and fix issues fast. Powered by our security operations platform, Expel offers managed detection and response (MDR), remediation, phishing, vulnerability prioritization, and threat hunting. For more information, visit our website, check out our blog, or follow us on LinkedIn and Twitter.

## About this report

The trends detailed in the report reflect incidents our security operations center (SOC) identified through investigations into alerts, email submissions, and threat hunting leads in the third quarter of 2023. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries, from July 1, 2023 to September 30, 2023. A combination of time series analysis, statistics, customer input, and analyst instinct informed our insights and surfaced patterns and trends. We share the report to help guide strategic decision-making and operational processes for your team.

### WANT TO LEARN MORE?

- Get a free trial
- Learn about the problems we solve
- Watch an overview video
- Subscribe to our blog
- Hear what our customers are saying about Expel

### MEET THE AUTHORS


**Aaron Walton**
Detection & Response Analyst

**Ben Brigida**
Director, SOC Operations