expel®

Quarterly Threat Report

Q1 2023

www.expel.com

Contents

Q1 by the numbers 4

Incident types 4

Response speed 5

Key findings 6

Quarterly spotlight 9

Conclusion 10

About Expel 11

About this report 11

Want to learn more? 11

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 the top ways you can protect your organization.

If you're a repeat reader, you may notice this report looks a little different from what you're used to. Good eye! We're cutting to the chase this time around—in both format and content. Now there's less about what happened again, and more about new things we saw in our security operations center (SOC)—and what you can do about them.

The trends in our quarterly report are based on incidents our SOC identified through investigations into alerts, email submissions, or threat hunting leads in the first quarter (Q1) of 2023. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries. In the process, we looked for patterns and trends to help guide strategic decision-making and operational processes for your team.

But, just like in previous quarters, our goal remains: by sharing how attackers got in, and how we stopped them, we'll translate the security events we detect into strategic actions for your organization.

Q1 by the numbers

Incident types

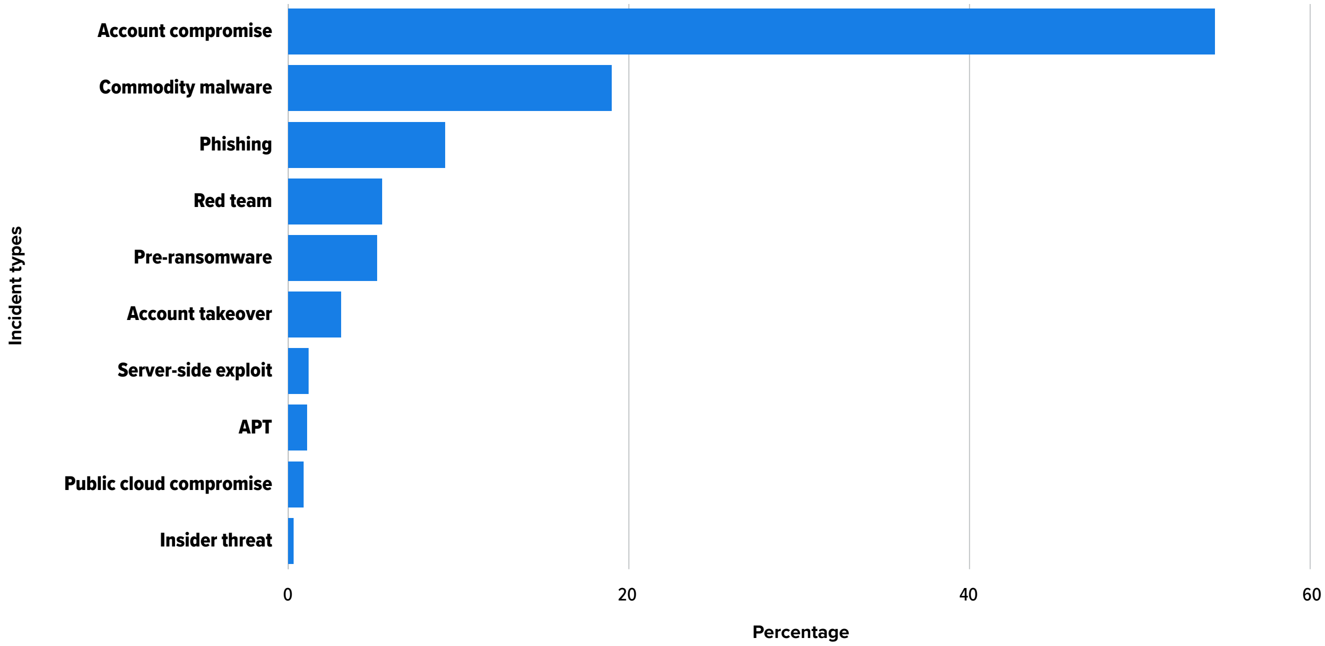
- Identity-based attacks [account compromise, account takeover (ATO), and long-lived access key theft] accounted for 57% of all incidents identified by our SOC.
    - For context, you might have heard us say this before, and it's still true: "identity is the new endpoint." Identity threats—which, in the context of this report, mean attackers attempting to gain access to a user's identity to perpetuate fraud—are the predominant threat our SOC sees time and time again. (Check out our 2023 Great eXpeltations annual threat report or our Q3 QTR from last year for proof.)

> **Identity-based attacks** (account compromise, account takeover, and long-lived access key theft) **accounted for 57% of all incidents** identified by our SOC.

- ATO in Microsoft 365 (M365) accounted for 50% of all incidents.
- Six percent of all Q1 incidents were account compromises in Okta. Less than 1% of account compromises we identified were in Google Workspace.
- Long-lived access key theft in popular cloud environments like Amazon Web Services (AWS) and Google Cloud Platform (GCP) accounted for 1%.
- The deployment of commodity malware and malware families linked to pre-ransomware operations accounted for 24% of incidents.
- Hats off to the good guys: authorized penetration tests, red team, and purple teams made up 6% of the incidents our SOC detected.
- Activity associated with advanced persistent threats (APTs) made up 1% percent of incidents. APT groups are still active, but make up a small percentage of total incident volume.

The bar graph below shows that an effective detection and response strategy is identity-oriented and endpoint detection and response (EDR) tools alone don't provide broad enough coverage.

CHART 1: Incidents detected by the Expel SOC in Q1



Response speed

The median alert-to-fix time for critical incidents our SOC handled in Q1 was 21 minutes—one minute faster than Q4 2022. That's the total time from when an alert landed in Expel Workbench™ to when we notified our customer of an incident.

> The **median alert-to-fix time** for critical incidents our SOC handled in Q1 **was 21 minutes**.

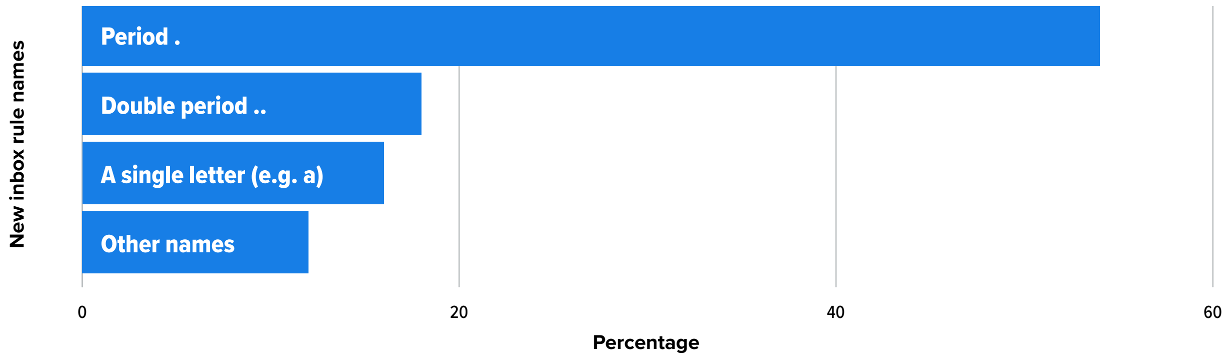
Key findings

One-hundred percent of the ATO activity we identified occurred in M365. M365 ATO can involve a variety of unauthorized actions performed by an attacker who has gained control over a compromised account.

- New inbox rules created by an attacker to automatically delete or hide certain emails from a compromised account comprised 50% of all M365 ATO activity. By deleting specific emails, an attacker can reduce the chance of the victim or email administrators spotting unusual activity.
- Of those new inbox rules created by an attacker in M365, 54% were named ".", 18% were named ".." and 16% were named with a single letter. The most common inbox rules set up by attackers? Automatically deleting specific emails or marking certain emails as "read" and then moving them to the "Archive" and "RSS Subscriptions" folders.
- Twenty-five percent of ATO activity we identified was for the registration of a new multi-factor authentication (MFA) device in Microsoft Azure. Why? Registering a new MFA device allows an attacker to maintain persistent access to a compromised M365 account.
- The creation of new inbox rules to automatically forward emails to an attacker-controlled account made up 5% of the ATO activity we identified in M365. These rules allow attackers to monitor victim email communications and intercept sensitive information at will (😳).

How to protect your organization: implement alerts for new Outlook inbox rules created with suspicious names—two to three characters in length, or repeating characters could be a clue. By the way, employees should also keep an eye on their own inbox rules. They can check their Outlook inbox for any abnormal or suspicious rules they didn't set up by clicking "File" and then "Rules & Alerts" to review the rules they've implemented.

CHART 2: New inbox rule names used by hackers



Attackers bypassed MFA in popular SaaS applications like Okta and M365 by stealing session cookies, launching MFA fatigue attacks, registering malicious OAuth applications, and authenticating using legacy protocols. We saw a particular increase when it comes to session cookie theft in M365.

- Five percent of all identity-related incidents in Q1 involved frameworks such as Evilginx2 to steal login credentials and session cookies for initial access and subsequent bypassing of MFA. This represents an important shift: threat actors are moving away from authenticating using legacy protocols to bypass MFA in M365. Instead they adopt frameworks to launch Attacker-in-the-Middle (AiTM) phishing campaigns—a new tactic effective at end-running MFA defenses.
- In almost all situations involving M365 session cookie theft, once attackers access the email account, they typically query the email inbox for the phishing email that contains a link to their proxy site. Then they move the email to the deleted items folder to hide evidence of the attack. Finally, they register a new MFA device to establish persistence before the session cookie expires.
- Time-based one-time passwords (TOTPs) and push notifications for MFA help protect against credential stuffing and password spraying, but they don't stop AiTM phishing and session cookie theft.

How to protect your organization: FIDO2 (Fast ID Online 2) and certificate-based authentication can stop AiTM attacks. However, many organizations don't use FIDO factors for MFA. In this case, deploy phish-resistant MFA. If that's unrealistic, disable email, SMS, voice, and TOTPs, and instead opt for push notifications. Then configure MFA or identity provider policies to restrict access to managed devices as an added layer of security and deploy Okta's adaptive multi-factor authentication (AMFA).

Five percent of incidents could have resulted in ransomware deployment had we not intervened—a drop of six percentage points from Q4 2022.

- Attackers favored the use of zipped JavaScript files, disk image (ISO), short-cut (LNK), and HTML application (HTA) files to gain initial entry.
- As Microsoft continues making it easier for organizations to block macros in files downloaded from the internet, ransomware threat groups and their affiliates seem to have completely abandoned their use of visual basic for application (VBA) macros and Excel 4.0 macros to gain initial entry to Windows-based environments.

How to protect your organization: configure JavaScript (.js, .jse), Windows Script Files (.wsf, .wsh), and HTML for application (.hta) files to open with Notepad. By associating these file extensions with Notepad, you mitigate a common entry point for ransomware operators.

While we saw the exploitation of a software vulnerability to gain initial access in only a small percentage of Q1 incidents, hackers tended to exploit one- to two-year-old vulnerabilities.

- The top vulnerabilities exploited in Q1 for unauthenticated remote code execution and unauthorized read and write activity were:

CVE #	Vulnerability description
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability
CVE-2022-21587	Oracle E-Business Suite Unspecified Vulnerability
CVE-2021-4034	Red Hat Polkit Out-of-Bounds Read and Write Vulnerability
CVE-2020-14882	Oracle WebLogic Server Remote Code Execution Vulnerability

- The fact that criminals are exploiting one- to two-year-old vulnerabilities shows that organizations may not understand which vulnerabilities pose the biggest threats to their environment. Often vulnerability management alone isn't enough to identify the most important vulnerabilities to patch.

How to protect your organization: assess which vulnerabilities pose the greatest risk in your environment, and prioritize the patching of these. Work to understand the severity of the vulnerability and the criticality of the assets impacted. This will help your organization more effectively eliminate the risks that pose the biggest threat to your business without chasing down an overwhelming list of known vulnerabilities. (P.S. if you need help with that, our new Expel Vulnerability Prioritization offering can help!).

Fake invoices and charges, highly urgent requests, and fear of opportunity loss were the top themes in phishing emails.

- The most common email subject used in phishing emails remains no subject line at all. Email security technology tends to pick up on patterns in unwanted emails, and either outright blocks or redirects them to spam or junk folders. A blank subject line may give one less data point for an email security tool to take automatic action, increasing the chance that these emails reach their intended recipients.
- In some cases, attackers send these emails simply to see if the destination address is a reachable inbox, and once confirmed, they send malicious content as a follow-up. In this case, messages with blank subject lines are part of a reconnaissance effort in the attack lifecycle.
- Our Phishing team also identified a high volume of banking change phishing emails in Q1 immediately following the collapse of Silicon Valley Bank. This is a stark reminder that attackers are opportunistic, move quickly, and use the threat of financial impact to drive action.

How to protect your organization: educate team members to be extra cautious when they receive an email with a blank subject line, or one that emphatically implores the recipient to act, lest they cause their organization some sort of financial harm or cause them to miss out on a big personal opportunity or windfall. Employees should mark suspicious emails as phishing attempts or spam, and if possible forward these messages to your company's security team for investigation.

Quarterly spotlight

In Q1, misuse of popular cloud storage and file synchronization services like Google Drive accounted for a small, but increased, percentage of incidents our SOC identified. In these incidents, employees with legitimate access to Google Drive uploaded gigabytes of information, including sensitive intellectual property. (FYI, we can configure our SaaS app integrations to alert on atypical account activity for situations involving unusual file uploads, data transfers, and access to sensitive files to combat situations like this.)

We won't speculate on the motivations in these incidents—which we'd qualify as insider threats—but organizations should be aware of potential risks associated with cloud storage and file synchronization services.

How to protect your organization:

- Implement detections for unusual activity.
- Regularly review and audit user access and permissions.
- Enforce strong access controls and permissions management.

Conclusion

Imagine for a moment that the citizens of Troy had received a warning like this:

The Greek invaders may attempt to infiltrate our city by building a great phish and hiding men inside it.

If you see a giant wooden phish:

- *Report it to the nearest city guard immediately.*
- *Do not, under any circumstances, open the gates and bring it inside.*

The ancient Greeks would have had a much harder time infiltrating the infrastructure of ancient Troy had the city's citizens had access to the sort of intelligence and education available to organizations like yours.

Identity attacks, ATOs, cookie theft, and the other tactics described in this QTR work wonderfully—unless the targets are informed and vigilant. In that case, the attacks don't work so well at all. And while hackers sometimes innovate something completely new, recent QTRs and our 2023 Great eXpeltations annual report indicate that they prefer the tried and true. If it ain't broke, well, you know the saying...

This is good for us defenders. We have access to lots of tools and resources, and when we share more with each other, we're "stronger together." (We couldn't help throwing in a reference to the most recent RSA Conference theme. Want to reminisce some more about that event? You can check out our round-up blog.) As always, let us know if you have comments or questions.

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 first quarter of 2023. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries, from January 1, 2023 to March 31, 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 a demo video
- Subscribe to our blog
- Hear what our customers are saying about Expel

MEET THE AUTHORS

Jon Hencinski
VP, Security Operations
@jhencinski

Team builder and people leader on a mission to help the industry "SOC" the right way. Believes a SOC can be a great place to work–but highly effective management is required!

Ben Brigida
Director, SOC Operations
@The_Real_BenB

Passionate about helping customers, employees, and coworkers. Focused on finding the bad guys and leading with empathy.