expel®

Quarterly Threat Report

Q2 2023

www.expel.com

Contents

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 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 second quarter (Q2) of 2023. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries. 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.

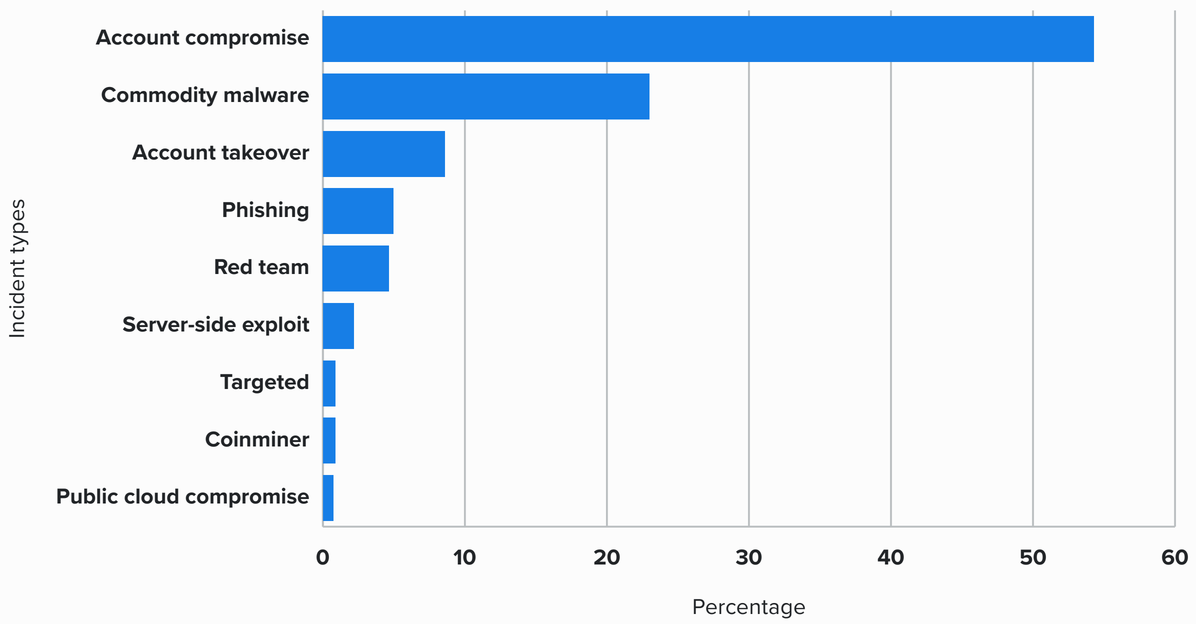
Q2 by the numbers

Incident types

- Identity-based attacks (account compromise, account takeover [ATO], and long-lived access key theft) accounted for 64% of all incidents identified by our SOC. This increased seven percentage points compared to our Q1 stats.
    - 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 details.)
- More than half (56%) of *all* incidents were account compromise or ATO in Microsoft 365 (M365). (For context, M365 accounts for 14% of all devices we monitor, but this is still a significant percentage.)
- The deployment of commodity malware and malware families linked to pre-ransomware operations accounted for 23% of incidents in Q2, in line with what we saw last quarter.
- Eight percent of the incidents our SOC identified this quarter were found via integrations with identity access management (IAM) solutions, such as Duo, Okta, and OneLogin.
- Authorized penetration tests and red team/purple team exercises accounted for slightly fewer than 5% of the incidents our SOC detected in Q2, trending down from the 6% we saw in Q1 of this year and more than 8% in Q3 and Q4 of 2022. Security leadership tends to work with red and purple teams more towards the end of the calendar year, so this downtrend during the earlier part of the year reflects that consistent behavior.
- Long-lived access key theft in popular cloud environments like Amazon Web Services (AWS) and Google Cloud Platform (GCP) accounted for 2%—up from 1% last quarter.
- Activity associated with advanced persistent threats (APTs) accounted for 1% percent of incidents. As heard about in the news, APT groups are still active, but continue to make up a small percentage of total incident volume.

Identity-based attacks (account compromise, account takeover [ATO], and long-lived access key theft) **accounted for 64% of all incidents** identified by our SOC.

CHART 1: Incidents detected by the Expel SOC in Q2



Response speed

The median alert-to-fix time for all incidents our SOC handled in Q2 was 21 minutes—matching Q1 2023. (Alert-to-fix time is 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 all incidents our SOC handled in Q2 **was 21 minutes**.

Key findings

Session cookie theft via adversary-in-the-middle (AiTM) phishing attacks tripled, accounting for 15% of all phishing attacks we identified in Q2.

- Identity-related incidents employing frameworks such as Evilginx2 to steal login credentials and session cookies for initial access and subsequent bypassing of multi-factor authentication (MFA) increased threefold—growing from 5% in Q1 to 15% in Q2.
- This represents an important and ongoing shift: now that Microsoft has disabled legacy protocols, threat actors are adopting more frameworks to launch AiTM phishing campaigns—a relatively 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. If the stolen session cookie came from a managed asset, it can appear that the adversary is logging on from that managed asset. Unfortunately, this means you should refrain from tuning out any and all logins from managed assets.
- Finally, attackers register a new MFA device to establish persistence before the session cookie expires. Heads up: this means that once attackers register their own device, they're able to fulfill the MFA requirement *without* tricking a user into doing it for them.
- 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: Build detections for newly registered MFA devices. Be suspicious of new devices registered using a proxy, virtual private network (VPN), or suspicious location. Use strong authentication methods such as Fast ID Online 2 (FIDO2) and certificate-based authentication. If FIDO is not an option, deploy phish-resistant MFA or opt for push notifications instead of performing MFA by email, SMS, voice, or TOTPs.

Malware families linked to pre-ransomware operations along with commodity malware accounted for 23% of all incidents.

Before we begin, some clarification. We report malware as an incident when it successfully lands on a managed asset. Pre-ransomware refers to malware that has been known to result in ransomware if it isn't stopped. Pre-ransomware generally includes initial access tools and remote access tools. For context, here are some definitions.

- **Initial access tools:** also called Loaders or Droppers, these tools attempt to get past defenses before they download/load other tools or malware.
- **Remote access tools (RATs):** aptly named, RATs enable remote access. RATs can include legitimate commercial tools the attacker abuses (e.g. LogMeIn), custom attacker-built tools, or a mix of purpose-built tools with nasty and powerful features sold to attackers by an individual or group.

Commodity malware can be just as dangerous as pre-ransomware malware. This broad category indicates the malware is available for purchase, making it easy for attackers to buy and leverage for attacks. Here are some of the types of commodity malware we see, and what they attempt to do:

- **Infostealer** accesses sensitive data, like passwords, cryptocurrency wallets, and other information stored in the user's browsers or on their 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.

With those definitions out of the way, here are the trends from Q2:

- Something interesting: new commodity malware targeting MacOS has hit the market and threat actors have deployed it against organizations. Somewhat new to Mac, and new to us this quarter, the Infostealer malware works by tricking users into entering passwords so it can access their Keychain, the app Apple uses to store passwords. It shows up under "Infostealer" in Chart 2.
- Elusive malware continues to use JavaScript files, LNK, and HTA files to gain entry (as seen in Chart 3).

Somewhat new to Mac, and new to us this quarter, the **Infostealer malware works by tricking users into entering passwords** so it can access their Keychain, the app Apple uses to store passwords.

Chart 2: Malware types detected by the Expel SOC in Q2

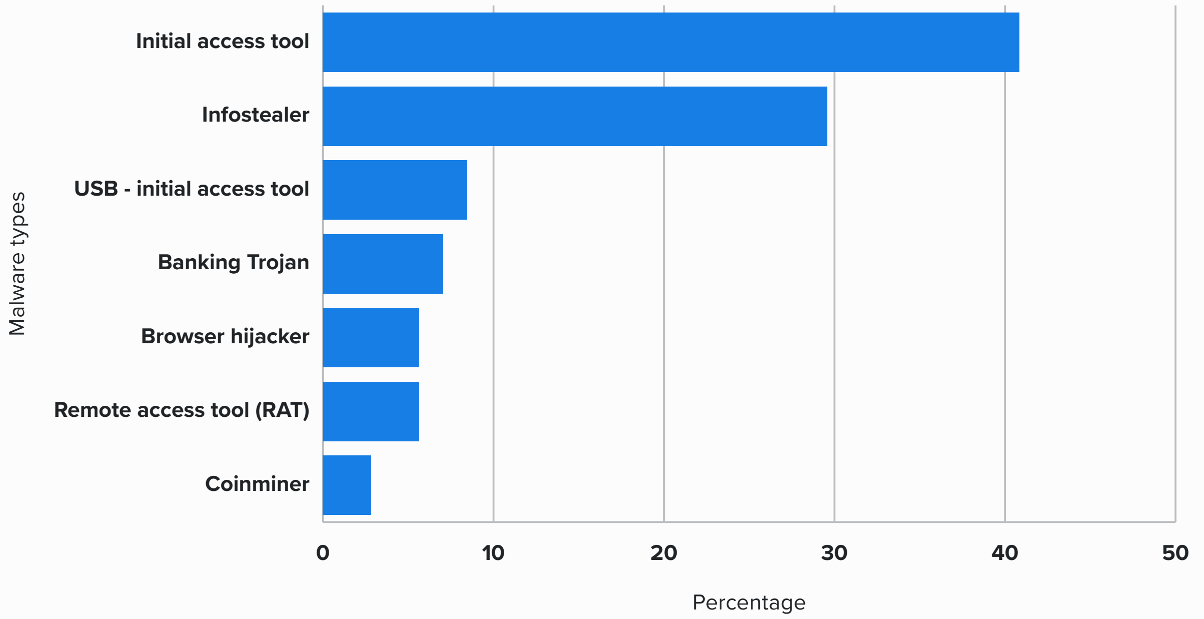
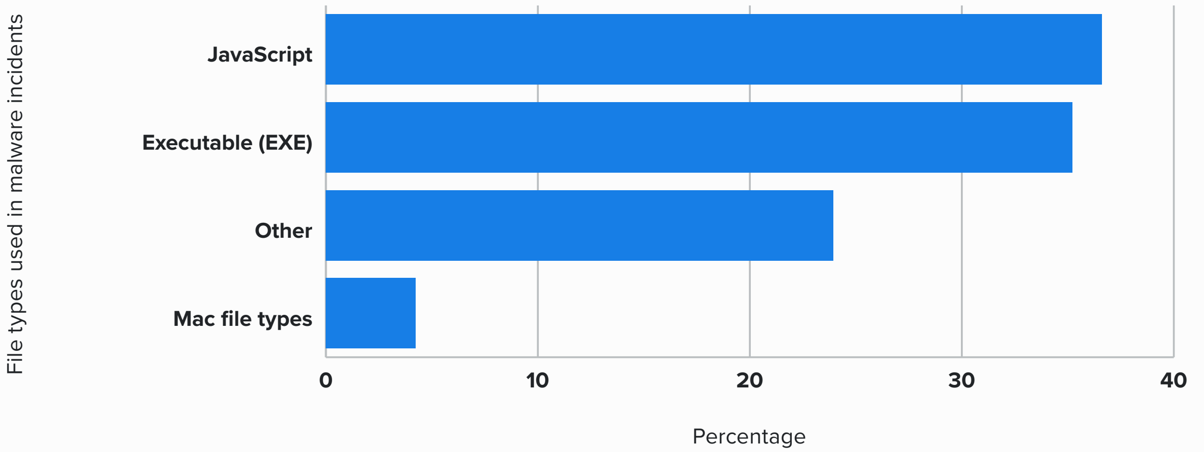


Chart 3: File types used in malware incidents detected by the Expel SOC in Q2



How to protect your organization: Collaborate with your IT teams to determine what remote access tools employees can use in your environment. If you don't have a list of tools, we strongly recommend making one. By having a firm grasp on how your employees access the network, you can improve your ability to identify when unauthorized access occurs.

At least three threat groups are using the same social engineering technique for tricking users into running malicious files.

- Our SOC saw an increase in the use of a social engineering technique closely associated with SocGholish. We're pretty familiar with it.
- Here's how SocGholish works: the threat actors gain access to a commonly used website and implement malicious code that presents users with a popup they can't close. The popup tells users to update their browsers.
- If users click the "Update" button, they'll receive a JavaScript file which executes malicious code to give the threat actor access to the host and the network.
- Defenders struggle to block these attacks because they leverage legitimate, but compromised, websites, so security teams can't just block them.
- Why are we calling this out? Because our SOC observed multiple threat actor groups using this social engineering technique to infect systems and gain remote access.
- In addition to the threat actor best known for this technique, SocGholish, the RogueRaticate and ZPHP groups are using this approach.
- While they follow similar approaches, their delivery methods differ slightly: SocGholish uses a JavaScript file to install Cobalt Strike, a penetration testing tool. RogueRaticade uses .url files and HTA files to install the NetSupport RAT. ZPHP uses a JavaScript file to install a NetSupport RAT.

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.

Attackers targeting vulnerabilities—very new and very old—resulted in the Q2 doubling of server-side exploit incidents.

- The MOVEit Transfer zero-day (see Table 1) topped the list as the most common root cause, followed closely by an exploit from a decade earlier (yup, you read that right—a *decade* earlier 🤯).
- The fact that criminals exploit very new and very old vulnerabilities (even in the same attacks) shows how difficult it can be to identify, prioritize, and fix vulnerabilities that pose the greatest threats to an environment.

Table 1: The top vulnerabilities exploited for unauthenticated remote code execution and unauthorized read and write activity

CVE #	Vulnerability description
CVE-2023-34362	MOVEit Transfer with escalated privileges and potential unauthorized access to the environment
CVE-2013-3900	WinVerifyTrust Signature Validation Vulnerability (malware attacks related to BATLOADER, and a known use in ransomware attacks)
CVE-2020-1472	ZeroLogon elevation of privilege vulnerability on domain controllers
CVE-2023-26360	Deserialization of untrusted data for arbitrary code execution

How to protect your organization: With so many patches to install and so little time, assess which vulnerabilities pose the greatest risk in your environment and prioritize patching those. Work to understand the severity of the vulnerability and the criticality of the assets impacted. This helps your organization more effectively eliminate the gaps that pose the most risk to your business without bogging down in an overwhelming list of known vulnerabilities. (P.S. We can help with that. Check out our new vulnerability prioritization offering.)

Seven percent of the email phishing submissions sent to our SOC in Q2 were malicious, while 93% proved benign.

- In previous reports (think: the Q1 QTR and Great eXpeltations year-end report), we covered attackers' tendency to leave subject lines blank, or urge individuals to act out of fear of financial harm or other reprisals. That certainly remained true in Q2. Now, let's look at the accuracy of the submitters themselves.
- Because we can see network and endpoint detection and response (EDR) logs as well as SaaS application logins, we're able to scan a customer's environment and answer the pivotal question: "did anyone get compromised?" (i.e., users who didn't submit the email and actually submitted credentials or downloaded and executed malware—an important step beyond who opened the email or clicked a link).
- We found 0.04% of all submissions (roughly 0.6% of malicious emails) resulted in actual compromise. That number is low as a percentage point, but remember it only takes one success to ruin your day. And volume matters here—that amounts to dozens of compromises in Q2 alone.
- About 93% of the emails that our customers' employees submitted to Expel Phishing for investigation turned out to be benign. This shows that people exercise an abundance of caution, and we agree that it's better to be safe than sorry. This also indicates that some organizations could benefit from more automation in their phishing triage processes to handle the large volume of reported emails.

How to protect your organization: Since we continued seeing attempts with subject lines that were blank or with emphatic calls to action, keep pushing your team members to be extra cautious when they receive these emails. Employees should mark suspicious emails as phishing attempts or spam, and if possible forward these messages to your company's security team or security operations provider for investigation.

Quarterly spotlight

MOVEit Transfer zero-day

The MOVEit Transfer zero-day exploitation took many organizations by surprise and had repercussions that reached far and wide. (For context, a “zero-day” means attackers exploit a vulnerability that the software provider hasn’t had the chance to fix, let alone distribute the fix to their customers). The Clop Ransomware gang carried out the attack and successfully stole data from a large number of victims. An SQL injection flaw made the attack possible, allowing the attackers to access files as a highly privileged account.

We’re sharing some lessons learned from defending against the MOVEit Transfer exploits below.

1. **The speed of notification matters as much as the speed of the response.** You can have the best plan, but if you aren’t aware something bad is happening, you’ve already lost. You must be aware and able to move quickly. Tune communication channels to notify you *immediately* when attackers strike. We notify our customers about big events as quickly as possible through a “threat bulletin” (essentially an urgent notice for things we hear about or see hitting our customer base). If you aren’t an Expel customer, you should identify a rapid, reliable source and plug in today. Some organizations use social media and paid threat intel feeds to get alerts on threats.

2. **Understand risks to your environment.** Knowing about vulnerabilities is important, but you also must understand the significance of them to your environment. Over the years, attackers have only exploited a small percentage of vulnerabilities.

    a. Not all vulnerabilities are created equal and attackers know what they’re looking for. It's important to understand what qualities make a vulnerability attractive, implement mitigations preemptively, and patch quickly when vendors or the security community identify vulnerabilities.

    b. Attackers find web-server exploits incredibly valuable. Knowing this, it’s well worth considering more mitigations, such as web application firewalls, to limit your exposure.

    c. Vulnerability management (VM) tools are a great start, but without some process for prioritizing vulnerabilities, VM tools can quickly overwhelm security and IT teams. Look to reduce the noise with prioritization solutions (like Expel Vulnerability Prioritization), that surface the vulnerabilities that pose the greatest risk to the org and provide it with specific guidance on how to address them quickly.

3. **Planning is important.** Practice your incident response (IR) plan. You should know your assets backward and forward, have a process to push pause with your tech via containment and account disablement (and know who needs to approve it) to buy yourself time, and configure additional detections. Also, ready your team to apply mitigations as quickly as possible.
4. **Stay vigilant.** We saw attackers attempting to exploit the MOVEit Transfer vulnerability long after the news broke. We recommend creating a detection leveraging all the available IOCs; also, consider initiating a proactive hunt.

TL;DR—Zero-day exploits and other dangerous cyber events happen; it's the nature of the business. If you take these steps, **you'll be better positioned to weather the storm** when it hits.

Conclusion

As the old adage says, forewarned is forearmed. Our main observation this quarter is that we're seeing shifts in how attackers operate, which means defenders need to shift our thinking and planning, too.

For starters, the session cookie theft/AiTM tactic (which *tripled*), represents a fresh, refined approach to phishing (a long-time scourge of SOCs everywhere). Threat actors are migrating away from older methods and toward fairly recent innovations in bypassing MFA defenses. SOCs must also evolve, and the good news is that effective defenses exist.

Second, the rise in commodity malware is problematic for a couple of reasons: 1) it's annoyingly effective, and 2) it dramatically increases the pool of potential attackers because you no longer have to be a sophisticated developer to have sophisticated tools. Beware of Infostealer, banking Trojan, Browser hijacker, Coinminer, and whatever cybercrime-as-a-service groups decide to market next—and stay alert, because they won't issue a press release.

Finally, just because a vulnerability isn't new, that doesn't mean it isn't trouble. One of Q2's biggest stories was an exploit that's a *decade* old. If you don't have strong vulnerability prioritization, you need to look into it.

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 second quarter of 2023. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries, from April 1, 2023 to June 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