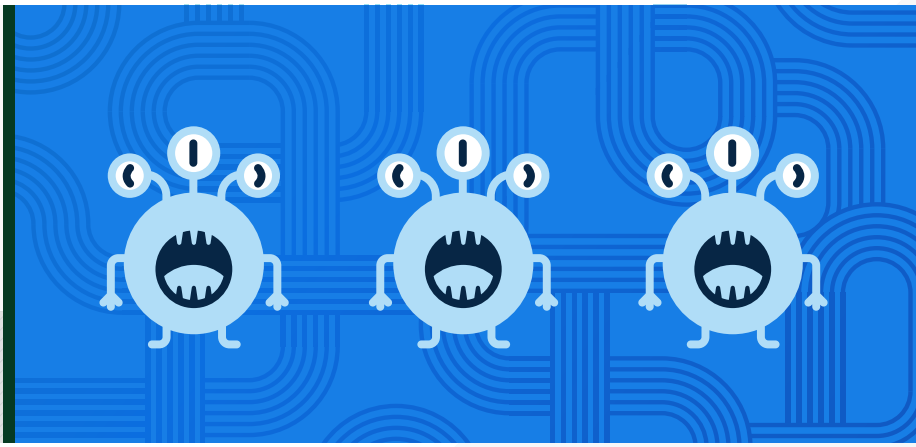
expel

Quarterly Threat Report

Q2 2022



www.expel.com

Contents

Too long, didn't read: the TL;DR from our SOC

Welcome to the second Expel Quarterly Threat Report. These reports provide data and insights on the attacks we're seeing, how to spot them, and the top ways you can protect your organization.

Theses trends are based on incidents our security operations center (SOC) identified through investigations into alerts, email submissions, and threat hunting leads in the second quarter (Q2) of 2022. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries, from April 1, 2022 to June 30, 2022. In the process, we looked for patterns and trends to help guide strategic decision-making and operational processes for your team. We used a combination of time series analysis, statistics, customer input, and analyst instinct to identify these key insights.

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

But before we get into the details (or if you're short on time), here's the bottom line up front:

"Identity is the new endpoint." Identity-based attacks (credential theft, credential abuse, long-term access key theft) accounted for 56% of all incidents identified by our SOC.

- Business email compromise (BEC) and business application compromise (BAC, access to application data) accounted for 51% of all incidents.
- Identity-based attacks in popular cloud environments like Amazon Web Services (AWS) accounted for 5%.
- Effective detection and response strategy is more than endpoint detection and response (EDR)—it's identity-oriented.

Ransomware threat groups and their affiliates have all but abandoned the use of visual basic for application (VBA) macros and Excel 4.0 macros to gain initial entry to Windows-based environments.

- In Q1, a macro-enabled Microsoft Word document (VBA macro) or Excel 4.0 macro was the initial attack vector in 55% of all pre-ransomware incidents. In Q2, that number fell to 9%, a decrease of 46 percentage points.
- This change is likely in response to Microsoft's announcement that it would block macros by default in Microsoft Office applications.
- Instead, ransomware operators opted to use disk image (ISO), short-cut (LNK), and HTML application (HTA) files to gain initial entry.

Fourteen percent of identity attacks against cloud identity providers satisfied the multi-factor authentication (MFA) requirement by continuously sending push notifications.

- Fast ID Online (FIDO) factors provide the best protection. But if FIDO-only factors for MFA are unrealistic for your organization, disable email, SMS,

Ransomware threat groups and their affiliates have all but **abandoned the use of VBA macros and Excel 4.0 macros to gain initial entry** to Windows-based environments.

voice, and time-based, one-time passwords (TOTPs). Instead, opt for push notifications.

- Limit push notifications to one per minute to reduce the likelihood of brute-forcing.
- Then configure MFA or identity provider policies to restrict access to managed devices only, as an added layer of security.

BEC in Microsoft Office 365 (O365) remained the top threat to organizations in Q2.

- Forty-five percent of all Q2 incidents were BEC attempts in O365. None of the BEC attempts we identified were in Google Workspaces.
- Nineteen percent of BEC attempts bypassed MFA in O365 using legacy protocols, a 16% increase compared to Q1.
- Organizations should disable legacy protocols like IMAP and POP3. This step is critical, especially if you've gone through the process to enable MFA. Once you turn those off, strongly consider disabling BasicAuthentication to prevent any pre-auth headaches on your O365 tenants.

The top subject lines in malicious emails that resulted in an employee click or compromise were: "Review document" and "Available?"

- Our data shows that social engineering themes that create urgency, a fear of missing out (FOMO), or potential financial loss are most likely to get a person's attention and result in action (open, click, interact).

Common misconfigurations and exposed long-term credentials resulted in cloud security incidents.

- Five percent of incidents were the result of misconfigurations and exposed long-term credentials in AWS.
- We recommend performing scans for exposed credentials using open-source tools like gitleaks.
- Also, remove unnecessary AWS identity and access management (IAM) access keys and rotate access keys often to ensure least privilege in AWS IAM security policies.

Q2 by the numbers

Incident types

Identity-based attacks (credential theft, credential abuse, long-term access key theft) accounted for 56% of all incidents handled by our SOC in Q2—down nine percentage points compared to Q1.

BEC (unauthorized access into email apps) and BAC (unauthorized access into application data) incidents made up 51% of all incidents, while identity-based attacks in popular cloud environments like AWS accounted for 5%.

The deployment of commodity malware and malware families linked to pre-ransomware operations accounted for 34% of incidents—up 8% compared to Q1.

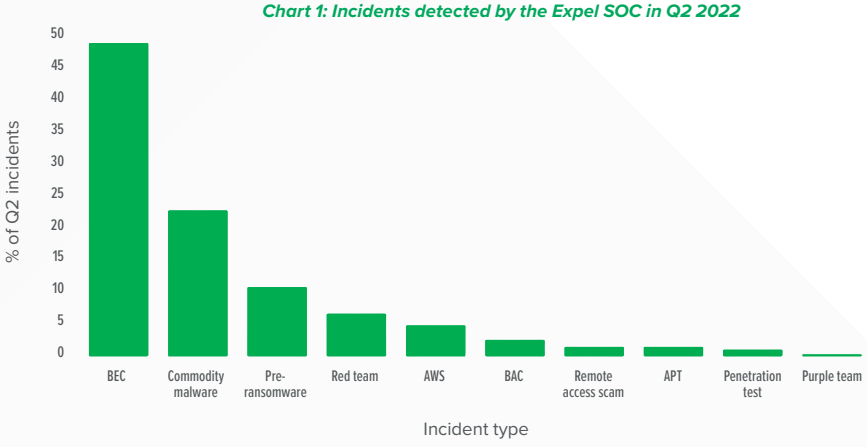
Hats off to the good guys: 7% of the incidents our SOC detected were authorized penetration tests, red teams, and purple teams. This percentage is in line with what we've seen previously.

Two percent of incidents were attributed to activity associated with advanced persistent threats (APTs). 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 EDR tools alone don't provide broad enough coverage.

The bottom line: we agree with Allie Mellen, independent senior analyst, who tweeted on July 26, 2022, "Identity is the new endpoint."

Chart 1: Incidents detected by the Expel SOC in Q2 2022



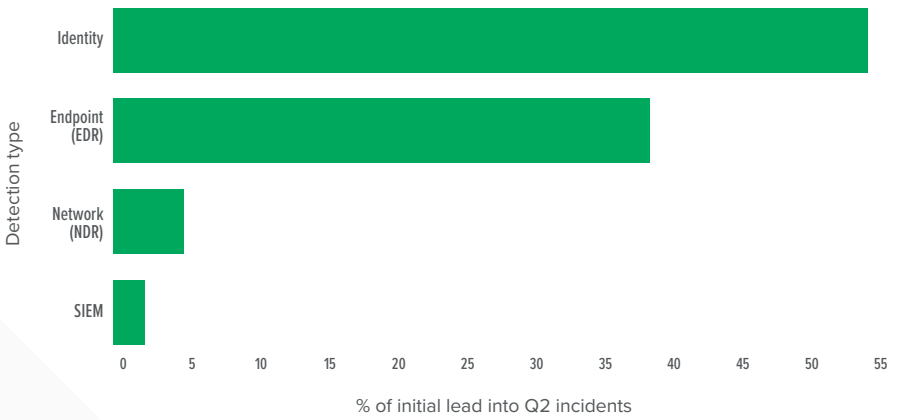
Incident leads by tech type

An effective detection and response strategy is more than EDR—it's identity-oriented. In Q2 of 2022, 54% of all incidents our SOC identified began with an initial lead from an integration with a cloud application or identity provider—38% of incidents started with an initial lead from an EDR integration. While network detection and response (NDR) and SIEM make up only 7% of initial leads into Q2

An effective detection and response strategy is more than EDR—**it's identity-oriented**.

incidents, these technologies provide SOC analysts with significant investigative capabilities and power orchestration in the Expel Workbench™.

Chart 2: Incidents detected by the Expel SOC in Q2 2022



Alert and investigative orchestration

To improve our SOC's scale and quality, we automate a lot of our analysts' repetitive tasks—things like "grab the Windows event log" or "let's take a look at 30 days of authentication activity for a given user." This frees analysts up to focus on risk-based decisions for our customers vs. spending time fighting with a query language to retrieve results.

How much does orchestrated automation contribute to freeing up analysts? Automation, not humans, completed key investigative actions 77% of the time we sent an alert to our SOC for review. Having analysts spend less time taking manual steps improves scale and levels up quality by standardizing investigative steps.

Response orchestration

Orchestration not only improves scale and quality in our SOC, but also accelerates remediation. When our SOC identifies an incident, analysts investigate to uncover the scope and create remediation actions to reduce risk. Workbench can automatically complete remediation actions for our customers, such as containing a host, disabling an account, removing phishing emails, or adding attacker indicators of compromise (IOCs)/hashes to a 'deny' list.

In Q2, the median time to complete a remediation action not automated through orchestration was two hours. What happens when a remediation action is automated via orchestration? That median time drops to seven minutes—a **1640%** improvement.

Response speed

The median alert-to-fix time for critical incidents our SOC handled in Q2 was 28 minutes—up three minutes compared to Q1. That's the total time from when an alert landed in Expel Workbench to when we notified our customer of an incident.

Automation, not humans, completed key investigative actions 77% of the time we sent an alert to our SOC for review.

Incident volume by day

Tuesday and Friday were the busiest days of the week, accounting for 46% of incident activity volume. Saturday and Sunday accounted for only 8% of all incident activity volume.

The key takeaway? Our data suggests we can continue to expect a low volume of incident activity on Saturdays and Sundays compared to typical business working days. However, organizations should consider seasonality in security operations work and lower (but not zero) work volume on weekends. This helps staff appropriately and ensure the right escalation procedures are in place (if needed).

Chart 3: Incident activity by day

Incident volume by day

Organizations should **consider seasonality in security operations work** and lower (but not zero) work volume on weekends.

How do we **use automation**?

Learn more

Business email compromise (BEC)

TL;DR

BEC accounted for 45% of all incidents; with 100% occurring in O365. Nineteen percent bypassed MFA using legacy protocols, an increase of 16 percentage points compared to Q1.

Representing 45% of all incidents, BEC attempts remain the top threat to our customers. All of the BEC attempts occurred in O365. Conversely, we didn't identify any BEC incidents in Google Workspaces.

For context, we monitor roughly twice the amount of O365 tenants as we do Google Workspaces. But the fact that we didn't identify a single BEC attempt in Google Workspaces is certainly interesting.

One of the most notable findings in our data showed that 19% of BEC attempts in O365 bypassed MFA using legacy protocols. This represents an increase of 16 percentage points compared to Q1.

How does this work?

With original deployments of O365 tenants, Microsoft by default enables IMAP and POP3 in O365 Exchange as well as BasicAuthentication.

IMAP and POP3 don't support MFA, so even if you have MFA enabled, attackers can still access these mailboxes.

BasicAuthentication allows attackers to authenticate with clients past any pre-authentication checks to the identity provider, which can lead to account compromises or account lockouts from password spray or brute force attacks.

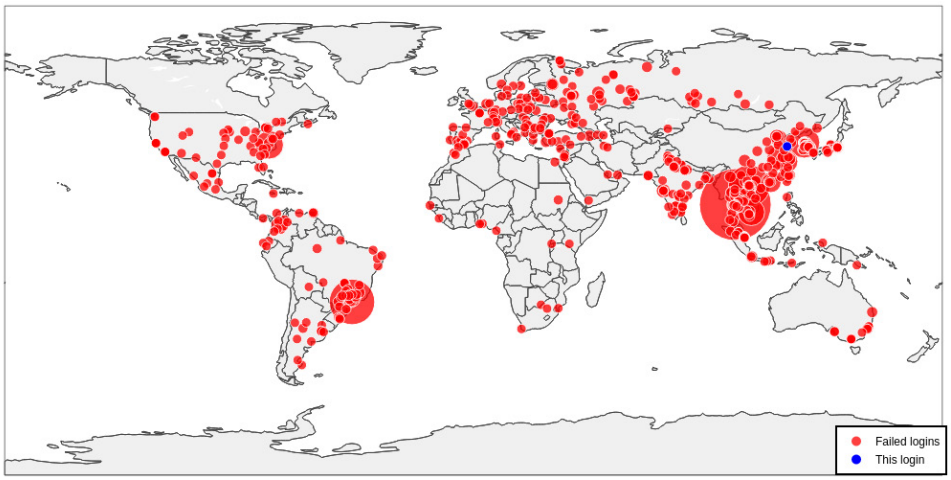
What can you do? Disable legacy protocols like IMAP and POP3 immediately. This step is critical, especially if you've gone through the process to enable MFA. Once you turn those off, strongly consider disabling BasicAuthentication to prevent any pre-auth headaches on your O365 tenants.

Our SOC didn't identify any BEC attempts in O365 that bypassed MFA by abusing OAuth applications—compared to 2% in Q1.

In this scenario, a BEC threat actor sends a phishing email asking a victim to grant permissions to an OAuth application. When the victim grants permission to the application, OAuth sends a security token associated with the victim to the BEC threat actor allowing them to access the victim's data.

The old saying goes, "a picture is worth a thousand words." The image below (on page 9) shows the location of failed login attempts for one O365 account using geo-IP data over a 30-day period. The red dots represent failed login attempts while the blue dot shows the login that triggered (another) alert. Are these attempts to break into the O365 account of a high-level executive? Nope—it's an O365 account for an employee in the hospitality industry.

One of the most notable findings in our data showed that **19% of BEC attempts in O365 bypassed MFA using legacy protocols**.



BEC failed login attempts for one account over a 30-day period

The key takeaway? Threat actors use a wide range of network infrastructure, including IP addresses associated with VPN services and hosting providers, to bypass conditional access policies. Single-factor authentication backed by conditional access policies is simply not enough to prevent unauthorized access. Our recommendation? Combine conditional access policies with MFA in O365. We strongly recommend phish-resistant FIDO security keys.

BEC attempt trends

Our SOC observed BEC attempts across multiple customer environments, targeting access to payroll management systems—specifically Workday.

The goal of these attacks? Payroll and direct deposit fraud.

Here's how it typically plays out:

- An attacker compromises an employee's O365 account via phishing and bypasses MFA using BasicAuthentication—usually occurring from VPN and hosting IPs.
- Once inside the O365 mailbox, the attacker accesses available documentation and discovers a path to reset the employee's Workday password.
- The attacker creates Outlook inbox rules within the compromised employee's email account to delete or move emails related to workday.com, myworkday.com, and/or emails that have keywords such as 'payroll' or 'assistance needed.' When the attacker makes a payroll request in Workday, this prevents the employee from seeing a Workday email notification of the change.
- The attacker modifies the employee's Workday direct deposit settings, adding the attacker's direct deposit information so that 100% of the employee's paycheck is deposited into an attacker-controlled bank account. Yikes.

What can you do? Make sure you're enforcing MFA in Workday and other payroll management systems. You can also implement approval workflows for changes to direct deposit information and implement step-up authentication for access to sensitive resources within Workday. (P.S. Have you disabled legacy protocols yet?)

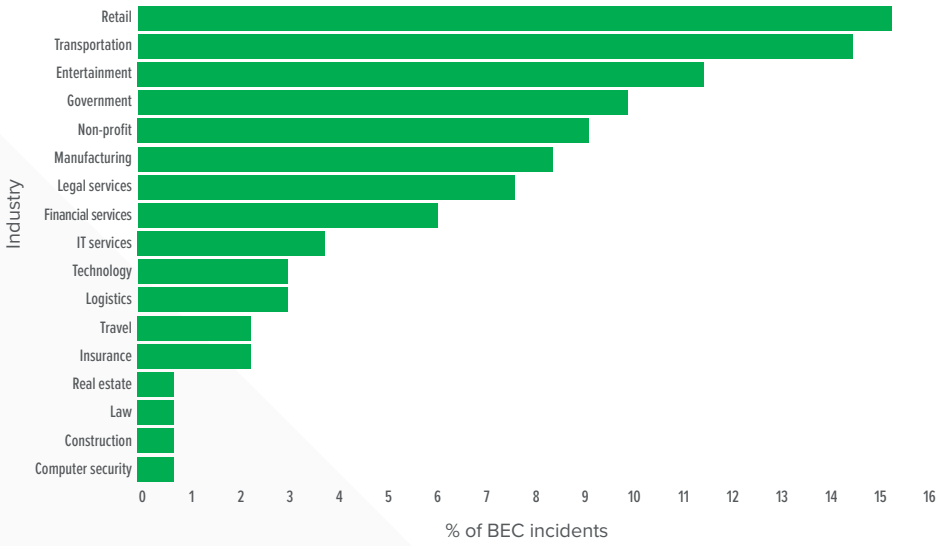
Single-factor authentication backed by conditional access policies is **simply not enough to prevent unauthorized access**.

BEC targeting by industry

Threat actors targeted retail firms the most, followed by transportation organizations.

The bar graph shows the percentage of BEC attempts our SOC identified in Q2. The data shows that BEC fraud isn't an industry-specific problem. A company's yearly revenue is by no means a predictable measure of potential BEC targeting either—BEC attempts to perpetuate fraud can happen anywhere, to anyone.

Chart 4: BEC targeting by industry



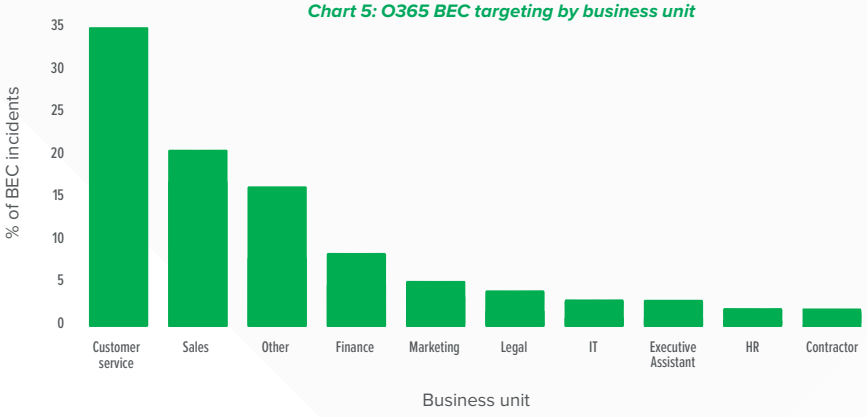
BEC targeting by business unit

Threat actors targeted employees working in customer service and sales departments the most, followed by finance, marketing, and legal teams.

The bar graph shows the percentage of BEC attempts by business units identified by our SOC in Q2. Why so much targeting of customer service and sales roles? These roles focus on building outside relationships. That means employees in these roles likely open up a lot of emails from people outside their organization.

If you invest in training so employees learn to recognize potential red flags associated with phishing emails, consider spending extra time with your customer service and sales organizations.

Chart 5: O365 BEC targeting by business unit



A company's yearly revenue is by no means a predictable measure of potential BEC targeting either—**BEC attempts to perpetuate fraud can happen anywhere, to anyone**.

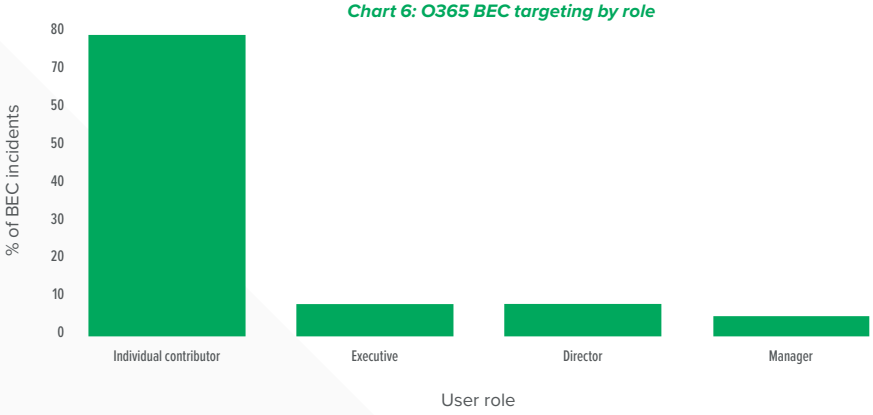
BEC targeting by role

Threat actors targeted employees working in individual contributor roles in 78% of BEC attempts—manager, director, and executive targeting accounted for 22%.

The bar graph below shows compromise by employee role. Our data shows that BEC targeting is likely a bit of a numbers game, given there are far more employees working in individual contributor roles than in management.

Even though director-level and executive-level targeting accounted for only 16% of BEC attempts in Q2, it's worth noting that employees at these levels are targeted. It's important that security controls span your entire organization.

Chart 6: O365 BEC targeting by role



BEC targeting frequency

Twenty-one percent of our customers experienced at least one BEC attempt in O365.

When we look at BEC targeting frequency (how often threat actors target an organization), 9% of our customers were targeted more than three times. For one large retail customer, our SOC identified 19 BEC attempts in their O365 tenant alone. The takeaway? BEC happens everywhere and remains a constant threat to organizations.

HOW TO PROTECT YOUR ORGANIZATION

1. Make sure you're running MFA wherever possible using phish-resistant FIDO security keys.
2. Disable legacy protocols like IMAP and POP3. These legacy protocols don't support any sort of modern authentication, which means an attacker can bypass MFA completely by using an IMAP/POP3 client. Once you turn those off, strongly consider disabling BasicAuthentication to prevent any pre-auth headaches for your O365 tenants.
3. Next, implement extra layers of conditional access for your riskier user base (such as executives or employees with access to sensitive data) and high-risk applications. You can create a conditional access policy to require MFA registration from a location marked as a trusted network, preventing an attacker from registering MFA from an untrusted network.

Want to learn more about **how Expel can stop BEC**?

Let's chat

Business application compromise (BAC)

TL;DR

Three percent of incidents were BAC attempts in Okta and OneLogin. Fourteen percent of BAC attempts in Okta satisfied the MFA requirement by continuously sending push notifications via Duo to the victim until they authorized the request.

While some attackers might want access to your email for fraud purposes, others have their eyes on a bigger prize: the data behind your applications.

More and more organizations use cloud access identity providers like Okta or OneLogin to provide a single sign-on (SSO) experience for their employees. This means an attacker can use a stolen credential to access more than just email.

Earlier in our report, we shared that our SOC observed BEC attempts in O365 as a means to access capital management systems—specifically Workday. The same is true for Okta.

Here's how a threat actor does it:

- An attacker compromises an employee's Okta account via phishing.
- To bypass MFA in Okta, the attacker performs a brute-force attack of Duo push notifications until the target employee accidentally authorizes the fraudulent request.
- If Workday is enrolled in SSO via Okta, the attacker authenticates into the compromised Okta account and accesses Workday.

How to spot it

So what can you do to detect—and hopefully prevent—these costly attacks? Here's what we recommend for security teams:

- Alert for multiple Okta sessions from the same user with multiple, non-mobile operating systems.
- Alert for potential brute force Duo push requests.
- Alert on Duo authentications where the access and authentication IP addresses represent a distance that's likely geo-infeasible (a.k.a. they're way far apart).
- Alert when Duo blocks an anomalous push notification, as this can indicate a compromise of a username and password combination.

HOW TO PROTECT YOUR ORGANIZATION

1. Deploy phish-resistant MFA. (FIDO security keys for the win!)
2. If FIDO-only factors for MFA are unrealistic, disable email, SMS, voice, and TOTPs. Instead, opt for push notifications. Then configure MFA or identity provider policies to restrict access to managed devices as an added layer of security.
3. Implement a pre-auth policy for network zones in Okta.
4. Consider blocking access to Okta from suspicious network zones based on IP address(es), autonomous system numbers (ASN), IP type, or geolocation. Why? Clients from blocked zones can't access any Okta URLs, and requests are automatically blocked before authentication.
5. Deploy Okta's adaptive multi-factor authentication (AMFA). Okta's AMFA service reduces risk by blocking authentication attempts with previously unseen authentication characteristics, such as impossible travel, unusual locations for the environment, or a new device for the account. Admins can define the actions Okta takes and the variables it considers through policies in the Okta console.

Want to learn more about **how Expel can spot identity threats**?

Let's connect

Pre-ransomware

TL;DR

Pre-ransomware accounted for 10% of all incidents—up 100% compared to Q1. Threat actors all but abandoned the use of VBA and Excel 4.0 macros for initial entry, likely in response to Microsoft's announcement that it would block macros by default in Microsoft Office applications. Instead, they opted for ISO, LNK, and HTA files.

Our SOC attributed 10% of incidents to pre-ransomware activity. If we hadn't detected and remediated this activity, the threat actor would likely have ransomed the target organization.

The data focuses on the deployment of malware we've linked to potential ransomware operations. This includes initial droppers/downloaders and backdoors enabling remote access that threat actors might sell to a ransomware affiliate.

Initial entry

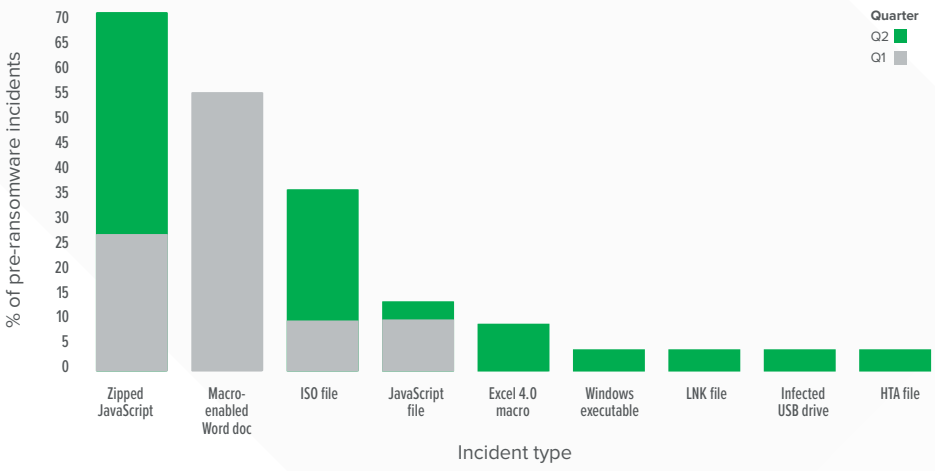
The top attack vectors used by ransomware groups to gain initial entry were:

1. Zipped JavaScript files (44% of all pre-ransomware incidents)
2. ISO files (26% of all pre-ransomware incidents)
3. Excel 4.0 macros (9% of all pre-ransomware incidents)
4. LNK files (4% of all pre-ransomware incidents)
5. JavaScript files (4% of all pre-ransomware incidents)

Our SOC didn't detect any pre-ransomware activity where a threat actor exploited a software vulnerability for initial access.

The below bar graph shows pre-ransomware attack vectors for Q1 and Q2 2022. The height of the bar represents, as a percentage, how much a particular attack vector led to pre-ransomware incidents.

Chart 7: Pre-ransomware malware attack vectors



Pre-ransomware accounted for 10% of all incidents—**up 100% compared to Q1**.

In Q1, a macro-enabled Microsoft Word document (VBA macro) or Excel 4.0 macro was the initial attack vector in 55% of all pre-ransomware incidents. In Q2, VBA macro initial attacks dropped to 0% and Excel 4.0 macro attacks fell to 9%.

Threat actors all but abandoned the use of VBA and Excel 4.0 macros for initial entry, likely in response to Microsoft's announcement that it would block macros by default in Microsoft Office applications. Instead, attackers opted to use ISO, LNK, and ZIP files that store other files for initial access. In fact, the use of ISO files for initial access increased 15% compared to Q1.

The good news is that these techniques still require user interaction. Meaning, an employee has to interact with an email and then download, extract, and 'run' malicious code for the threat actor to gain initial access.

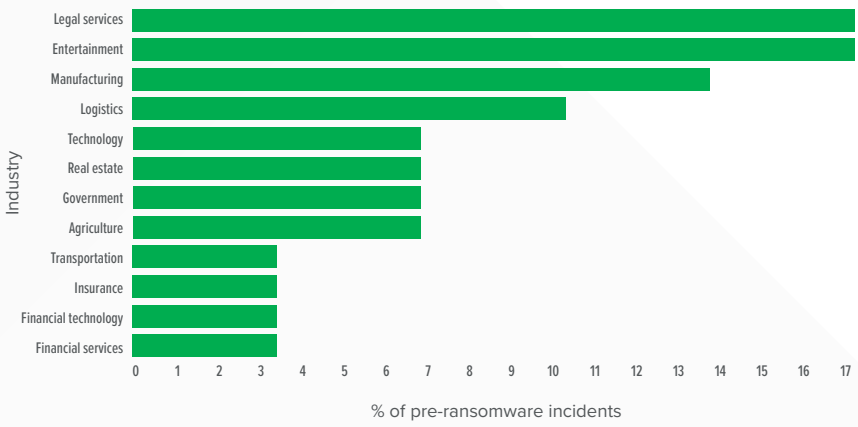
What can you do? Block ISO files at email and web gateways. But proceed with caution here, as many organizations use these files in the regular course of business. Our recommendation? Consider unregistering ISO file extensions in Microsoft Windows Explorer. By doing so, ISO files will no longer be recognized by Windows and double-clicking won't result in program execution.

Ransomware targeting by industry

Ransomware threat groups targeted the legal services and entertainment industries the most, accounting for 34% of all pre-ransomware incidents. The manufacturing and logistics services industries followed, accounting for 24% of the pre-ransomware incidents our SOC detected.

We also see that ransomware, much like BEC, isn't an industry-specific problem.

Chart 8: Ransomware industry targeting



Detection opportunities

The top process executed for initial access was the genuine Windows-based Script host process, wscript.exe. The key takeaway? Organizations should monitor native Windows OS binaries and popular office productivity applications for signs of malicious activity related to threat actors "living off the land."

The **top process executed for initial access** was the genuine Windows-based Script host process, wscript.exe.

Here are a few examples of native Windows OS binaries used for initial access:

- The Microsoft Mshta utility, mshta.exe, loads a command line from an entry stored within the Windows registry.
- The Microsoft Excel process, Excel.exe, launches the Register Server (regsvr32) to execute a file from the active Windows User profile.
- A scripting process other than PowerShell (like wscript.exe) launches a PowerShell process with encoded commands.
  - Suspicious behaviors related to scripting processes, like wscript.exe or cscript.exe.
  - Execute a .vbs, .vbscript, or .js file from a Windows user profile.
  - Initiate an external network connection.
  - Spawn a cmd.exe process.

HOW TO PROTECT YOUR ORGANIZATION

1. 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 malware.
2. Unregister ISO file extensions in Microsoft Windows Explorer. In doing so, Windows will no longer recognize ISO files and double-clicking won't result in program execution.
3. Disable Excel 4.0 macros. In October 2021, Microsoft announced that they would disable Excel 4.0 macros by default, but it's important to understand if they're still enabled for your organization.
4. IT administrators should set policies that block active content in Office docs that arrive by email. Microsoft also started providing more granular controls for macros, ActiveX content, and Office add-ins in emailed Office docs in early February 2022.
5. Don't expose remote desktop protocol (or any other service you don't need to) directly to the Internet.

Want to learn more about **how Expel stops ransomware attacks**?

Let's talk

Phishing

TL;DR

Eighteen percent of phishing emails submitted to our team for review were malicious. The top subject lines in malicious emails that resulted in an employee click or compromise were "Review document" and "Available?" Our data shows that social engineering themes that create urgency, FOMO, or potential financial loss spur the most action (open, click, interact).

Customers send our phishing team suspicious emails to determine if they're malicious or just unwanted spam. This gives us unique visibility into the various phishing attacks launched to perpetuate BEC fraud, gain initial access to a target organization, or even phish for AWS account root user credentials.

Eighteen percent of the phishing emails our analysts reviewed were malicious. These malicious emails contained links to download malware, links to credential harvesting sites, or attachments that contained malware droppers.

Top subject lines

Threat actors have some go-to subject lines for attempted phishing attempts. Of all malicious emails our phishing team reviewed, below are the most frequently used subject lines. The top subject line? No subject line. Seventy-nine percent of the malicious emails we analyzed left the subject line blank, a trend consistent with previous quarters.

Table 1: Top subject lines used in malicious emails

Top subject lines	Percentage
Blank subject	79%
Fax Delivery Report	4.3%
Order Confirmation	3.2%
Business Proposal Request	2.8%
Request	2.4%
INQUIRY	2.2%
Meeting	2%
'=Office365Alert@Microsoft.com=	1.5%
Review financial document	1.2%
Request	1.2%

Eighteen percent of phishing emails submitted to our team for review **were malicious**.

For an attacker, getting a phishing email through email security controls is only the first step. For the attack to succeed, the potential victims must then:

1. Open the phishing email.
2. Click a malicious link that downloads malware or loads a credential harvesting site.
3. Interact with malicious content and 'run' malware or submit credentials.

Though threat actors typically keep the subject lines blank, those malicious emails don't generate the most clicks. The chart below shows the top ten subject lines used in malicious emails that got an employee to open and click content or, in some cases, resulted in a security incident. The top subject lines in malicious emails that resulted in an employee click or compromise? "Review document" and "Available?"

Table 2: Top ten subject lines used in malicious emails that resulted in clicks

Subject line:	Percentage
Review document	1.1%
Available?	1.1%
Swift confirmation	1%
Please DocuSign:	1%
Urgent request	1%
Request For Quotation	1%
We found suspicious links	< 1% (0.86%)
URGENT : INVOICES	< 1% (0.83%)
Payroll review	< 1% (0.66%)
Voice Message Attached From	< 1% (0.14%)

Our data shows that social engineering themes that create urgency, FOMO, or potential financial loss spur the most action (open, click, interact).

HOW TO PROTECT YOUR ORGANIZATION

1. Make sure you're running MFA wherever possible using phish-resistant FIDO security keys to significantly reduce the risks associated with credential theft.
2. Consider deploying a secure email gateway (SEG) to monitor incoming and outgoing emails for signs of an attack.
3. Invest in training so employees learn to recognize potential red flags associated with phishing emails when they land in their inbox.
4. Educate specific business units on the phishing campaigns that might target them. For example, finance teams may come across financial-themed campaigns with popular subject lines, such as "URGENT:INVOICES," while recruiters may see résumé-themed phishing lures.
5. Use anti-spoofing controls such as DMARC, SPF, and DKIM to prevent email spoofing.

Penetration testing, red teams, and purple teams

TL;DR

Nine percent of incidents were authorized penetration tests, red team, and purple team exercises. Red and purple teams preferred Cobalt Strike for post-exploitation (post-ex) and command-and-control (c2)—a combo of RDP, WMI, and PsExec to move laterally. Red teams most often choose ScoutSuite for cloud security assessments in AWS.

Nine percent of incidents detected by our SOC were authorized penetration tests, red team, and purple team exercises, which allow organizations to test their security controls, remediation processes, and investigative capabilities.

One of the most important findings in our data was that 22% of red team engagements were performed in AWS environments. Today's modern SOC not only detects malware on a Windows laptop but also simultaneously detects unauthorized access into your cloud services. How'd we do it? Our SOC used a combination of detections written by our team using AWS CloudTrail logs and GuardDuty.

Red team and purple team engagements provide a good reality check of an organization's investigative capabilities. They help determine if, given an alert, your SOC can identify an initial entry point, or where else a red team used a compromised account. Our SOC performed an average of 13 investigative actions when chasing a red or purple team. Alerts provide leads, and investigation uncovers the scope. If you can scope, you can make it really hard for a red team to succeed.

These engagements also stress test your remediation processes. The median number of remediation actions for red teams and purple teams our SOC caught in Q2 was four. This included containment for infected hosts, password resets for compromised accounts, and blocking file execution of known payloads. Why does this matter? Effective red and purple team exercises emphasize both detection *and* remediation.

Some general themes in our data:

- Red and purple teams preferred Cobalt Strike as the post-ex and c2 framework.
- Multiple red teams used CrackMapExec for enumeration and lateral movement via Server Message Block (SMB).
- Red teams used LaZagne and Mimikatz to steal Windows credentials.
- Red teams moved laterally via remote desktop protocol, Windows Management Instrumentation (WMI), and through ImPacket's PsExec module.
- On the cloud infrastructure side, red teams preferred ScoutSuite to perform assessments in AWS.

HOW TO ENABLE YOUR ORGANIZATION

1. Red team exercises should emphasize response. Talk about remediation ahead of time. Ask hard questions like, "What would we do if that account was compromised?"
2. Review your incident response (IR) plan with the team. It's important to build muscle memory around your IR process before a red team exercise.
3. Use an MSSP or MDR? Chat with them. Understand the rules of the road for responding to red team activity. One of your red team goals likely includes assessing your MSSP/MDR. That's great, but understand what you can expect before you get started.

Want to learn more about **how Expel responds to red team exercises**?

Let's chat

Incident response (IR) monitoring

TL;DR

One-hundred percent of the IR engagements our SOC supported in Q2 were ransomware attacks. Threat actors deployed Conti ransomware in 23% of the IR engagements we supported.

We partner with IR consulting firms to provide 24x7 SOC monitoring during IR engagements. The Expel Workbench helps IR consultants get around-the-clock monitoring up and running quickly for new engagements. Technology onboarding requires a few simple steps and Workbench provides a seamless experience so our SOC has the situational awareness needed to be effective.

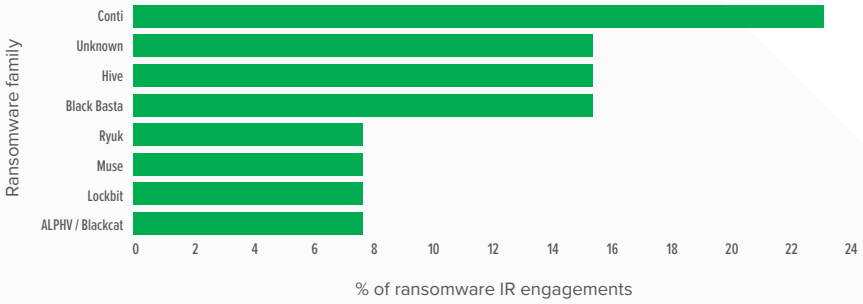
A big part of our value-add is our SOC's ability to triage alerts, investigate, and complete remediation actions on behalf of our IR partners. This creates space for them to focus on the overall investigation and not get distracted chasing down activity not related to the breach.

For a typical IR engagement our SOC supported in Q2, we:

- Triaged 20 alerts related to attacker activity
- Launched 14 investigations to better understand the detected activity
- Provided 14 remediation actions to reduce risk for the organization
- Monitored the environment for malicious activity not related to the ongoing incident

Chart 9 illustrates how often threat actors deployed a ransomware family for the IR engagements we supported in Q2. Attackers deployed Conti ransomware most often, followed by the Hive and Black Basta families.

Chart 9: Ransomware malware families deployed



Our SOC tends to spend most of its time chasing attackers in the earlier phases of the attack lifecycle (a good thing!). Partnering with IR consulting firms gives us unique visibility into what attackers are doing in later phases, providing new experiences for our analysts and leading to improved detection and strategic recommendations for our customers.

HOW TO PROTECT YOUR ORGANIZATION

1. Consider a retainer to reduce your IR time. You can operate under pre-negotiated terms and communication channels to get a response started quickly.
2. Review your IR plan with the team. It's important to build muscle memory around your IR process before an incident.

Want to **partner with Expel for your IR engagements**?

Let's connect

Looking ahead to Q3

Based on the activity we've seen in our SOC over the last several quarters, we anticipate several trends and tactics for Q3:

- Microsoft's Q1 announcement that it would block macros by default in Office applications changed attacker behavior. In Q2, hackers all but abandoned the use of VBA and Excel 4.0 macros for initial entry, opting to use ISO, LNK, and ZIP files that store other files for initial access. We expect this trend to continue. Is the era of the "dropper doc" behind us? Maybe.
- Attackers will continue to find ways to bypass legacy MFA for cloud apps and cloud identity providers. Fourteen percent of BAC attempts in Okta satisfied the MFA requirement by continuously sending push notifications via Duo to victims until they authorized the request. We'll likely see further adoption of this technique.
- Finally, we've consistently seen BEC as the top threat to organizations, and there are no indicators suggesting this will change. However, we expect more BEC attempts as a means to access payroll management systems vs. a path to perpetrate wire transfer fraud.

Finally, **we've consistently seen BEC as the top threat to organizations**, and there are no indicators suggesting this will change.

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. Expel offers managed detection and response (MDR), remediation, phishing, and threat hunting. For more information, visit our website, check out our blog, or follow us on LinkedIn and Twitter.

WANT TO LEARN MORE?

- Learn about the problems we solve
- Watch a video demo
- Subscribe to our blog
- We're hiring! Find the right role for you
- See what Expletives say about working at Expel

Authors: Jonathan Hencinski, Ben Brigida, Myles Satterfield, and Simon Wong
Contributors: Joshua Chou, DeShawn Luu, Ray Pugh, Hiranya Mir, and Brandon Dossantos