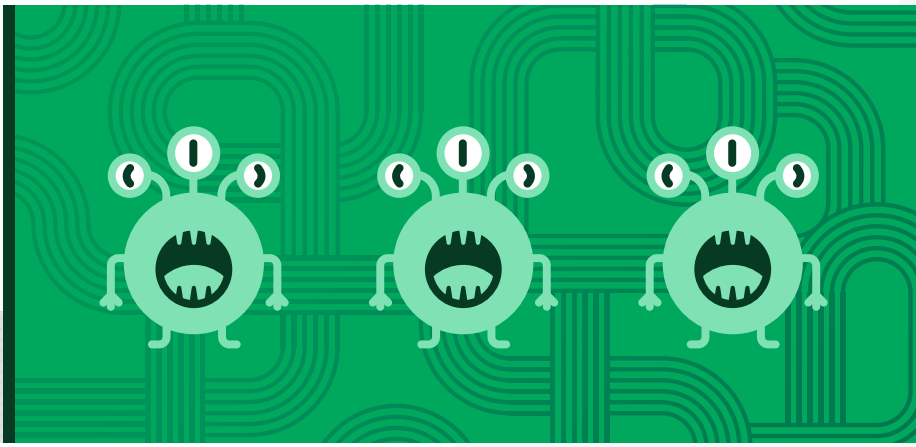
expel

Quarterly Threat Report

Q1 2022



www.expel.com

Contents

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

Welcome to the first-ever Expel Quarterly Threat Report! Since July 2021, we've brought you monthly attack vector blog reports that dug into the biggest threats we saw across the incidents we investigate for our customers. Now, we're changing things up to bring you these reports on a quarterly basis to provide even more data on what we're seeing, detection opportunities, and resilience recommendations that can protect your organization. Think: Great eXpeltations annual report, but for the quarter.

The trends in our quarterly report are based on incidents our security operations center (SOC) identified through investigations into alerts, email submissions, or hunting leads in the first quarter (Q1) of 2022. We analyzed incidents across our customer base, spanning organizations of various shapes, sizes, and industries, from January 1, 2022 to March 31, 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:

Business email compromise (BEC) in Microsoft Office 365 (O365) was the top threat.

- **57% of all Q1 incidents were BEC attempts** in Microsoft Office 365 (O365). None of the BEC incidents we identified were in Google Workspaces or involved accounts with FIDO security keys.
- **24% of our customers experienced at least one BEC attempt in O365**. Eight percent of our customers were targeted more than three times.
- **Two percent of BEC attempts in O365 bypassed multi-factor authentication (MFA)** by abusing OAuth applications. Typical remediation steps of clearing sessions, resetting the victim's password and MFA token don't work in this scenario — Security or IT teams must remove the malicious OAuth application and its permissions. Reduce risks associated with malicious OAuth applications by restricting users from registering new applications to Azure AD.
- **Our data showed a spike in BEC targeting the week of Valentine's Day**. During this period, our Expel Phishing service identified campaigns to harvest email credentials using Valentine's Day themed lures — preying on people's hearts.

Opportunistic attacks to deploy pre-ransomware or commodity malware was the second most frequent threat.

- **22% of Q1 incidents were opportunistic attempts** to deploy commodity malware or a pre-ransomware downloader.
- **None of these incidents exploited a software vulnerability for initial access.** All of the incidents used a self-installation attack technique like zipped JavaScript files, zipped executables, and malicious macros in Microsoft Office docs and Excel spreadsheets.

Business application compromise (BAC) in Okta accounted for 6% of incidents.

- **Seven percent of those BAC attempts in Okta satisfied the MFA requirement** by continuously sending Duo push notifications to the victim until they accepted.

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

- **Three percent of incidents were the result of misconfigurations and exposed long-term credentials** in Amazon Web Services (AWS) and Google Cloud Platform (GCP).

Spoiler: Google Chromebooks, phish-resistant FIDO keys, and Google's Advanced Protection Program can get you *really* far with corporate security.

- **None of the incidents we identified were from malware deployed to Chrome OS**. And none of the BEC incidents we identified involved accounts with FIDO security keys.

Q1 by the numbers

Incident types

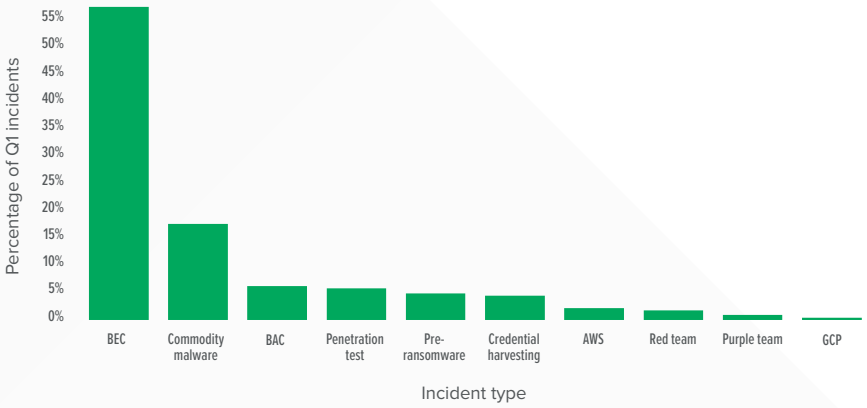
Identity-based attacks accounted for 65% of all incidents handled by our SOC in Q1. BEC (unauthorized access into email apps) and BAC (unauthorized access into application data) accounted for 63% of all incidents, while identity-based attacks in popular cloud environments like AWS and GCP accounted for 2%.

The deployment of commodity malware and malware families linked to pre-ransomware operations accounted for 26% of incidents — meaning organizations of all shapes and sizes should create and test strategies to defend against ransomware attacks.

A nod to the good guys: Nine percent of the incidents our SOC detected were authorized penetration tests, red team, and purple teams. (This is your sign to pentest your controls, red team your response!)

The bar graph below shows that most of the attacks never executed code on a managed asset. When we look at the data, we see an attack surface that touches traditional enterprise technology, cloud infrastructure, and cloud applications. What does this tell us? In most organizations, endpoint detection and response (EDR) tools alone don't provide broad enough coverage.

Incidents detected by the Expel SOC in Q1 2022



Response speed

Security and IT teams often ask us, "how long does it typically take your SOC to respond?" It's a good question. Almost everything we do in security operations is latency sensitive. The longer an alert waits for an analyst to pick it up, the more time an attacker has to cause trouble.

We found the median alert-to-recommendation time for critical incidents in Q1 was 25 minutes. That's the total time from when an alert landed in Expel Workbench to when we notified our customers for all critical incidents.

Identity-based attacks accounted for 65% of all incidents handled by our SOC in Q1.

Business email compromise (BEC)

TL;DR

BEC accounted for 57% of all incidents our SOC observed; with 100% occurring in O365. Two percent of BEC attempts bypassed MFA by abusing OAuth apps, while 3% bypassed MFA using legacy protocols.

Representing 57% of all incidents, BEC attempts were 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 than 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 2% of the BEC attempts in O365 bypassed MFA by abusing OAuth applications. In this scenario, a BEC threat actor used phishing to have a victim grant permissions to an OAuth application. When the victim granted permission to the application, a security token associated with the victim was sent to the BEC threat actor (the application developer) which allowed them to access the victim's data.

Typical remediation steps of clearing sessions, resetting the victim's password and MFA token won't work in this scenario. Security or IT teams must remove the OAuth application and revoke its permissions. Restricting users from registering new applications to Azure AD can reduce risks associated with malicious OAuth applications. Three percent of BEC attempts in O365 bypassed MFA by authenticating into an account using a legacy protocol. These legacy protocols don't support any sort of Modern Authentication (Modern Auth), which means an attacker can bypass MFA completely by using an IMAP/POP3 client.

What can you do? 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 Basic Authentication to prevent any pre-auth headaches on your O365 tenants.

Two percent of the BEC attempts in O365 bypassed MFA by abusing OAuth applications.

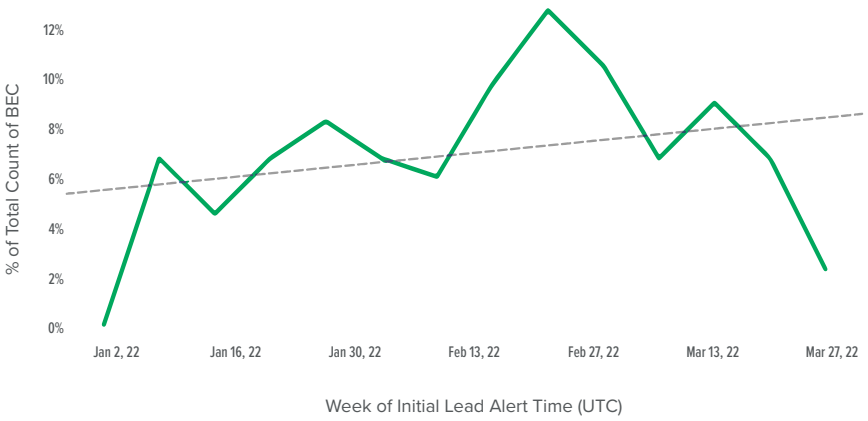
BEC attempt trends

Most people equate BEC with wire transfer fraud. BEC, however, is much more — it includes payroll, romance, real estate, and lottery scams. So when we think about Valentine's Day, the romance scammers were here for it. Our data shows that our SOC identified an uptick in BEC attempts in O365 in the days immediately before and after February 14, 2022.

Below is a time series of the percentage by week of BEC attempts in O365 identified by our SOC between January 1, 2022 and March 31, 2022.

The overall trend-line, here plotted in gray, shows a gradual increase in the number of BEC attempts. We also see a spike of BEC attempts between February 6, 2022 and February 20, 2022. During this period, our Expel Phishing service identified campaigns to harvest email credentials using Valentine's Day themed attempts — exploiting victims' hearts.

Time series of BEC attempts our SOC identified spanning January 1, 2022 and March 31, 2022



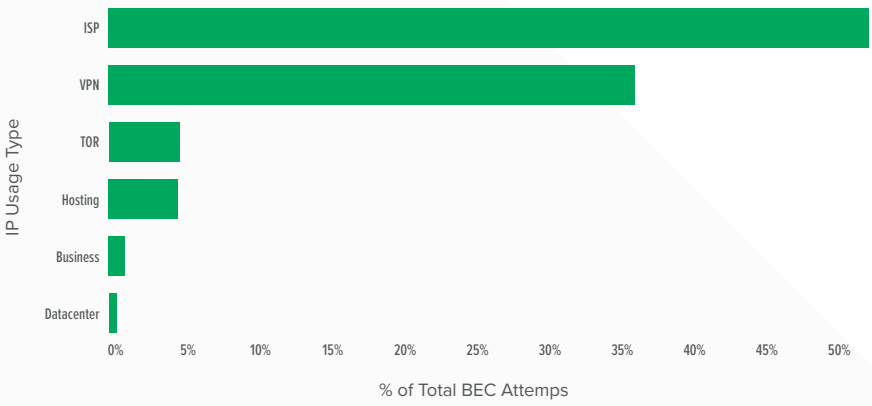
BEC tactics

Network infrastructure

In Q1 of 2022, 45% of attempts to authenticate into a compromised O365 account originated from an IP address associated with VPN services and hosting providers. Fifty-five percent of attempts originated from IP addresses associated with an Internet service provider (ISP).

Our data shows that conditional access policies to reduce the risk of unauthorized access aren't enough. Our recommendation? Combine conditional access policies with MFA in O365. We strongly recommend phish-resistant FIDO security keys.

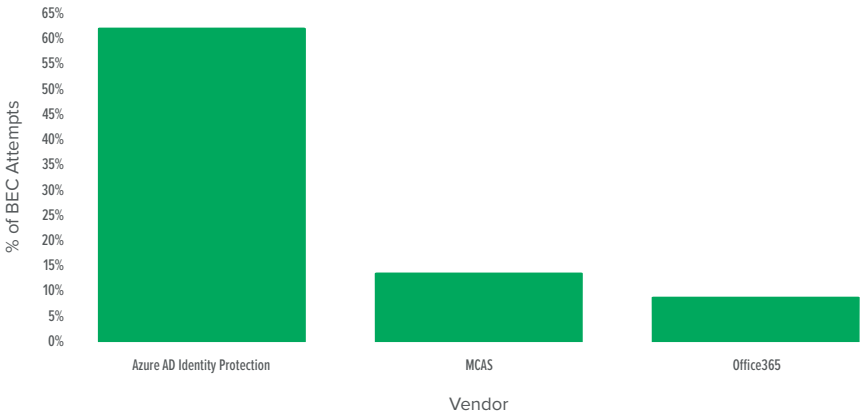
IP usage type for the source IP address recorded during authentication using stolen credentials



Detecting BEC in O365

Our SOC identified 97% of the BEC attempts when a BEC threat actor attempted to authenticate into an O365 account using stolen credentials. Only 3% of BEC attempts in O365 were identified after account takeover. Meaning, we spotted when a BEC threat actor attempted to authenticate into an O365 account using a stolen credential, versus alerting on activity consistent with account takeover — like setting up evil inbox rules to conceal phishing activity originating from a compromised account.

BEC attempt lead alert percentages by technology



Our integrations with Microsoft Azure AD Identity Protection, O365, and Microsoft Cloud App Security (MCAS) provided the initial lead into 85% of BEC attempts.

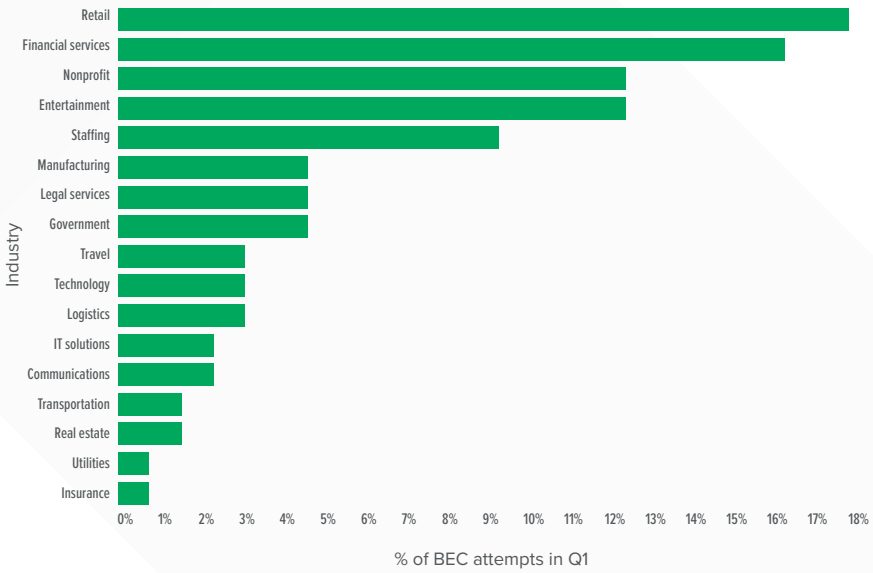
Pro tip: If you're struggling to wrap your arms around BEC, the Azure AD Identity Protection tool can provide visibility into identity-based risks.

BEC targeting by industry

Threat actors targeted retail firms the most, followed by financial services.

The bar graph below shows the percentage of BEC attempts our SOC identified in Q1. 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 fraud attempts can happen anywhere, to anyone.

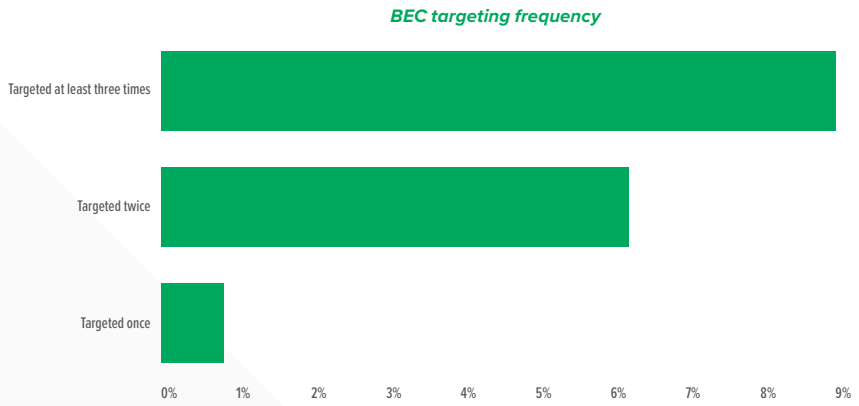
BEC targeting by industry



BEC targeting frequency

Twenty-four 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), 8% of our customers were targeted more than three times. For one large retail customer, our SOC identified 22 BEC attempts in their O365 tenant alone. The takeaway? Not only is BEC happening everywhere, it's 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 Auth, which means an attacker can bypass MFA completely by using an IMAP/POP3 client. Once you turn those off, strongly consider disabling Basic Authentication to prevent any pre-auth headaches on 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.
4. And finally, consider using Azure AD Identity Protection or Microsoft Defender for Cloud Apps. These advanced security services from Microsoft build data models for each user that make it easier to spot atypical authentication activity.

Want to learn more about **how Expel can help with BEC**?

Let's Chat

Business application compromise (BAC)

TL;DR **Six percent of incidents were BAC attempts in Okta. Seven percent of BAC attempts in Okta satisfied the MFA requirement by continuously sending Duo push notifications to the victim until they accepted.**

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.

What does the data look like?

Six percent of incidents were BAC attempts in Okta. We didn't identify a BAC attempt in OneLogin during the period. But for context, we monitor more than 10 times the amount of Okta tenants compared to OneLogin.

One of the most significant findings in our data showed that 7% of BAC attempts in Okta successfully satisfied the MFA requirement by continuously sending Duo push notifications to the victim until they accepted.

Detecting BAC in Okta

Of the BAC attempts we identified in Okta, we detected 57% by monitoring for atypical authentication activity. In all of these attempts, the threat actor attempted to authenticate into an Okta account from an IP address associated with a Tor exit node or VPN service.

We detected 47% of BAC attempts in Okta through employee-reported suspicious activity. In this context, an employee reported a notification of potentially suspicious activity from Okta or Duo. The lesson here? Encourage your employees to report suspicious activity and have a defined, repeatable process to investigate.

HOW TO PROTECT YOUR ORGANIZATION

1. Deploy phish-resistant MFA. (FIDO security keys for the win!)
2. Implement a pre-authentication policy for network zones in Okta.
3. 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.
4. 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.

Interested in guidance from Expel about **spotting suspicious authentication** activity?

Let's Chat

Pre-ransomware

TL;DR

Pre-ransomware accounted for 5% of all incidents. Threat actors used macro-enabled Word documents and zipped JavaScript files as the initial attack vector in 82% of all pre-ransomware incidents.

While our data shows that BEC was the top threat, many of the organizations we protect continue to worry about ransomware attacks, and rightly so.

Our SOC attributed 5% 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.

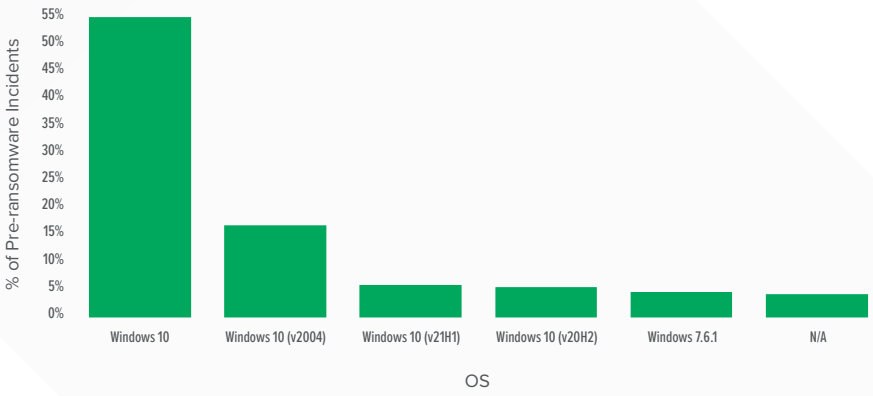
The data focuses on the deployment of malware we've linked to ransomware operations. This includes initial droppers/downloaders and backdoors enabling remote access that can be sold to a third-party.

Operating system targeting

Before we get into attack vector data, let's talk about operating system (OS) targeting. All of the computers we saw targeted were running a version of the Windows OS — including workstations and servers. Eighty-two percent of targets were running versions of the Windows 10 OS and 9% were running Windows 7.6.1.

This doesn't mean that ransomware doesn't exist for Linux, Chrome OS, or macOS — or that attackers can't use computers running those operating systems as an initial foothold. It's merely a data point for pre-ransomware targeting context.

Pre-ransomware malware OS targeting



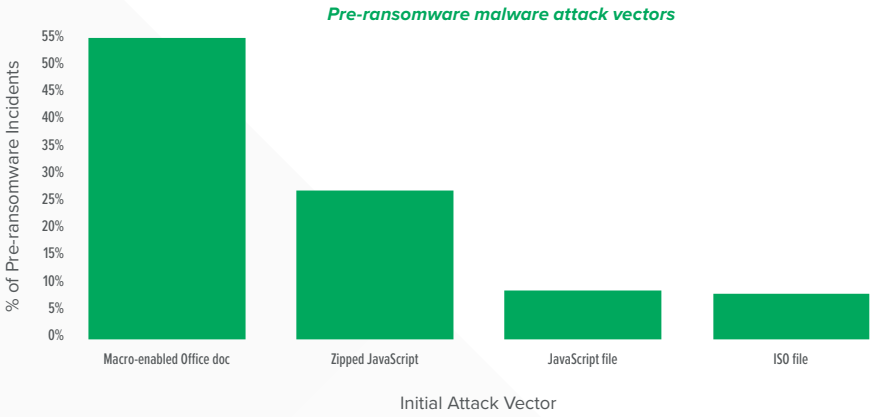
82% of targets were running **versions of the Windows 10 OS** and **9%** were running **Windows 7.6.1**.

Initial entry

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

1. Macro-enabled Office documents (55% of all pre-ransomware incidents)
2. Zipped JavaScript files (27% of all pre-ransomware incidents)
3. JavaScript files (10% of all pre-ransomware incidents)
4. ISO files (10% of all pre-ransomware incidents)

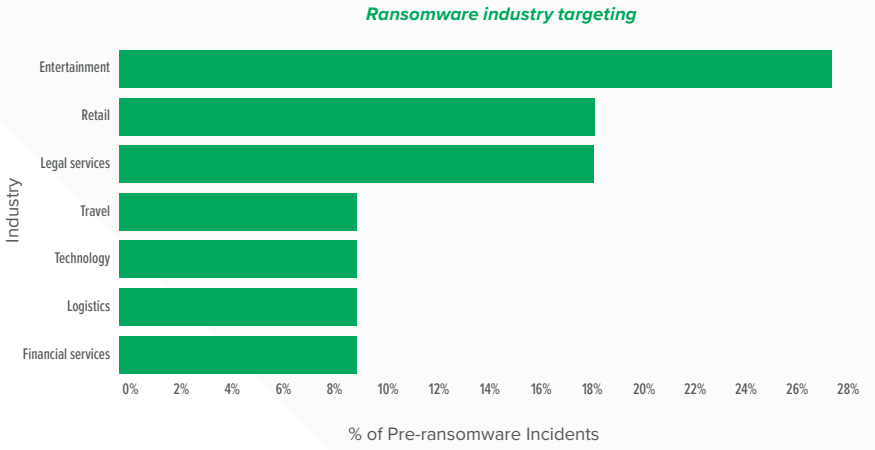
Our SOC didn't detect any pre-ransomware activity that exploited a software vulnerability for initial access. A key component in defending against ransomware attacks is monitoring and reducing the self-installation attack surface on the Windows OS by associating Windows Script Host (WSH) files with notepad, and disabling XLM and VBA macros in files downloaded from the internet.



Ransomware targeting by industry

Ransomware threat groups targeted the entertainment industry the most, accounting for 27% of all pre-ransomware incidents. The retail and legal services industries followed behind, each accounting for 18% of the pre-ransomware incidents detected by our SOC.

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



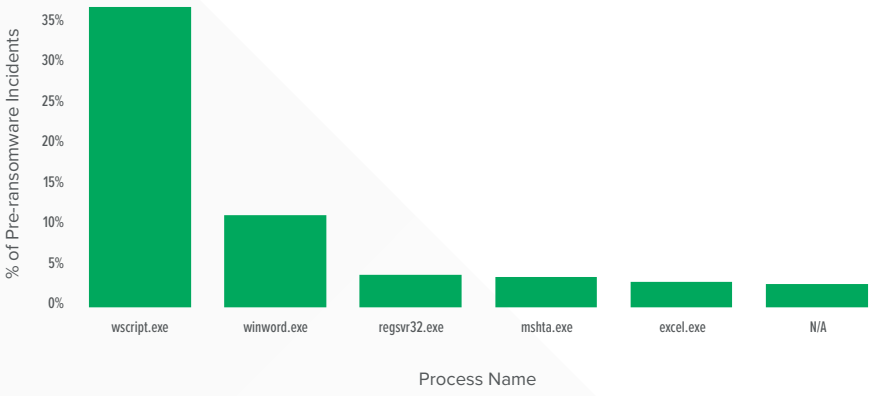
Detection opportunities

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.

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

- 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.

Top native Windows OS binaries and popular office productivity applications executed for initial pre-ransomware access



HOW TO PROTECT YOUR ORGANIZATION

1. Defend the self-installation attack surface on Windows by disabling macros in files downloaded from the internet and associating WSH files with Notepad.
2. Deploy MFA everywhere, especially for remote access (we recommend phish-resistant MFA).
3. Don't expose Remote Desktop Protocol (or any other service you don't need to) directly to the Internet.
4. Patch and update regularly.
5. Deploy EDR policies in "block" mode.

Want to get the most up-to-date guidance and intelligence about **rapidly evolving ransomware trends and tactics**?

Let's Chat

Commodity malware

TL;DR

17% of incidents were related to commodity malware, with 48% of commodity malware deployed via infected removable media, XMRig, SolarMarker, Emotet, and Asyncrat top detected families.

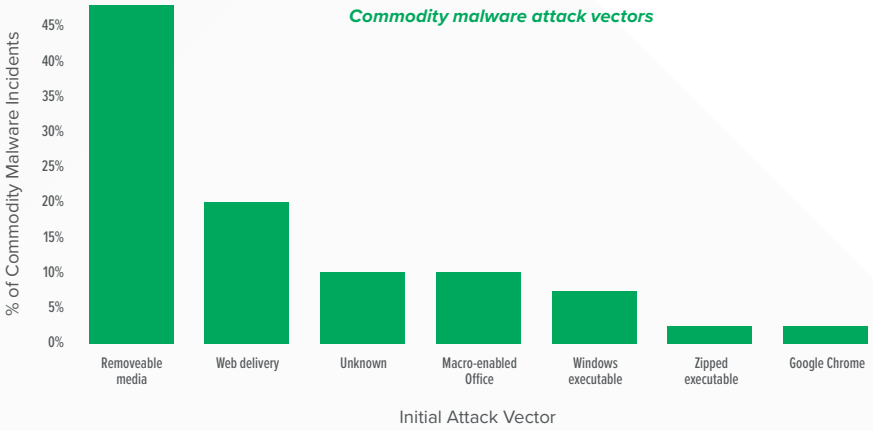
Our SOC identified that 17% of all incidents were the result of threat actors deploying commodity malware on Windows-based systems.

Top attack vectors

The top attack vectors used to deploy commodity malware include:

1. Removable media (48%)
2. Web delivery (20%)
3. Macro-enabled Office doc (10%)
4. Executable/zipped executable (10%)
5. Evil Google Chrome extension (2.5%)

The biggest surprise in our data was that infected removable media drove 48% of commodity malware infections. What was once old is now new again.

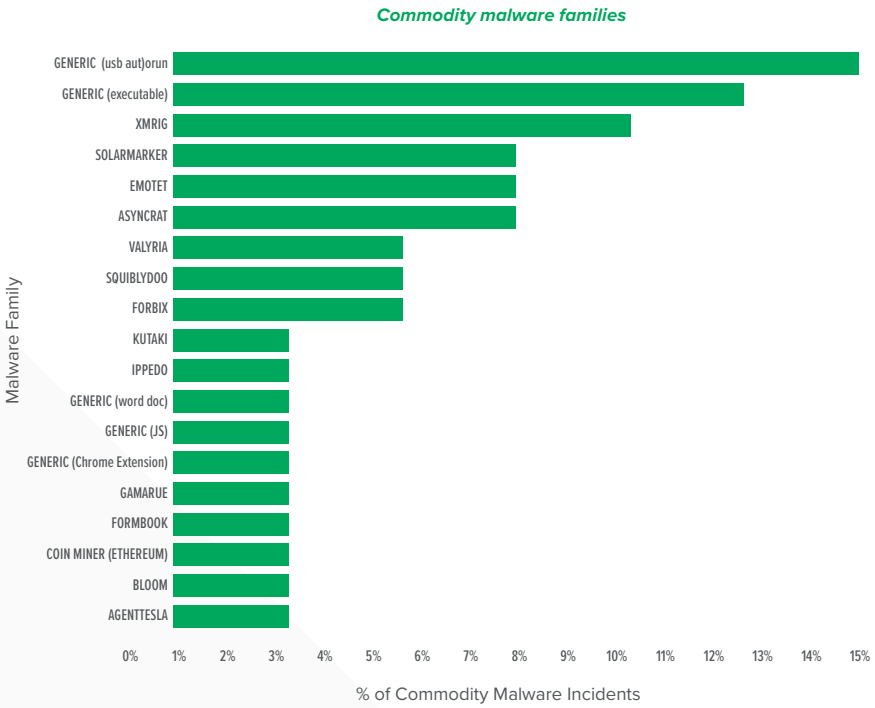


Commodity malware families

If we exclude generic droppers from infected removable media and XMRig, our SOC detected that a crypto currency miner for the Monero blockchain, SolarMarker, Emotet, and Asyncrat were the top malware families. You really don't want these running on your network.

The **biggest surprise in our data was** that infected removable media **drove 48% of commodity malware infections**.

As an example, SolarMarker usually installs a backdoor and steals credentials stored in browsers, but it can also target additional sensitive info stored on the infected system.



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. 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.
3. IT administrators should set policies that block active content in Office docs that arrive by email. Microsoft also recently announced that they'll provide more granular controls for macros, ActiveX content, and Office add-ins in emailed Office docs.
4. Set policies to ban (or strongly discourage) removable media.

Want to learn how Expel can help you **detect commodity malware**?

Let's Chat

Cloud infrastructure

TL;DR **Common cloud misconfigurations and long-lived credentials were the root cause of 100% of incidents identified in the cloud.**

Misconfigurations and exposed long-term credentials in Amazon Web Services (AWS) and Google Cloud Platform (GCP) accounted for 3% of incidents.

These incidents break down into two categories:

1. Admins accidentally setting AWS S3 Buckets to Public
2. Threat actors gaining access to exposed long-lived credentials in AWS and GCP, which resulted in unauthorized access

On the AWS side of the house, we detected multiple instances where threat actors performed Denial of Service (DoS) attacks, SQL injection attacks, and unauthorized crypto currency mining by creating new EC2 instances with exposed long-lived credentials.

For AWS GuardDuty customers, pay particular attention to findings for EC2 instances generating traffic consistent with DoS attacks or when an EC2 instance generates activity consistent with a DNS rebinding attack.

On the GCP side of the house, we observed an attacker attempting to use an exposed service key from an atypical location to create a new service account key to maintain access to the environment using the Google SDK. Our SOC quickly scoped and fixed the issue.

The bottom line is that misconfigurations and long-lived credentials caused all the cloud infrastructure incidents in Q1.

HOW TO PROTECT YOUR ORGANIZATION

1. Scan for exposed credentials using open-source tools like gitleaks.
2. Remove unnecessary AWS Identity and Access Management (IAM) access keys and rotate access keys frequently.
3. Ensure least privilege in AWS IAM Security Policies.

Want to learn more about **how Expel can help identify potential security incidents** in your cloud environment?

Let's Chat

Phishing

TL;DR

Ten percent of phishing emails submitted to our team for review were malicious. Only 12% of the employees who had their credentials stolen via a phishing attack had forwarded the email to our analysts for further review. Interestingly, the subject line most used for malicious emails is a blank entry. Why? We see attackers use a blank subject line most often when they're trying to develop a relationship with the target to carry out an attack at a later date.

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.

Only 10% of the phishing emails reviewed by our analysts were malicious. The rest were a mix of benign and spam emails.

The most interesting trend in our data showed that only 12% of the employees who had their credentials stolen via a phishing attack forwarded the email to our analysts for further review. This means only a small percentage of employees recognized potential red flags after submitting credentials to a harvesting site controlled by an attacker.

The other trend in our phishing data showed that only 10% of credential harvesting emails contained obvious spelling and grammar errors.

Top subject lines

Below are the top subject lines used in emails that were confirmed malicious by our phishing team. The top subject line? No subject line. More than two-thirds of the attackers we observed left the subject line blank.

Top subject lines	Percentage
Blank subject	67.48%
Fax Delivery Report	9.01%
Business Proposal Request	5.83%
Request	4.20%
Meeting	4.07%
You have (1*) New Voice Message	3.46%
Re: Request	2.10%
Urgent request	2.03%
Order Confirmation	1.83%

HOW TO PROTECT YOUR ORGANIZATION

1. Make sure you're running MFA wherever possible using phish-resistant FIDO security keys to significantly reduce risk associated with credential theft.
2. Invest in training so employees learn to recognize potential red flags associated with phishing emails when they land in their inbox.
3. Educate specific business units on the phishing campaigns that might target them. For example, developers may see AWS-themed campaigns, while recruiters may see resume-themed phishing lures.

Phishing remediation a problem for your organization?

Let's Chat

Penetration testing, red team, and purple teams

TL;DR

Nine percent of incidents were authorized penetration tests, red team and purple team exercises. Cobalt Strike was the preferred post-ex and c2 framework — a combo of RDP, WMI, and PsExec to move laterally.

A quick nod to the good guys: Nine percent of incidents detected by our SOC were authorized penetration tests, red team, and purple team exercises. These exercises allow organizations to test their security controls, remediation processes, and investigative capabilities.

These 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 compromised account was used by a red team. Our SOC performed a median number of 16 investigative actions when chasing a red or purple team. Alerts are 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 the first quarter was four. This included host 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-exploitation and command-and-control framework.
- Most of the red teams using Cobalt Strike injected BEACON into another process to evade detection (we still caught them).
- Multiple red teams executed SharpShooter for payload generation.
- Red teams used Lazagne and Mimikatz to steal Windows credentials.
- In one red team, an operator ran Seatbelt to perform "safety" checks.
- Red teams moved laterally via Remote Desktop Protocol, Windows Management Instrumentation (WMI), and via ImPackets's PsExec module.
- On the cloud infra side, red teams preferred ScoutSuite to perform posture assessments in AWS.

HOW TO PROTECT YOUR ORGANIZATION

1. The emphasis of a red team should be 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 so important to build muscle memory around your IR process before a red team exercise.

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

Let's Chat

Looking ahead to Q2

We see the use of OAuth applications to bypass MFA in O365 as particularly concerning. While we detected this technique in only 2% of incidents, traditional remediation steps won't remove the attacker's access. We're expecting to see increased adoption of this technique throughout the remainder of 2022.

We anticipate that self-installation techniques will remain the top attack vector for pre-ransomware and commodity malware. Side note: We're really encouraged by the steps Microsoft is taking to disable Excel 4.0 macros by default and by their announcement to give IT professionals more granular control over active content attached to emails. "Secure by default" is how we'll make the most progress in mitigating the self-installation attack vector.

Finally, attackers will continue to find ways to bypass legacy MFA. Seven percent of BAC attempts in Okta satisfied the MFA requirement by continuously sending Duo push notifications to the victim until they accepted. Organizations should prioritize MFA for their employees using phish-resistant FIDO security keys.

This is the way. (Can you tell we're big Star Wars fans at Expel?)

"Secure by default" is how we'll make the most progress in mitigating the self-installation attack vector.

About Expel

Expel is a managed detection and response (MDR) provider whose vision is to make great security accessible. The company offers 24x7 security monitoring and response for cloud, hybrid and on-premises environments. Expel uses the security signals customers already have so organizations can get more value from their existing security investments. And Expel connects to customer tech remotely through APIs, not agents, so its security operations center (SOC) can start monitoring a customer's environment in a matter of hours, letting their internal teams get back to focusing on the most strategic security priorities that are unique to their business. 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