expel

Great expeltations

Cybersecurity trends and predictions

2022

www.expel.com

Contents

A message from merk (aka our CEO)

Welcome to Great eXpeltations 2022, Expel's first annual cybersecurity trends report.

Among other reasons, my co-founders and I started Expel to bring more transparency into cybersecurity. And since the start, that's been one of our core values. So as part of that commitment, we're sharing the most important threats and trends our security operations center (SOC) identified last year and their advice on what to do about them.

This report, written by our SOC leadership team, aggregates data from every incident our team investigated in 2021. It covers our full customer base, from small and midsize companies to enterprise orgs at every phase of the security journey across every industry we serve.

For each of the top trends our SOC dives into, they'll tell you what they saw, how to detect these threats and protect your org, and what to expect for 2022. Our leadership team also shares some of our thoughts and predictions for cybersecurity this year. We hope this info can help as you create your strategy for managing risk in the year ahead.

We've had the same motto at Expel for the last year: lock arms, up the mountain. It's a reminder that we can get through anything together. This also applies to cybersecurity and how we, as a community, need to work together. It's not about individual rockstars, it's about the strength of the collective team. So as we kick off 2022 and face the exciting moments and challenges ahead, let's do so together, helping make everyone a little safer this year.

Lock arms, up the mountain.
merk

Dave Merkel
CEO, Expel

"We hope this info can help as you create your strategy for managing risk in the year ahead."

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

The trends and predictions we discuss in this report are based on incidents our SOC identified through investigations into alerts, email submissions, or hunting leads in 2021. We analyzed incidents spanning January 1, 2021 to December 31, 2021, looking for patterns and trends that can 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: translate the security events we're detecting into security strategy for your org. We'll accomplish this by sharing the top trends we're seeing and guidance on how to spot the bad actors and make it harder for them to break in.

We've also included an appendix that shares our alert-to-fix time across critical incidents and our SOC quality control (QC) data for 2021.

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) should be considered public enemy number one.

50% of all incidents we identified were BEC. Almost 100% of those incidents were in Microsoft Office 365 (O365). Less than 1% of the BEC we identified was in Google Workspace.

Ransomware attack numbers hit record highs.

Threat actors *mostly* relied on employees of the target org accidentally self-installing malware for initial entry.

83% of opportunistic attempts to deploy commodity malware or a ransomware stager on a Windows device used a "self-installation" attack vector like Zipped JavaScript files, Zipped executables, and malicious macros in Microsoft Office docs and Excel spreadsheets.

Cryptojacking was the free Red Team the Internet needed.

35% of the web app compromises we identified resulted in deployment of a crypto miner. Orgs experiencing this type of incident patched the exploited vulnerabilities 100% of the time... and by doing so, removed an entry point for ransomware.

Effective security starts with asset management.

Being able to answer, "Are we running that software?" or "Are we vulnerable?" was so important in a year filled with scary pre-authorization remote code execution (RCEs) and supply chain attacks leading to privileged remote access.

Finally, Google Chromebooks, phish-resistant FIDO keys, and Google's Advanced Protection Program can get you *really* far in terms of 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.

MEET THE AUTHORS

Jon Hencinski

Director, Global Operations

@jhencinski

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

Ben Brigida

Director, SOC Operations

@The_Real_BenB

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

Ray Pugh

Manager, Security Operations

@RpughIII

SOC work is both exciting and rewarding when you're surrounded by the right people and focused on a noble mission. Fueled by a passion for helping others.

Business email compromise (BEC)

Targeting emails and application data

Here's the deal...

BEC should be considered public enemy number one. For the past five years, this class of fraud resulted in the most financial losses reported to the FBI. In 2020 alone, BEC attacks resulted in the loss of $1.8 *billion* stolen from companies.

Every CISO and CFO should give BEC their attention. Our 2021 data suggests BEC fraud is only growing in reach and financial impact.

Before we jump into the data, an important trend to note: beginning in early 2020 and continuing throughout 2021, many of our customers migrated to single sign-on (SSO), specifically Security Assertion Markup Language (SAML) authentication. This means that attackers can hit more than just mail providers as an easy target to harvest credentials. The term BEC also includes attempts to access popular cloud access identity providers like Okta and OneLogin.

Since launching our managed detection and response (MDR) service in 2018, we've seen the age-old cat and mouse game where with the advancement of good (like conditional access policies) comes the advancement of evil (Yahoo boy turns on his VPN) — particularly when it comes to BEC.

What we saw last year

Fifty percent of all incidents we identified were BEC attempts in O365. Sixty-four percent of customers that used popular SaaS applications like Microsoft O365, Okta, and Google Workspace experienced at least one BEC fraud attempt.

Of the BEC attempts we identified:

- 90% were in O365
- 9% in Okta
- Less than 1% in Google Workspace

BEC accounted for 30-60% of all incidents every month. The graph below shows the percentage of identified incidents each month that were BEC or business application compromise (BAC) attempts compared to all other incident types (ransomware, Advanced Persistent Threat (APT), Red Team, etc.).

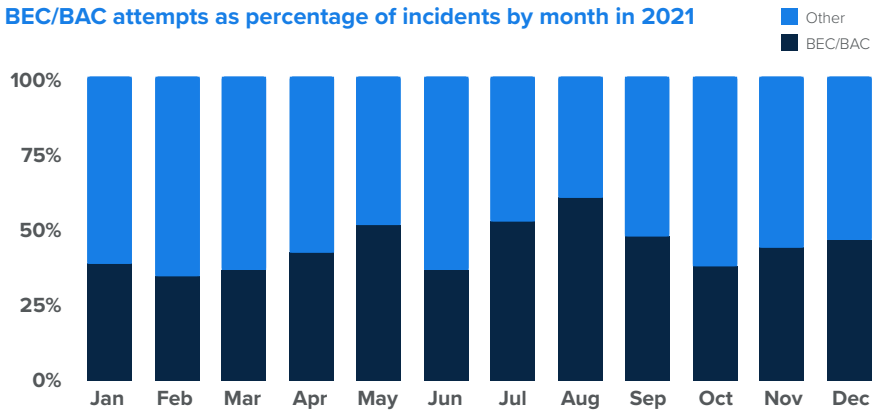
TL;DR: BEC should be considered public enemy number one. BEC attempts accounted for 50% of all incidents we identified in 2021.

What we saw last year

- 64% of customers using popular SaaS apps experienced a BEC attempt.
- 90% of all BEC incidents occurred in O365.
- 9% of all BEC incidents occurred in Okta.
- Less than 1% of all BEC incidents occurred in Google Workspace.
- Attackers used VPNs and hosting providers to bypass conditional access policies.
- Attackers authorized using legacy protocols to bypass multi-factor authentication (MFA) in O365.
- Attackers hijacked authenticated Duo network sessions by acting as a "Man-in-the-Middle" (MitM) to intercept and satisfy MFA.
- Employees accepted malicious Duo push notifications.

How to protect your org

- Deploy MFA everywhere (we recommend phish-resistant FIDO security keys).
- Disable legacy protocols in O365.
- Implement conditional access policies in Azure.



OK, why so much BEC in O365 but not Google Workspace?

Microsoft has a suite of great products to alert on malicious webmail activity. But O365 also has some default configurations that orgs must change to enhance security, whereas Google Workspace's more stringent security settings come out-of-the-box.

With original deployments of O365 tenants, IMAP and POP3 were enabled by default in O365 Exchange, as well as Basic Authentication. IMAP and POP3 don't support multi-factor authentication (MFA), so even if you have MFA enabled, attackers can still access these mailboxes. Basic Authentication allows attackers to authenticate without satisfying any pre-authentication checks to the identity provider, which could lead to account compromises or account lockouts from password spray or brute force attacks.

Microsoft intended to do away with Basic Authentication by default, but postponed this rollout because of the COVID-19 pandemic. They've since announced their plan to disable Basic Authentication starting October 1, 2022.

Google, on the other hand, disables these configurations in Workspace by default but provides the option to enable them retroactively. This helps prevent similar BEC attacks in Google Workspace off the bat.

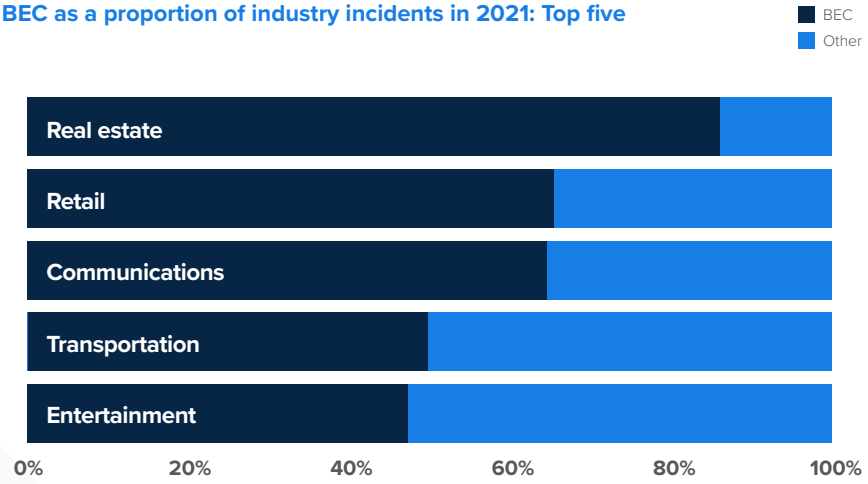
Targeting by industry

Real estate was the top targeted industry in 2021 among the industries we serve. This industry experienced the greatest proportion of BEC attacks vs. all other incident types observed in the industry. However, the data also tells us that BEC fraud isn't an industry-specific problem. An org's yearly revenue or industry is by no means a predictable measure of potential BEC targeting.

As if you need another reason to enable MFA everywhere, our data suggests that orgs with single-factor webmail are much more likely to experience BEC attempts. Thanks, Captain Obvious. But for real, our data backs this up. So enable MFA everywhere — particularly phish-resistant FIDO security keys if you can.

Enable MFA everywhere — particularly **phish-resistant FIDO security keys** if you can.

BEC as a proportion of industry incidents in 2021: Top five



Analyzed data included industries with 2+ customers and 11+ incidents in 2021

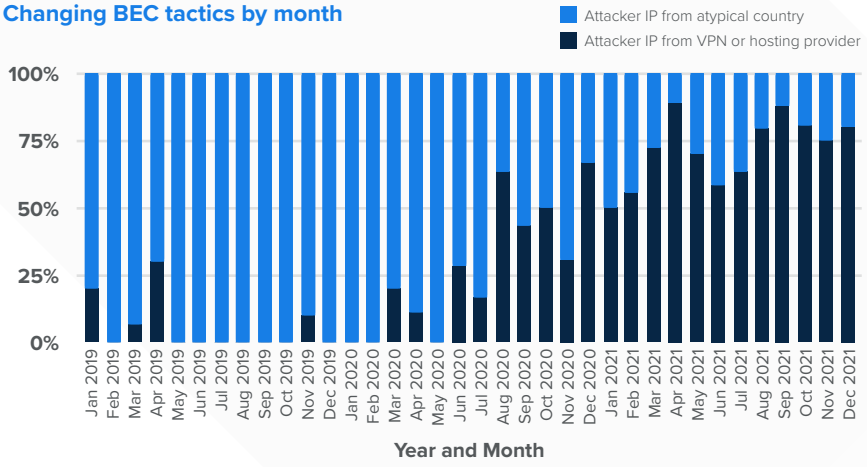
BEC tactics

Network infrastructure

Since 2019, we've seen a 50% increase in the use of VPN services and hosting providers to access compromised accounts. Using these services allows attackers to bypass conditional access policies that deny logins from certain countries by geo-IP records. BEC threat actors' rising use of VPN services and hosting providers is likely a response to orgs increasingly using conditional access policies, rather than an attempt to improve tradecraft.

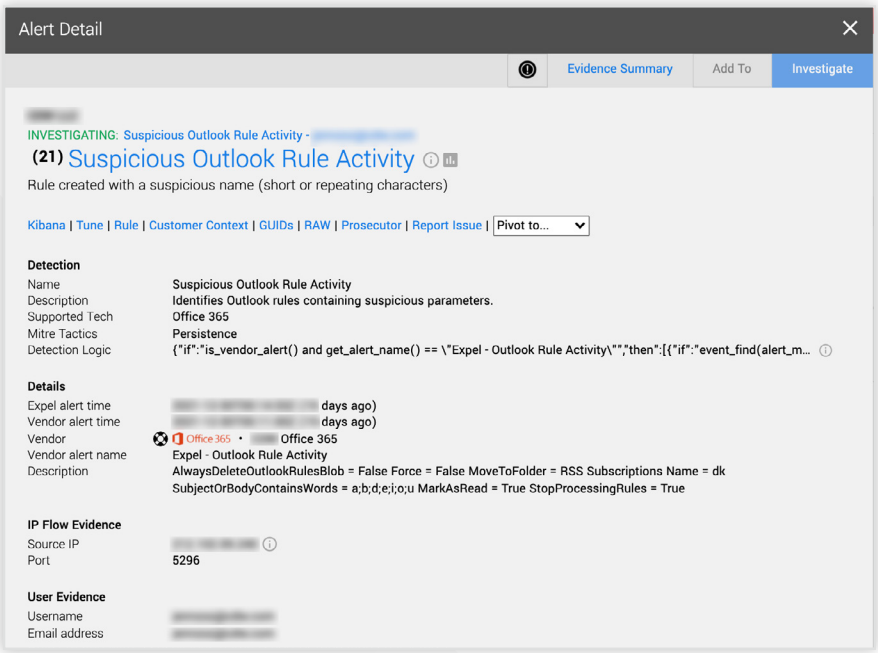
This trend continued in 2021. The graph below shows the monthly percentage of BEC attempts where a threat actor accessed a compromised SaaS app account from an IP address geo-located in an atypical country (light blue bars) vs. from a popular VPN or hosting provider (dark blue bars). You can see a dramatic shift in tactics starting around Q3 2020 when a lot of orgs were settling into "fully remote" and amping up security protocols for the remote environment — so threat actors adapted in response.

Changing BEC tactics by month



Account takeover in O365

Another BEC tactic: a threat actor accesses a victim's O365 mailbox and sets up inbox rules to redirect emails while the attacker perpetuates credential theft. There are common hallmarks of this type of account takeover. In 2021, BEC threat actors were big fans of the RSS subscription folder. They used this folder to redirect emails more than any other.



Alert detail view in Expel Workbench™ (the platform we built and use to provide our MDR service), showing BEC account takeover activity to redirect emails to the RSS Subscriptions folder.

What else did we see?

1. Inbox rules to automatically forward emails to the junk email or notes folders.
2. Inbox rules to automatically delete messages.
3. Inbox rules to redirect messages to an external email address.

MFA interception

We expect to see attackers using MFA interception techniques more frequently in 2022. This differs from just sending a user MFA prompts until they accept. For example, we saw attackers trick a user into visiting a fake SSO page, like Okta, that they control. The attacker then redirected the user to a page masquerading as the Duo Security MFA page that was also hosted by the threat actor. The attacker hijacked the user's authenticated network sessions by acting like a Man-in-the-Middle (MitM).

We expect to see attackers **using MFA interception techniques more frequently** in 2022.

So, how do we detect this? There are two devices (and their IP addresses) in the Duo Authentication Logs associated with a Duo Push Authentication event:

- Access Device — the device from which the user is requesting the Duo Push.
- Authentication Device — the device approving or rejecting the Duo Push.

For a legitimate authentication event, we can assume that the access device and the authentication device are in close proximity to each other, and since we have the IP addresses of both devices, we can build a detection off this assumption. If the IP proximity doesn't line up, it's likely a MFA interception attempt.

Detection opportunities

Detecting BEC attempts boils down to three key areas:

1. **Email inspection**
   - To prevent and detect phishing emails trying to steal employee credentials.
   - To spot when a threat actor uses an employee's account to send phishing emails.
2. **Authentication monitoring**
   - To detect use of stolen credentials.
3. **Account monitoring**
   - To detect hallmark signs of BEC account takeover.

Authentication monitoring

Before building any BEC detection, ask two key questions:

1. How can the environment and its applications and data be accessed?
2. Of those entry or access points, are there any single-factor methods?

If O365 is single-factor authentication, start there. Build a baseline of what's happening. Then take a look at successful and failed authentications from IP addresses geo-located in countries that might be a bit odd for your org. Building alerts for unusual authentication patterns is a "test, learn, iterate" process. You test a theory, you learn from it, and then you iterate and improve.

If you're looking for a cheat code: Azure AD Identity Protection and Microsoft Defender for Cloud Apps build data models for each user that make it easier to spot atypical authentication activity. These services also include enhanced logging capabilities.

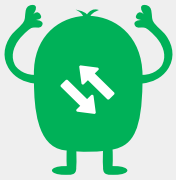
In fact, Azure AD Identity Protection and Microsoft Defender for Cloud Apps provided the most initial BEC leads per device last year out of all the vendor tech we monitor to detect BEC. When controlling for the number of customers deploying each product, Azure AD Identity Protection identified three times more BEC leads and Microsoft Defender for Cloud Apps identified nearly two times more BEC leads than the base O365 product.

Account takeover

Here are a few things we typically watch for:

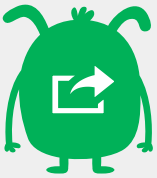
Inbox rules that automatically forward emails to hidden folders

Inbox rules that automatically delete messages



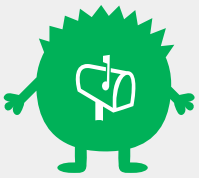
Inbox rules that redirect messages to an external email address

Inbox rules that contain BEC keywords (check out the top keywords we've spotted)



New mailbox forwarding to an external address

Successful mailbox logins within minutes of denied logins



New mailbox delegates

Logins from proxy or VPN services

How to protect your org

We're going to focus on BEC in O365. However, if you're worried about protecting your Okta (or similar provider) users and data, we've also included some recs for that. Note that our recs will be specific to Okta as these were the incidents we responded to.

Forty-eight percent of the BEC attempts we identified in O365 were stopped by conditional access policies or by the second factor in the authentication process (most often a digital security token). These are still incidents because the employee's password (the first factor) was compromised, and we've seen BEC threat actors persist to bypass conditional access policies using VPNs and hosting providers, or bypass MFA by authenticating using legacy protocols.

Bottom line: if conditional access policies or MFA stop unauthorized access, that's a win. But don't forget to reset an employee's password if you see signs that the first factor in the authentication process was compromised.

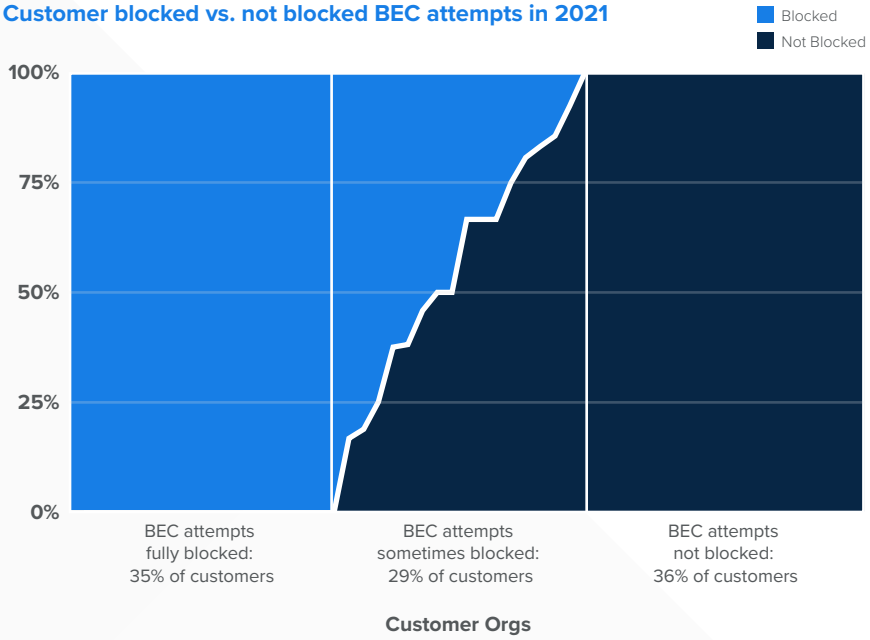
48% of the BEC attempts we identified in O365 were stopped by conditional access policies or by the second factor in the authentication process (most often a digital security token).

The graph below shows the percentage breakdown of blocked vs. not blocked BEC attempts we observed in O365. In most blocked cases, the threat actor compromised the employee's password but couldn't authenticate because of conditional access policies and MFA.

Some additional context on the data:

- About a third of our customers have conditional access policies, backed by MFA, and they've disabled legacy protocols on their O365 tenant(s).
- About a third of our customers have conditional access policies, backed by MFA, but are still running legacy protocols — which means MFA can be bypassed.
- About a third of our customers have *some* conditional access policies, but lack MFA and are running legacy protocols.

Customer blocked vs. not blocked BEC attempts in 2021



If you're struggling with BEC in O365:

1. Make sure you're running MFA wherever possible using phish-resistant FIDO security keys.
2. Disable legacy protocols like IMAP and POP3. This one is critical, especially if you've gone through the process to enable MFA. 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. 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 (executives or employees with access to sensitive data, for example) and high-risk applications. You can even create a conditional access policy to require MFA registration from a location marked as a trusted network. This prevents 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.

If you're worried about what's happening in Okta:

1. Deploy phish-resistant MFA. FIDO security keys for the win!
2. Implement 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.
   - 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 like 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.

Looking ahead

Unfortunately, BEC isn't going away. Microsoft is making some important changes this year, but the threat isn't going to disappear.

As the industry moves towards 'secure by default,' attackers will continue to increase the number of MFA intercept attacks they perform. Security vendors need to continue to implement features like Okta AMFA and user behavior analytics (UEBA) to add security steps to the process in the presence of unusual login features.

While it can be a momentary pain for users, the impact of denying logins or disabling webmail accounts pales in comparison to the $1.8+ billion price tag associated with BEC over a year. The industry needs to continue to err on the side of caution and lock accounts with suspicious behavior.

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

Let's Chat

Ransomware

Here's the deal...

Ransomware attack numbers hit record highs in 2021.

A May 2021 ransomware attack forced Colonial Pipeline to shut down its 5,500-mile natural gas pipeline for five days. The result? More than 10,000 gas stations across the Southeastern U.S. ran out of fuel.

In July 2021, Kaseya, an IT solutions company used by many managed service providers (MSPs) and enterprise orgs, announced it was the victim of a large-scale supply chain attack carried out by the REvil gang. REvil exploited Kaseya VSA, a remote monitoring and management (RMM) tool, through a zero-day vulnerability (CVE-2021–30116) to deploy ransomware, encrypt files, and demand ransom payments from MSPs and end user customers.

The attack had a major impact on the tech, critical infrastructure, and food production industries.

Things got so bad last year that on July 14, 2021, the U.S. government launched StopRansomware.gov, the first interagency initiative to address the growing threat of ransomware. This is a great resource for individuals and orgs of all sizes looking to learn more about the threat of ransomware and how to improve their security posture.

Before we get into the data, it's important to provide some background. As an MDR, our goal is to stop attacks *before* they result in a ransomware incident. You don't need fancy detections to tell you your files have been encrypted — the ransomware does that for you. We want to make sure it doesn't get to that point.

The data we share focuses on *how* and *when* in the attack lifecycle we identified and stopped ransomware attacks before an encryption event. Our focus is on spotting initial compromise or when a ransomware threat group establishes a foothold within a target org.

Bottom line: we strive to stop ransomware attacks as early in the attack lifecycle as possible... and the data shows we've succeeded.

What we saw last year

Nearly 13% of all opportunistic attacks we identified in 2021 *could* have resulted in ransomware deployment had we not intervened. We attributed a vast majority of this ransomware activity to the REvil gang prior to its October 2021 coordinated takedown.

Targeting by industry

Among the industries we serve, the legal services industry experienced the greatest proportion of ransomware incidents. But like BEC, the data also tells us that ransomware attacks aren't an industry-specific problem. Neither industry nor annual revenue provide predictable measures of

TL;DR: Ransomware attack numbers hit record highs in 2021. The good news? You can stay ahead by monitoring and controlling the "self-installation" attack surface on Windows.

What we saw last year

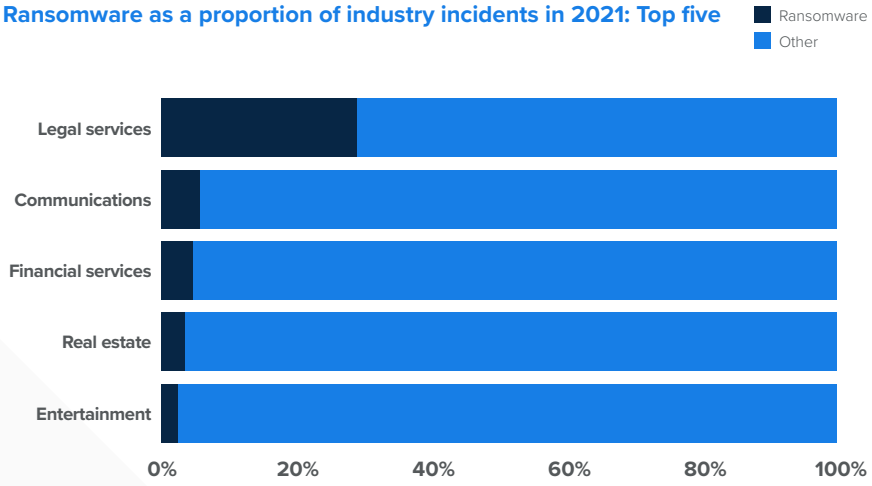
- Ransomware accounted for 13% of all opportunistic attacks.
- 83% of attacks used a "self-installation" technique for initial entry.
- Only 4% of attacks exploited a software vulnerability for initial entry.
- 100% of attacks targeted a computer running Windows.
- We attributed a vast majority of the ransomware activity to the REvil gang (prior to takedown).

How to protect your org

- Create a ransomware incident response (IR) plan... and test it!
- Defend the self-installation attack surface on Windows.
- Deploy MFA everywhere, especially for remote access (with phish-resistant MFA).
- Don't expose Remote Desktop Protocol (or any other service you don't need to) directly to the Internet.
- Patch and update regularly.

potential ransomware targeting. This is an everywhere and everyone problem.

Ransomware as a proportion of industry incidents in 2021: Top five



Analyzed data included industries with 2+ customers and 11+ incidents in 2021

Operating system targeting

Before we share 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 — this includes workstations and servers. 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 context.

Attack vectors

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

1. "Self-installation" techniques (83% of all ransomware incidents).

   These happen when employees unintentionally install malware by "double clicking" a Zipped executable or enabling a malicious macro in an Office doc. These are not exploits!

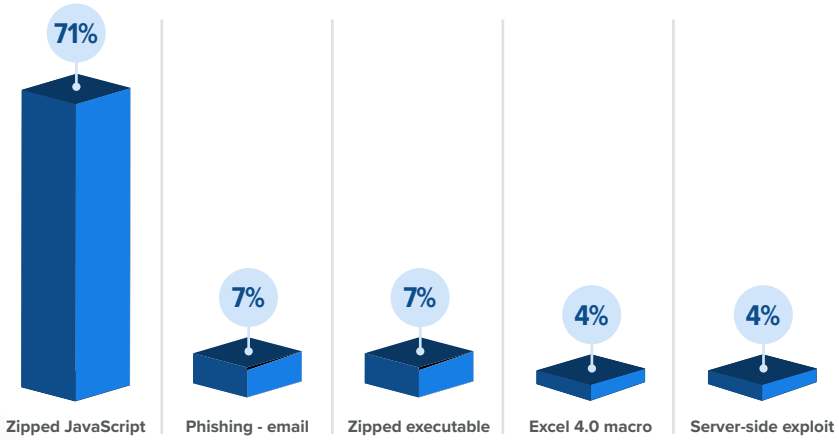
2. Exploitation of a software vulnerability on the perimeter (4% of all ransomware incidents).

   Also known as the, "oh yeah, we forgot about *that* server," or the, "oh yeah, that server," category.

3. Abuse of third-party access (3% of all ransomware incidents).

   These are supply chain attacks or use of compromised third-party privileged credentials.

Top ransomware attack vectors in 2021



Eighty-three percent of all ransomware incidents we identified used a self-installation attack technique to gain initial entry to a computer running Windows. Here's a breakdown of those techniques:

- Zipped JavaScript files (71% of all ransomware incidents)
- Zipped executables (7% of all ransomware incidents)
- Excel 4.0 macros (4% of all ransomware incidents)

Four percent of the time, attackers exploited a software vulnerability on the perimeter to gain initial entry. In each case, attackers targeted servers running a version of the Windows OS and exploited a vulnerable version of WordPress, the popular content management system.

A smaller percentage of ransomware incidents were the result of compromised third-party credentials with privileged access to the target org, usually through remote access using Microsoft's Remote Desktop Protocol (RDP) or a Citrix gateway.

Bottom line: while patching and updating are certainly an important part of your security program, the data shows a clear need to control your "self-installation" attack surface on Windows — in other words,"Do Windows right." We'll share more about what that means below.

Malware families

Of the ransomware incidents we identified in 2021, only 3% were stopped after the initial infection phase. In other words, 97% of the time, we stopped a potential ransomware incident before ransomware could be delivered, either immediately after an attacker exploited a web server or a malicious downloader, or after a stager executed on a workstation.

So when analyzing the malware families that attackers deployed for ransomware events, we include the incidents that we stopped before ransomware delivery. The top malware families we attributed to identified ransomware operations were:

- Gootkit loader (44% of incidents)
- SocGholish framework (15% of incidents)
- Cobalt Strike's Beacon agent (3% of incidents)

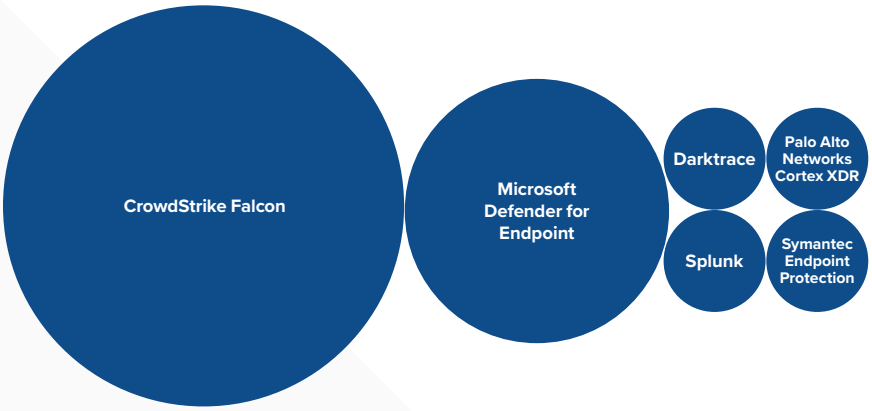
83% of all ransomware incidents we identified used a self-installation attack technique to gain initial entry to a computer running Windows.

Detection opportunities

Initial leads by tech integration

In 2021, we used our integrations with popular endpoint detection and response (EDR), network, and security information and event management (SIEM) tech to stop ransomware incidents. The visualization below shows the initial leads into ransomware activity provided by various tech integrations. The size of each bubble is based on the number of lead alerts generated by that tech that enabled us to stop a ransomware attack. For context, we monitor twice the number of customers with CrowdStrike Falcon compared to Microsoft Defender for Endpoint.

Ransomware leads by tech integration in 2021



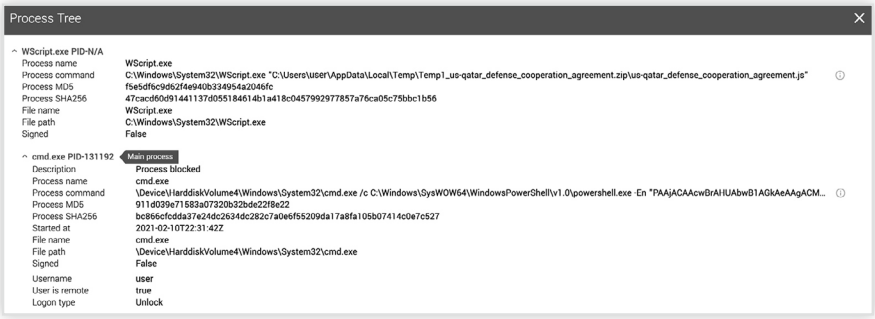
Top behavioral patterns

We've listed below some of the top behavioral patterns we alert on that helped us spot ransomware activity before any damage could be done. Alerting on behavioral patterns like these helps spot all kinds of malicious activity, not just ransomware threat groups trying to infiltrate your network. However, since every environment is different and typical user behavior can differ by org, some tuning and filtering may be required to make sure these patterns don't alert on legitimate behavior in your environment.

Endpoint behavioral patterns

Alert when...

- **Installation**:
  - 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.
- **Command and control (C2):** PowerShell executes a base64 encoded command and the process initiates an external network connection.



Expel Workbench endpoint process tree detail view showing a REvil gang attempt to infiltrate a network using a Zipped JavaScript file

Top Windows processes to monitor

If you're looking for more general guidance on which Windows processes you should monitor, our ransomware incident data indicates that the following were the top processes attackers used to gain entry in 2021:

- PowerShell
- CMD shell
- Wscript.exe
- RegSvr32.exe
- W3wp.exe

Network behavioral patterns

We want to give a (non-sponsored!) nod to Darktrace here. While, from a practitioner's perspective, many Darktrace models require tuning and filtering to reduce benign alerts, it enabled us to identify network patterns that helped us stop ransomware activity.

It's worth noting that these network behavioral patterns ship with their product. However, this doesn't mean you can't also alert on these network patterns using the tech you've already invested in.

Alert when...

- **Entry**: a network connection to a rare destination purports to be a popular video conferencing service (like Zoom).
- **Installation**: you see a PowerShell network connection to a rare external destination.
- **C2**: you see an HTTP connection with a PowerShell user-agent.
- **Elevate**: you see a high volume of Kerberos ticket requests and DNS requests for internal host names from the same source.

Our take: it's best to start with a hunting-based approach to answer questions like, "How often over a 30-day period do we see HTTP-based outbound connections with a PowerShell user-agent?" or, "When we see PowerShell initiate an outbound external connection, what are the typical destinations?" Then apply your learnings and enable new network-based behavioral alerts for activity that's not normal for your org.

Don't forget decision support

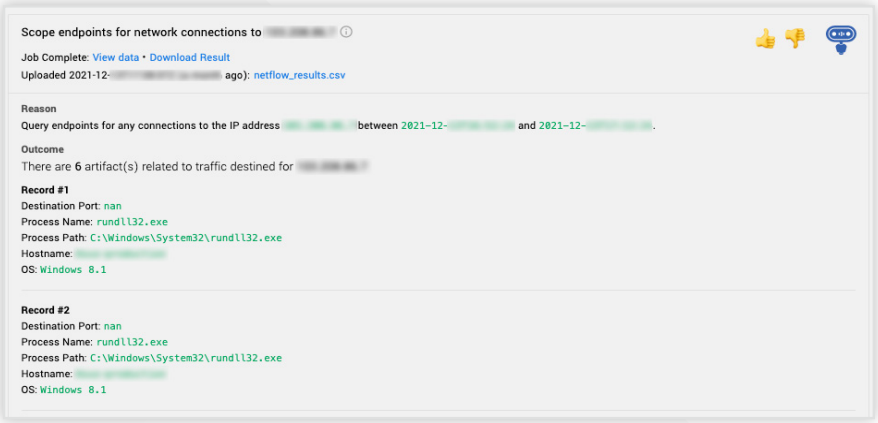
We use decision support tech to enable our SOC analysts to answer the right questions about a security event in an easy way.

In doing so, we reduce cognitive load and hand off highly-repetitive tasks to automation (aka our bots). It's a key component of how we make sure our analysts aren't burned out.

Given a network alert for a specific behavior or content pattern, SOC analysts will pretty much always want to know what process initiated that network connection.

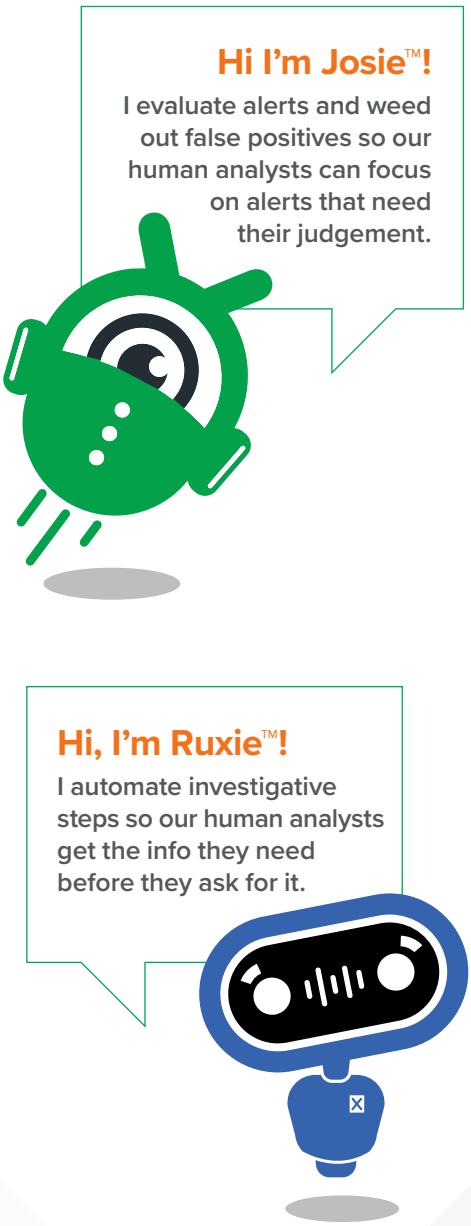
In the example below, a Palo Alto Networks firewall alerted on network traffic consistent with Cobalt Strike's Beacon agent. When an alert like this is created in our Expel Workbench platform, our bots, Josie™ and Ruxie™, automatically issue a query and provide answers to two key questions:

1. How many endpoints are communicating with the destination address?
2. What process initiated the network connection?



Expel Workbench network alert orchestration to query endpoints talking to a destination address

For anyone wondering, yes this was [rundll32.exe connecting out to the Internet](). No, that's not normal. And yes, this was absolutely a Beacon agent connecting back to the configured C2 server. Behold the power of near real-time decision support!



How to protect your org

Our top five recs to protect your org from ransomware attacks:

1. Defend the self-installation attack surface on Windows.
2. Deploy MFA everywhere, especially for remote access (we recommend phish-resistant MFA).
3. Don't expose RDP (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.

As we mentioned before, around 83% of ransomware incidents we identified used a self-installation attack vector to gain an initial foothold on a computer running the Windows OS.

You can 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 primary entry point for ransomware — and for a lot of other threat types! Note that PowerShell files (.ps1) already open by default in Notepad.

We also regularly see attackers using another pesky attack vector, Excel 4.0 macros, to gain initial entry. Microsoft supports Excel 4.0 macros in all versions of Microsoft Office. However, 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 org.

Microsoft also recently announced that they'll provide more granular controls for macros, ActiveX content, and Office add-ins in emailed Office docs starting in early February 2022.

The TL;DR here is that IT administrators should set policies that block active content in Office docs that arrive by email.

We also recommend that orgs deploy MFA everywhere — preferably using phish-resistant FIDO security keys. This is *really* worth the investment. Also: don't expose RDP (or any other services you don't need to) directly to the Internet and make sure to patch and update regularly.

One last piece of advice: have a ransomware incident response (IR) plan and test it!

A real-life security incident isn't the best time to test your IR plan. We think a great IR plan emphasizes roles and responsibilities, communication, reporting, how to handle data, and how to prepare for the emotions your team will experience. Stress test your plan regularly — we recommend once a quarter — to make sure everyone knows what to do when a bad thing happens. Dare we say you can even make IR testing fun? We made it far more interesting by turning it into a game.

A real-life security incident **isn't the best time** to test your IR plan.

Looking ahead

The launch of StopRansomware.gov, the first U.S. government interagency initiative to address the growing threat of ransomware, was a big deal. We're excited and encouraged by the amount of intel sharing we're seeing as a result.

But products must become more secure by default to counter rising ransomware attacks. Ransomware gives attackers a lucrative opportunity to monetize access to a network. Vendors must do more to make it easier for the good side to win here.

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. This is the way. (We may be big Star Wars fans here...)

Secure by default is how we'll make the most progress in mitigating the self-installation attack vector. Unfortunately, we think the ransomware upward trend will continue to increase until secure by default becomes the rule vs. the exception.

Remember, with the advancement of good comes the advancement of evil. Attackers will drop using Excel 4.0 macros for a new attack method that works. Stay vigilant.

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

Let's Chat

Supply chain targeting

Here's the deal...

2021 sent us a bunch of reminders that you just can't trust the Internet. As a security professional, you know this already. But, it turns out, we place a lot of trust in the software and services we use every day that connect to the Internet.

Much of the incident data and learnings we've shared to this point have followed a common pattern: a threat actor chooses a target, then launches a phishing attack or exploits a system that's accessible via the Internet to gain initial access. What happens next depends on the attacker's motivation.

But when a large percentage of widely-used apps and websites rely on a compromised provider or software repository? Not good.

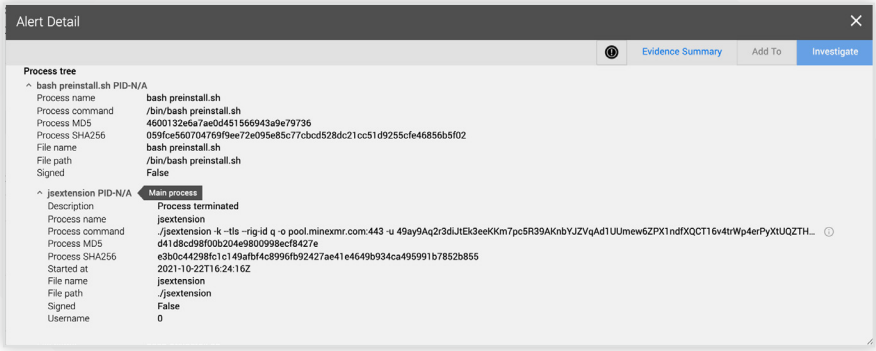
Let's walk through an example and we'll share ways you can protect your org.

What we saw last year

Compromised NPM (node package manager) package, ua-parser-js

On October 22, 2021, a threat actor compromised a popular NPM package (ua-parser-js) by compromising the developer's account and uploading malicious versions of the ua-parser-js package. Installing evil versions of the package resulted in the deployment of a coin miner and, in some instances, a backdoor. It was a big deal.

When servers pulled down and executed the malicious ua-parser-js package, we generated an alert for a script that launched with command line arguments typically seen with XMRig coin miners.



Expel Workbench alert for compromised NPM package that resulted in deployment of the Monero coin miner

The alert was just the starting point. We then answered two *really* important questions:

1. *When* did the evil coin mining script get there?
2. *How* did the evil coin mining script get there?

TL;DR: You can't trust the Internet. You knew this already. But asset management and a tested IR plan can help your org stay ahead.

What we saw last year

- Popular open source repositories were compromised to deploy coin miners.
- Asset management was critical for responding to supply chain compromises like Kaseya.

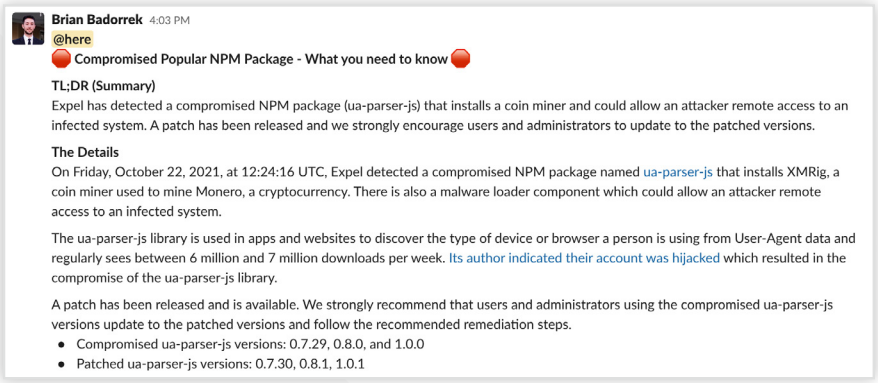
How to protect your org

- Plan for supply chain attacks — run a tabletop IR.
- Have plans for alternative supply chain providers.

A quick investigation of process and file creation activity uncovered that the malicious coin mining script landed on the system when a seemingly compromised version of the NPM package named ua-parser-js was downloaded and installed.

When dealing with a supply chain attack on an NPM package that's downloaded from an open source repository over seven million times each week, mitigation becomes the top priority to minimize damage. For something of this magnitude, we armed our customers with information about the attack and what they needed to do to stop it.

Here's how that played out in practice:



Brian Badorrek 4:03 PM

@here

Compromised Popular NPM Package - What you need to know

TL;DR (Summary)

Expel has detected a compromised NPM package (ua-parser-js) that installs a coin miner and could allow an attacker remote access to an infected system. A patch has been released and we strongly encourage users and administrators to update to the patched versions.

The Details

On Friday, October 22, 2021, at 12:24:16 UTC, Expel detected a compromised NPM package named ua-parser-js that installs XMRig, a coin miner used to mine Monero, a cryptocurrency. There is also a malware loader component which could allow an attacker remote access to an infected system.

The ua-parser-js library is used in apps and websites to discover the type of device or browser a person is using from User-Agent data and regularly sees between 6 million and 7 million downloads per week. Its author indicated their account was hijacked which resulted in the compromise of the ua-parser-js library.

A patch has been released and is available. We strongly recommend that users and administrators using the compromised ua-parser-js versions update to the patched versions and follow the recommended remediation steps.

- Compromised ua-parser-js versions: 0.7.29, 0.8.0, and 1.0.0
- Patched ua-parser-js versions: 0.7.30, 0.8.1, 1.0.1

Customer-wide notification Expel sent about the compromised NPM Package, ua-parser-js, and what to do

In summary: a behavioral alert, backed by sound investigative processes, uncovered an ongoing supply chain attack that resulted in recs to our customers on how to take mitigating action *before* experiencing negative downstream consequences.

Detection opportunities

How do you detect something like this before the issue is publicly known? You build, deploy, and continuously improve alerting for behavioral patterns that suggest something is amiss.

For the most part, you don't detect the zero-day exploit — you alert when your Microsoft Internet Information Services (IIS) worker process spawns a Windows cmd shell, then spawns a PowerShell download cradle.

You constantly ask questions like: "What would it look like if our web app is compromised?" and "Do we have the right level of visibility into those systems?" and "Can we simulate an attack against that system to build or improve detection workflows to better protect those systems?"

You can try and detect the zero-day, but your time is likely better spent building detection workflows to alert when something's amiss.

Build, deploy, and continuously **improve alerting for behavioral patterns** that suggest something is amiss.

How to protect your org

Here are some things you can do:

1. Plan for supply chain attacks. The term “supply chain” can mean different things to different orgs, but for many tech companies, your supply chain includes a long list of cloud services that facilitate your day-to-day business.
2. Have plans for alternative supply chain providers. We’re not saying you need to have a hot backup for all your cloud services. But you should at least plan for rapid provider shifts if a catastrophic event happens. This should be largely in line with your business continuity plans (which you’ve tested — right?).
3. Prioritize asset management. When you learn about a compromised major vendor or software repository, you must be able to effectively answer, “Are we impacted?”
4. Be creative. Failures of imagination are a real thing. It can be difficult to dream up attacks like SolarWinds Orion or vulnerabilities like Heart Bleed. When planning tabletops, ask people around your company: “What’s the worst thing that could happen?” You might be surprised by the scenarios others are worrying about.

Looking ahead

We don’t think supply chain attacks are going away. In fact, if the total cryptocurrency market capitalization continues to increase, we predict that supply chain attacks targeting popular open source repositories will also increase as a method to deploy coin miners on a massive scale.

Want to learn more about how Expel can help with **supply chain targeting**?

Let’s Chat

Cryptojacking

Here's the deal...

Exploitation of web apps to deploy cryptocurrency coin miners was the free Red Team the Internet needed in 2021. Cryptojacking incidents push orgs to patch vulnerable systems — and by doing so, remove a potential entry point for something more evil like ransomware.

Of the web app compromises we investigated that resulted in deployment of a coin miner in 2021, orgs took recommended actions to patch the exploited vulnerability 100% of the time.

What we saw last year

Thirty-five percent of web app compromises resulted in deployment of a coin miner.

Attackers typically exploited vulnerabilities that were one to three years old, with CVE-2019-9193 at the top of the list.

So here's the key takeaway: for the most part, we didn't see cryptojacking incidents result from the weaponization of a zero-day or one-day vulnerability. Threat actors instead used older, known vulnerabilities that were left unpatched on internet-facing servers.

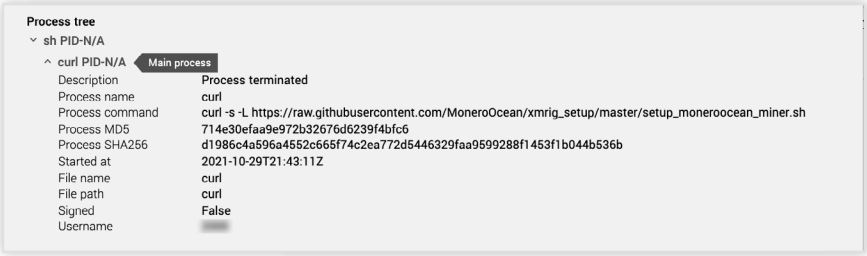
In terms of OS distribution, we saw a 50:50 split between compromised Windows and Linux servers. This isn't surprising given we're talking about internet-facing servers running popular web apps.

XMRig was the most prevalent miner, accounting for 26% of all cryptojacking incidents, with miners for the NiceHash, Bitcoin, and Ethereum blockchains accounting for the rest.

Detection opportunities

To spot someone stealing your org's computing power to mine for coins, you can set up alerts for process command line arguments, strange process lineages, or network connections to well-known crypto mining pool domains or to access crypto mining utilities.

In the example below, a Bourne shell launched the curl utility to download Monero crypto mining malware from a GitHub repository.



Expel Workbench alert for cryptojacking

TL;DR: 35% of web app compromises we identified resulted in crypto miner deployment. Orgs that experienced these incidents patched the exploited vulnerability 100% of the time, also removing a potential entry point for ransomware.

What we saw last year

- 35% of web app compromises deployed a coin miner.
- Attackers mainly exploited one to three-year-old vulnerabilities.
- 100% of orgs remediated and mitigated exploited vulnerabilities.
- XMRig accounted for 26% of all cryptojacking incidents.
- Monero, NiceHash, Bitcoin, and Ethereum coin miners accounted for the rest.

How to protect your org

- Patch and update regularly.
- Consider services like Shodan and Censys to see what the Internet can see about your attack surface.

You can use EDR, SIEM, or network tech to build tactical alerts like this, as well as behavioral alerts. We think tactical alerts (like a connection to a crypto mining pool) have value, but behavioral detections to spot when a web app does something that it doesn't typically do (like spawn a shell) are far more comprehensive.

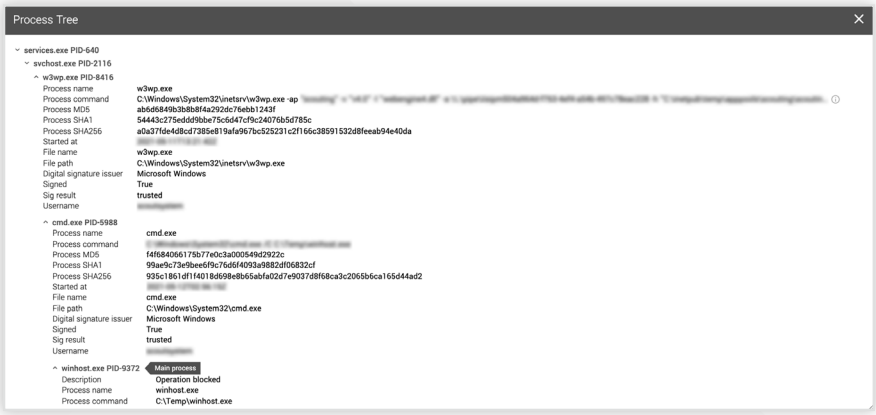
Top behavioral patterns

Here are some top behavioral patterns we alerted on to spot web app compromises that resulted in cryptojacking:

Alert when...

- The IIS worker process, w3wp.exe, or any other web server process running on Windows spawns a process that can interpret and execute code like cmd shell or PowerShell.
- The Apache server process or any other web server process running on Linux spawns a shell like bash or Bourne.
- A database process like postgres spawns a Dash shell.

In the example below, we saw that the IIS worker process spawned a cmd shell to execute "C:\Temp\winhost.exe". Our investigation uncovered that threat actors exploited the CVE-2019-18935 vulnerability to deploy XMRig.



Expel Workbench process tree for web app exploitation to deploy XMRig

Investigator's tip: if you're responding to a server infected with any type of malware (regardless of its role), answering the question, "How did the malware get there?," is a critical step to understand the potential scope and impact of the incident.

When investigating a server infected with malware, first consider: 1) What's the role of the server and 2) How can someone access the server?

The answers to these questions will help your investigation.

How to protect your org

Highly effective patch management is rooted in asset management. You can't patch or update systems you don't even know you have.

We highly recommend checking out services like Shodan and Censys to learn more about the services and devices your org has connected to the Internet. Shodan monitor even lets you set up notifications and initiate scans (again, not sponsored... we're just fans!).

Other steps you can take:

1. Implement network layer controls to detect and block network communications to crypto mining pools.
2. Forward computing resource alarms to your SIEM to alert your team of overtaxed resources potentially deployed for cryptojacking.
3. Confirm your EDR coverage across all your endpoints.

Looking ahead

Unfortunately, we expect this problem to worsen. As cryptocurrency market cap increases, so do the potential profits for prospective attackers.

Financially-motivated threat actors predictably follow the money, so defenders must prepare. Fortunately, attacker entry points for cryptojacking overlap with those for other threat types like ransomware, so focused efforts to reduce your cryptojacking attack surface can help protect against multiple problems.

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

Let's Chat

Looking ahead to 2022...

Thoughts from our leadership team

ATTACK TRENDS

"**Nation state use of cyber attacks continues to evolve**. For example, last year we saw multiple instances of state-driven cyber attacks targeting infrastructure that impacts the broader civilian population. The line of 'acceptable' in the realm of nation state cyber operations continues to move, and different countries draw that line in a variety of ways. Expect to see more lines moving in 2022." **— Dave Merkel, Chief Executive Officer**

"**'Secure by default' operating systems and applications will move security forward for almost every class of attack**. Microsoft announcing its intent to disable legacy protocols in Office 365, to disable Excel 4.0 macros by default, and to give IT professionals more granular control over active content in email attachments are important initiatives that will have a massive impact. Let's not forget that Microsoft also put an end to domain fronting in Azure in 2021. Initiatives like this make it harder for threat actors. But always remember, with advancement of good comes the advancement of evil. Stay vigilant." **— Jon Hencinski, Director, Global Operations**

"Ransomware used to be a primary method of attack, so data encryption and ransom would occur immediately after infection. But we now see more and more attackers using ransomware as a way to maximize profit after they've extracted as much other value as they can from an environment. Instead of maintaining access, attackers tack on ransomware after they achieve their initial goal, whether that's credential access or data exfiltration. This behavior has literally paid off, so **we'll likely see more ransomware appearing at the end of attacks not traditionally associated with ransomware** — for example, business email compromise." **— Ben Brigida, Director, SOC Operations**

"It's only a matter of time until we see a surge of attacks in cloud-based environments. **There will come a point when common attack tactics like business email compromise are less accessible and profitable, and we'll see threat actors become more focused on cloud providers** like Google Cloud Platform (GCP), Azure, and Amazon Web Services (AWS) as a result. Now more than ever, it's critical to make sure you're adhering to security best practices, including testing detection and response capabilities." **— Ray Pugh, Manager, Security Operations**

"**As the total market cap of cryptocurrency continues to rise, increased cryptojacking will follow**. And the growing financial incentives will only entice more cybercriminals to participate. The silver lining here is that, by taking cryptojacking incident remediation seriously, organizations remove a potential entry point for ransomware." **— Jon Hencinski, Director, Global Operations**

EVOLVING SECURITY OPERATIONS

"We're seeing security operations centers (SOCs) and security operations in general become increasingly data-driven. **Security ops will continue to shift away from measuring things like volume towards more meaningful measures of efficiency and effectiveness that drive operational decisions to balance speed and quality**. We're also shifting away from basic visibility and detection measures towards metrics that answer questions like 'what did we do right, what did we do wrong, and what could we do better?' These types of metrics can drive iterative improvement across detection, investigation, response, and remediation." **— Yanek Korff, Chief Operating Officer**

"Security operations will continue to work more hand-in-hand with the rest of the technical operations of a business. This is going to drive greater demand for people with varied backgrounds — in particular, **experience with software development, DevOps, and cloud technologies will become increasingly valuable**." **— Matt Peters, Chief Product Officer**

"Organizations will continue to see increased interconnectivity between departments, teams, and their technologies. This is especially true as they adapt to the new normal, which involves supporting a hybrid workforce and, as a result, adopting more cloud-based solutions. **Security operations teams will need to expand their primary focus from threat detection to proactively analyzing their company's tech stack — looking for risky behaviors, misconfigurations, violations of best practices, and so on.** When they identify risks, they'll need to respond with the same swiftness as they respond to ransomware, because these activities represent opportunistic attack vectors that can be exploited by bad actors." **— Peter Silberman, Chief Technology Officer**

CYBERSECURITY TALENT

"Cybersecurity skills are always in demand, and the 'Great Reshuffle' will encourage companies to think differently about their recruiting practices. **There's an influx of people entering security from nontraditional backgrounds and the way people gain skills has changed — a college degree isn't the only path**. Identify 'launch roles' where you can hire for traits and train for skills. Partner with coding bootcamps and other organizations that focus on bringing underrepresented groups into tech and security. These are great first steps towards finding your next amazing hires. Plus, welcoming a diversity of ideas and experiences drives creativity and strengthens a team." **— Amy Rossi, Chief People Officer**

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

2021 at Expel

Awards

- Deloitte Technology Fast 500™, #18
- Exabeam: MSSP/MDR of the Year U.S. and Canada
- Forbes: America's Best Startup Employers
- FORTUNE and Great Place to Work®: Best Medium Workplaces 2021
- FORTUNE and Great Place to Work®: Best Workplaces in Technology 2021
- FORTUNE and Great Place to Work®: Best Workplaces for Millennials 2021
- FORTUNE and Great Place to Work®: Best Workplaces for Women

Industry Recognition

- The Forrester Wave™: Managed Detection and Response, Q1 2021
- IDC MarketScape for U.S. Managed Detection and Response Services
- Gartner 2021 Market Guide for Managed Detection and Response Services
- Aite-Novarica Group Threat Hunting Impact Report

News

- Series E Fundraise and $1B+ valuation
- Partnership with Out in Tech
- Partnership with Blacks In Technology Foundation

Product and Feature Launches

- Expel Workbench™ for Amazon Web Services
- Expel for Microsoft
- Hunting in the cloud

Top Attack Vectors from our SOC

- December 2021
- November 2021
- October 2021
- September 2021
- August 2021
- July 2021

Appendix

Appendix A: Alert-to-fix times

There's nothing more strategic than defining where you want to get to and measuring your progress. Strategy informs what "good" means and measurements tell you if you're there or not.

When we set out to build our SOC here at Expel, we set a target that for every incident we identify, we'll respond faster than pizza delivery (30 minutes or less!).

For 2021, our median alert-to-fix time across critical incidents was 21 minutes. Our fastest time was 55 seconds.

We define alert-to-fix time as the time between when an Expel alert arrives in our queue and the first remediation action is assigned to (or performed on behalf of) the customer.

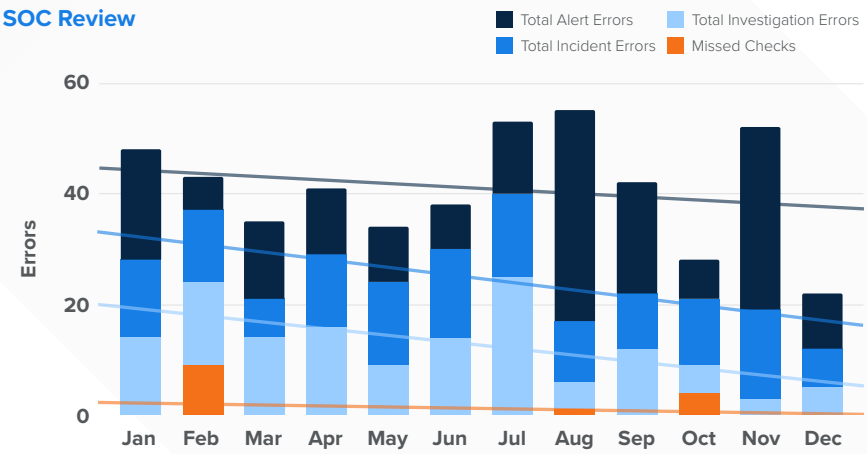
Appendix B: SOC quality control

There's a common assumption that you have to choose between scale and quality.

When we set out to build our SOC here at Expel, we didn't want to trade quality for efficiency — it just didn't feel right.

Every day, we perform a QC check based on a set of manufacturing standards to answer: "Is our work quality improving or are things getting worse?" You can find out more about our SOC QC program here. The graph below shows trend data for errors across our categories of work performed in 2021.

The outcome? Our SOC quality improved as we scaled.



expel

Ready to talk to a human?

www.expel.com/contact-us

844.397.3524