CYREBRO

2022 Attack Vector Landscape Analysis

TABLE OF CONTENTS

Introduction

Looking back at the world of cybersecurity in 2021

In the age of COVID-19, security issues have come to the front all around the world. As remote work becomes more common, the attack vector grows and the fear of a data breach grows. Now is a time of change in the world of security and CYREBRO is making sure that its users stay one step ahead of the malicious actors who are out to cause damage to unsuspecting businesses.

The Research Approach

To provide more context to the cyber trends seen across the globe, CYREBRO collected data from over one million computer entities, and analyzed the number of events, alerts, and cases we have intercepted and investigated from the beginning of 2021. We also took a more holistic look at the range of investigation types and threat vectors that appear in the data.

This report shows CYREBRO's findings throughout 2021. Our data has been collected through our interactive managed SOC platform for a select group of over a million computer entities that offer a representation of the market, including SMBs and enterprise organizations, as well as a wide array of industries.

ORGANIZATIONS ANALYZED BY CYREBRO

12
Industry Sectors

200
Companies

Micro
SMB
Large
Enterprise

Key Findings

Vulnerability exploitation, not phishing, was the top threat vector

Software and IT are at the biggest risk for attacks, accounting for 25% of attacks across all sectors

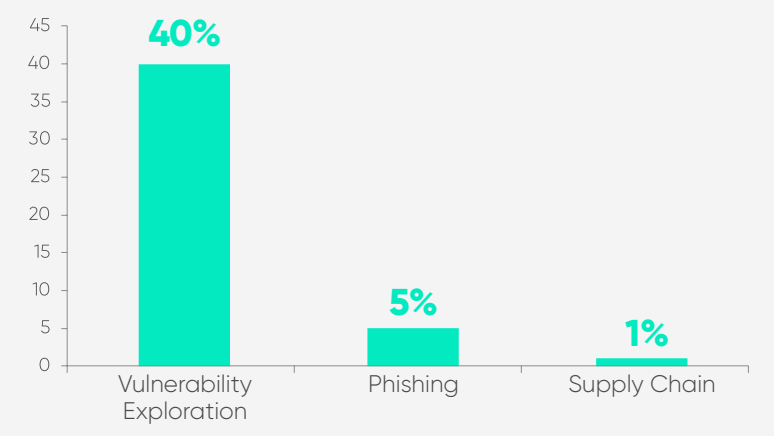
81%

of phishing attacks were on SMBs

40%

the increase in investigations for SMBs from Q1 to Q4

Top 3 Threat Vectors



46%
of attacks come from vulnerability exploitation, phishing, and supply chain attacks

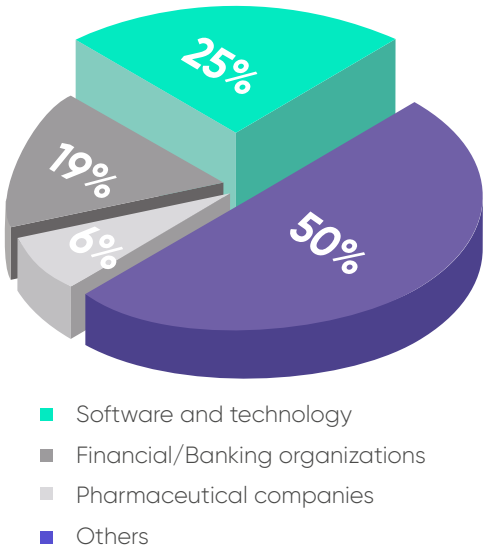
We first analyzed the most frequently occurring threat vectors across all computer entity data, in order to provide more insight into the threat vectors that companies in different sectors are facing.

1. VULNERABILITY EXPLOITATION

Despite the unavoidable presence of phishing in our day-to-day lives, vulnerability exploitations have grown to become the most common threat vector in 2021. With 18,325 vulnerabilities discovered across the industry in 2020, this growing section of the threat landscape is our top concern for businesses of all sizes.

Since the beginning of 2021, 40% of attacks that CYREBRO investigated have been based on vulnerability exploits; this stark increase from 2020 shows that a considerable number of attacks are coming from sophisticated threat actors who have the technical know-how to push a security team to its limits.

Of the vulnerability exploitation attacks that CYREBRO intercepted across our top three sectors, 25% of them were against software and technology companies and 19% against financial/banking organizations. Despite media coverage around cybercriminals and attacks on medical organizations, attacks on health and pharmaceutical companies only accounted for 6% of attacks.



Vulnerability exploitations refer to exploits in software or web apps that allow attackers to access sensitive data. Examples include SQL injections and poorly built software such as the slew of exchange server issues in 2021.

HOW DO VULNERABILITY EXPLOITATIONS HAPPEN?

Vulnerability exploitation can occur almost anywhere in a business, but the most common attack vectors include:

- **Legacy servers**, namely out-of-date Windows-based and Linux-based servers that have not been updated to tackle threats known to the cybersecurity community. Multiple critical updates have been rolled out for both of the main server types throughout the year in order to stop exploitation.
- **Exchange servers** have been targeted throughout 2021, most notably the various attacks against Microsoft's Exchange Servers throughout the year. High-profile attacks include the suspected Chinese-backed attack on Microsoft servers in July.
- Known weaknesses in **Firewall vendors** have become a major flaw in the security posture of businesses that thought commercial solutions would act as a layer of defense against ransomware, exploits, and other malicious threats.

DEFENDING AGAINST VULNERABILITY EXPLOITATIONS

Within any given enterprise, the risk of vulnerability exploitation is measured through intelligent risk assessment tools that provide risk scores and assessments of how best to approach the problem. But preparing to understand your vulnerabilities can be tackled through the MITRE ATT&CK Enterprise Matrix. From here, discovering known best practices for handling vulnerabilities in your setup and how to harden it.

There are valuable tools for both red and blue teams, but some of the most important processes include:

- The most integral part of defending against vulnerability exploitations is updating and patching existing systems. Security professionals must update software to mitigate a wide range of security issues such as known vulnerabilities and corrupt software.
- M1045 - **Code signing** stops internal threat actors from changing important code by requiring all edits to be signed. This means that disgruntled employees will be held accountable if they attempt to maliciously modify the system, discouraging them from acting on impulse.
- M1056 - Vulnerability scanning **pre-compromise preparation**; closing the attack vector is the only effective practice to stop adversaries from finding entry points and taking control of sensitive data.

Staying up to date about the latest vulnerabilities is another way to avoid exploitation. CYREBRO's threat intelligence team regularly publishes Critical Threat Intelligence Alerts (CTI Alerts), with the goal of sharing information about the latest threats and vulnerabilities, as well as recommended mitigation tactics and patches, because we believe access to good cybersecurity should be available to all.

2. PHISHING

Despite the unavoidable presence of phishing in our day-to-day lives, vulnerability exploitations have grown to become the most common threat vector in 2021. With 18,325 vulnerabilities discovered across the industry in 2020, this growing section of the threat landscape is our top concern for businesses of all sizes.

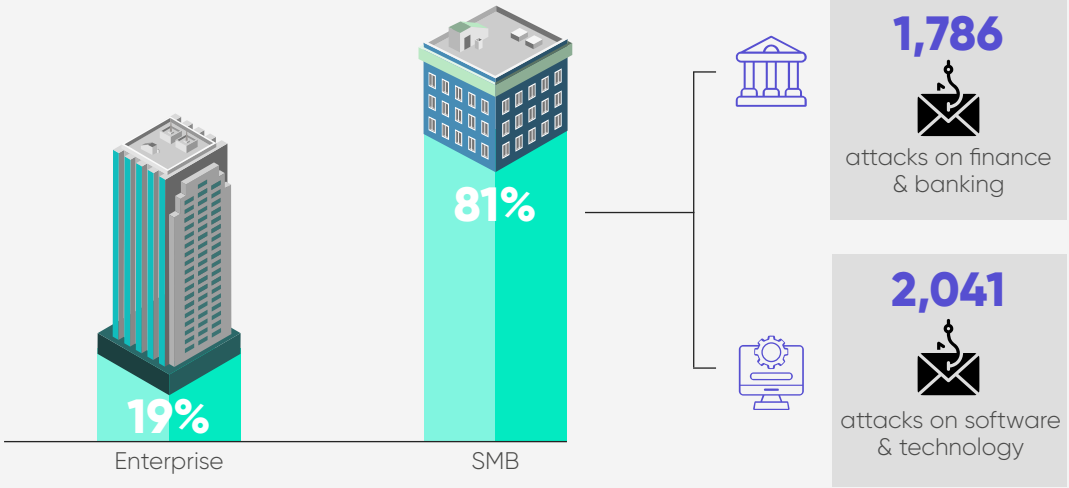
Formerly the most common type of cyberattack, phishing in its various forms is well-known to most people. Although removed from its former top spot, the COVID-19 crisis has led to an overall increase in phishing attacks.

Now accounting for 5% of all attacks, a total of 10,503 cases, that CYREBRO investigated in the sample data, phishing attacks saw a sharp increase in 2020 and continued to be a pain for both businesses and the wider public.

With SMBs making up 81% of all the phishing attacks, we found:

- 1,786 phishing attacks against finance/banking SMBs, and
- 2,041 phishing attacks against software and technology SMBs.

Phishing attacks by company size



In addition, a large amount of phishing attacks go unreported. Although CYREBRO has intercepted and analyzed over 3,000 phishing attacks last year, the true number of attempts is likely much larger.

Although making up a much smaller section of the overall threat landscape, 75% of all businesses reported experiencing phishing attacks with big names like Microsoft, DHL, and LinkedIn amongst the most common spoofed sources for phishing emails or smishing attacks.

HOW DOES PHISHING HAPPEN?

The three most common types of phishing are:

1. **Standard phishing** is sending out emails with the intention of the receiver clicking on a wayward link. That link may trick the user into handing over credentials, PII, or otherwise let threat actors access the system.
2. **Spear phishing** is a phishing attack that has a particular target, generally a high-profile member of an organization or a celebrity. Attackers may use obfuscation to trick a non-technically literate CEO into believing a malicious email has been sent by a security professional within the company.
3. **Whale phishing** is spear phishing that is solely focused on catching "whales" within an organization - C-level executives, administrators, and any other high profile individuals within an industry.

Phishing threats are social engineering attacks that prey on naive employees and lead to severe data breaches when targeted through spear or whale phishing attack techniques.

DEFENDING AGAINST PHISHING

The MITRE ATT&CK framework can be used to explain the attack cycle and offers known solutions to the problems. When used intelligently, defending against phishing attacks is possible through these five techniques.

- M1021 - **Blacklisting/restricting content** manually creates a list of known dangerous sources, but it is resource-heavy to maintain. This tactic should be used in addition to another security measure.
- M1031 - **NIPS** (network intrusion protection system) that can detect malware that attempts to compromise the system.
- M1049 - Effective **anti-virus/anti-malware** solutions that detect known phishing campaigns and the associated malware.
- M1054 - **Software assisted configuration** such as anti-spoofing methods and authenticating software stop malware as soon as it is recognized
- Effective **user training**. Training employees to recognize and avoid the risk of phishing.

3. SUPPLY CHAIN ATTACKS

As multinational corporations gain better cybersecurity defenses, threat actors find that gaining access through conventional means like vulnerability exploitations or phishing attacks becomes more difficult. Advances in security technology have made them easier to detect and now the adversary is turning to the supply chain to move the threat outside an organization's area of control.

Instead of wasting time by focusing on finding a weakness in the Fort Knox-like defenses of a well-defended company, looking further down the supply chain is an easy way to find a way in. Software supply chain attacks i ncreased by 650% in 2021, with an emphasis on next generation attacks, where bad actors are proactively injecting vulnerabilities into open source projects.

Making up 1% of all attacks logged and recognized by CYREBRO, supply chain attacks are often difficult to identify until it's too late. Enterprise-level companies are particularly exposed due to the greater number of tools, endpoints, and individual users, a quarter of our enterprise-level technology clients facing supply chain attacks.

HOW DO SUPPLY CHAIN ATTACKS HAPPEN?

Security teams need to identify threats outside of their area of control which requires extensive threat hunting capabilities - something that not all companies place enough emphasis on.

Targeting weaker components in the overall chain of supply allows adversaries to circumvent otherwise hardened cybersecurity measures by causing problems in the tools, software, operating systems, and other services that the companies rely on.

As an allegory, imagine this was a warzone. Instead of trying to destroy a whole tank, the attackers focus on compromising the bolts that hold it together - the same is true for cybersecurity professionals who find their security posture is surprisingly weak against ransomware infections or can't implement proper accounts management procedures.

DEFENDING AGAINST SUPPLY CHAIN ATTACKS

Successful threat hunting campaigns can stop threats from targeting an attack on vendors further down the supply chain. Organizations need to focus their threat-finding missions on their own vendors and the security posture of the vendors. To use a number of tools for threat hunting missions effectively, security professionals must also gather information about threats from published reports.

To find best practices for defending against supply chain attacks, the MITRE ATT&CK framework includes two methods for hardening your systems and protecting valuable assets:

- M1016 - Running your own **vulnerability scanning** software to identify weaknesses in your security posture before adversaries capitalize on them. This is especially useful when identifying tools or software that are frequently targeted by cyber-criminals.
- M1051 - **Update software** to identify compromised tools, development environments, repositories, applications or operating systems, or even hardware that has been tampered with.

Threat Vectors to Keep an Eye on

A variety of other attacks make up plenty of the general, non-security-focused media's coverage of the risks that security professionals face every day, but they make up a comparatively smaller proportion of the overall attacks that threaten the security posture.

Accounting for over 50% of all attacks that CYREBRO responded to and prevented, these vectors were less prominent than our findings about vulnerability exploitations, phishing, or supply chain attacks. The list of other attack vectors is non-exhaustive.

In accordance with the MITRE ATT&CK framework, these practices have corresponding best practices for cybersecurity professionals. These are listed underneath the threats themselves.

BRUTE FORCE ATTACKS aim to access systems by guessing passwords through software that input a large number of password attempts automatically.

To battle password guessing tactics like **brute force attacks**, the following methods are

effective:

- M1018 - **User Account Management** is used after a known breach within an organization, resetting the account that has been compromised or was subjected to a brute force attack.
- M1027 - **Password policies** should be in place to create strong and reliable passwords as well as recycle old passwords out of the system.
- M1032 - **Multi-factor authentication** stops password guessing attacks by requiring the user to interact with an additional form of authentication. Hardware 2FA devices or biometric keys are becoming more and more popular each year.
- M1036 - **Account Use Policies** are the processes used to restrict account usage after suspicious activity. For example, the account is locked after 5 failed log-in attempts.

DDOS ATTACKS work by disrupting normal services through an overload of requests to a server. Usually operated through botnets and C&C servers, they can take down a business by forcing the network offline.

- M1037 - In the face of **DDoS attacks**, security teams must quickly and appropriately **filter network traffic**. Depending on the severity of the attack, the problem may be filtered effectively on-site or through the help of 3rd party specialists.

FRAUD is another broad vector that includes many different types of attacks as well as techniques for in-person and virtual infiltration. A variety of methods may be used to gain credentials fraudulently, such as data leaks, malware such as keyloggers, or in-person social engineering infiltration.

- Mitigation techniques depend on the kind of fraud that is carried out. For example, preventative tactics to handle leaked credentials or a sophisticated copy of an ID badge are obviously different. For managing credential fraud, M1027 - **Password Policies** are the best way to stop the risk. This involves forcing new passwords at set intervals, disallowing reused passwords, and implementing strong password practices such as the number and special characters requirements.
- An insider threat is when an internal agent becomes a threat to the system, possibly through radicalization or an employee with a high level of permissions becoming disgruntled. This tactic needs to be mitigated through M1045 - **Code Signing** and effective system modification policies that stop unauthorized changes from being pushed to the network on a system-wide level.

MALWARE covers everything from a simple virus that slows down a system to network disabling worms, ransomware, or botnets that bring a great deal of risk to normal business operations.

- constantly updating software, operating systems, development environments, etc. in order to cut down the amount of known risk that your company faces (M1051) and
- proactively scan your company's vulnerabilities to identify weaknesses that would allow malware to slip through (M1016).

Effective employee training (from entry-level to the C-suite) is also necessary to mitigate the potential for malware exposure.

MISCONFIGURATION can refer to intentional and unintentional weaknesses in individual endpoints or a network that can be used to gain access by malicious third parties. Intentional weaknesses may be configured by an insider threat or a threat actor who has gained permissions.

To stop misconfiguration in your networks, the following policies are recommended by the MITRE ATT&CK framework:

- M1026 - **Privileged account management** follows the principle of least privileges necessary. Even if an administrator's account is compromised, the adversary will not be able to execute malicious code or access sensitive data if the system by default does not allow admin access without a request for credentials.
- M1045 - **Code signing** stops internal threat actors from changing important code by requiring all edits to be signed. This means that disgruntled employees will be held accountable if they attempt to maliciously modify the system, discouraging them from acting on impulse.

- M1046 - Monitoring **boot integrity** stops your systems from running if the operating system is compromised. This stops backdoors, kernel-level threats such as rootkits and botnets, and protects the network in case of infection.

RANSOMWARE is probably the most infamous type of cybersecurity attack thanks to high-profile attacks such as WannaCry and the REvil attacks.

Ransomware in the media

Looking at the Colonial Pipeline ransomware attack on May 7, 2021, we can see the destructive nature of these security issues. The attack stopped the American-based oil pipeline company for a week and caused several problems in Texas.

Because the cyber-attack was so successful (from the perspective of DarkSide, the Eastern European threat actors), the oil industry giant was forced to pay out $4.4 million. This mighty figure was paired with the related data leak that had occurred a few days prior - an estimated 100GB of sensitive data was stolen by the cybercriminals in this pair of targeted attacks.

CYREBRO Investigation Data: A Deeper Dive

Here we are presenting a full breakdown of the number of events, alerts, and investigations that were reviewed, and how this data reflects what is being felt across the cybersecurity industry at large, and observations about the trends we have seen.

From the large number of events that we have monitored, the cases we've investigated, and the real-life impacts that have been felt by our customers, we have an in-depth view of the real-time changes occurring in the cyber space, and their potential impacts for businesses in the future. These insights enable CYREBRO to adapt to and proactively defend against the adversaries who threaten our customers.

CYREBRO collected data from over one million computer entities, and analyzed the number of events, alerts, and cases we have intercepted and investigated from the beginning of 2021, as well as the full investigations that we have launched in the name of protecting our clients and their data.

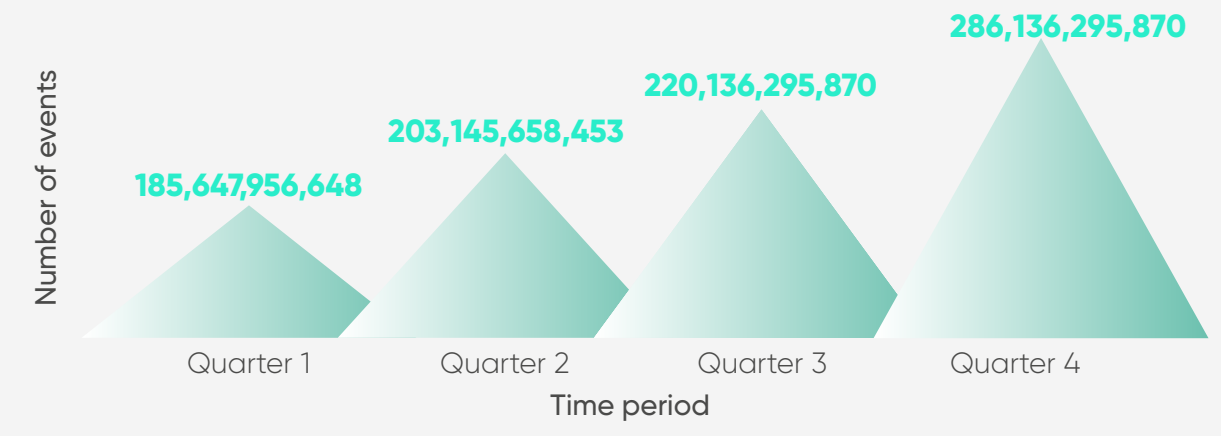
TOTAL NUMBER OF EVENTS

Event: An event is any log that is processed from computer entities. It's an observed change to the normal behavior of a system, environment, process, workflow, or person.

After reviewing events from over 1 million computer entities since the beginning of 2021, we're seeing a steady increase in the number of events monitored, amounting to an 18.6% increase in the number of investigations from the first quarter to the third quarter.

54.1%

increase in the number of events from the first to fourth quarter

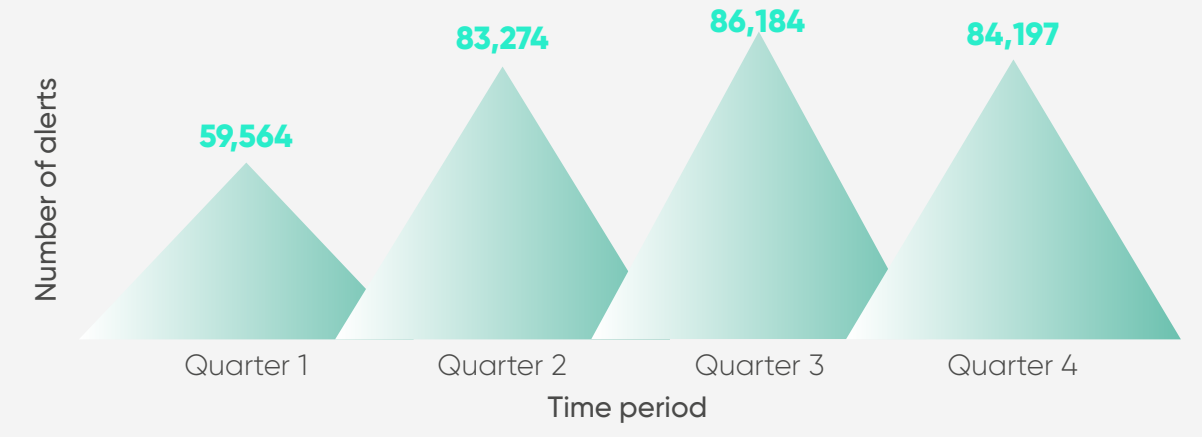


*Over 1,000,000 computer entities monitored

TOTAL NUMBER OF ALERTS

Alert: An alert is one or more events that correlate to a programmed alarm rule within the SIEM. Events are correlated to create alerts.

In 2021, we saw a consistent uptick in the number of alerts within the sample that CYREBRO observed. With 313,219 alerts logged throughout 2021, we saw a continuous increase in the overall number of potential threats that our customers are facing.



*Over 1,000,000 computer entities monitored

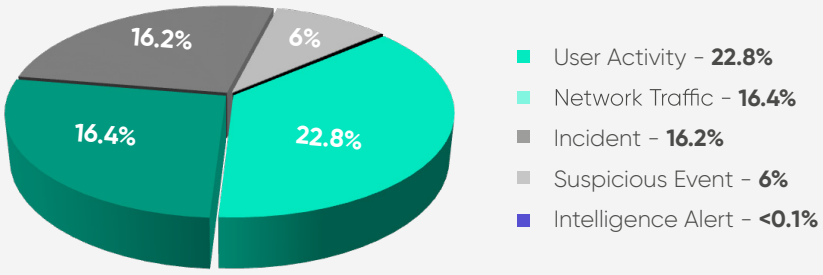
This growth in alerts has not meant that our false positives have become unmanageable - actually the opposite. Each quarter, we are refining our logics and tools to help cut out the white noise and find only the genuine threats. Our SIEM technology has been updated to include 859 rules, of which 453 are new since June 2021. This improved ruleset allows the CYREBRO team to better recognize and analyze potentially malicious events that appear on our clientele's end-points, including better automatic responses to known threats.

CYREBRO Investigations By Quarter in 2021

QUARTER 1

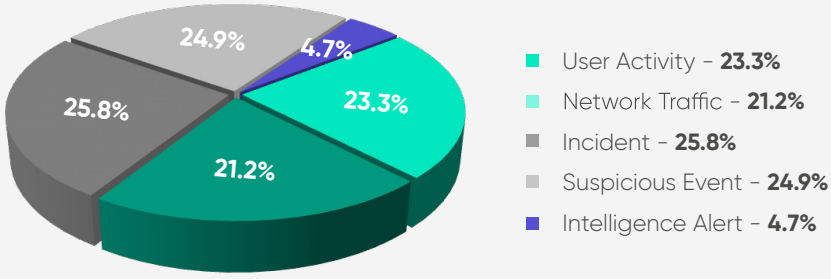
In the first quarter of 2021, CYREBRO mainly found that user activity (including events such as a new user being added to an admin group or lateral movement across a network) was the most prevalent event type that warranted investigation.

We can see a high level of vulnerability exploits that have allowed adversaries to engage in lateral movement after a breach as well as threats related to potentially malicious packages being sent to or even through the network. Taking suspicious emails to stand for phishing in this situation, it is clear that CYREBRO's clients are experiencing fewer phishing attacks than we would expect from the industry's 2020 data.



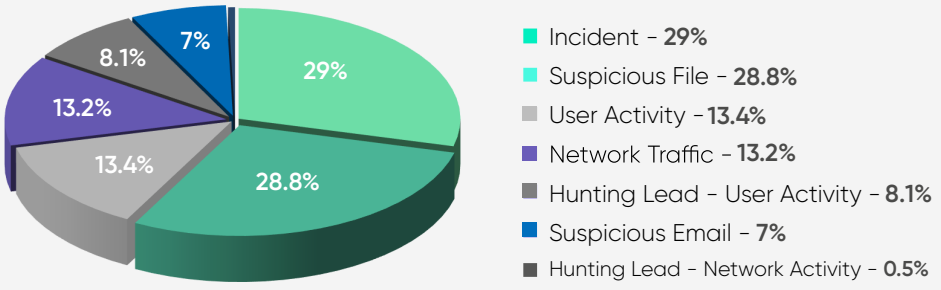
QUARTER 2

The second quarter of 2021 saw an increase in suspicious file investigations and a steady level of user activity threats.



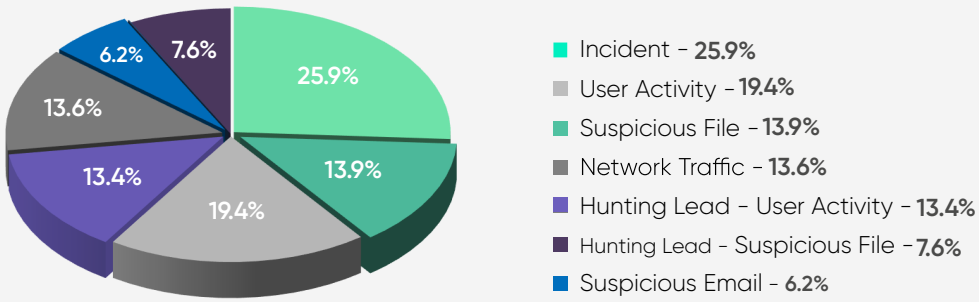
QUARTER 3

With the growth in "incident" investigations, we can see that adversaries are trying new methods that gain access to sensitive data. We also saw more suspicious files appearing on systems, which implies that adversaries are gaining access through phishing attacks or database injections.



QUARTER 4

Up to and including the fourth quarter, we are now seeing a spread of attack types, as well as an increase in incidents identified from threat hunting efforts. This is in part thanks to CYREBRO's continuing improvements in regards to the SIEM optimization, threat hunting, and other security packages, allowing for greater control over the information we glean from the kinds of threats that we are facing. CYREBRO clients benefit from the "crowd wisdom" of insights from other client investigations, and that can be seen by the increase in "hunting lead" incidents as well.



The greatest threats so far have been incidents and suspicious files, matching with our analysis of the security landscape – new vulnerability exploits and phishing are consistently the most common attack vectors that adversaries are using to infiltrate systems and harm our clients. Thanks to CYREBRO's continuously evolving approach to defense, we have stopped and investigated over 15,000 incidents and over 14,000 instances of suspicious files appearing on systems.

Investigation Type Breakdown

USER ACTIVITY

In an effort to identify all human-driven behavior on a network, we have linked any investigation that concerns a user's actions. This investigation type broadly contains everything from administrator interaction with the network to lateral movement across a network by an adversary that has penetrated the primary defences.

NETWORK TRAFFIC

This investigation type is based on events within layers 3 and 4 in the OSI Network Model. As these investigations are only concerned with the Networking and Transport layers, investigations are mostly concerned with suspicious IP addresses or domains being accessed from an endpoint system.

SUSPICIOUS EMAIL

As phishing is amongst the most common threat vectors that we at CYREBRO observed over the last year, suspicious email has been a point of interest for our SOC team recently. Suspicious email investigations cover phishing attacks as well as other email-based abuse such as fraud or impersonation.

INTELLIGENCE ALERT

For investigations that are not based on collected events or information contained within the SIEM such as OSINT investigation or darknet threat hunting, intelligence alerts are logged into the CYREBRO system.

SUSPICIOUS FILE

Regardless of how a suspicious file has found its way onto the network, any investigation that is based around a suspect file is logged under the suspicious file investigation. All investigations that centered around a suspicious file and its legitimacy is logged under suspicious file.

HUNTING LEAD – USER ACTIVITY

When the user activity is of a low level, they are logged as hunting lead – user activity. These user activity alerts are not serious enough to be considered standalone alerts, but they assist in building a fuller picture of an attack story.

HUNTING LEAD – NETWORK TRAFFIC

In the same way that "hunting lead – user activity" alerts are logged separately from general user activity alerts, "hunting lead – network traffic" investigations are low-level OSI layer 3 and 4 investigations that are not considered serious enough to constitute a full alert. Although they may not inform us about a full alert on their own, they are useful as a building block in creating an entire attack story.

INCIDENT

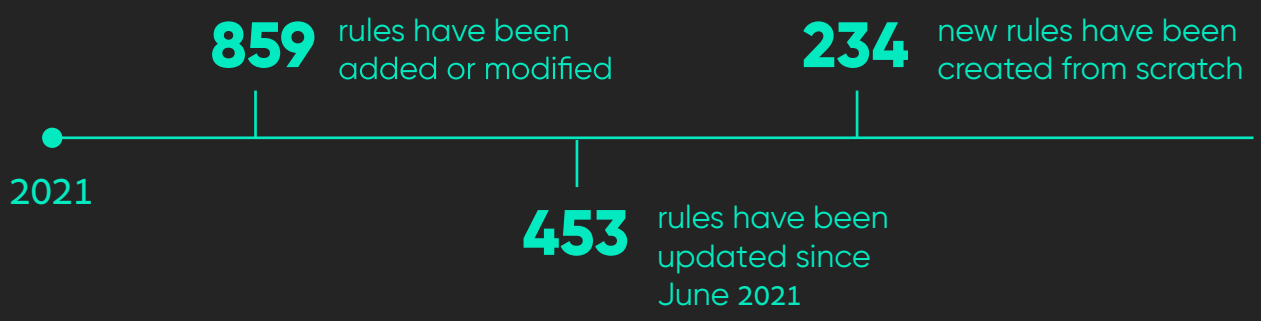
This is the most general of all the categories that we measured. In essence, an incident is anything that the SOC observes that cannot be sorted into another category.

SIEM Optimization

Building and refining the rules that our SIEM uses was an ongoing process over the course of 2021. In 2021 there were 859 rules added or modified in the SIEM, and we are constantly optimizing and tuning them to make the SIEM more effective for our customers.

The ongoing SIEM optimization process has continued with the expansion of our clientele, meaning that our security response is ever-evolving to meet the defensive needs of our customers. This expanded rule list now automatically recognizes risks and known threats, allowing better security responses for all businesses types and sizes.

With CYREBRO's SIEM, our clients have received a continually evolving event management solution that is filtering event data with a greater level of detail than before and alerting important individuals straight away to get the right help our clients need. Our updated logics provide better coverage for major threats as they emerge and stop threat actors in their tracks.



Investigation Reflection on the Industry

VULNERABILITY EXPLOITS IN 2021

As Risk Based Security stated in its 2021 Mid Year Report[1] – Vulnerability QuickView and 2021 Mid Year Report – Data Breach QuickView, there were 12,723 vulnerabilities discovered throughout the course of the last year. Of the vulnerabilities discovered, 1,425 are remotely exploitable and now have a mitigating solution and a shocking 900 vulnerabilities are known to vendors and still unpatched.

As talented adversaries turn to exploitable vulnerabilities to gain access to sensitive data and systems, the number of vulnerabilities that are known to organizations and developers as well as shared or sold on the dark web means that these 900 vulnerabilities[1] are in urgent need of professional attention.

Thankfully, an overall 24% drop[2] in the number of data breaches across the industry shows that more effective defensive measures are in place and are stopping threat actors in their tracks. This has been most clear in the 32% drop from 27.8 billion records leaked in 2020 to 18.8 billion[2] recorded in 2021 – with consistent and intelligent defensive measures such as CYREBRO's SOC/SIEM solution, we have seen a drop in successful breaches, even if the adversary is attempting more attacks across more attack vectors.

PHISHING IN 2021

Classically the most popular attack vector, the number of phishing attacks was consistent over the course of 2021 after a sharp increase in 2020. With 12%[3] of companies facing over 100 individual attempts throughout the year and a total of 200,000[3] phishing attempts in total, this has been the chosen tactic of many adversaries who do not have the technical know-how to penetrate vulnerable systems.

As the FBI reported in 2020, there was a sharp rise (indeed, 11 times as many) in reported phishing attacks from 2016 up to 2020. This has leveled out over the past year and that fits with CYREBRO's research – even though the number of phishing attacks is large in comparison to almost all other attack vectors, it is not eclipsing the very real danger of vulnerability exploitations that are not getting enough attention from software developers and security professionals alike.

Indeed, CYREBRO's own records show a distinct drop in the number of phishing attacks in the 3rd quarter of 2021 in comparison to the 1st and 2nd quarters. For that reason, we now think it is high time that end-user training should now be expanded to help non-security workers from becoming the victim of more advanced threats.

Takeaways

As we have seen over 2021, vulnerability exploits and phishing attacks are still hot topics for security professionals. Dealing with these problems effectively is a never-ending battle of staying one step ahead of the adversary. Using powerful tools like CYREBRO's SOC Platform to identify and stop these threats is a good way for a business to navigate the stormy sea that is the attack vector landscape.

In terms of actionable changes, best practices still dictate swiftly updating all software whenever patches and updates are available as well as training to help workers at end-points to recognize phishing attacks and other behavior which shows the telltale signs of a threat actor who has gained access to the system.
For more robust solutions to these security issues, enlisting proven security solutions such as CYREBRO will help your organization to guard against the ever-changing threat landscape.

About CYREBRO

CYREBRO was founded to help companies take cyber protection to new and unprecedented heights. We revolutionize cybersecurity operations by putting the power of a Security Operations Center (SOC) in the hands of any user in any organization. Our team of cybersecurity experts has developed the industry's first cloud-based, technology-agnostic interactive SOC Platform.

From strategic monitoring to proactive threat hunting, accelerated response, and enhanced compliance, the full scope of needs is covered. With its intuitive interface, and advanced automation and intelligence, the CYREBRO Platform enables all this without the need to invest in new solutions or hire in-house or external experts. Both Fortune 500 companies and SMBs alike can equally and profoundly improve their security posture with clarity, simplicity, and cost-efficiency.

A Complete SOC Solution

CYREBRO integrates all your security tools, solutions and technologies into a single platform, transforming cybersecurity information overload into visibility and meaningful context and clarity in real-time. Managed by the platform's cyberbrain which optimizes the threat-detection and alert process, you get a single, centralized view of all your cybersecurity incidents. You always know which threats affect which assets, how severely, and their root cause.

Learn more about CYREBRO