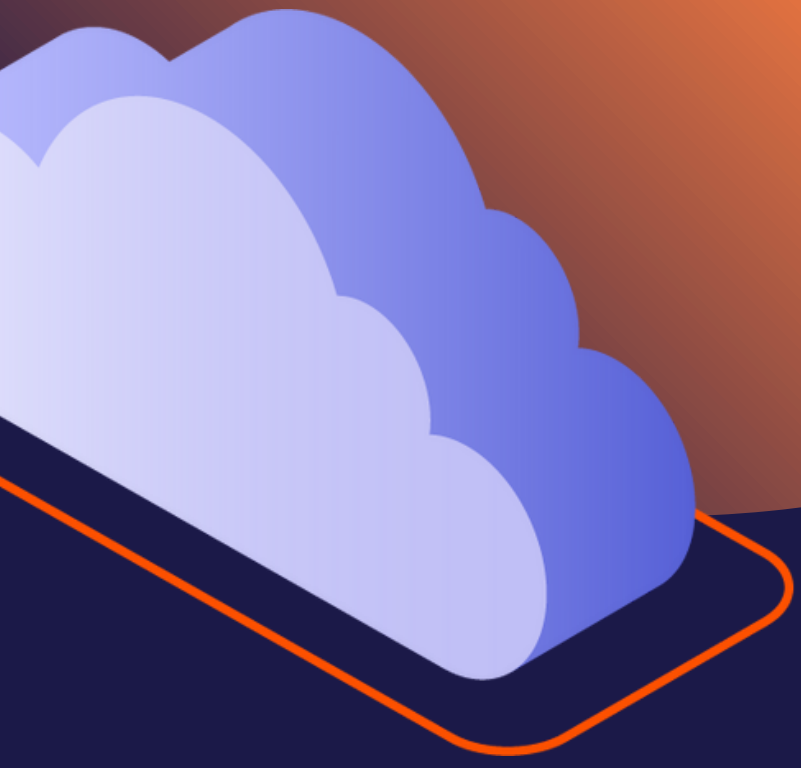
2023 Annual Report: Cybersecurity Trends & Insights

Presented by Perception Point



*Note: This report is based on data collected in 2022

PERCEPTION POINT™

Executive Summary

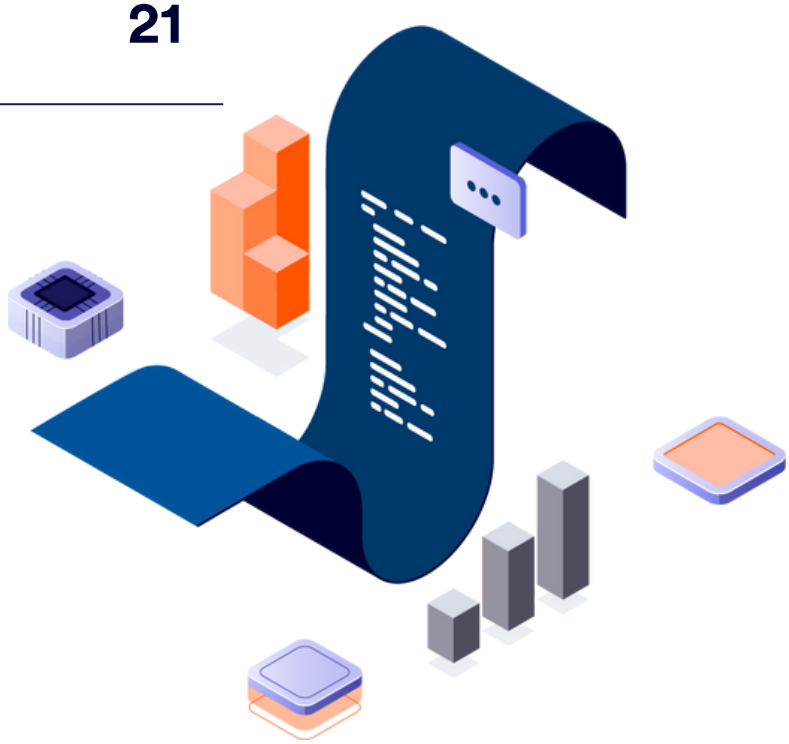
The global cyber threat landscape is rapidly evolving and expanding as attackers adopt more sophisticated techniques in order to breach organizations. The need for effective cybersecurity measures to protect an organization's most valuable digital assets has never been greater. Over the past year, it has become increasingly clear that concentrating resources on one attack vector is not enough to provide sufficient protection. While email and the browser still comprise the top vectors of all cyber attacks, by analyzing the attack trends of 2022, Perception Point has identified a dramatic surge in other channel-based attacks. This has led to the understanding that as organizations increase reliance on web-based tools and SaaS applications in the workplace, attackers are never far behind, ready to enhance their levels of sophistication to target emerging channels including cloud storage (AWS S3, OneDrive, Google Drive), collaboration apps (Sharepoint, Teams, Slack), Salesforce, and Zendesk.

In this report, Perception Point analyzes the most pervasive attacks its advanced threat detection platform detected in 2022, noting a particular increase in account takeover attacks in the latter half of the year as well as an ongoing growth in phishing attacks. This report examines cyber threats through distinct lenses based on the intelligence gathered by Perception Point's proprietary detection engines and its managed incident response service.

Key Takeaways:

- The total number of attacks increased by 87%, emphasizing the growing threat that cyber attacks now pose to organizations.
- There was a 356% growth in advanced phishing attacks attempted by threat actors in 2022, in addition to a 83% growth of Business Email Compromise (BEC) attacks.
- While email and the browser remain the leading attack vectors, 2022 saw a 161% surge in attacks on all other channels, such as cloud storage and collaboration apps.
- Advanced attacks, which are complex, sophisticated, and difficult to detect and mitigate, made up 2% of all threats.

Table of Contents



Top Attack Trends of 2022

As we look back at the cybersecurity landscape of 2022, it is clear that the year was marked by several unique and concerning attack trends. Perception Point's cybersecurity analysts reported a variety of new attack methods, a shift in the severity of the attacks, and a broadening of the attack surface. In this section, we will take a look at the trends that shaped this year's cybersecurity landscape.

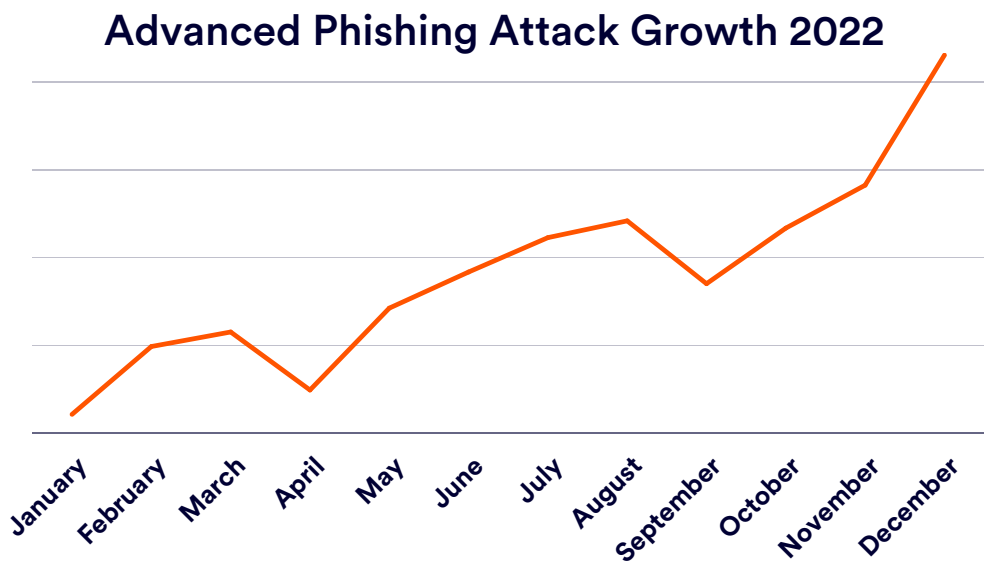
Advanced Phishing

Advanced phishing was one of the most common attack trends of the year, growing by 356%. Attackers use malicious links embedded in emails or websites to execute their payload. These attacks can involve the use of obfuscation techniques, such as URL redirection, making it difficult for the victim to identify the true (malicious) destination of the link.

The attacker typically sends an email with a link to a malicious website that deceptively looks like a legitimate website. This technique is often referred to as "cloaking" and can be used to hide the malicious content from the user while also evading detection from most email security vendors. Once the user is tricked into providing their credentials, the attacker can then use the information to gain access to the user's accounts and systems.

While HTML-based phishing attacks were consistently present throughout the year, it was not until August '22 that we saw a dramatic increase in attacks, more than doubling the amount of attacks caught in the previous month (July '22).

Advanced phishing attacks grew by 356% in 2022



Click here to learn about a cyber attack in which attackers disguise HTML phishing sites as XML files, allowing attackers to bypass and evade most detection platforms

Password-Protected Malware

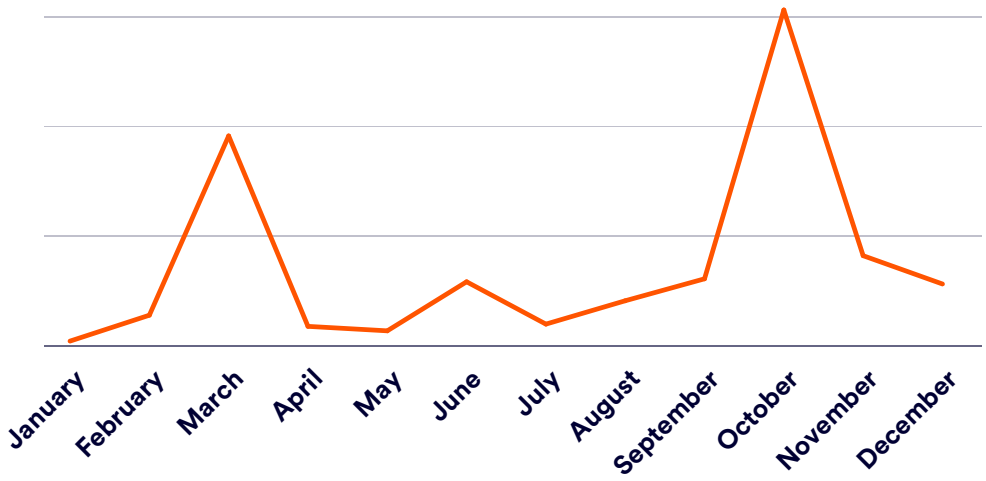
Password-protected malware was also a major trend in 2022, with attackers using strong encryption to protect malicious payloads and prevent detection by most security solutions. This form of malware typically encrypts user data, requiring the user to decrypt it. This type of attack was particularly dangerous because it was often used to steal passwords and other sensitive information.

We observed two major spikes in this type of attack, possibly correlating to the beginning of the Russian invasion of Ukraine in March '22 and October '22. In March '22 the pervasiveness of this attack increased by tenfold to that of the previous month (February '22). Then in October we saw another surge, the numbers tripling that of the month prior.

Click here to learn more about this type of attack.

Nearly 60% of all password-protected malware attacks occurred in March (22%) and October (35%)

Password-Protected Malware Growth 2022



Phone Scams

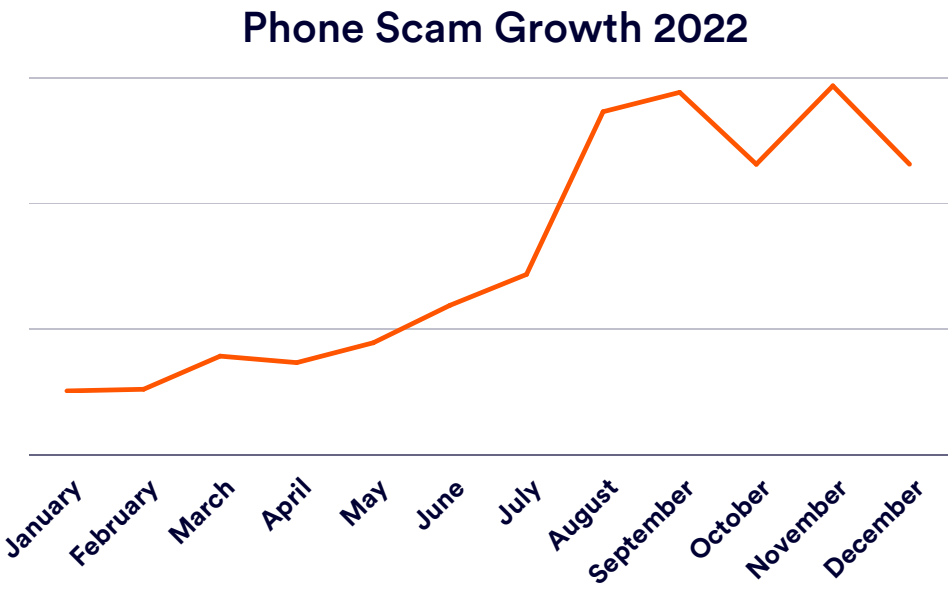
Phone scams were also prevalent in 2022, with malicious actors using social engineering and targeted messages to scam victims into giving up personal or financial information. These scams involved malicious actors posing as legitimate companies in order to gain access to sensitive information. Once the scammers had access to the information, they could use it for their own gain.

A typical phone scam starts with an email. Scammers use the display name of a legitimate company to appear as though they themselves are that vendor.

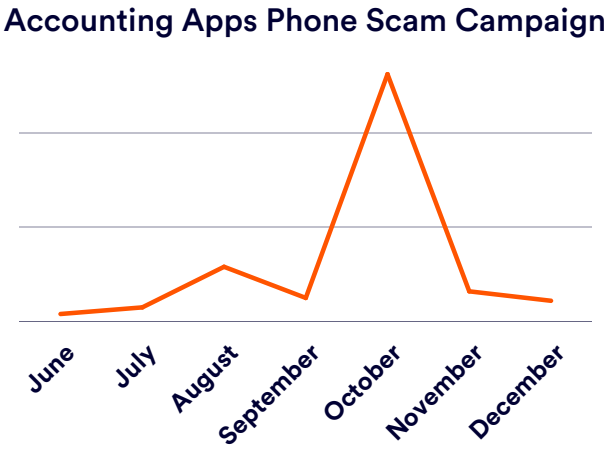
In the email, scammers include a receipt. This is a common method, as a receipt allows the attacker to organically slip in the phone number that they want the user to call. To make the receipt seemingly even more realistic, scammers provide information about the fake order and a number to call for support. Scammers also add details in the footer of their emails for more “legitimacy”, like buttons to report spam, unsubscribe, or read the private policy. All of these spoofed specifics serve to bolster the legitimacy of the phone number, which scammers want their targets to call.

Once they have their targets on the line, scammers pose as helpful experts. In reality, their goal is to have the victim willingly offer up your personal information (date of birth, address, ID numbers, etc.) and/or financial details. Attackers can also leverage calls to convince you to provide them with access to your computer.

By the end of 2022, phone scam attacks grew 363%



Beginning in August, our team noticed a unique subset of phone scams in which the attackers signed up for popular accounting application services like Xero to increase the legitimacy of their invoice request. By sending the invoice through third-party accounting software, the user is more likely to trust the source of the invoice. Upon viewing the fake invoice, users are then prompted to call the provided phone number for help, going through the motions of a phone scam.



Our IR team used a Sender Policy Framework (SPF) to verify the identities of the senders. As it turned out, the emails originated from the same domain as non-fraudulent invoices and the IP addresses corresponded to the legitimate IP addresses of Xero. This made these phone scams all the more dangerous, as attackers attempted to evade detection by abusing legitimate services.

Perception Point was able to detect this highly evasive cyber threat, despite it eluding most other email security solutions. Utilizing a combination of machine learning algorithms, advanced heuristics and a deep understanding of the attack surface, we were able to detect the threat before it could cause any damage.

Click here to learn more about sophisticated phone scam attacks

Business Email Compromise

In 2022, business email compromise (BEC) attacks grew by 83%. In these attacks, cybercriminals use fake emails to impersonate legitimate businesses and request large sums of money or confidential data from employees or business associates.

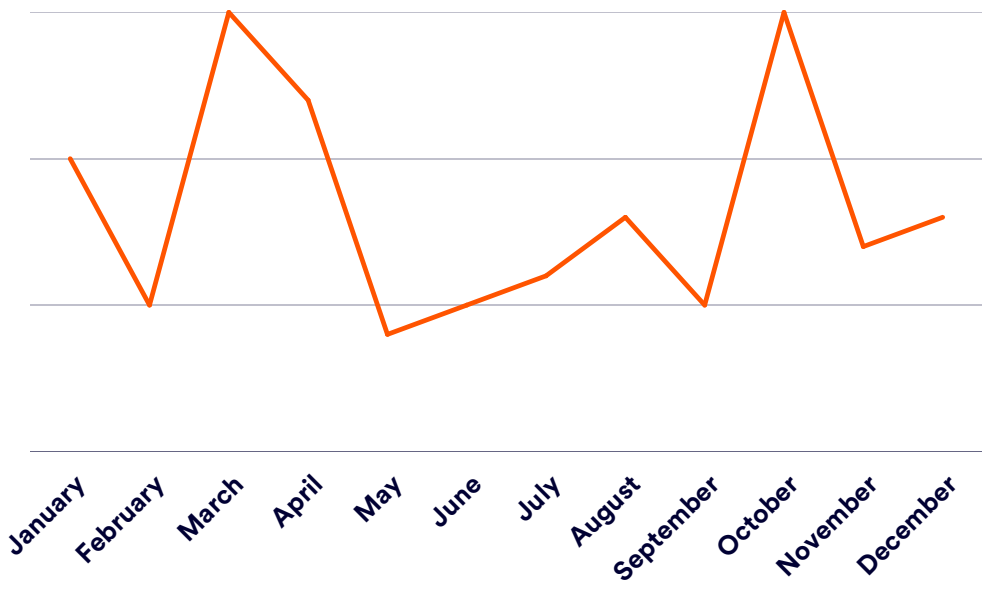
Impersonation-based attacks are becoming increasingly more difficult to detect as attackers exploit the fact that employees in the modern enterprise are the least secure facet of its security systems. Employees, who are often preoccupied and easily accessible, can be easily tricked into making mistakes. Despite the fact that legacy security systems (like secure email gateways) were created to prevent malicious files and URLs from bypassing normal defenses, most BEC attempts are mainly or completely text-based and do not have malicious content. Rather, they use complex and well-researched social engineering tactics to deceive people, making traditional email security solutions ineffective.

In 2022, business email compromise attacks grew by 83%

"Impersonation and account takeover attacks via business email compromise (BEC) are increasing and causing direct financial loss, as users place too much trust in the identities associated with email, which is inherently vulnerable to deception and social engineering."

-Gartner 2023 Market Guide for Email Security

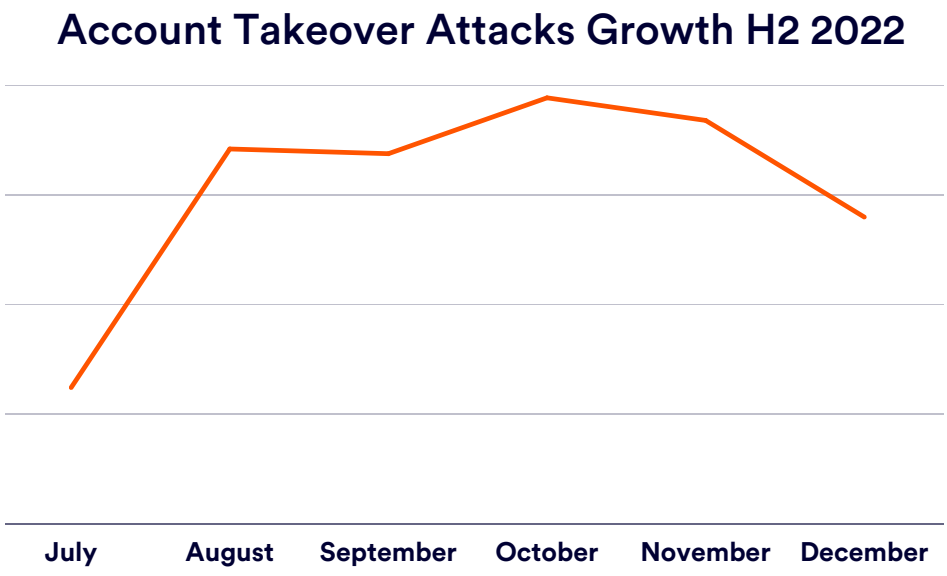
Business Email Compromise Growth 2022



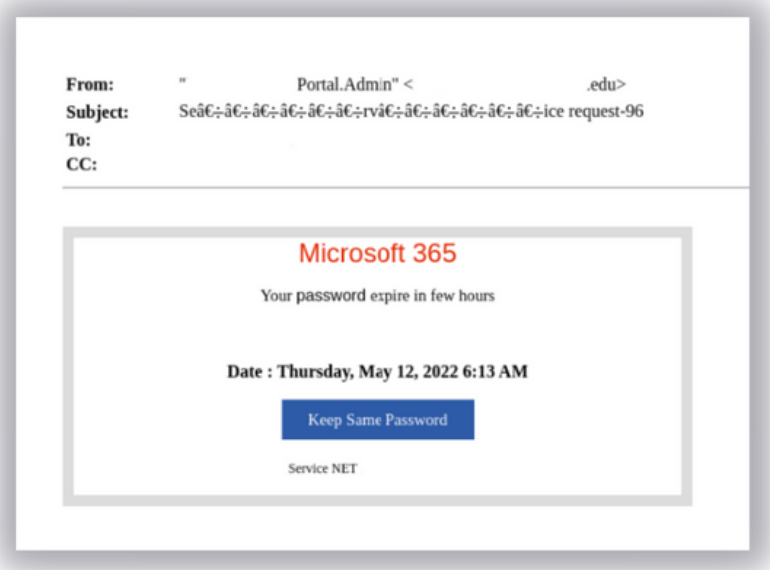
Account Takeover (ATO)

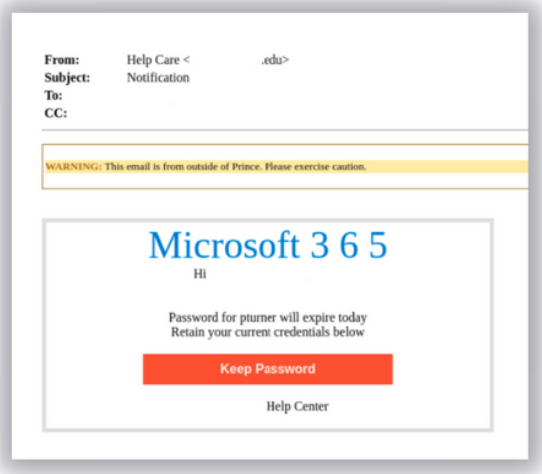
Over the past few months, one of the top concerns for our customers has been Account Takeover (ATO) attacks. Just as its name implies, ATO is when an attacker gains access to a user's email or cloud collaboration application via stolen credentials. What is most alarming about ATO attacks is that there are no telltale signs to look out for if an organization has been breached.

These attacks usually originate from phishing emails, in which a victim is lured into entering their credentials on a spoofed website. With the user's credentials, the attacker gains access to their various accounts and typically furthers the ATO cycle by using the compromised account to send out more phishing emails. However, attackers usually monitor the compromised user's account, waiting for the right opportunity to begin their campaign. By posing as the compromised user, the attacker's phishing efforts seem more legitimate, as recipients assume the email was sent from a known individual.

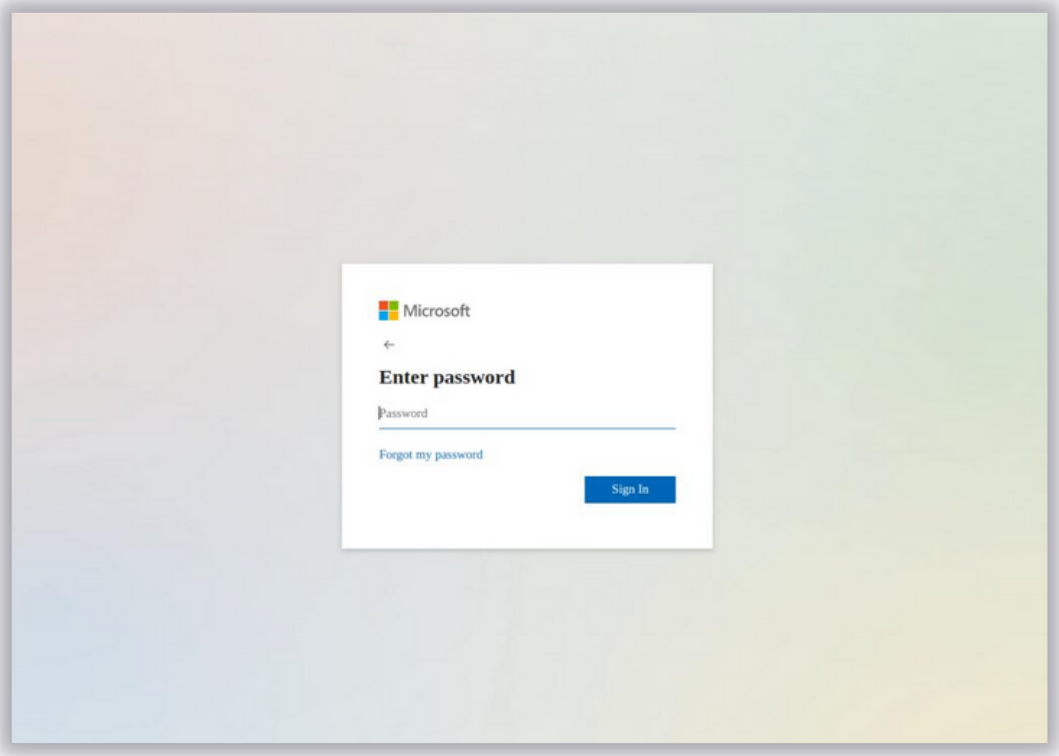


One of the ATO campaigns our researchers observed targeted major American universities. In these attacks, threat actors compromised legitimate university-affiliated domains to send out emails spoofing Microsoft 365.





After clicking the link contained in the email, targets are redirected to a phishing site with a fake Microsoft login page. The goal of the attack is to steal user credentials to continue the ATO-phishing cycle.



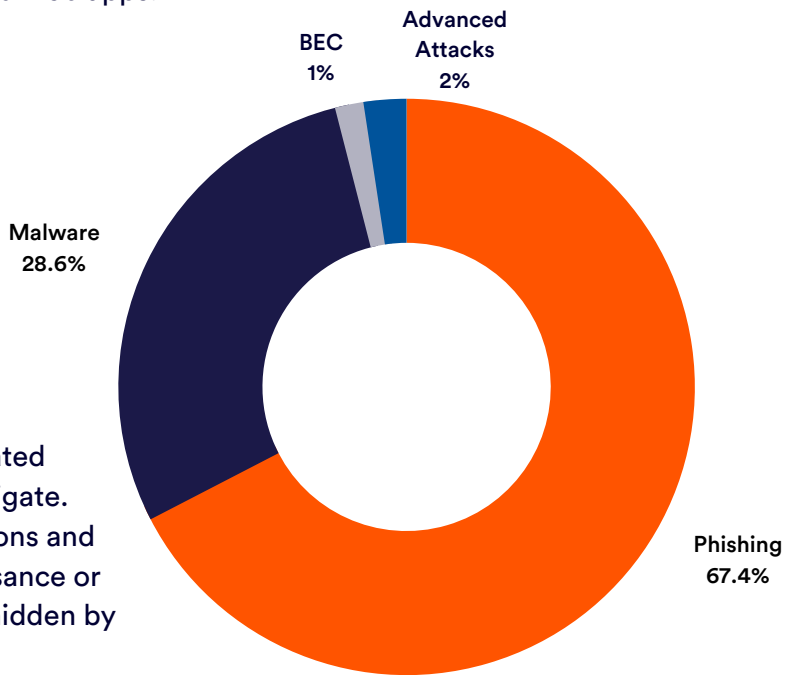
Click here to learn more about this attack

Attacks by Type

In this section, we examine the different types of cyber threats we saw over the course of the year. We look at the prevalence and severity of phishing, malware, business email compromise (BEC), and advanced attacks.

It is important to note that when examining attack types, we drew data from all channels: email, web browser, file scanning, cloud storage, and web apps.

Phishing accounted for 67.4% of all incidents in 2022, followed by malware at 28.6%. Perhaps most notable, however, is advanced attacks making up 2% of all threats. While this number may seem minor, on the contrary, this smaller percentage represents a subset of attacks that could be more detrimental to an organization than the other categories combined.



Advanced attacks are complex and sophisticated attacks that can be difficult to detect and mitigate. They are often targeted at specific organizations and may involve multiple steps such as reconnaissance or malware delivery. These attacks can also be hidden by advanced evasion techniques.

In order to prevent advanced attacks from reaching our customers, Perception Point leverages the recursive unpacker, a tool that breaks content into smaller units, and the HAP™ (hardware-assisted platform), our proprietary next-gen dynamic engine that combines CPU-level data with innovative software algorithms to neutralize unknown threats.

Rather than detecting malware, the HAP works at the exploit stage. By targeting attacks at this stage, the HAP cannot be bypassed by zero-days.

Zero-day attacks leverage a software vulnerability that is either unknown or unaddressed by the vendor. The problem is that common APT modules (sandboxes and CDRs) rely on known data or behaviors. Thus, when you combine an unknown bug with evasion techniques, seasoned attackers can easily circumvent the detection methods of these solutions.

Though advanced attacks only made up 2% of all threats in 2022, these attacks often cause the most damage for organizations.

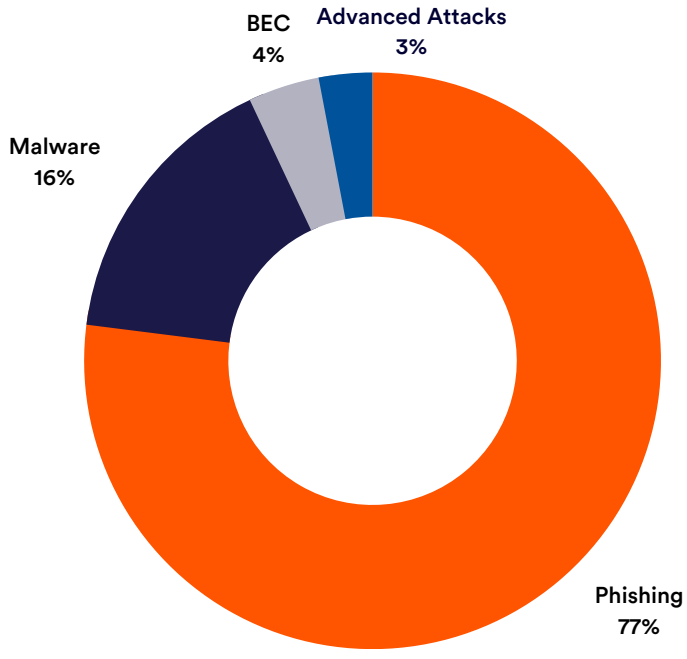
Attacks by Channel

The growth of cloud computing and mobile technologies has enabled organizations to increase their collaboration and communication capabilities, creating new and innovative ways of working. However, this increased use of cloud communication channels has also created a new set of security blind spots for malicious actors to exploit. While email and web remain the primary threat vectors for attackers, the introduction of cloud-based applications and storage apps, which are often overlooked when it comes to security, are becoming increasingly attractive targets. In 2022, there was a 161% surge in events across all other channels. As attackers continue to look for new ways to penetrate an organization's systems, these types of applications need to be monitored and protected to ensure that the organization's data remains secure. In this section, we will explore the types of attacks that are launched through email, web browsers, file uploads, Amazon S3 Buckets, Salesforce, enterprise communication apps, cloud storage, and cloud collaboration channels.

According to an Osterman Research paper, "Many newly adopted cloud collaboration apps and services have only been around for a few years. Worryingly, the rate of malicious incidents against these new apps and services is already 60% of what organizations experience against their email services. Threat actors have responded quickly to the emergence of new channels for employee productivity and collaboration."

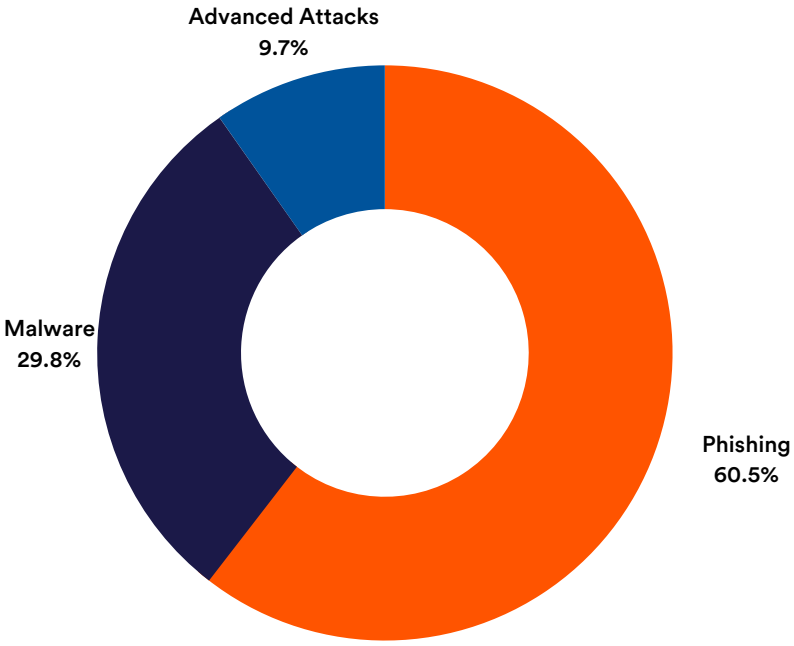
Click here to download the full Osterman Research report, "The Rise of Cyber Threats Against Email, Browsers and Emerging Cloud-Based Channels."

EMAIL

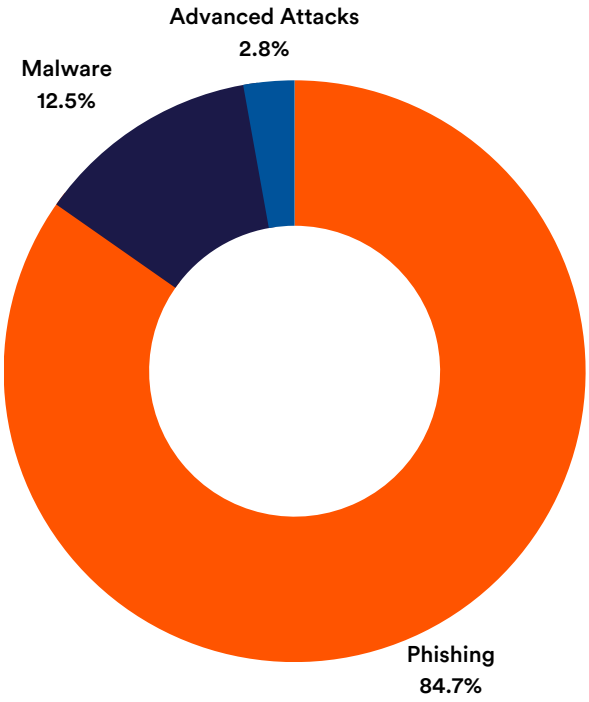


Attacks by Channel

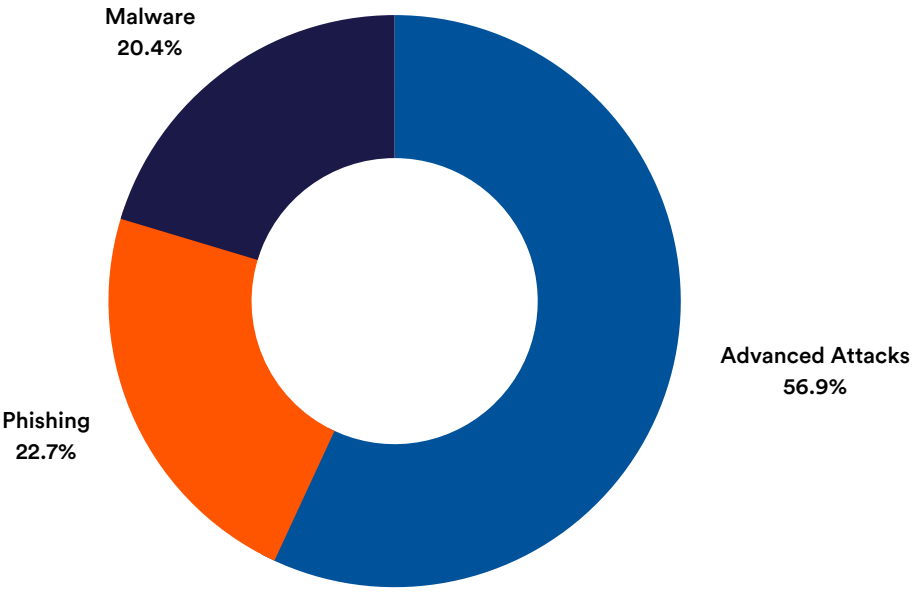
WEB BROWSER



FILE UPLOAD

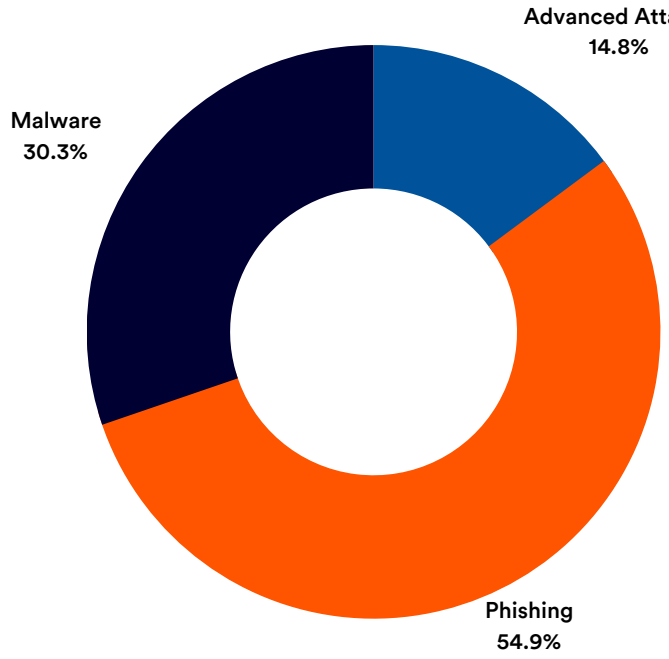


AMAZON S3 BUCKETS

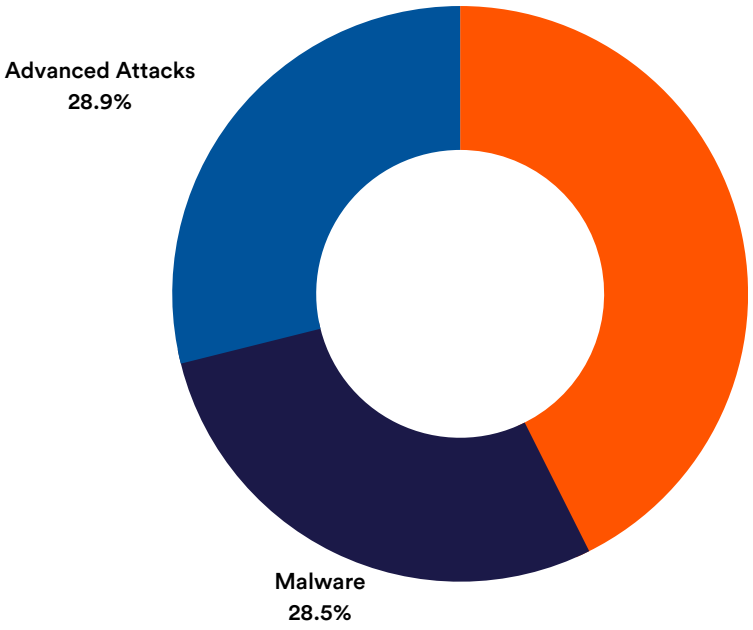


Attacks by Channel

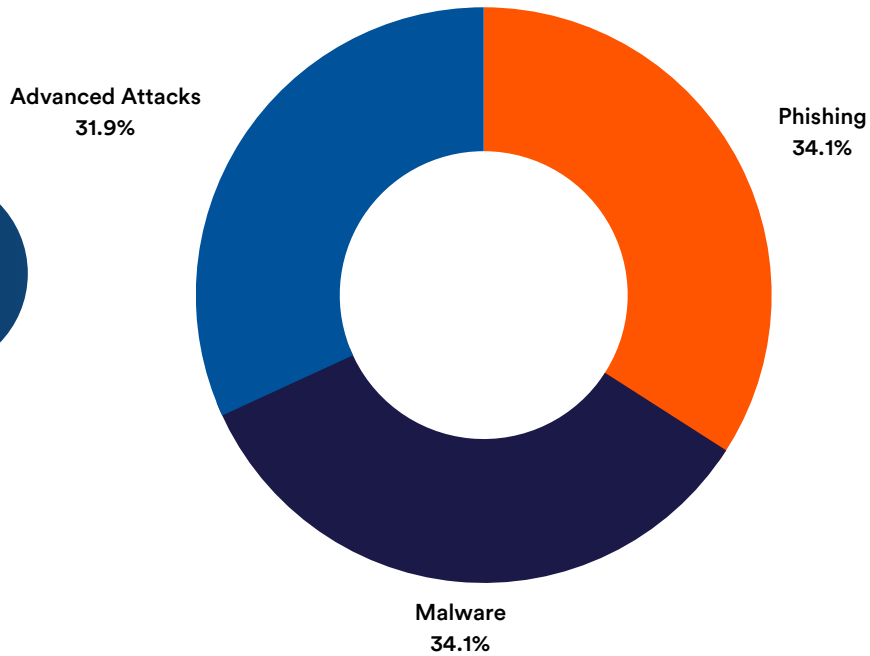
SALESFORCE



ZENDESK



FILE STORAGE



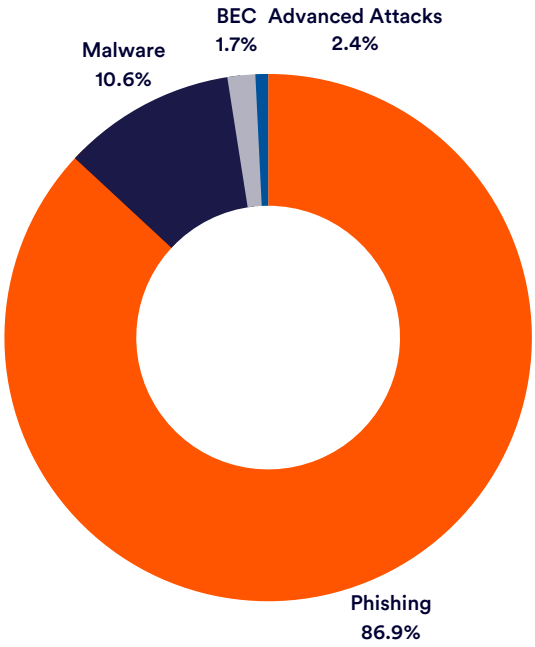
Vendor Comparisons

One of the major benefits of Perception Point's Advanced Email Security solution is that it is an Integrated Cloud Email Security (ICES) solution and can easily be deployed on top of any security platform. This means that the customer can continue to leverage their existing security service (such as Microsoft EOP or Defender) and Perception Point provides an additional layer of defense by detecting malicious content that other solutions miss, or fully replace it. In this section we highlight attacks we prevented for customers that use Perception Point as a safeguard on top of their existing security solutions.

Proofpoint

One of our customers is a publicly traded $2.1B company in the financial services industry. They use Proofpoint as their email protection provider, but added Perception Point Advanced Email Security as an additional layer of defense.

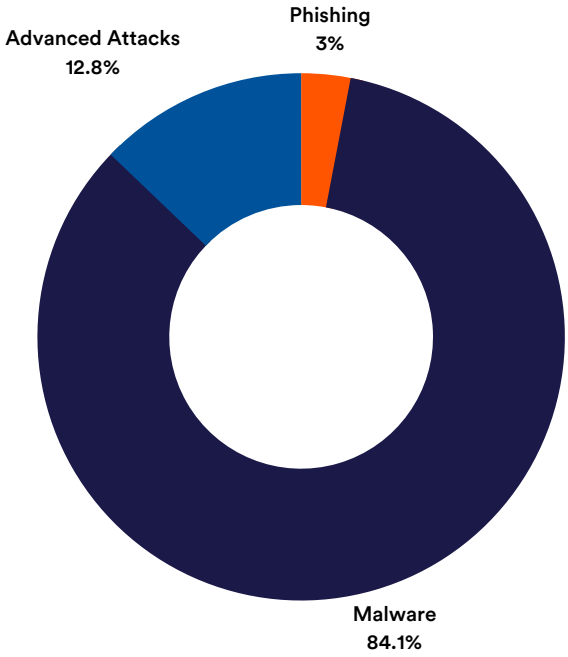
Perception Point received all the traffic deemed clean by Proofpoint. Of that traffic, 7% was intercepted; 87% of the malicious emails were phishing attacks.

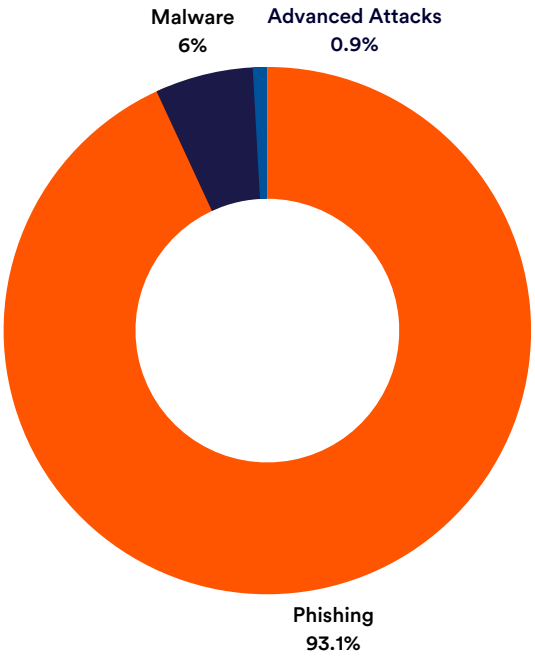


Forcepoint

This customer is a full-service financial institution, serving both consumers and businesses. They use Perception Point Advanced Email Security on top of Forcepoint's email security solution.

After Forcepoint, Perception Point intercepted 6% of the supposed "clean" mail; 84% of the malicious content was malware, followed by 13% advanced attacks.





Symantec

This customer is a multinational electrical manufacturing company that added Perception Point Advanced Email Security on top of Symantec's email security solution. Perception Point intercepted 7% of the content Symantec had marked as clean; 93% of all malicious attacks were phishing, followed by malware, which comprised 6% of malicious attacks.

Traditional defenses alone are no longer enough to guarantee protection. Rather, it is now essential to have proactive security measures to defend against advanced threats. After all, it only takes one successful attack to cause a major breach and potentially catastrophic damage to an organization.

Microsoft

Perception Point Advanced Email Security is a popular choice for customers seeking enhanced protection beyond Microsoft's security options. While some customers use both solutions in conjunction, in this section we focus on two customers that use Perception Point's advanced threat detection verdicts in place of Microsoft's. One customer uses Exchange Online Protection (EOP), Microsoft's native email security offering, while the other employs the more sophisticated Microsoft Defender.

It is important to note that Microsoft employs a Spam Confidence Level (SCL) score to determine the likelihood of an email message being spam or malicious. A lower SCL score is assigned to legitimate messages, while higher scores are given to those suspected of being spam or malicious. Microsoft uses these scores to decide whether to block delivery to the recipient.

In the following case studies, we compare the verdicts given by Microsoft to Perception Point's comprehensive verdicts.

Microsoft EOP

Our customer is a $9.684B international food & beverage company with 18,000 active email accounts. Despite having Microsoft EOP, this customer has opted to use Perception Point's verdicts instead.

In 2022, Microsoft EOP accurately identified 98.7% of all clean emails but misclassified 1.3%. When it comes to spam emails, EOP had a success rate of only 13.6%, misclassifying a staggering 86.4%. However, the most concerning statistic is that EOP misclassified 58.8% of all malicious emails, accurately identifying just 41.2%.

Microsoft EOP	Clean	Spam	Malicious
Microsoft Correct	98.70%	13.60%	41.20%
Microsoft Misclassified	1.30%	86.40%	58.80%

Microsoft Defender

This customer is a leading global industrial gases and engineering company, with over $33B in sales, committed to safeguarding its 65,000+ employees. To bolster the capabilities of Microsoft Defender, the customer utilizes Perception Point Advanced Email Security for final verdicts.

Throughout 2022, Microsoft Defender correctly classified 98.2% of all clean emails, misclassifying 1.8%. Defender correctly classified 23.6% of all spam emails, misclassifying 76.4%. For malicious emails, Defender correctly classified 41.8%, misclassifying 41.8%.

Defender	Clean	Spam	Malicious
Microsoft Correct	98.20%	23.60%	58.20%
Microsoft Misclassified	1.80%	76.40%	41.80%

These findings underscore the importance of carefully evaluating Microsoft EOP and Defender as viable email security options. While Microsoft Defender's detection mechanisms are more effective than EOP's, there are still significant gaps in coverage that suggest that relying solely on Microsoft's security offerings may not be enough to fully protect organizations against modern threats.

The low success rate of Microsoft's Spam Confidence Level has serious consequences for organizations that rely on it for email security. It not only impacts the user experience negatively but also poses a significant security risk. When malicious emails are not accurately identified, they can enter users' inboxes and cause significant damage. The threat posed by such emails is compounded by the fact that users may not be aware of the malicious content due to the false labeling of the emails. This can result in the further spread of malicious content and cause additional harm to the organization.

Therefore, it is crucial that Microsoft EOP and Defender users consider supplementing their email security with a reputable provider to mitigate this apparent disparity in protection.

Brand Impersonation

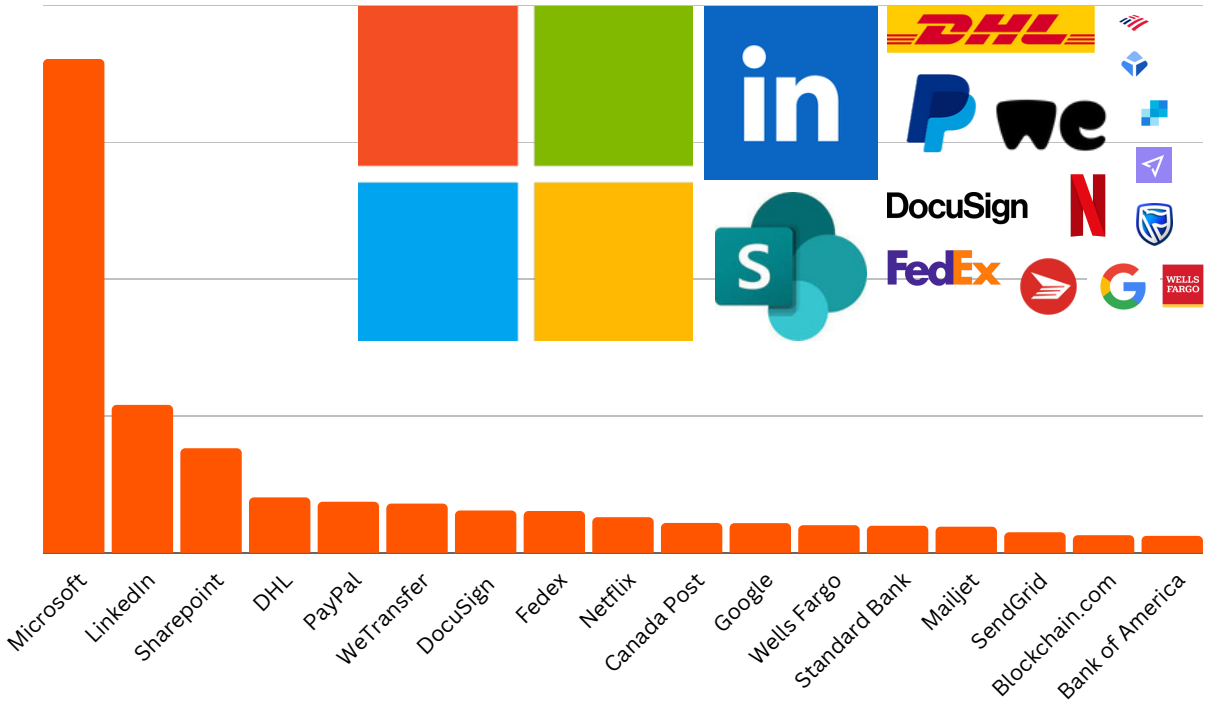
In 2022, attackers used a variety of methods to exploit unsuspecting victims and their data. One of the most common methods used was to impersonate popular brands. Attackers concentrated on impersonating the most well-known and used brands, as these companies had the most potential to trick victims into trusting that an email or URL was legitimate.

Brand impersonation is a form of cybercrime where attackers create fake emails or websites that appear to be from a legitimate company or organization. These emails or spoofed websites are designed to deceive recipients into providing personal information, such as passwords, account numbers, or other confidential data. Brand impersonation is a serious security threat, as it can lead to identity theft and other forms of fraud.

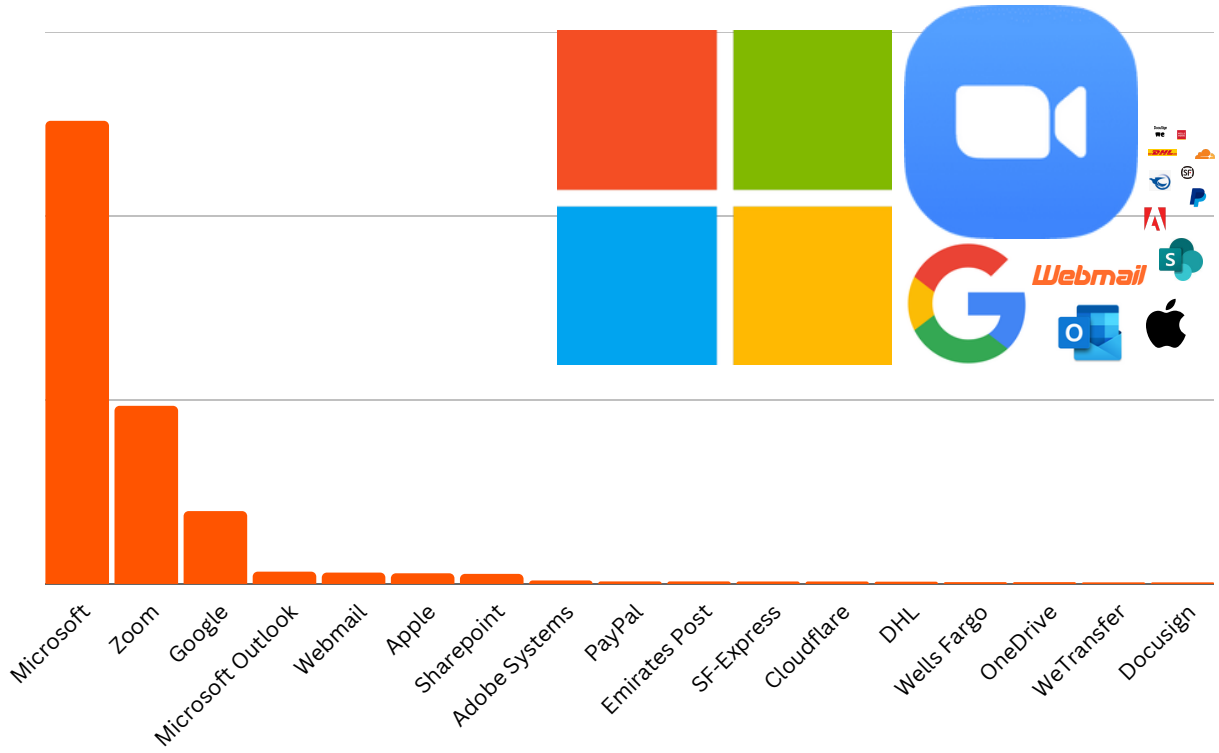
Threat actors may use logos, fonts, and other design elements to mimic the look of a legitimate email or website. They may also try to create a sense of urgency by claiming that you must act quickly or your account will be closed. Alternatively, they may use a generic greeting, instead of addressing the user by name.

Throughout 2022, Microsoft was the top impersonated brand in malicious email messages. Microsoft was impersonated 3.3x more than the next most impersonated brand, LinkedIn.

Following Linkedin, attackers frequently impersonated SharePoint, DHL, PayPal, and WeTransfer in their malicious emails. The graph below displays the top 17 most impersonated brands for email in 2022.



Attackers also sent emails with malicious links, leading to spoofed websites. In these cases, Microsoft was also the most impersonated brand. Microsoft was impersonated more than 2.6x than the second most impersonated brand, Zoom. Following Zoom, attackers created spoofed sites for Google, Outlook, Webmail, and Apple. The graph below shows the 17 most spoofed brand websites in 2022.



Impersonated brands can be difficult to detect. Attackers send emails and URLs with highly sophisticated, near-identical branding. What makes Perception Point's platform particularly effective against this threat is our list of protected brands. This list includes thousands of brands that our IR team regularly updates and adds to with a brand's legitimate domain, logos, and the like so that the platform can instantly identify a spoofed brand from a real one.

Final Words

It is clear that the cyber threat landscape is constantly changing and advancing, and organizations need to keep pace in order to remain secure. The report revealed that attackers are increasingly relying on more sophisticated techniques and targeting new channels, including cloud storage, collaboration apps, Salesforce, and Zendesk. Organizations must take steps to protect their most valuable assets by adopting a comprehensive approach to cybersecurity that encompasses multiple attack vectors in order to mitigate their risk.

About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection, investigation, and remediation of all threats across an organization's main attack vectors - email, web browsers, and cloud collaboration apps. The solution's natively integrated and fully managed incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights; providing proven best protection for all organizations.

Deployed in minutes, with no change to the enterprise's infrastructure, the patented, cloud-native and easy-to-use service replaces cumbersome legacy systems to prevent phishing, BEC, spam, malware, zero-days, ATO, and other advanced attacks well before they reach end-users. Fortune 500 enterprises and organizations across the globe are preventing attacks across their email, web browsers and cloud collaboration channels with Perception Point.

To learn more about Perception Point, visit our website, or follow us on LinkedIn, Facebook, and Twitter.