DESIGNED FOR
Microsoft 365
ENVIRONMENTS

2024

CYBER SECURITY REPORT

AN IN-DEPTH ANALYSIS OF THE MICROSOFT 365 THREAT LANDSCAPE

HORNETSECURITY

HORNETSECURITY

CYBERSECURITY REPORT 2024

About Hornetsecurity

Hornetsecurity empowers companies and organizations of all sizes to focus on their core business by protecting email communications, securing data, and ensuring business continuity and compliance with next-generation cloud-based solutions.

Our flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market, and includes email security, compliance, and backup.

What is the Cyber Security Report?

The Cyber Security Report (formerly Cyber Threat Report) is an annual analysis of the current cyber threat landscape based on real-world data collected and studied by Hornetsecurity's dedicated Security Lab team. Hornetsecurity processes more than 3.5 billion emails every month. By analyzing the threats identified in these communications, combined with a detailed knowledge of the wider threat landscape, the Security Lab reveals major trends. It can make informed projections for the future of Microsoft 365 security threats, enabling businesses to act accordingly. Those findings and data are contained within this report.

What is the Security Lab?

The Security Lab is a division of Hornetsecurity that conducts forensic analyses of the most current and critical security threats, specializing in email security. The multinational team of security specialists has extensive experience in security research, software engineering, and data science.

An in-depth understanding of the threat landscape established through hands-on examination of real-world viruses, phishing attacks, malware, and more is critical to developing effective countermeasures. The detailed insights uncovered by the Security Lab serve as the foundation for Hornetsecurity's next-gen cyber security solutions.

How to Use This Report

This report is divided into five sections:

Chapter 1 contains the Executive Summary. If you're only interested in the highlights, you'll want to review this section.

Chapter 2 focuses on the current threat landscape of the Microsoft 365 platform.

Chapter 3 covers current concerns and discussions regarding the most significant threats and trends from 2023.

Chapter 4 contains predictions from the Security Lab about cyber security threats in 2024, along with advice and guidelines to help protect your business.

Chapter 5 lists all the references, supporting links, and data sets used in this report.

Table of Contents

Chapter 1 – Executive Summary

By leveraging its huge user dataset, Hornetsecurity is uniquely positioned to conduct a detailed examination of email-based threats and distill this into important insights for IT security professionals. Email continues to be an essential communication channel. However, in our analysis of more than 45 billion emails, 36.4% are categorized as "unwanted." 96.4% of unwanted emails are spam or rejected outright due to external indicators, and just over 3.6% were flagged as malicious.

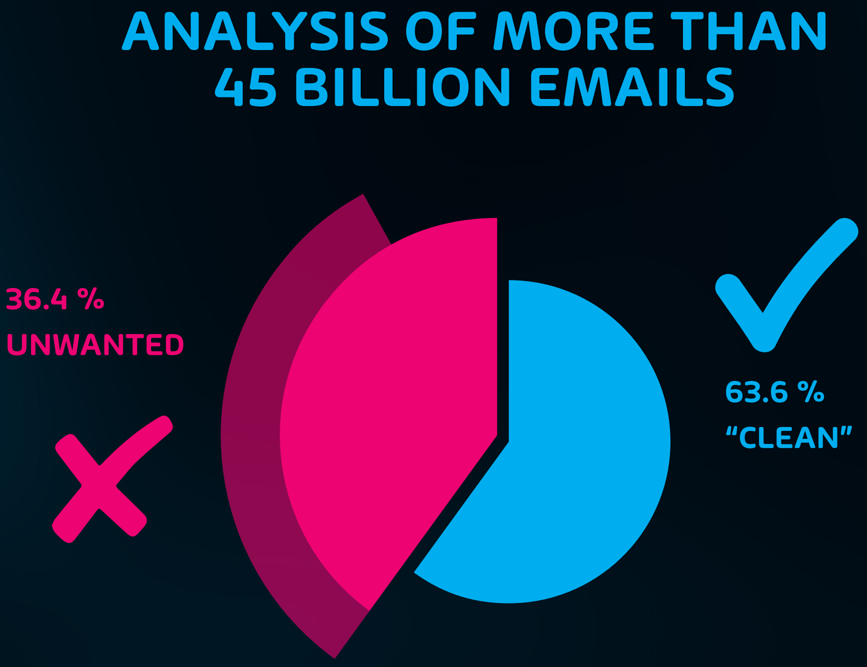


Fig. 1: Classification of emails scanned by Hornetsecurity

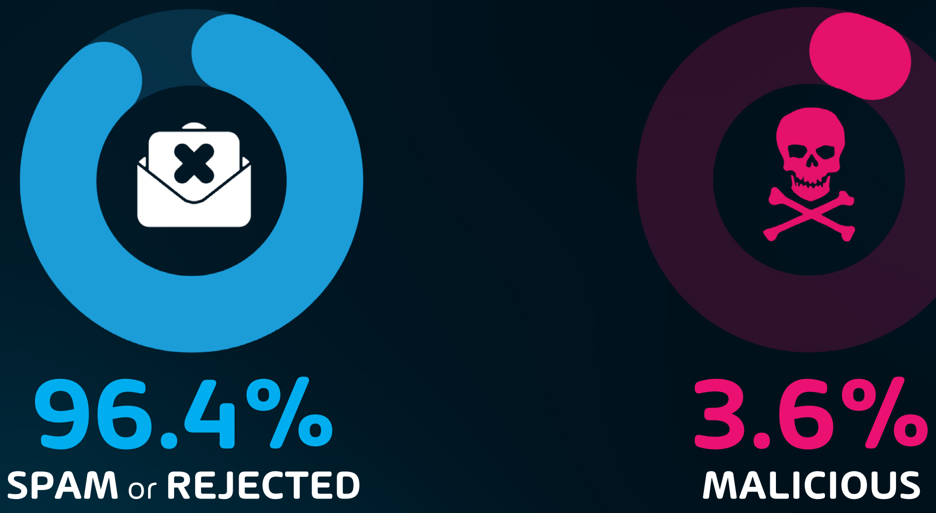


Fig. 2: Classification of unwanted emails

Another high-level statistic that we look at when it comes to email-based attacks is the style of attack. Our findings for this data period show that phishing retains its top spot, accounting for 43.3% of email-based attacks. This is nearly a 4% increase over the previous year. The second most common attack type during 2023 was the use of malicious URLs in email at 30.5%, which was a significant 18% increase over last year's report.

Fig. 3: Email-based attacks

Alongside types of attacks, we monitor the types of attachments that are currently being leveraged by threat actors to deliver malicious payloads. HTML files (37.1%) and PDFs (23.3%) were observed most frequently during the data period, along with Archive files (20.8%) in third place. HTML file usage saw a 16.1% increase by threat actors throughout the data period, as well as an 11% increase in PDF file usage. This was largely driven by threats like Qakbot and similar botnets that utilize these file types to facilitate the spread of their software. Also of note is a notable decrease in the use of DOCX files by 9.5% and XLSX files by 6.7%. These used to be popular file types for use by threat - actors, and since Microsoft switched to having macros disabled by default in Office, the use of these file types has dropped dramatically.

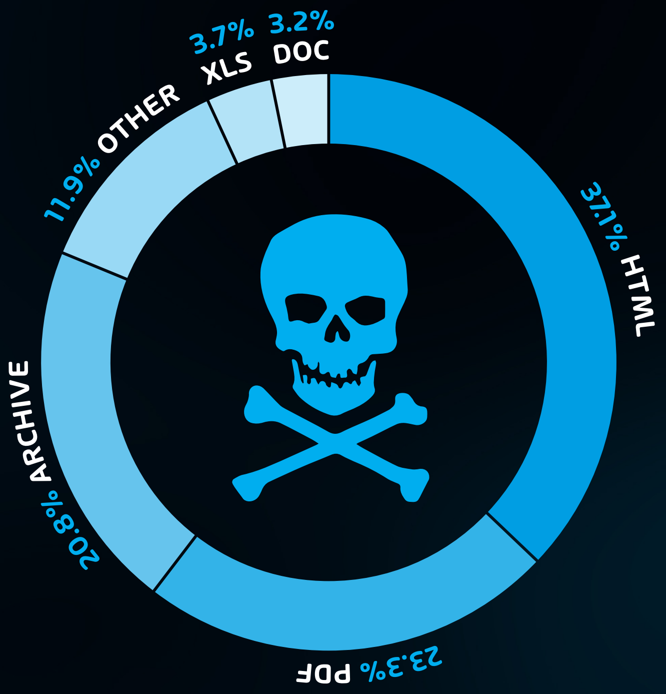


Fig. 4: Most-used file types in malicious emails

The industry email threat index was roughly the same across most business verticals during the data period. The email threat index is a measurement we track that measures the number of attempted email threats against the number of clean emails delivered based on industry vertical. This provides a good idea of what types of businesses are currently being targeted by threat actors. Like last year, our data shows that almost every type of business is currently under threat. In short, if your organization has the ability to pay a ransom, you are a target. That said, research organizations, the entertainment sector, and manufacturing are at the height of the spectrum, with slightly more attacks being levied at those types of organizations vs others.

One final email security area that we track is the use of brand impersonations. This helps us inform our product teams, our customers, and the community as to what types of brand-oriented phishing are currently being used in the ecosystem. Our data for this report shows that shipping brands remain a popular choice.

For example, DHL (26.1%), Amazon (7.7%), and FedEx (2.3%) all made the top 10. Other notable names on the list are Microsoft (2.4%), LinkedIn (2.4%), and Netflix (2.2%). Most of these instances are cases where threat actors were after end-user credentials either to sell, or for use in other attacks.

26.1%	DHL
7.7%	AMAZON
2.4	LINKEDIN
2.4	MICROSOFT
2.2	NETFLIX
2.3	FEDEX

Fig. 5: Brands/organizations exploited

The question of data safety within the Microsoft cloud ecosystem continues to be a large part of the cloud conversation today. Several recent security breaches, including one by Chinese nation-state threat actors, have many (including the US Government) re-evaluating their security posture in the cloud era. This has also brought up the question of vendor overdependence and how much reliance organizations should put on one single vendor.

Microsoft has also changed its long-time stance on the need for backups when it comes to M365 data. For a considerable period, their stance was a simple "backups are not needed", with the cloud provider relying solely on the retention capabilities built into M365. However, Microsoft seems to have put an end to that advice with a hastily announced new M365 backup application and an associated API during the summer months. That said, there has been no additional news regarding this newly announced backup product as of the time of writing.

Right-sizing share and object permissions within M365 are topics that we discuss in this report as well. With the ease of sharing and collaboration that M365 provides, it's very easy for sensitive data to leak out of M365 tenants. This can happen completely by mistake or maliciously. SharePoint Online and OneDrive for Business have been the "file servers" of the cloud era for some time now, so many organizations face the stark reality of trying to manage sharing and permissions in M365 AFTER they've grown out of control. This will continue to be an area that businesses will need to look at in 2024 and is primed to grow as a source of data leakage in the future as well.

Email continues to be one of the primary methods threat actors use to launch attacks, and a robust email security strategy is essential for navigating the compounding threat landscape and developing security resilience in 2023.

Chapter 2 – The Current Microsoft 365 Threat Landscape

On an annual basis, Hornetsecurity's dedicated Security Lab reviews the company's extensive data set and analyzes the state of global email threats and communication statistics. In addition, the team regularly conducts forward-thinking exercises and provides insight into potential future threats. This chapter focuses on reviewing the data from November 1, 2022, to November 1, 2023, which forms the basis for projections of the changing threat landscape laid out in Chapter 4.

Email Security Trends

Despite increasing usage of collaboration and instant messaging software, such as Microsoft Teams, email continues to be a top area of concern in terms of cyber attacks. Even though we've seen a slight decrease in the number of emails categorized as Threats/AdvThreats - 3.6% this year, compared to 5.48% from last year (When looking at "Unwanted" emails), the risk to businesses around the globe remains high. Attacks are becoming more sophisticated than ever, and with AI-enabled attacks on the rise, businesses need to stay alert and not get complacent in their security posture. More detailed data follows below.

By reviewing more than 45 billion emails collected over the current reporting period (1 November 2022 – 1 November 2023), the Security Lab has made the following determinations:

Spam, Malware, Advanced Threat Metrics

Email continues to be one of the primary methods that threat actors use to launch attacks. This is exemplified in our data, which classified 36.4% of all emails as "Unwanted," meaning they are not genuine communications desired by the recipient. The below chart shows our breakdown of unwanted emails along with clean emails.

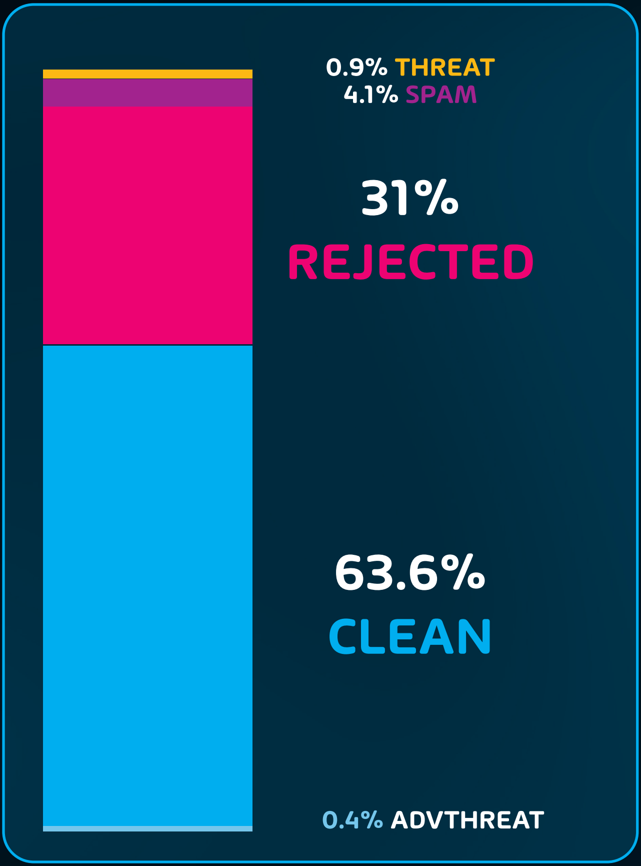


Fig. 6: Unwanted emails along with clean emails

This is in contrast to last year's reported number of 40.5% of all emails being categorized as "unwanted", showing a decrease (albeit slight) in unwanted emails year over year in terms of percentage. Considering that we processed just 25 billion emails for last year's report vs 45 billion this year, the current threat posed by email-based threats remains HIGH.

During the data period for this year, we found the breakdown of just **unwanted** emails as follows:

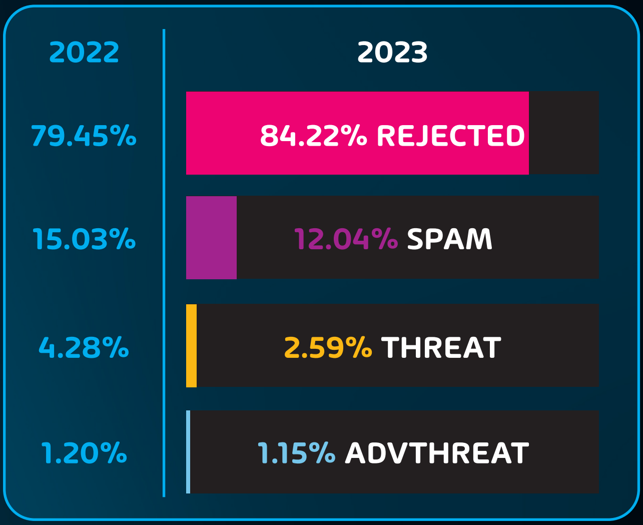


Fig. 7: 2023 Unwanted Emails by Category

CATEGORY	DESCRIPTION
Spam	These emails are unwanted and are often promotional or fraudulent. The emails are sent simultaneously to a large number of recipients.
Threat	These emails contain harmful content, such as malicious attachments or links, or they are sent to commit crimes like phishing.
AdvThreat	Advanced Threat Protection has detected a threat in these emails. The emails are used for illegal purposes and involve sophisticated technical means that can only be fended off using advanced dynamic procedures.
Rejected	Our email server rejects these emails directly during the SMTP dialog because of external characteristics, such as the sender's identity, and the emails are not analyzed further.

NOTE: To provide a little more detail, the "Rejected" category refers to emails that Hornetsecurity services rejected during the SMTP dialog because of external characteristics, such as the sender's identity or IP address. If a sender is already identified as compromised, the system does not proceed with further analysis. The SMTP server denies the email transfer right at the initial point of connection based on the negative reputation of the IP and the sender's identity.

Attack Techniques Used in Email Attacks

In our data analysis of emails from the data period, we observed the below breakdown of attack types used in email attacks:

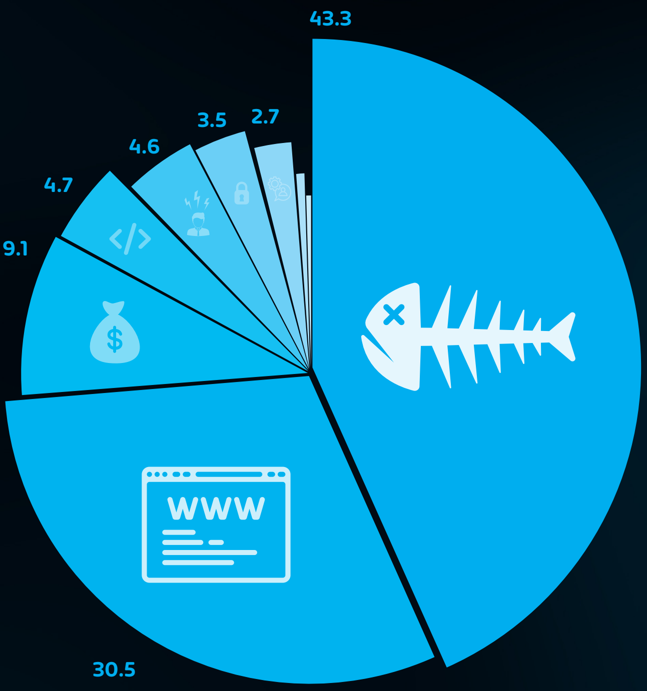


Fig. 8: Attack Techniques Used in Email Attacks 2023

Unsurprisingly, phishing and the use of malicious URLs remain near the top of the list and continue to be popular (and highly successful) attack types for threat actors. When looking at the data from last year (shown below), several comparisons can be made:

2022 %	2023 %	ATTACK TECHNIQUES
39.6	43.3	Phishing
12.5	30.5	URL
8.2	9.1	Advanced-Fee Scam
1.8	4.7	HTML
3.7	4.6	Extortion
3.5	3.5	Exe. in Archive/Disk-Image
1.1	2.7	Impersonation
2.8	1.0	Maldoc
0.4	0.6	PDF

Fig. 9: Attack Techniques Used in Email Attacks 2022 and 2023

In fact, if you look at just the stats for the use of malicious URLs and NOT accounting for all other attack types, that amounts to a 144% increase over the previous data period. Meaning the amount of malicious URLs we've seen in email threats has more than doubled in the last year.

Social engineering and email-based threats continue to be one of the top methods threat actors use to gain an initial foothold in a target organization. We've also seen a rise in cases where target users are social engineered to interact with a malicious link, so the use of malicious URLs goes together with the overall increase in phishing.

Attachment Use and Types in Attacks

Email attachments continue to be one of the most frequently used methods of delivering an attack payload in 2023. Threat actors continue to use attachments to hide malware as well as to add an air of authenticity to their malicious communications. Additionally, some rudimentary spam/malware filters may be unable to scan compressed attachments, increasing the risk for certain organizations.

The breakdown of the file types used for the delivery of malicious payloads over the data period is shown below:

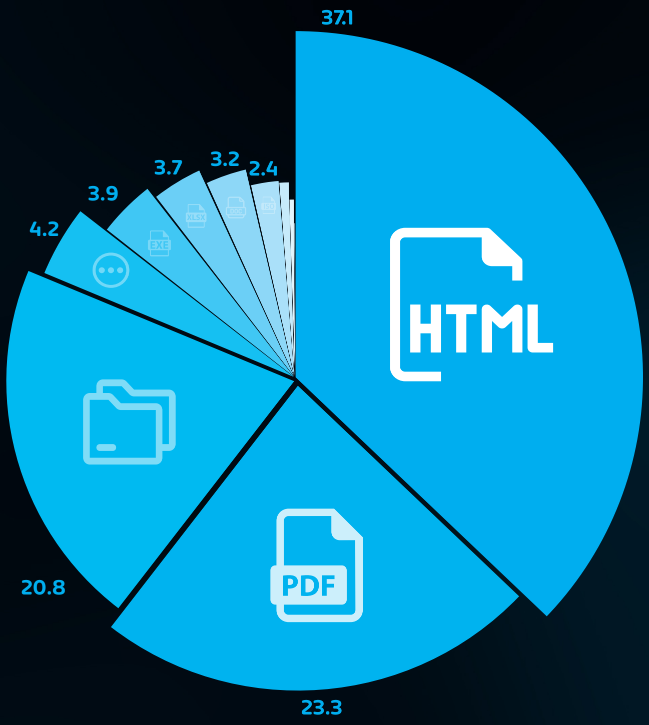
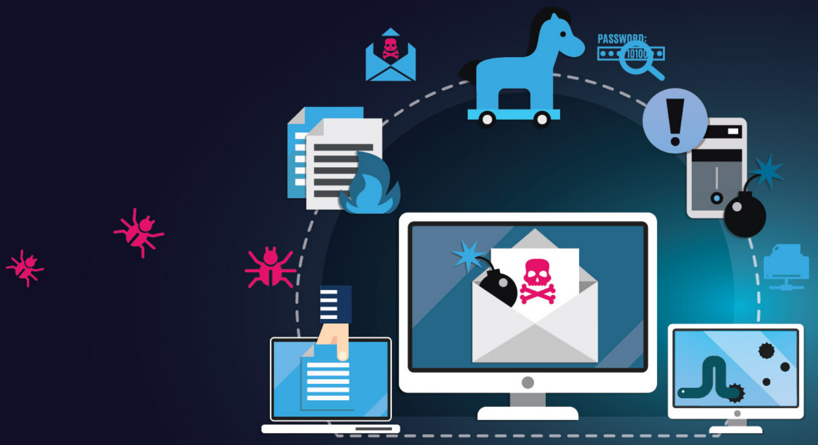


Fig. 10: File-Types for Malicious Payloads 2023

Despite the decrease in HTML files used in email-based attacks that we talked about earlier, HTML is the number one attachment file type used by attackers, with PDF in second place, followed by Archives in third place. HTML, in the first place, comes as no surprise due to the fact that HTML is a file type that can be read and interacted with on just about any platform. Regardless of the target user's operating system, the HTML file will be able to be opened, increasing the chance of success for the threat actor.



When we compare the above data with last year (shown below), there are a number of differences that stand out.

	2022	2023	
HTML	21.0	37.1	HTML
PDF	12.4	23.3	PDF
	28.0	20.8	ARCHIVE
⋯	4.8	4.2	OTHER
EXE	4.3	3.9	EXECUTABLE
XLSX	10.4	3.7	EXCEL
DOC	12.7	3.2	WORD
ISO	5.4	2.4	DISK IMAGE FILES
<>	0.7	0.8	SCRIPT FILE
N	0.0	0.4	ONENOTE
✉	0.1	0.1	EMAIL
LNK	0.1	0.0	LNK FILE
PPTX	<0.1	0.0	POWERPOINT

Fig. 11: File-Types for Malicious Payloads 2022 and 2023

Over the last year, there has been some activity amongst cyber-criminal groups and in the industry that can explain these changes. With regards to the increase of HTML and PDF files, we can attribute this somewhat to Qakbot. Despite the disruption of Qakbot by Global authorities during the summer of 2023, Qakbot did see quite a bit of activity this year. Qakbot was known to use both HTML and PDF documents to aid in its infection of target machines. That said, this will continue to be a popular deployment mechanism for future malware/botnet operators as well.

The large decrease in the use of DOCX and XLSX files compared to last year can be attributed to Microsoft's new practice of blocking macros in Office by default. This makes those file types less appealing to threat actors.

Email Threat Index for Business Verticals

One of the key areas we review on an annual (and monthly) basis is the number of threats being levied at different industry verticals. This allows us to determine if there are given campaigns or targeted attacks at certain businesses. It also provides some insights that businesses can use to help determine if they are at increased risk of attack or not.

One key change that we observed in last year's data was the fact that the industry threat index was roughly the same across all sectors. Said data supported the conclusion that it doesn't matter what business sector you're in. If your organization has the ability to pay a ransom, you ARE a target. Our data for this year (below) shows that the trend continues. The threat index is mostly the same amongst the top ten verticals.

That all said, there were some industries that were targeted slightly more than others.

- **Research Industry** - We see research organizations end up as targets simply for the intellectual property they typically handle.
- **Entertainment Industry** - Organizations of this type typically fall into gambling, or ticket sales. etc. These organizations become a target due to the large amount of money involved. Look at the 2023 attack on MGM and Caesars Entertainment, for example.
- **Manufacturing** - Manufacturing has a long history of being targeted frequently by threat actors. This typically comes down to threat actors going after intellectual property. Many see this sector as an easy target for ransomware and production disruption due to the nature of their network security and the fact that they often utilize a large number of insecure IoT devices.

The table below shows the threat index rating for major industry verticals.

3.0	RESEARCH INDUSTRY
3.0	ENTERTAINMENT INDUSTRY
3.0	MANUFACTURING INDUSTRY
2.9	MEDIA INDUSTRY
2.9	HEALTHCARE INDUSTRY
2.7	TRANSPORT INDUSTRY
2.6	HOSPITALITY INDUSTRY
2.6	AUTOMOTIVE INDUSTRY
2.5	UTILITIES
2.5	INFORMATION TECHNOLOGY
2.5	EDUCATION INDUSTRY
2.4	UNKNOWN
2.4	CONSTRUCTION INDUSTRY
2.4	MINING AND METAL INDUSTRY
2.4	FINANCIAL INDUSTRY
2.4	AGRICULTURE INDUSTRY
2.3	PROFESSIONAL SERVICE
2.3	RETAIL INDUSTRY
2.2	REAL ESTATE INDUSTRY
1.8	LOGISTICS INDUSTRY
2.4	GLOBAL MEDIAN
99.3	GLOBAL MAXIMUM

Fig. 12: Annual Industry Threat Index

NOTE: The threat index value is determined by the following calculation:

Threat Index Percentage = number of malicious emails (Threat+AdvThreat) / (the number of malicious emails (Threat+AdvThreat) + the number of clean emails) multiplied by 100 - Excluding spam and info mail

Note on methodology

Different (sized) organizations receive a different absolute number of emails. Thus, we calculate the percent share of threat emails from each organization's threat and clean emails to compare organizations. We then calculate the median of these percentage values for all organizations within the same industry to form the industry's final threat score.

Brand Impersonation

Brand impersonation continues to be a major email attack technique targeting end users in 2023.

Brand impersonations during the data period continue to follow the usual trends. DHL, Amazon, and FedEx all remained within the top ten. This has been on an upward and repeated trend for some time. The COVID pandemic drove a large increase in online shopping, and that practice has stuck with consumers ever since. Threat actors know this, and if they can land a convincing shipping-related phishing message in the target's mailbox at just the right time, they have a high chance of success.

Also notable is the inclusion of Microsoft, LinkedIn, and Netflix within the top 10. Microsoft being here is primarily driven by attempts at gaining access to Microsoft Cloud services credentials by current popular adversary-in-the-middle attacks utilizing reverse-proxy toolkits like the W3ll Phishing Kit.

These styles of attacks are adept at bypassing MFA protections and can be quite tricky to protect against.

LinkedIn and Netflix brand impersonation is a bit more nuanced for threat actors. Compromised LinkedIn accounts give attackers access to vast amounts of information regarding whatever account they've compromised, along with connections of the compromised account. We've also seen cases where threat actors use a compromised LinkedIn account to ultimately attack another LinkedIn user by posing as a trusted business connection. Netflix brand impersonation is primarily seen as a means to take over accounts and either sell them or attempt to use those same credentials in credential- stuffing attacks.

Our data over the reporting period regarding this point is shown below:

26.1	DHL
18.5	OTHER
7.7	AMAZON
5.7	POSTBANK
2.5	STRATO
2.4	LINKEDIN
2.4	MICROSOFT
2.3	FEDEX
2.2	NETFLIX
2.1	1&1

Fig. 13: Top 10 Annual Impersonated Brands

NOTE: Brand impersonation data is heavily affected by regional variation. Several German brands are listed here due to our large customer base in Germany.

Safety of Data in the Cloud

While talking about the state of security in the Microsoft 365 space, it's quite more than email, isn't it? M365 has changed the way that organizations conduct business. More frequently, businesses are utilizing the additional features in M365, and so the discussion about the state of M365 security must pass beyond just the borders of email.

The remaining sections of this report discuss many security considerations within Microsoft cloud services, but it's worth discussing the overall state and culture of current Microsoft security. That's to say, it's not currently great. Microsoft has had several security concerns over the last several years. This includes multiple security breaches, such as the Storm-0558 situation, multiple on-prem Exchange Server vulnerabilities, and the leakage of 32TB data out from a cloud storage account.

Note

For a more comprehensive discussion regarding recent Microsoft Cloud security issues, please see this podcast episode where Andy Syrewicze and Paul Schnackenburg talk about the issue at length.

All this brings into question the idea of Microsoft's role in securing your business. Currently, Microsoft's security culture is being questioned by many in the industry, and it brings the idea of vendor overdependence to the fore.

What is Vendor Overdependence?

Vendor Overdependence is the practice of placing many or nearly all core businesses processes and procedures into the hands of a single vendor partner. The problem with the arrangement is if the vendor has issues of some sort, then the business suffers disproportionately as a result.

A couple examples:

1. Offsite backups have long been a standard for IT best practices. This applies to data stored within M365 as well. Relying on the retention capabilities of M365 or leveraging the M365 backup product from Microsoft (when it is finally released) is akin to storing backups on the same storage / platform as production system. If the Microsoft cloud is unavailable, then possibly so are the data recovery methods.
2. The size and scope of the Microsoft Cloud makes them a target for threat actors. Attackers know that if they beat Exchange Online Protection for one customer, they've likely done so far ALL M365 customers. This is a case where a third-party security solution can provide better capabilities than the native provider, especially against high-severity attacks
3. It's rare, but there have been cases where the Microsoft Cloud becomes unavailable for a time. The last year has seen several Azure Active Directory (Now called Azure Entra) outages, that have made it impossible for customers to access their data in M365.

Microsoft currently holds an extremely large market share with Microsoft 365. Many in the industry question the practice of using the same vendor for both productivity/collaboration software and security. There is a potential conflict of interest in that if there is a failure or problem with one of said vendor's security products, it may NOT adequately disclose or fix such issue due to the risk of losing business in the productivity/collaboration space.

Again, organizations each need to make their own decision when it comes to this matter. Still, considering recent security concerns, and, ultimately, where Microsoft's responsibility ends with regard to your data, the choice comes into focus.

What is Microsoft Responsible for?

Many ask: "If Microsoft isn't taking care of my data and security, what are they really responsible for?" The current stance from Microsoft on this question has remained the same in 2023. To fully understand, you must be familiar with Microsoft's Shared Responsibility Model.

The critical bit is that the shared responsibility model states, "The Responsibility is always retained by the customer for":

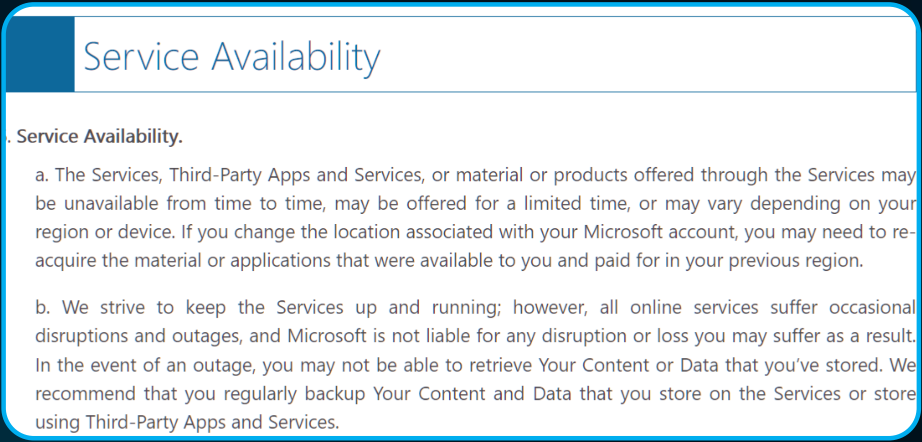
- Information and Data
- Devices (Mobiles and PC)
- Accounts and Identities

Essentially, the customer is responsible for securing and protecting their information and data. Microsoft is not. As organizations move to the cloud, they must consider this when protection strategies are implemented.

That said, Microsoft has changed a long-time stance in 2023 on the use of backup applications with M365. At a Microsoft conference earlier this year, Microsoft announced Microsoft 365 Backup. A service was shown to provide basic backup capabilities for M365. Despite this, very little to no additional information has been released since this limited announcement. The important part of this announcement is not the service itself but the change of Microsoft's historic stance of "you don't need to backup data in M365". Many in the industry see this as being driven by one of two things:

1. Microsoft has finally capitulated and now agrees that a focus on data retention alone is NOT enough in M365.
2. Microsoft simply wants a piece of the M365 backup market now that they've seen there is a large market for such a service.

Both options seem likely, with option two being bolstered by the fact that they have also released a backup API that vendors can use as well, for a fee. Regardless, the message is clearer than ever. Businesses ARE responsible for the protection of any data that they place within Microsoft Cloud services.



Service Availability

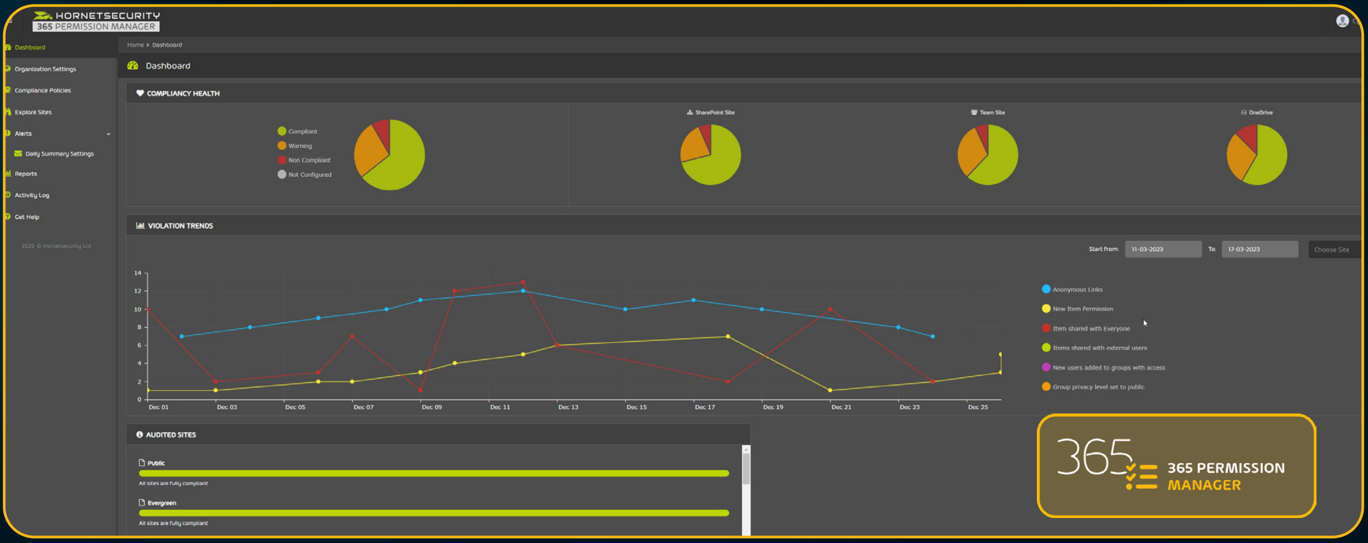
. Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

The Struggles of Proper Permissions Management in M365

Another particularly pernicious challenge for IT is sharing permissions in SharePoint and OneDrive for Business sites. Today's business environment consists of collaborative virtual teams, often in separate businesses, sharing documents in various ways. It's not feasible to lock this down (this only drives users to use unsanctioned forms of cloud document sharing – impacting IT's visibility), nor can you leave the door wide open with links to sensitive data being shared indiscriminately. The built-in tools to manage this in Microsoft 365 are fragmented across various portals and clunky to manage at scale, making permissions management in the Microsoft Cloud also a large area of concern regarding the state of security in M365. That said, Hornetsecurity's unique 365 Permission Manager makes managing sharing policies across thousands of accounts a breeze, including being able to audit who's got access to what and aligning access to different sites with company risk management.



Start from: 11-03-2023 To: 17-03-2023

Public
All sites are fully compliant

Evergreen
All sites are fully compliant

Chapter 3 – An Analysis of the Major Security Incidents and Cybersecurity News of 2023

There have been several notable attacks and security concerns in 2023 that directly relate to the data collected for this report. This section focuses on those attacks.

Storm-0558

Over the last 12 months, several high-profile security incidents affected the Microsoft 365 cloud service, but the most impactful one was definitely the Storm-0558 attack. In summary, the Chinese state-sponsored hacking group Microsoft designates as Storm-0558 compromised an engineer's account back in 2021. Even though the production environment is isolated from the corporate network, in April 2021, a consumer signing system (part of Azure AD, now Entra ID) crashed and generated a crash dump. This was moved to the production network for debugging, and the automated system designed to detect credentials in dumps failed. Thus, when the attackers breached this one account, they gained access to the dump and the key.

This enabled them to mint their own keys, even though the key in the dump had expired, and because of a failure to separate consumer keys (Hotmail, Xbox, etc.) from corporate keys (M365, Azure), the system to validate this wasn't enforced, only documented, these keys were valid. This allowed the attackers essentially a „back door key" to any M365 tenant (and any Azure tenant, although there's no evidence that this was used). At the time of writing, this „only" resulted in the breach of a few dozen email accounts at the US State Department and the theft of 60,000 emails.

This is possibly the most severe cloud breach ever, compromising the identity platform in a way that clearly undermines trust in the cloud, and in Microsoft's platform(s). To be clear, detecting this malicious activity by companies using M365 was very difficult, and only in June 2023 did a security analyst at a US federal agency detect suspicious MailItemsAccessed events and reported this to Microsoft and CISA. This agency only had these logs because they paid for Microsoft's highest M365 licensing SKU, E5.

This breach has had the following results – Microsoft has finally changed its approach to log availability for different licensing levels, and all corporate SKUs now have extended log access. This was first called for back in 2020 after the Solarwinds attack. Also, the US Cyber Security Review Board's (CSRB) next report will focus on this breach. Whether and how much this breach will force a reckoning at Microsoft and get them to improve their overall security game remains to be seen.

nOAuth

Another security flaw, dubbed nOAuth, exploited the common use of email accounts as identifiers, and applications registered in Entra ID (formerly Azure AD) that allowed sign-ins with consumer accounts. Microsoft does warn explicitly against using email as an identifier in these claims, but this doesn't diminish the complexity and risks associated with registering multi-tenant applications in Azure.

The MGM / Caesers Entertainment Cyber attacks

Two of the most notable breaches in the last couple of months are those of MGM and Caesar's casinos. Whilst not exhibiting the same symptoms, both nevertheless contain important lessons for protecting your business. In the MGM case an attacker from the Scattered Spider group used social engineering in a phone call to trick a help desk representative to reset all MFA methods for their Okta Super Administrator account, which they then used to set up federation to impersonate users.

Once compromised, reportedly 6 TB of data was exfiltrated, and corporate data was then encrypted in a ransomware attack.

MGM chose not to pay and have reported that they expect the overall cost to them to be $100 million, apparently, they have up to $ 200 million in cyber security insurance coverage. They had widespread outages of systems as they worked on recovery, and the reputational damage probably extends far beyond the monetary, especially as the attackers obtained sensitive data from customer interactions prior to March 2019.

Caesars were compromised through a breach at a third-party IT service provider and did elect to pay the ransom (originally the attackers wanted $30 million but this was negotiated down to $ 15 million).

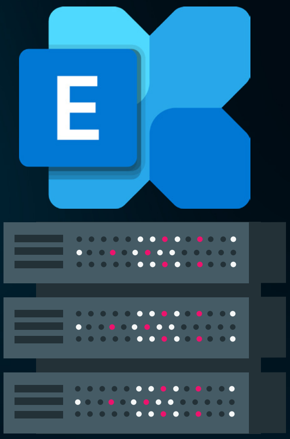
There are several lessons from these breaches to apply to improving your organization's cyber resiliency:

- Would your help desk staff have been vigilant enough to spot this attack? Train your users to be aware of all attack vectors, not just phishing emails. Vishing („Voice Phishing") is more effective than a simple email, especially as often the required personal details needed to impersonate someone are publicly available on LinkedIn, Facebook, and company websites. Qishing (QR code phishing) is another method gaining in popularity.
- Don't allow your help desk to reset MFA and passwords for high privilege accounts. Your authentication is only as strong as your reset methods, and if someone can trick a help desk user to add or reset MFA methods, it's often „game over".
- Monitor and alert on the addition of federated organizations in your IdP (Identity Provider), whether that's Okta, Ping, Entra ID in Microsoft 365, or Google.

  This vector was used by attackers in the Solarwinds breach back in 2020 and is still popular.
- Demand proof of cyber security resiliency by your third-party providers. Modern business is intertwined, so that even if your staff do everything right, you might still be breached because of lax security at a trusted provider.

Microsoft Exchange Vulnerabilities

Some organizations still run Exchange server on-premises, often in a hybrid configuration with Microsoft 365. These servers remain a prime target for attackers, in 2021 we had ProxyShell, followed by ProxyNotShell in 2022, and then in August 2023 patches for three Remote Code Execution vulnerabilities were released. In total there were 31 Exchange Server vulnerabilities in 2021, 18 in 2022 and 23 (so far) in 2023. Our recommendation is to decommission your on-premises Exchange Servers and complete the migration to Exchange Online as soon as possible.



YEAR		EXCHANGE SERVER VULNERABILITIES
2023	🐞	23 so far
2022	🐞	18
2021	🐞	31

Fig. 14: Exchange Server Vulnerabilities

The Disruption of Qakbot

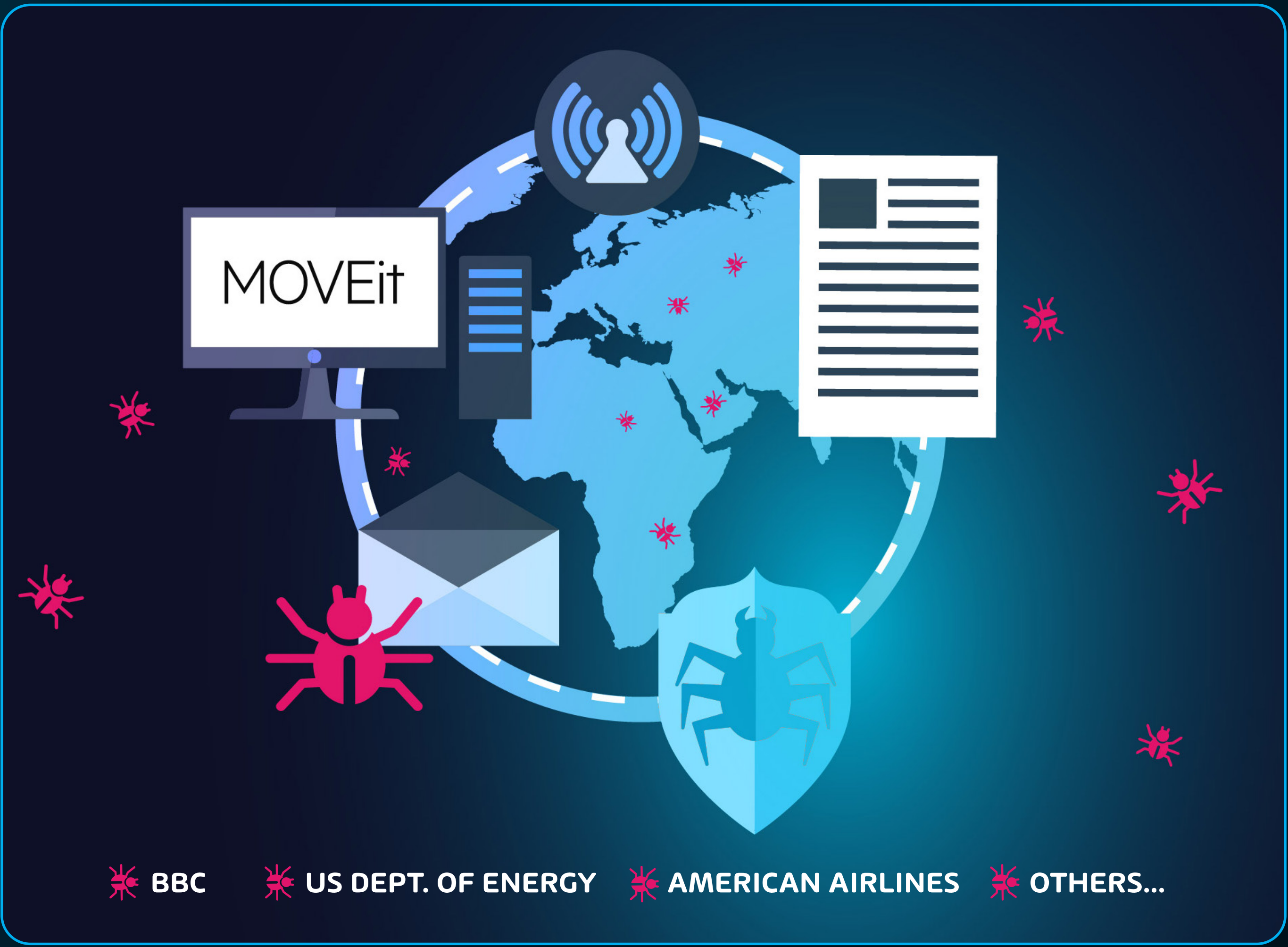
Qakbot was a well-known malicious botnet used by threat actors for a significant period of time. It was responsible for countless attacks across the web, and was covered by the cybersecurity media, and security researchers (including us!) at length.

In August of this year, the FBI and partner law enforcement organizations around the world successfully took control and shut down the Qakbot botnet. While this is no doubt a good thing, it does leave something of a vacuum. Those threat actors associated with Qakbot aren't going to give up on attacks. They'll either work to bring Qakbot back, or will move onto other tools. As we discussed in an episode of the Security Swarm Podcast, the DarkGate malware looks to be a possible contender to fill the void left by Qakbot. Security teams will need to be on the lookout for this malware and others as we move into 2024.

The MOVEit Supply Chain Attack

It wouldn't be a complete year in Cybersecurity news without major supply-chain styled attacks. There were several such attacks in 2023, but the MOVEit supply-chain attack, was by far the worst. MOVEit is a software application that provides file-transfer services for a large number of businesses across the globe. The attack consisted of the exploitation of several vulnerabilities (mostly SQL injection vulnerabilities) in the MOVEit codebase and was used to steal the personal info of countless victims. Victims included organizations such as the BBC, US Dept. of Energy, American Airlines and others.

This style of attack continues to highlight the need for effective, and agile patching processes within business IT departments. Despite the release of mitigations and patches, many organizations have remained vulnerable to these attacks for too long, and the security industry and software vendors must continue to work on solutions for mitigating the impact of future supply chain attacks.



Did We Get Last Year's Predictions Right?

We made some predictions in last year's Cyber Security Report of the type of attacks we'd see in 2023, and largely we were right.

Some criminal groups did shift to the perceived "softness" of southern hemisphere government targets, with Costa Rica, Ecuador, and Chile in 2022, followed by Brazil, Bermuda and Colombia in 2023, not to mention numerous targets in the East Asia region. We thought Business Email Compromise would overtake ransomware as the most popular attack vector, but it turns out the ransomware "business" is still healthy and heading for their overall second largest income year in 2023 at around $900 million (after $939 million in 2021).

MFA bypass techniques are increasing their sophistication and ease of use, just as we predicted, given the growth of businesses protecting identity with MFA. We're finding enterprising attackers using Teams external messages as phishing lures, with many users unaware of this vector, but the new Teams client not being built in Electron will at least make the client safer.

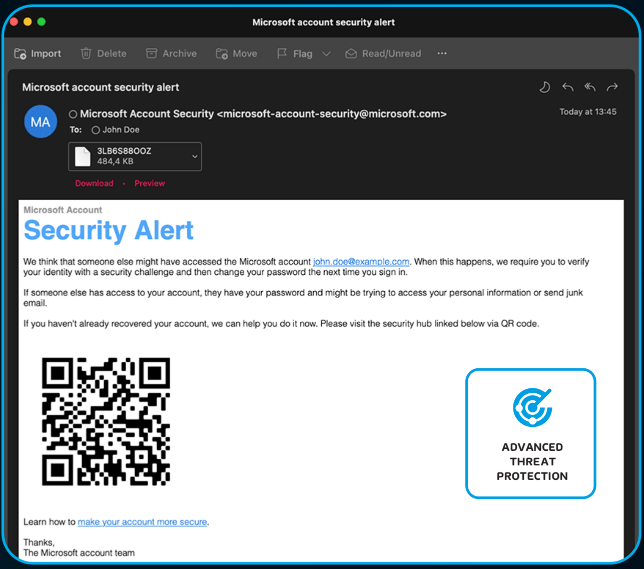
The theft of tokens from a compromised machine and then being re-used in further attacks have increased, as indeed have overall cookie robbery to aid in identity theft, personified by the FBI takedown of the Genesis marketplace in April 2023 in operation Cookie Monster.

We also looked at mobile spyware and its importance, with Predator and Pegasus being used by various nations, not only to spy on criminals, but also on dissidents, political enemies, and journalists (Greece is one example). Microsoft 365 as a platform hasn't gotten any less complex to configure securely. As we predicted the time span between a vulnerability being made public and exploit code being made available is ever shortening, challenging SOC teams to keep up.

Information Operations (IO) and disinformation is an increasing risk to business and society in general, particularly with X's (formerly Twitter) lack of content moderation under the new management standing out as an example, and with ChatGPT and other Large Language Model generative AI making it easier than ever to produce disinformation at scale.

One "prediction" that wasn't in last year's Cyber Security Report, but which has proven particularly salient recently is the inclusion of QR code email phishing in Hornetsecurity's Advanced Threat Protection platform. The last few months have seen a huge increase in this attack vector with other email hygiene solutions struggling to protect end users against malicious links embedded in QR codes.

Finally, we were right in predicting the rise of passwordless solutions, although we didn't see passkeys becoming as popular as they have in the consumer space.



Microsoft account security alert

○ Microsoft Account Security <microsoft-account-security@microsoft.com>
To: ○ John Doe
Today at 13:45

3LB6S88OOZ
484,4 KB

Microsoft Account

Security Alert

We think that someone else might have accessed the Microsoft account john.doe@example.com. When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now. Please visit the security hub linked below via QR code.

Learn how to make your account more secure.

Thanks,
The Microsoft account team

Attacks on APIs are also rapidly increasing as we said in last year's report, and this is an area that security teams will need to focus on as it's often "hidden in the background, part of the plumbing" infrastructure with little monitoring. The breach at Optus in Australia (10 million customers) in late 2022 is one example, but there are many others.

The Security Lab's Predictions for 2024

Every year, as part of this report, the Security Lab team at Hornetsecurity looks at the state of the industry, our data, attack trends, and more to make a series of predictions for the coming year. This serves to inform businesses what potential threats they may face in the coming year, along with how the industry may change. The following are the Security Lab predictions for 2024.

AI Will Continue to Drive the Cybersecurity Industry

With the release of OpenAI's ChatGPT in late 2022, and it's increasing popularity in early 2023, generative AI quickly began to alter the cybersecurity industry. It has become immediately apparent that generative AI could be used by novice threat actors to not only launch attacks, but even learn HOW to launch attacks. In fact, we did some of our own research on this in the Security Lab and posted some of our findings in the very first episode of the Security Swarm Podcast.

These new capabilities drove an increase in cyber-attacks throughout the year and continued to push the level of concern even higher. One piece of good news remains though on threat-actor use of generative AI. The fact is seasoned attackers already had these skills, and so novice threat actors looking to leverage tools like ChatGPT to launch attacks still need to put a considerable amount of time into understanding the entire attack chain for a given attack due to the fact that generative AI is not able to do that for them.

That said, one of our predictions for this coming year is that threat actors will continue to develop their darkweb variants of ChatGPT (such as DarkBERT and WormGPT) to better understand and be able to automate additional portions of the attack chain. This will lead to more capabilities for novice threat actors and speed up the rate of cyber attacks in the industry. The ability for LLMs to credibly translate text into other languages also opens "new markets" for criminals, particularly as many of those countries aren't culturally as used to phishing attacks for example.

Additionally, one potentially interesting attack we've yet to see on a large scale is a threat-actor attack AGAINST a generative-AI service. Most likely this would be done covertly and the end goal would be to poison the AI's responses for the sole purpose of spreading misinformation. Any attack of this style will be highly sophisticated and most likely nation-state driven, if (and when) it happens.

While the cybersecurity news-cycle has focused almost entirely on the negative impacts of generative AI on our industry, there is some good news as well. As the cybersecurity arms race continues, security experts and vendors are putting generative AI to use in defensive toolkits as well. There have even been some initiatives from AI organizations like OpenAI, that have created grant programs specifically designed to assist cybersecurity organizations "AI-Enable" their offerings. We predict this will manifest in a number of ways - from using AI for outlier detection, log analysis, simulated attacks (see more below), threat-modeling, and more.

Businesses will need to stay apprised of these evolutions and adjust their security posture accordingly in the coming year.

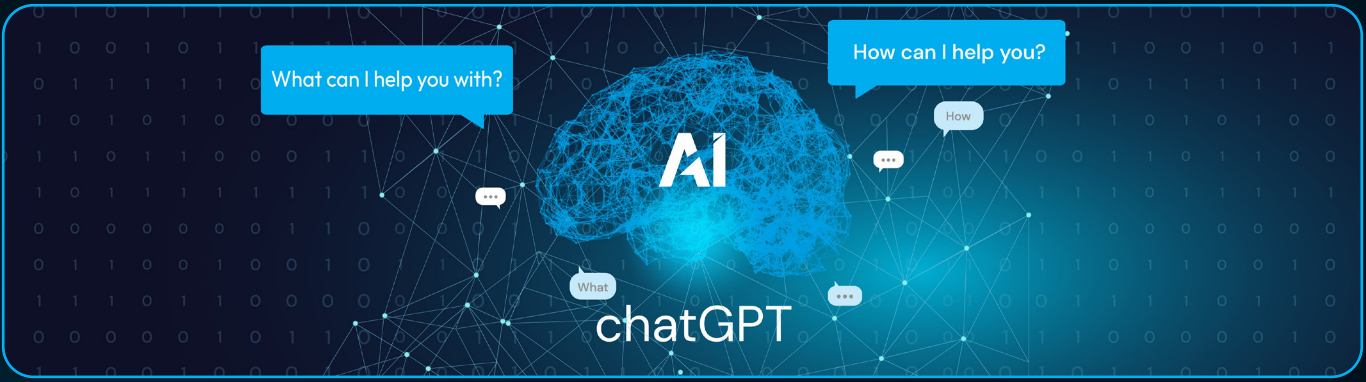
LLM (Large Language Model) Sparring Partners for Blue Teams

This prediction really falls into the previous discussion about generative-AI, but it's interesting enough to warrant its own section.

One thing that has historically been difficult for blue teams is proper threat-actor simulations. Sure, you can hire an outside organization, or bring your own penetration tester onto the payroll, but their view of the target environment is likely to be skewed by previous knowledge of the environment. Cost could potentially be an issue as well.

This is an area where Large Language Models (LLMs) could play an important role in security operations. An AI-simulated attacker could run multiple attack simulations against your organization. This plays an important role in not only finding unknown vulnerabilities in your infrastructure, but it also serves to train team members on how to safely respond during an attack.

We predict that LLMs will start to be used in new software solutions in an effort to fill this need.



Technologies Like Co-Pilot Will Drive a Need in Increased Code Security and Code Quality Scanning

Another AI-related prediction, but an important one. Technologies like Co-Pilot are making coding easier than ever. They do present one core problem though. If vast numbers of programmers are using code generated with co-pilot, isn't there a chance that some like code will be generated across multiple responses? What if a service like Co-Pilot were to fall victim to a LLM poisoning attack like we mentioned earlier? Also, would threat actors be able to use co-pilot as a blueprint for how targets may be building applications?

You see the issue here. How do organizations:

1. Verify that the code generated by co-pilot is unique and will not lead to litigation issues
2. Verify that the code is unique enough (and secure enough) that it will not be an easy target for threat actors.
3. How do businesses know that the code generated by AI-tools is free from malicious code?
4. How do businesses build the needed processes around these types of tools for proper code review to address the previous points?

We predict that all of these concerns will drive a need for improved code security and quality scanning processes in the coming year.

MFA Bypass Attacks Will Increase

MFA bypass attacks will increase in volume and sophistication. As businesses in general move to stronger forms of authentication than the criminal's "best friend" username and password, attackers are adapting. A number of "MFA bypass kits" have appeared that streamline the process of setting up a proxy to act as an Attacker-in-the-Middle – presenting a convincing login page for the user, and as they enter their credentials (including an MFA prompt), these are passed to the real login page, thus signing the user in to the legitimate service, while the kit grabs a copy of the session cookies, allowing the attacker to impersonate the user. Examples include Evilginx (open source) and the W3LL panel and associated tools to facilitate Business Email Compromise. Various MFA technologies have different strengths, ensure your business uses the strongest ones for access to sensitive data and applications.

XDR and MDR Adoption Increases

The trend and the need for increased security in the industry is only accelerating. As a result, we predict an increase in the adoption of XDR (Extended Detection and Response) and MDR (Managed Detection and Response) solutions across all sectors.

With the pervasive nature of cyber threats, no single solution serves as adequate protection. Businesses need to adopt a multi-layered approach, and this includes proper logging and dissemination of security events across an organization's entire digital estate. Without proper visibility many attacks go completely unnoticed and CISOs and technology leaders are starting to prioritize their level of security visibility.

Increases in Supply Chain Attacks

Supply chain attacks are something that isn't really new for us in the industry. There have been a number of supply chain attacks in recent history including a March 2023 supply chain attack involving 3CX as well as the well known MOVEit attack from early summer 2023. The problem with this style of attack is the potential impact. Both cases mentioned above here put countless organizations and the private data of millions at risk.

As digital services become more ingrained in our society, they become more far reaching, and ultimately, more of a target.

Threat actors know that if they can breach a vendor that provides such a service, they are more likely to get a large payday. Not only can they hold the data ransom, but many will also then turn around and sell said data on the dark web in a double-extortion campaign. That's not the only risk though. In the case of the MOVEit supply chain attack, the exploit gave attackers easy access to every affected organization. So instead of just being able to attack a single organization, EVERY business using the affected software is at risk for data leakage, and extortion as well.

As a result, we can easily make the prediction that these style of attacks will continue and increase in the coming year.

The Complexity of the Cloud will Continue to Cause Security Incidents

One of the predictions we made last year focused on how the increasing complexity of the cloud would lead to further security incidents. We're ready to make that prediction again for the coming year as well.

As businesses continue to adopt cloud technologies at a rapid scale, and with the increase in cloud-related innovation in the industry, security sometimes seems like an after thought. There have been countless examples of Amazon S3 buckets being left unsecured, and even a breach of 38TBs worth of data right from under Microsoft's nose due to a misconfigured Azure storage account. These are just examples involving cloud storage. This isn't counting massive adoption of cloud APIs, increasingly complex network configurations, a growing "work from anywhere" workforce...etc. With these complexities, comes the increased likely hood to make mistakes, and it will lead to further breaches in the coming year.

Increased 5G Adoption and Carrier Dependence on Network Slicing VNI will Drive Mobile Network Attacks

Mobile devices have become ubiquitous in everyday life. In an attempt to keep up with society's insatiable need for more bandwidth, most mobile carriers have rolled out 5G infrastructure in their networks. In order to facilitate this many carriers have begun relying on a strategy known as network slicing. This is where the carrier will divide their network up into multiple logical networks at various levels and will then rely on software defined network (SDN) to handle routing, switching and traffic management.

The issue with software defined networks is the "software" part of that equation. Software is (generally) more difficult to keep secure and can be leveraged by threat actors to launch attacks. In fact, the NSA and CISA have actually released a report about the dangers of network slicing and have provided some guidance on the practice.

That all said, with the increased footprint of 5G, growing dependence on mobile networks, and more reliance on SDN - we expect to see more attacks in the coming year focused on mobile networks.

More Capable Threat Actors and Shortening Dwell Times

As ransomware groups become more capable and complex, we're seeing a renewed effort in executing attacks in record time. As a result, dwell time is down significantly over the last year, and we expect to see that trend continue. Dwell time is the amount of time that threat actors linger on networks prior to taking aggressive action that may alert security systems or make their presence known. With the increase in zero-days and a cybersecurity industry frantically sprinting to keep up, attackers know that they must execute their attacks in record time prior to defenses being moved into place.

Again, this points to the fact that we continue to see evidence that threat-actor groups are becoming more sophisticated (CONTI for instance). These groups are now actively testing new vulnerabilities, studying anti-virus applications and coming up with workarounds and exploits. All this points to an increased likelihood of increased ransomware attacks as well as a deliberate effort to delete data backups in the coming year.

An Update on Quantum Computing and Encryption

In last year's report we covered a future risk: quantum computing being able to easily break today's encryption standards. Unlike other risks in this report, this isn't imminent (commercially available quantum computing services are still very error prone), but because encrypted data and network traffic recorded today might be easily broken in future, it's important to start planning.

The Cybersecurity and Infrastructure Security Agency (CISA) the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) agreed and recently released this short fact-sheet. Three out of the four standards we mentioned last year are now draft standards and are expected to be finalized in 2024.

How Much at Risk Will My Organization Be in 2024?

The short and simple answer here is, again, if your organization is capable of paying a ransom - you ARE a target. This is demonstrated by our data regarding the industry email threat index across all sectors. That said, if your organization handles sensitive data, is involved in the defense space or critical infrastructure, or holds highly valuable intellectual property, you are a higher priority target.

What Organizations Should Do to Defend Themselves

Start with the Basics

There's a tendency for organizations to react to specific threats and acquire point security solutions for each area, and thus focus on technology solutions, rather than covering the basics of security hygiene first. The vast majority of businesses that are breached don't fall victim to an obscure zero-day exploit or an advanced hacking technique. Their defenses fail because they didn't implement strong authentication (MFA, preferably phish resistant hardware), allowed simple passwords, set up users as local administrators on their devices or didn't train users to be cautious when clicking links in emails. Not validating backups by testing restore procedures can lead to a very bad day when ransomware strikes, as can having a lax patching policy.

In other words, take care of basic security hygiene first, which includes technology and processes and people. Start with a Zero Trust mindset:

- **Verify each connection** – just because a device is managed, doesn't automatically make it safe, and just because a user is connecting from a known network doesn't mean it's not an attacker, utilizing stolen credentials.
- **Use least privilege** – only give users and workload identities the permissions they need to fulfil their role and perform regular reviews to make sure given permissions don't accumulate.
- **Assume breach** – build your defenses as strong as your budget allows, but also work through the possible scenarios when they fail. If an attacker compromises a user, how will you detect that? How can you limit the ability of an attacker to move laterally in your environment?

A fuller list is available in the Open Groups ZT commandments.

Culture Eats Strategy for Breakfast

To transform your organization into a cyber resilient business will take time, effort, and persistence. You cannot turn your business into a well defended cyber fortress without involving everyone and helping them see how it affects them, and why they must be part of the solution.

When it comes time to roll out MFA, make sure the C-suite leads by example, and that they (and the board) understand the reason for adding the extra friction for authentication. Part of this culture shift is understanding that cyber resiliency isn't the IT departments, or the security department's job. IT can't secure workloads they don't know about, and if the marketing department is rolling out a website and a SaaS lead tracking solution without involving IT and security, the risk that this introduces belongs with the marketing department. Every technology choice or process decision that defines how a business will run caries risk, and how that risk will be managed needs to be transparent to the business so that they can make good decisions.

And an important lesson for IT and security departments is speaking the right language – risk management. If you start talking about technical details, and how it works, you'll lose anyone else in the business, but if you translate technology and process changes into business risk (or business opportunity) language, everyone should be onboard.

And this cyber resilient business isn't static, just like other risks to business (geopolitical, economic, competitors), it's ever changing and the business needs to continuously learn and adapt. Recent examples include the way attackers are bypassing or defeating "weaker" forms of MFA, with Attacker in the Middle toolkits or MFA fatigue attacks. And social engineering is an ever-present risk – would your helpdesk have been more successful in defending your business than those of Caesar's or MGM's?

A Balanced Security Strategy

It's clear that today's security ecosystem is more diverse and dangerous than it's ever been. As a result, businesses must think about implementing a balanced approach to security. This means being aware and taking steps to mitigate advanced threats that may be targeting a given businesses' industry while also making sure that the basics are handled as well.

No organization should rely on a single security application / appliance, but instead leverage a multi-tiered approach that covers the common vectors of attack as well as any that are specific to your business vertical. This includes:

- Next-Gen Spam/Malware detection with ATP for behavioural analysis to protect against the continued barrage of email-based threats we see in this industry
- End-User Security Awareness Training to train end-users to spot social engineering attacks and spear-phishing attacks
- Backup and recovery capabilities for BOTH on-premises data and data that lives in cloud services such as M365 for recovery purposes should a ransomware attack get through
- Compliance and governance features that help protect against accidental data leakage and ensure that compliance controls are met.

By layering security strategies with these capabilities, business can be confident in their security stance as we move into the coming year.

HORNETSECURITY

365 TOTAL PROTECTION

IMPROVE YOUR SECURITY

Hornetsecurity's 365 Total Protection is specially developed for Microsoft 365. It provides comprehensive protection for Microsoft cloud services through a seamless integration. 365 Total Protection simplifies your IT Security management from the start by being simple to set up and easy to use.

PLAN 1	PLAN 2	PLAN 3	PLAN 4		
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS		
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT	PHISHING & ATTACK SIMULATION	COMMUNICATION PATTERN ANALYSIS
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS	SECURITY AWARENESS	AI RECIPIENT VALIDATION
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT	ESI® REPORTING	SENSITIVE DATA CHECK

START FREE TRIAL

About the authors

Supported by data straight from our Security Lab

WRITTEN BY

Andy Syrewicze

Andy has over 20 years' experience in providing technology solutions across several industry verticals. He specializes in Infrastructure, Cloud, and the Microsoft 365 Suite.

Andy holds the Microsoft MVP award in Cloud and Datacenter Management and is one of few who is also a VMware Expert.

Paul Schnackenburg

Paul Schnackenburg started in IT when DOS and 286 processors were the cutting edge. He runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast, Australia. He also works as an IT teacher at a Microsoft IT Academy.

Paul is a well-respected technology author and active in the community, writing in-depth technical articles, focused on Hyper-V, System Center, private and hybrid cloud and Office 365 and Azure public cloud technologies.

He holds MCSE, MCSA, MCT certifications.

Chapter 5 – Resources

- https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
- https://www.bleepingcomputer.com/news/security/w3ll-phishing-kit-hijacks-thousands-of-microsoft-365-accounts-bypasses-mfa/
- https://www.hornetsecurity.com/us/podcast-us/can-you-trust-microsoft-security/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/us/services/365-permission-manager/
- https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
- https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
- https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility/
- https://www.descope.com/blog/post/noauth
- https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
- https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
- https://www.hornetsecurity.com/us/podcast-us/monthly-threat-report-discussion-october-2023/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/
- https://www.hornetsecurity.com/us/podcast-us/we-used-chatgpt-to-create-ransomware/
- https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/
- https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/
- https://www.hornetsecurity.com/us/podcast-us/generative-ai-in-defensive-tools/

- https://openai.com/blog/openai-cybersecurity-grant-program
- https://github.com/features/copilot
- https://github.com/kgretzky/evilginx2
- https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
- https://www.bleepingcomputer.com/news/security/the-moveit-hack-and-what-it-taught-us-about-application-security/
- https://www.theregister.com/2023/05/17/another_security_calamity_for_capita/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-leaks-38tb-of-private-data-via-unsecured-azure-storage/
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3459888/esf-members-nsa-and-cisa-publish-second-industry-paper-on-5g-network-slicing/
- https://therecord.media/ransomware-deployment-dwell-time-decreasing
- https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
- https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
- https://pubs.opengroup.org/security/zero-trust-commandments/
- https://salt.security/api-security-trends?