CYBER THREAT REPORT
EDITION 2021/22

The world of cybercrime never stands still. In the new **Cyber Threat Report** – Edition 2021/22 – the IT experts from Hornetsecurity once again take a close look at the gateway of email communication and analyze the latest cybercriminal scams. In doing so, they examine what threats have emerged in 2021, what has become of Emotet, and what companies need to be prepared for when opening their inboxes in the future.

With services developed in-house, such as Spam and Malware Protection, Advanced Threat Protection plus the fully comprehensive security suite for Microsoft 365, the email cloud security and backup provider Hornetsecurity now protects over 50,000 customers worldwide. At the same time, the security analysts can make well-founded statements on the current cybercrime threat situation based on evaluated filter data and their expertise.

Chapter 1: Cybercrime ranks among the greatest threats globally

According to the latest report "Hidden Costs of Cybercrime" by the American global computer security software company McAfee, the financial losses caused by cybercrime worldwide in 2020 amounted to **945 billion US dollars**[1]. In 2018, the monetary losses were around 600 billion US dollars[1]. Within just two years, the number has increased dramatically. These financial damages include, but are not limited to, **opportunity costs, system and productivity downtime, and damage to brands.**

Security and the smooth running of IT processes are now so important in social and economic life that the World Economic Forum, in its Global Risk Report 2021, ranks the failure of cybersecurity infrastructure and measures in companies, governments and private households among the most critical threats to the world today and over the medium term. The breakdown of IT security, could lead to enormous restrictions on economic activity, financial losses and geopolitical tensions, also posing a high risk to the stability of social life.[2]

Overall, more and more companies are recognizing the potential scale of the consequences of a cyberattack and the growing risk of falling victim to one. This is now being reflected in the **increasing investment by companies in their IT security: In 2020, global cybersecurity spending totaled approximately 133.8 billion US dollars.** For 2021, expenditures are estimated at around 150 billion U.S. dollars.[3]

Email continues to be considered one of the main gateways for cyberattacks in businesses, organizations and government institutions. Business email compromise and ransomware are the most dangerous attack types, and every year hackers use more deceptive methods to achieve their goals. Data theft, espionage and the installation of backdoors, are also a serious threat to public authorities and industry.

Chapter 2: Email Threat Review 2021 by the Security Lab

In the following article, Hornetsecurity Security Lab's threat researchers give an insight into the numbers around the state of global email threats. The experts evaluated and classified emails received in 2021.

Spam, threats and advanced threats: The unnoticed dangers in email traffic

About 300 billion emails are sent every day, and forecasts predict the number sent and received for private and business purposes to rise to 361.6 billion by 2024.[4]

Email continues to be the main means of communication for companies, through which sensitive information and internal company files are exchanged.

After analyzing the email traffic of the first half of 2021, the experts from Hornetsecurity Security Lab determined that a total of **60% of the emails received by Hornetsecurity could be classified as "clean"**, i.e. desired. These contribute both to productive exchange and normal operation. However, **40% of the emails received were accordingly classified as "unwanted".**

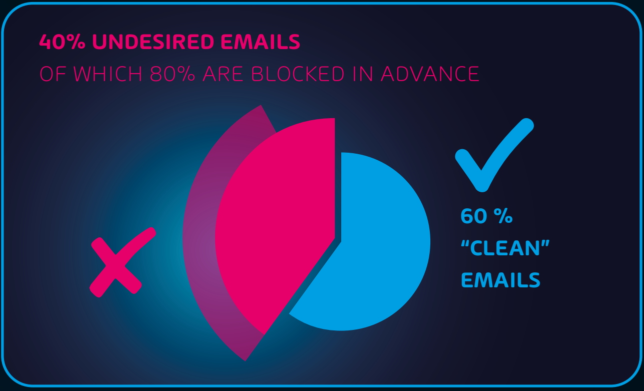


Fig. 1: Classification of emails scanned by Hornetsecurity

Of the unsolicited emails, **about 80% were already rejected in advance:** These include emails that were classified as spam using a real-time blackhole list, messages that attempted to use the Hornetsecurity mail servers as an open relay, and technical errors, graylisting, or unidentifiable email addresses.

The Security Lab classified 15.54% of all unsolicited emails as spam, 4% as threats, while 1% were detected by Hornetsecurity's Advanced Threat Protection and represent "advanced threats". These include CEO fraud, spear phishing or attacks with new types of malware, some of which are still unknown.

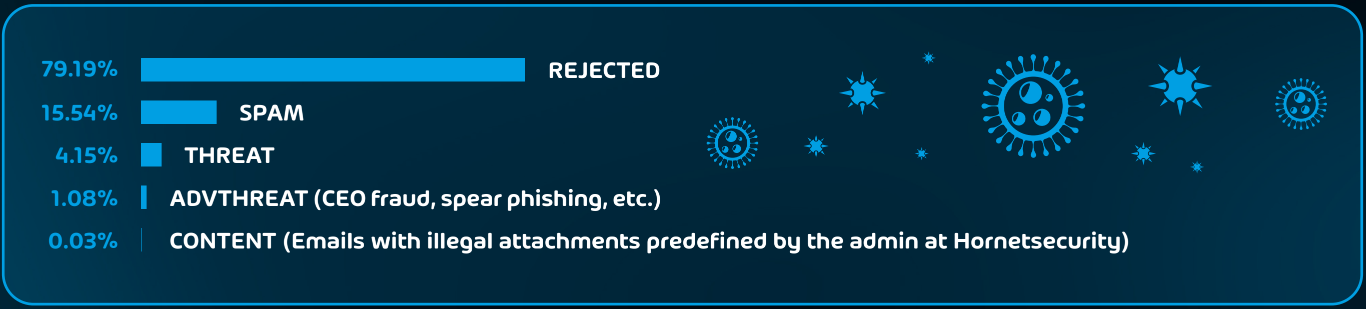


Fig. 2: Proportion of unsolicited emails by category

Attachments in malicious emails

To avoid detection by their victims' spam and virus filters, cybercriminals hide malware in their email attacks in various ways. In 2021, archive files were considered the most popular way, at 33.6%, to spread malware. The executable malware or the malware-infected document is compressed and attached directly to the attacking email. The hope here is that the target email system will be unable to scan the compressed attachments. Criminal actors with less "experience" often use this technique because it requires no technical knowledge.

In 15.3% of cases, cybercriminals used HTML files in their attack emails. In a phishing email, the phishing website is attached directly to the email as HTML, which is designed to get around URL filters and lure victims to the malicious websites to download the malware. That means no clickable URL is inserted in the email.

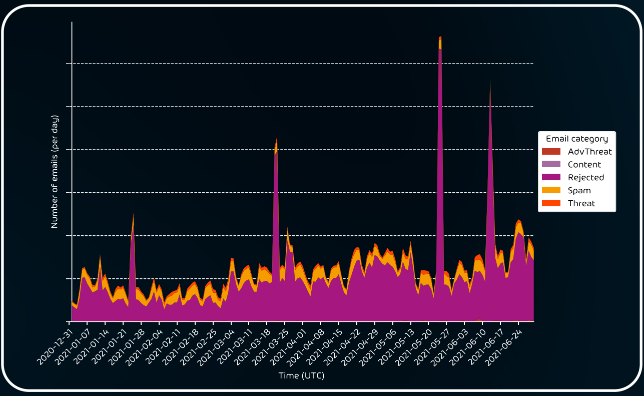


Fig. 3: Distribution of unsolicited emails by category in the first half of 2021

Over the past year Excel files (.xls, .xlsm, .xlsx, .xslb, etc.) with XLM macros have become increasingly popular (10.2% in the first half of 2021). Unlike VBA macro malware, XLM macro malware is detected less frequently, which makes it the malware of choice for many criminals. Numerous cybercriminals in fact use the same malicious document generator, called "EtterSilent", to draft their XLM macro documents.

Other file types used to compromise documents are PDF (14.5%), Word (4.8%) and PowerPoint (0.4%). PDF files, in contrast, are mainly used for spreading malicious links. Excel, PowerPoint and Word often contain macros.

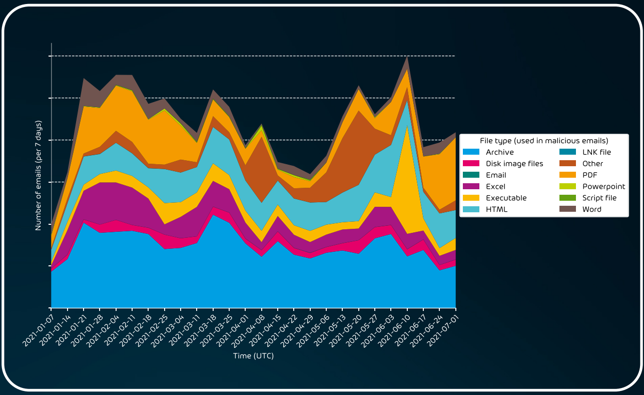


Fig. 4: Distribution of malicious email attachments per week (in the first half of 2021)

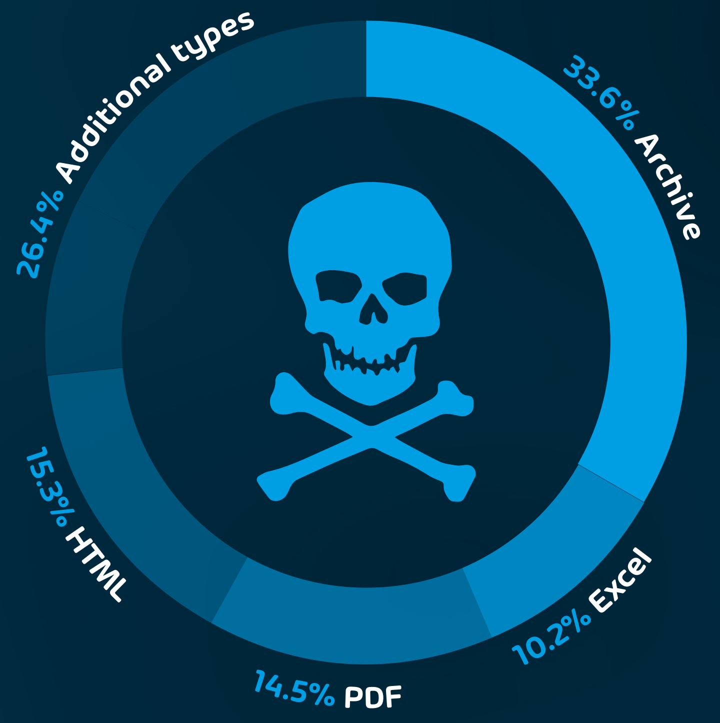


Fig. 5: Most-used file types in malicious emails

Industry Threat Index: These industries are currently particularly affected

In most cases, a malicious email is sent to a large number of email addresses. Nevertheless, some companies and industries are of particular interest to cybercriminals because they assume, for example, that such companies enjoy particularly high sales or have extremely sensitive and valuable data. The Security Lab experts use the Threat Index to determine the attack rate for different industries. In the first half of 2021, the manufacturing sector, research and development institutions, and public transport companies such as bus and rail, airlines, and cab companies, were predominantly targeted by cyberattacks.

4.9	MANUFACTURING
4.8	RESEARCH INDUSTRY
4.7	TRANSPORT
4.6	EDUCATION
4.6	MEDIA
4.5	AUTOMOTIVE
4.5	ENTERTAINMENT
4.2	HOSPITALITY
4.1	AGRICULTURE
4.1	HEALTHCARE

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

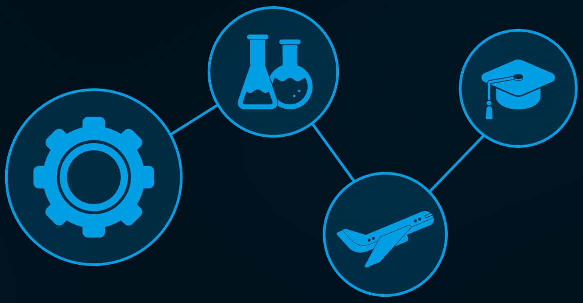
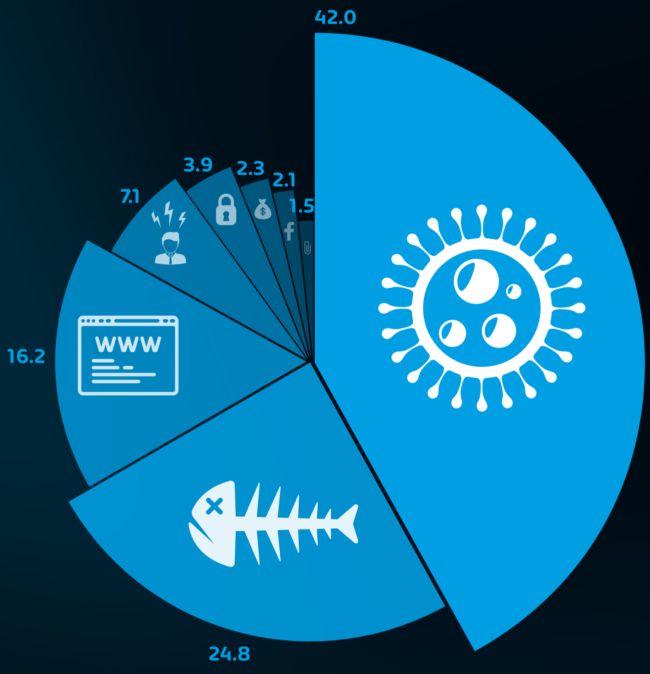


Fig. 6: Most threatened industries according to Threat Index*

* Threat Index % = number of malicious emails / (number of malicious emails + number of clean emails) * 100 – excluding spam and infomails

Procedures used by hackers in 2021

To get around virus and spam filters, hackers vary the content and presentation of their malicious emails. Phishing, brand impersonation and ransomware are just a few of the attack tactics used to get into their victims' inboxes undetected and ultimately "successfully". **Phishing emails are and will remain one of the most popular attack tactics:** Hackers use this methodology to try to obtain all kinds of sensitive data – from login credentials to credit card information. At 7.1%, "extortion" is also extremely popular among cybercriminals. The so-called "evergreen" here are the "sextortion" emails: The victim receives an email claiming that his computer was compromised while visiting a pornographic website and a video was recorded. If the victim wishes to keep the video from being put online, a ransom is to be paid.



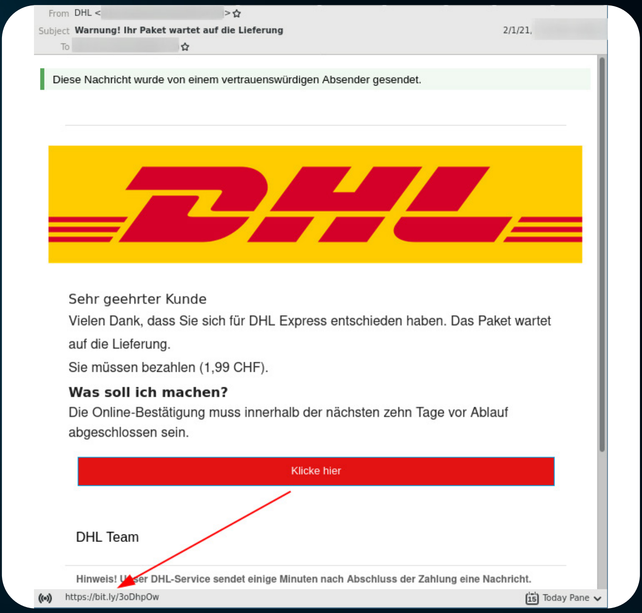
ATTACK TACTIC	%
Other	42.0
Phishing	24.8
URL	16.2
Blackmail	7.1
Executable in archive/disk-image	3.9
Advance-fee scam	2.3
Brand impersonation	2.1
Maldoc (malicious attachment)	1.5

Fig. 8: The most popular attack tactics in the first half of 2021

Amazon or Amaz0n? Beware of "Brand Impersonation"

Cyberattacks in which targeted companies are imitated are also known as **"Brand Impersonation"**. In these attacks, cyber criminals copy the corporate design of the imitated company and name the sender's address in such a way that it can hardly be distinguished from the original email address. As a rule, the goal behind this is to steal access data to user accounts or credit card data, but also to trick the recipient into clicking on a malicious link that will download malware unnoticed.

The statistics of the experts from Hornetsecurity Security Lab reveal that Amazon is the most copied company, at 17.7%. DHL is also a favorite of cyber criminals: During the Corona pandemic in particular, the number of (online) orders of all sorts of goods skyrocketed and many packages were sent and received. Emails announcing the arrival of a package are particularly easy for cybercriminals to forge. The email message is brief, the recipient usually does not question the origin if in fact a package is expected, and clicks on the tracking link. But this eventually leads to the download of a malicious program or to a phishing website, as seen in the following image:



From DHL <[redacted]>

Subject **Warnung! Ihr Paket wartet auf die Lieferung** 2/1/21, [redacted]

To [redacted]

Diese Nachricht wurde von einem vertrauenswürdigen Absender gesendet.

Sehr geehrter Kunde

Vielen Dank, dass Sie sich für DHL Express entschieden haben. Das Paket wartet auf die Lieferung.

Sie müssen bezahlen (1,99 CHF).

Was soll ich machen?

Die Online-Bestätigung muss innerhalb der nächsten zehn Tage vor Ablauf abgeschlossen sein.

Klicke hier

DHL Team

Hinweis! Unser DHL-Service sendet einige Minuten nach Abschluss der Zahlung eine Nachricht.

https://bit.ly/3oDhpOw

Fig. 9: Example of brand impersonation email with malicious URL

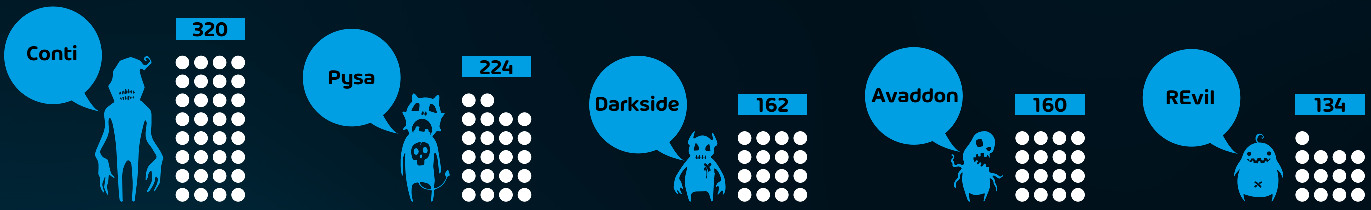
IMITATED BRAND/ORGANIZATION

17.7	AMAZON
17.1	OTHER
16.5	DEUTSCHE POST / DHL
12.7	DOCUSIGN
5.7	PAYPAL
3.5	LINKEDIN
3.0	MICROSOFT
2.5	1&1
2.3	O2
2.2	FACEBOOK
1.8	HSBC
1.2	FEDEX
1.1	EBAY
1.1	SANTANDER
1.0	FEDEX

Fig. 10: Brands/organizations exploited to infiltrate malware or to scoop up data

Ransom leaks & double extortion: Trend is growing

As early as two years ago, Hornetsecurity threat researchers predicted an upward trend of ransomware that also extorts its victims by threatening to disclose data. This development intensified in the following months. Before they encrypt the data on the victims' computers compromised by ransomware, the attackers copy the files to servers, through which they then threaten to publish this sensitive information on so-called leak pages. The hacker group behind the Conti ransomware is the most "industrious" and holds published data from 320 victims. The threat researchers from Hornetsecurity Security Lab also observed leaks on the following ransomware leak sites:



And 23 more: Babuk (70), Clop (52), Doppelpaymer (43), Nephilim (40), Lorenz (27), Ragnarok (22), Promethous (22), Everest (19), Xing Team (18), Astro Team (17), MountLocker (16), Grief (16), RansomEXX (16), Vice Society (14), RagnarLocker (11), Cuba (9), Networm (5), Egregor (5), Synack (4), LV (3), Hive (3), Suncrypt (3), Lockbit (2)

Fig. 11: The biggest leak sites by number of victims (number of people whose data was published on each site)

Analyses and evaluations by the Hornetsecurity Security Lab

Based on the observed developments of the "As a service" market in the darknet, security experts assume that in the future rising cybercrime will increasingly come from highly professional cybercriminals. Ransomware-as-a-service continues to be a major issue here, and the evolution of this criminal modus operandi poses an ever-increasing threat to enterprises, public institutions such as hospitals, and governments as well.

Overall, the ransomware trend is far from having reached its peak. According to Bleeping Computer, the ransomware group REvil has raked in $1 billion in Bitcoin within one year.[5] Backed by this money chest, masterminds of groups like REvil can, for example, hire professional penetration testers, who in turn track down further victims whose data is then also attacked by the hacker group.

Chapter 3: The "Threat-Highlights" of 2021

The year 2021 saw a few sensational events related to cybercrime, which we review in the following chapter.

The take-down of Emotet: The ups and downs of the world's most dangerous malware

The "most dangerous malware in the world" could finally be stopped. At the beginning of 2021, police units involved in the operation reported that the Emotet botnet had been dismantled.

Emotet was first discovered in 2014. At that time, it was a banking Trojan that stole banking data and login credentials. Over time, however, Emotet evolved into a malware-as-a-service (MaaS) operation that offered to distribute malware for other cybercriminals. In Germany alone, Emotet infected not only tens of thousands of private computers but also a large number of business IT systems. The Klinikum Fürth and the Kammergericht Berlin were just two of Emotet's many victims. The German Federal Criminal Police Office, or BKA, estimates the damage caused by Emotet in Germany alone at 14.5 million euros.

After successfully infecting a system, Emotet was able to read contacts as well as email content in mailboxes. To spread malware, Emotet replied to these emails highly authentically based on the information gathered, and the forgeries were very difficult to identify. This approach is also known as email conversation thread hijacking[6]. Hornetsecurity has published numerous blogposts about Emotet attacks such as this one.

On January 27, 2021, Europol announced that an international operation of law enforcement and judicial authorities, including from Germany, the Netherlands, Lithuania, Ukraine, France, England, as well as Canada and the United States, had taken over and dismantled Emotet's infrastructure.

Investigators gained control of the infrastructure by identifying various servers through which the malware was distributed. Step by step, large parts of the infrastructure were uncovered. The investigating authorities were thus able to prevent the perpetrators from accessing it and even to take over control of it from one of the suspected operators in Ukraine.

Emotet's C2 communications were cut and the information of the associated victims was shared with the country's responsible CERTs, who notified the victims to allow them to remove the malware.

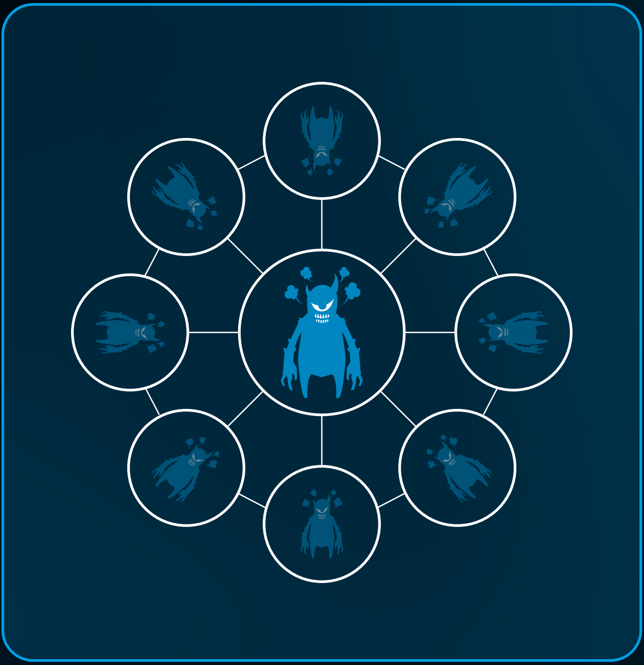
Up until the takedown, Emotet accounted for a full 20% of the malicious emails analyzed by Hornetsecurity. However, on November 15, Hornetsecurity's threat researchers once again registered the first activities of the malware. In the process, TrickBot malware was spread via malspam, downloaded and eventually the Emotet malware was installed. After that, the Emotet botnet was rebuilt and began again to send malspam from its botnet.

Emotet – the aftermath

With the demise of Emotet, new contenders have emerged to replace the botnet: While Quakbot has the necessary sophistication, its botnet is nowhere near as large as Emotet's. This makes large-scale distribution of the malware more difficult.

Others, such as the Cutwail botnet with its Dridex malspam, or the hackers behind the Hancitor malspam campaigns, can distribute malspam on a large scale but do not have the cunning of Emotet.

It must be anticipated that more players are planning to seize the title of "The world's most dangerous malware", since the existing customer base of Emotet's Malware-as-a-Service (MaaS) operation still exists and the approach could be exploited by other malware as well.[7]



Arrests around Clop, The Trick & Gozi

Besides the breaking of the Emotet botnet, there was other good news in 2021: Among others, the National Police of Ukraine arrested some people suspected of infecting companies with the Clop ransomware. The Clop ransomware operation continued uninterrupted nonetheless, giving threat researchers from the Security Lab reason to believe that the arrested individuals were not major masterminds behind the ransomware.

Another suspect, wanted since 2013 because of links to the Gozi malware, was also arrested. The suspect operated a bulletproof host that helped cybercriminals distribute the Gozi malware, the Zeus Trojan, and the SpyEye Trojan. In addition, the suspect is accused of initiating DDoS attacks and sending spam.

A co-developer of The Trick malware was also arrested in the U.S. and charged with 19 of 47 counts.[8]

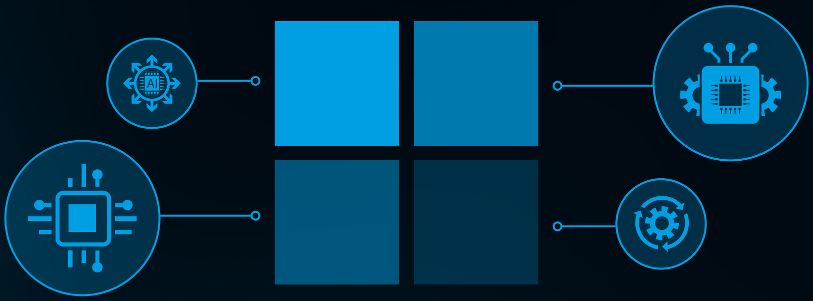
The Microsoft Exchange Hack

In March, Microsoft closed four vulnerabilities in different versions of Microsoft Exchange Server with an unscheduled security update. Yet soon after the release, mass infections of the unpatched Exchange servers began to spread via the Internet.

An estimated 250,000 servers were hit by the attacks. Even the White House urged those affected to install security patches in their respective Exchange systems, while the German Federal Office for Information Security (BSI), which deemed the threat situation to be extremely critical at the time, issued a red alert.

The mastermind is believed to be the Chinese hacker group Hafnium, which is state-sponsored and known for highly skilled and sophisticated attacks.[9]

In April 2021, even the FBI got involved. A court order authorized the FBI to penetrate corporate networks to remove webshells left behind by infections that could be used by cybercriminals to launch further attacks.[10]



Chapter 4: Forecasts and possible evolutions of cybercrime

Digitalization and the increasing networking of devices and accounts not only provide cybercriminals with more space for their schemes – cybercrime effortlessly crosses borders and continents, making it difficult to track. According to the Federal Criminal Police Office, crime is also increasingly shifting into the digital space. Crimes committed via the Internet have increased by 8.7% over the previous year, and cybercrime in particular has gone up by 7.9% in 2020 over 2019.[11]

A representative study by the Bitkom digital association revealed that 75% of the companies surveyed were attacked in 2018/2019. In 2020/2021, the figure was as high as 88%. In 2018/2019 the economic damages caused by theft, espionage and sabotage came to 103 billion euros. This number has since doubled. Current losses annually are around 223 billion euros.

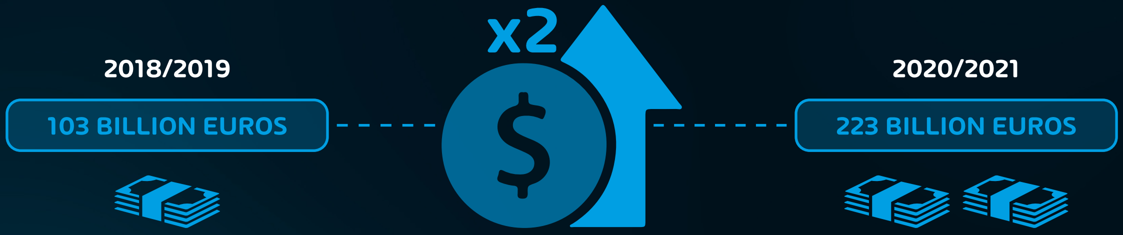


Fig. 12: Damage caused by cybercrime at companies in Germany according to Bitkom.

According to Bitkom, the main driver of the enormous increase is ransomware. The extortion malware encrypts files on computers and other systems and renders them unusable, until the operators pay up.

Damage caused by ransomware more than quadrupled (+358%) in 2018/2019 over previous years. Currently, one in ten companies (9%) consider its commercial existence to be threatened by cyberattacks.[12]

A Hornetsecurity survey of more than 820 companies also showed that **21% of respondents had already fallen victim to a ransomware attack**.

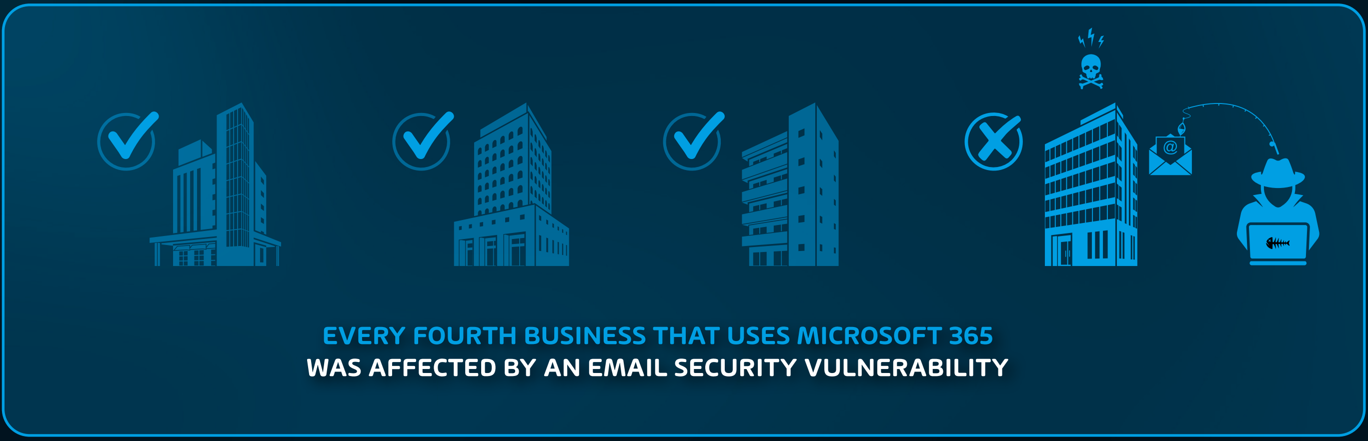
So despite the takedown of Emotet, it may yet be too early for companies to breathe a sigh of relief. Cybercrime remains a lucrative business, especially with increasing connectivity.

Focus on Microsoft 365

As of April 2020, Microsoft reported 258 million active users of the Office 365 suite. If just 10% of the computers in use are not adequately protected against cyber attacks, that makes a total of 25 million individual targets for hackers that are potentially easy to infiltrate.[13]

The Microsoft Exchange hack also shows that even state-sponsored hacker groups are increasingly focusing on Microsoft, as they know how much pressure a successful attack can put on affected companies and authorities.

As part of an email security survey of more than 420 companies that use Microsoft 365 for their email communications, Hornetsecurity found that **1 in 4 had fallen victim to an email security vulnerability at least once**.



EVERY FOURTH BUSINESS THAT USES MICROSOFT 365
WAS AFFECTED BY AN EMAIL SECURITY VULNERABILITY

Fig. 13: Hornetsecurity survey of 420 companies on Microsoft 365 security

For the most part, these could be traced back to phishing emails that found their way into users' inboxes.

As Microsoft 365 continues to proliferate as one of the most widely used cloud applications in the business space, hacking attacks on users are also expected to continue to rise.

About the Hornetsecurity Group

Hornetsecurity is a leading email cloud security and backup provider that secures businesses and organizations of any size worldwide. Its award-winning product portfolio covers all important areas of email security, including spam and virus filters, protection against phishing and ransomware, and legally compliant archiving and encryption. In addition, there is backup, replication and recovery of emails, endpoints and virtual machines. The flagship product is the market's most comprehensive cloud security solution for Microsoft 365. With more than 350 employees at 10 locations, the company headquartered in Hanover has an international network of more than 5,000 channel partners and MSPs as well as 11 redundant and secured data centers. Its premium services are used by over 50,000 customers, which include Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA and CLAAS.

Sources

(1) https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, S.6

(2) http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf, S.89 Global Risk Report 2021

(3) https://de.statista.com/statistik/daten/studie/1038510/umfrage/ausgaben-fuer-it-sicherheit-weltweit/

(4) https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/

(5) https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

(6) https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/

(7) https://www.hornetsecurity.com/de/threat-research/emotet-botnet-takedown/

(8) https://www.hornetsecurity.com/de/threat-research/email-threat-review-juni-2021/

(9) https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/ (May, 2021)

(10) https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

(11) Bundeslagebild Cybercrime 2020, BKA, p. 38

(12) https://www.all-about-security.de/management/angriffsziel-deutsche-wirtschaft-mehr-als-220-milliarden-euro-schaden-pro-jahr/

(13) https://securityboulevard.com/2021/06/microsoft-office-365-a-major-supply-chain-attack-vector/

HORNETSECURITY