E-BOOK

Cyber-threats.

The 15 most common cyberthreats and how to protect yourself

InterNetX

Table of contents.

EXECUTIVE SUMMARY 04

WHY YOU NEED CYBERSECURITY AWARENESS WITHIN YOUR ORGANIZATION 05

THE TOP 15 CYBERATTACKS AND HOW TO PROTECT YOURSELF 06

01. MALWARE 07

02. WEB-BASED ATTACKS 08

03. PHISHING 10

04. WEB APPLICATION ATTACKS 11

05. SPAM 13

06. DISTRIBUTED DENIAL OF SERVICE (DDOS) 14

07. IDENTITY THEFT 16

08. DATA BREACH 17

09. INSIDER THREAT 18

10. BOTNETS 20

11. PHYSICAL ATTACKS 21

12. INFORMATION LEAKAGE 22

13. RANSOMWARE 23

14. CYBERESPIONAGE 25

15. CRYPTOJACKING 27

DO NOT UNDERESTIMATE CYBERSECURITY:
RAISE YOUR DEFENCE. 30

REFERENCES & IMAGE CREDITS 31

ABOUT 34

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

Executive Summary.

In 2021, cyberattacks are expected to cause damage amounting to a total of $6 trillion[1]. If we think of this number as a country, it would be the world's third-largest economy after the United States and China.

Everyone should understand that **being targeted by a cyberattack today is not an "if" but rather a "when" hypothesis** you should expect to face with certainty. Thus, the number of cyberattacks is growing year after year. Since the pandemic hit, the FBI has reported a daily 300% increase in cybercrimes[2].
Current trends like cloud technology and remote working are causing more damage than ever before and the upcoming 5G technology is about to enable the connection of thousands of IoT devices, thereby becoming the new vulnerability to target on a large scale. By 2025, damage related to cybercrime is projected to reach $10.5 trillion annually[3].

Global cybercrime damage costs:

$6 TRILLION a year.

$500 BILLION a month.

$115.4 BILLION a week.

$16.4 BILLION a day.

$684.9 MILLION an hour.

$11.4 MILLION a minute.

$190,000 a second.

All figures (in USD) are predicted by 2021.

Morgen, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, Cybersecurity Ventures, 12 November 2020.

“ Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders.”

– Ronald Reagan, 40th President of the United States

1. Morgen, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, Cybersecurity Ventures, 12 November 2020.
2. Walter, J. COVID-19 news: FBI Reports 300% Increase in Reported Cybercrimes, IMC Grupo, 2 May 2020.
3. Morgen, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, see note 1.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

Why you need cybersecurity awareness within your organization.

Over the past years, cybercriminals have shifted to new targets. Victims are no longer only large multinational companies. Cyberattacks are being used to harm individuals, public and private organizations at all levels.

Each attack has its own structure and can lead to different consequences that make them more or less frightful. But the purpose remains the same: **Cybercriminals aim to make high profits from their cyberattacks at the expense of the victim.**
If the damage concerns identity or data theft, the victim can be hit at both a personal and economic level. Although there is still a gap in cybersecurity skills, and generally poor security practices put in place within organizations (such as unprotected data), defense against cyberthreats is evolving and becoming an important topic, with organizations increasingly investing in IT protection.

Forecasts see the **worldwide information security market reaching $170.4 billion** in 2022[4]. But let's face the truth: despite taking all technical necessary measures, **complete security will never exist.**

We are far away from finding ourselves in a secure digital environment. Cybercriminals today are using very sophisticated techniques and vulnerabilities can be spotted more easily.

Security policies, equipment, and technology are essential, but cybersecurity awareness must be pushed past the boundaries of IT departments. **Every person within the organization must understand exactly what the threats are, and what they look like.** Irresponsible and uninformed employees might be the weakest vulnerability in your organization. The real danger often comes from within and **the most successful weapon to counterattack cyberthreats is knowledge**, i.e. educating employees helps mitigate risks and safeguards the integrity of your business, communications, and data.

4. Contu, R. et al. Forecast Analysis: Information Security, Worldwide, Gartner, 14 September 2018.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

The Top 15 cyberattacks and how to protect yourself.

You can’t protect yourself and your organization from cyberthreats if you don’t know them. While terms like malware or spam sound quite familiar, the mechanics behind these is usually unfamiliar to most. The questions we want to address here are: What are the 15 most common cyberattacks to watch out for in 2021? And how can you protect yourself against them?

What we are going to present to you is not the kind of cyberterrorism attack that aims to destabilize the social order with much wider consequences and serious correlated damage in the real world. Although some cyberattacks can be attributed to hacktivism, i.e. actions aiming at companies and organizations for reasons of activism and protest, here we will focus on cyberattacks oriented towards a particular victim for reasons of personal or profit. In short, **we are going to talk about the kind of cyberthreats that usually target businesses.** Understanding how they are delivered, where they come from and what the major risks connected to them are will lead us to better understand how to protect ourselves. Let’s take a more detailed look at the 15 most common cyberattacks!

What is a cyberattack?

We can describe a cyberattack as an attempt to gain unauthorized access to networks, services, resources or system information. Quite often, the aim can also be to compromise the integrity of these systems and alter the confidentiality, integrity and availability of the data.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

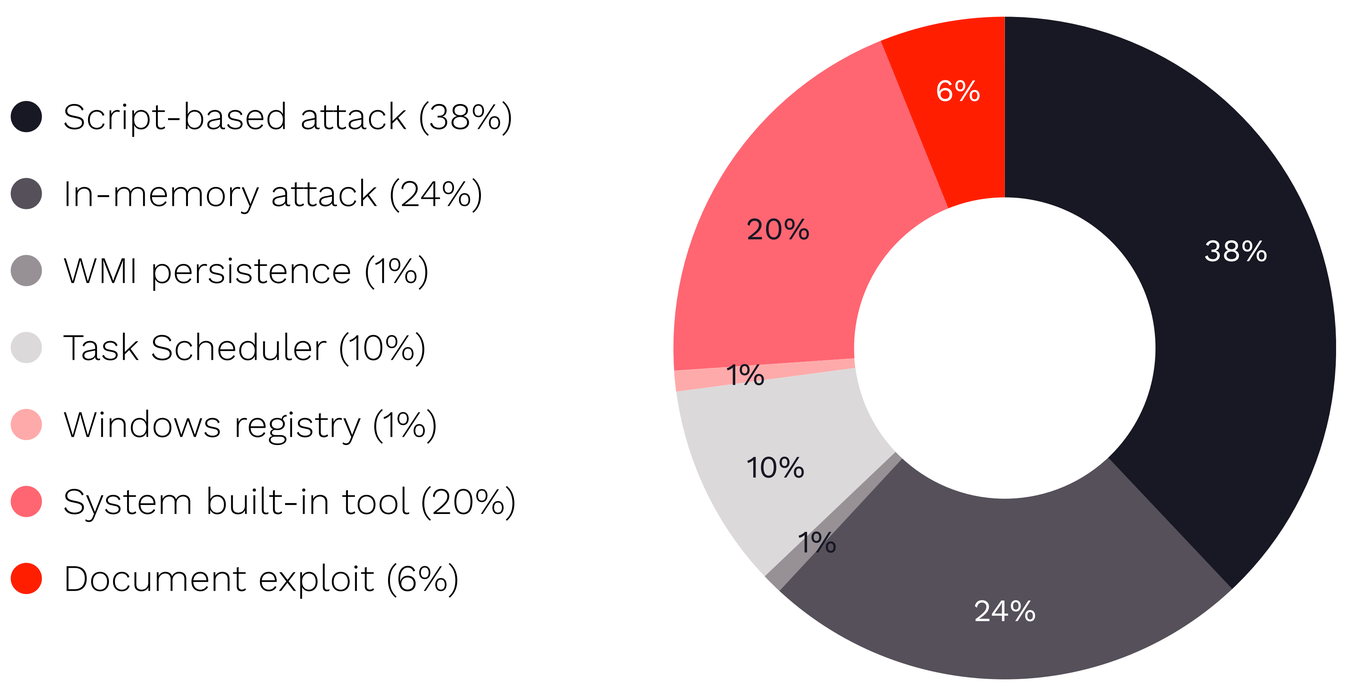
01. Malware

Malware combines the words malicious and software. In general, **we use malware to name any intrusive software developed by hackers.** Common examples include viruses, worms, trojans, spyware, adware and ransomware. **Malware clearly stands out as the number one cyberthreat in the European Union[5].** These malicious programs are specifically designed to get downloaded and installed on the computer without the user knowing about it or even realizing it. When the installation is complete, the software can cause severe damage such as a data breach.

In 2020, there was a noticeable shift (+13%) from consumer to business targets with the top 5 strains of malware being Trojan.Emotet, Adware.InstallCore, HackTool, WinActivator, RiskWare.BitCoinMiner and Virus.Renamer[6].

94% of all malware types in 2019 were delivered via email[7] and 46.5% of all malware in emails had a .docx file format. In 2018, **1 in 13 web requests led to malware[8].** Cybercriminals have updated their business model. In underground forums, they sell **MaaS (Malware as a Service)**: a kit with a loader, command, and control server (C2) plus a backdoor for controlling the infected computer.

Percentage of file-less events detected in Q1 2019



Johansen, A. G. What is fileless malware and how does it work?, Norton, accessed: 15 June 2021.

5. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Malware, 20 October 2020.
6. Ibid.
7. Verizon. 2019 Data Breach Investigations Report (PDF), accessed: 15 June 2021.
8. Symantec, Internet Security Threat Report, March 2018.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

How to protect yourself against malware

First and foremost, remember to always keep your computer and devices up-to-date. A good active antivirus should potentially cover your systems and networks. Use a mail spam filter to protect your mailbox and remove executable attachments. Be very careful when opening email attachments, before clicking on links or downloading anything from the web. Allow your firewall to decrypt the SSL/TLS traffic, emails and mobile applications. With the DigiCert Smart Seal, you can show your website visitors the status of the malware scan.

DISCOVER EFFECTIVE MALWARE PROTECTION AT INTERNETX

02. Web-based attacks

Cybercrime can use **web systems and services as a means to mislead victims.**

Malicious URLs or scripts to redirect the users to malicious content fall under this category. This is exactly what happens, for example, with watering hole attacks: a strategy used by cybercriminals after observations or simply by guessing the websites the target uses more often and infecting them with one or more malware.

In 2020, **39%** of all data breaches came through web applications[9].

Formjacking is another technique used to inject malicious code into the online payment forms of legitimate websites.

9. Verizon, 2021 Data Breach Investigations Report, accessed: 15 June 2021.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

Nowadays, **the attack surface is greater than ever before.** As of June 2021, there are over 64.3 million live websites that use Content Management Systems (CMS) on the entire internet[10], so they have become an important vector of web-based attacks. They open up a wide range of possibilities for hackers due to a large number of vulnerabilities connected to third-party plugins, often outdated. Web-based attacks can also target the availability of a website, its applications and APIs or cause brute-force attacks, which overwhelm the website with many login attempts[11].

How to protect yourself against web-based attacks

Always be careful to use the most updated browser version and related plugins. They could detect potential vulnerabilities or threats in the web pages. If you have any doubts, you could isolate the applications and create a sandbox in your browser. Tools such as adblockers or JavaScript blockers can hinder the execution of malicious codes in compromised websites. If you run your website in a CMS, keep the source code up-to-date. Newly released updates often include security patches. Furthermore, use an SSL certificate to encrypt communications and prevent data theft.

Not sure which SSL certificate you should choose for your website? We have the right certificate for each and every purpose.

DISCOVER SSL CERTIFICATE SOLUTIONS AT INTERNETX

10. BuiltWith, CMS Usage Distribution on the Entire Internet, accessed: 15 June 2021.
11. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Web-Based Attacks, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

03. Phishing

This is one of the most popular attacks you have almost certainly heard of before; **80% of reported security attacks in 2020 were based on phishing[12].**

During the COVID-19 pandemic, there was an increase of **667%** in phishing scams[13] within one month.

Phishing attacks today come through different platforms such as email, social media or messaging apps, but the underlying mechanism remains the same[14], i.e. **hackers pressure the target person to carry out a certain action.** This can be, for example, providing login or e-banking information, clicking a link that leads to a malicious website or installing malware. Once the user has done exactly what the criminal wants, the threat actor can access your accounts or log into your computer systems.

The most worldwide known version of phishing is probably the **Nigerian prince scam**, also called a 419 scam. The criminal contacts you with a story about a large amount of money trapped in a bank or about a large inheritance that is hard to access due to government restrictions or taxes in the local country. The scammer asks for your bank account details to help transfer the money and offers you a large amount in return.

Nowadays, **phishing attacks have become much more targeted** and can address you personally. These types of targeted scams are called spear phishing and they have become a significant part of cybercrime. In 2019, spear phishing was experienced by 88% of organizations worldwide[15].

12. Fruhlinger, J. Top Cybersecurity Facts, Figures and Statistics, CSO, 9 March 2020.
13. Symanovich, S. Coronavirus Phishing Emails: How To Protect against COVID-19 scams, Norton, 5 March 2020.
14. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Phishing, 20 October 2020.
15. Egan, G. State of the Phish 2020, (PDF), Proofpoint, 23 January 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

How to protect yourself against phishing

There is only one golden rule that applies here: Be careful who you give your information to. There are no technologies that can assure 100% prevention against scam emails. Carefully check the contact details of the sender and, before clicking on any links, analyze them by scrolling over the links with the mouse or copy and paste them into your browser to see what they look like. Only use a safe connection through HTTPS and always check the domain name.

04. Web application attacks

The internet has become a highly programmable environment. In recent years, the web has seen an increasing number of applications, software run on web servers, rather than locally on the operating system of the device. This is why **the security of web applications has become one of the biggest topics in the digital environment**. In 2019, a **52% increase of this threat year-over-year**[16] was registered. This is mostly due to the complexity of the source code which greatly increases the likelihood of unforeseen

20% of companies and organizations reported daily DDoS attacks in their web apps, with buffer overflow being the most common technique (24%), followed by HTTP flood (23%), resource reduction (23%), HTTPS flood (21%), and Low Slow (21%)[17].

16. SonicWall. 2020 SonicWall Cyber Threat Report, 4 February 2020.
17. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Web Application Attacks, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

vulnerabilities and malicious code manipulation. Furthermore, web apps often contain very sensitive data which can be quite lucrative and the attacks can be executed easily and launched automatically against thousands of targets at a time[18].

The targets of the cyberattacks are quite often the databases and the web applications used to store or deliver information, such as in the case of a SQL Injection attack, probably the most common and dangerous vulnerability to manipulate a backend database.

How to protect yourself against web application attacks

As a user, there is not much you can do to protect yourself against a compromised web application. Be sure to use an encrypted connection and an updated browser. It is the provider's responsibility to detect any possible vulnerabilities and deliver a bug-free web app. This can also be done using a professional software scanner. Web app firewalls can work to a certain extent. They might point out the vulnerability but can't eliminate the problem. Unfortunately, they can be bypassed by cybercriminals. Using a strong input and injection validation procedure will help only properly-formed data to pass. Implement an encrypted connection and, last but not least, rely on a professional service provider that is able to host your web application with the maximum security, availability and performance.

DDoS mitigation, encryption and DNSSEC protection. These are just a few of the reasons why you can rely on InterNetX hosting solutions.

DISCOVER WEB APPLICATION HOSTING SOLUTIONS AT INTERNETX

18. Imperva. Web Application Security, accessed: 15 June 2021.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

05. Spam

You might have received a fake invoice in your mailbox at least once. Any kind of unwanted message you receive without giving your consent falls under this category. **Spam is not only annoying, it also falls under the large category of cybercrime.**

Nearly **85%** of all emails sent worldwide are spam![19]

Spam messages are often connected to some kind of scam or fraud. In March 2020, riding the wave of the pandemic, scams experienced an **increase of 400%[20].**

Nowadays, **85% of the worldwide spam is sent by botnets**, a network of compromised computers[21]. Unlike phishing attacks that are targeted actions usually based on social engineering techniques, **spam is sent to a bulk list.** The user is encouraged to visit a compromised website, where eventually malware will do the rest. The message might include a fake message about the expiry of a domain, for example, asking the user to provide their bank account details. Do not fall for such malicious actions!

How to protect yourself against spam

Spammers are constantly harvesting new email addresses on the internet, so the most important piece of advice is to avoid posting your email address publicly. Your email client should do the first round of filtering, marking most messages with high potential as spam. If you consider a message to be suspicious, do not open any attachments but above all, do not reply! If you fail to do so, you are sending a clear message to the hackers saying this is an active email address. As a result, you will probably receive even more spam! There are many antivirus and

19. Cvetićanin, N. What's On The Other Side Of Inbox - 20 Statistics For 2021, DataProt, 11 February 2021.
20. O'Donoghue, C. et al. Coronavirus is Now Possibly The Largest-ever Security Threat - Here's How We may Be Able To Tackle It, Reed Smith, 24 March 2020.
21. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Spam, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

spam filtering tools that can help you detect emails containing malware and decipher malicious messages. Try not to use your business electronic address when registering for services, deal newsletters and similar. Although it does not prevent receiving spam, implementing an S/MIME certificate blocks other email-related threats that you might encounter with spam.

DISCOVER S/MIME SOLUTIONS AT INTERNETX

06. Distributed Denial of Service (DDoS)

Hackers can manage to exhaust the service or overload one or more elements of the network infrastructure systems. The impact ranges from unavailable services to entire websites, applications, or businesses taken offline. In such cases, we talk of a **Distributed Denial of Service (DDoS)** attack, where **the aim is to saturate the resources to block network communication.** This is the reason why servers and data centers are their favorite targets. By 2023, experts foresee 15.4 million DDoS attacks annually.[22]

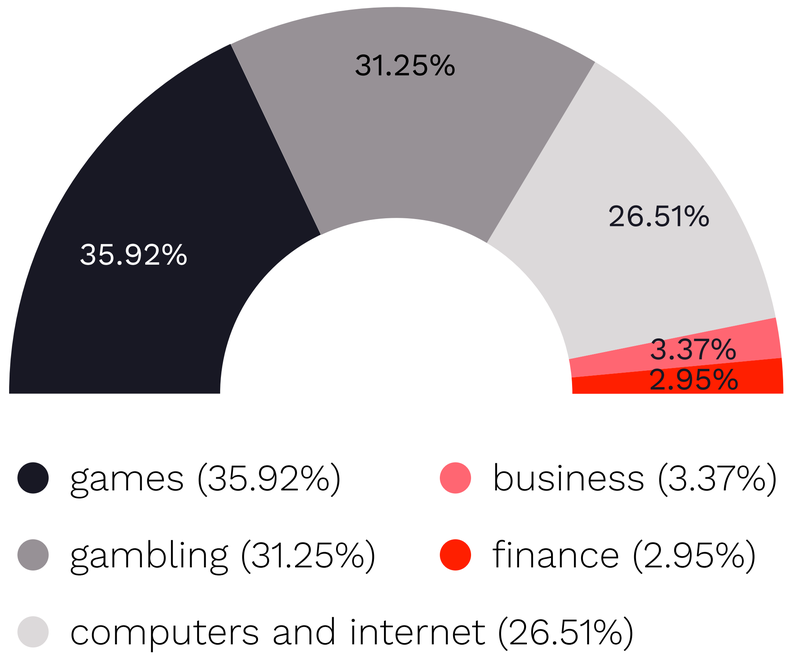
Compared to DOS (Denial of Service), DDoS attacks are much more dangerous as they use botnets, thereby reaching a greater range.

The top countries from which DDoS attacks originate are China (26%), United States (15%) and the Philippines (7%)[23]. While the most targeted countries are India (22.57%), Taiwan (14.79%), Hong Kong (12.23%), the Philippines (11.36%) and the United States (8.73%)[24].

22. Cisco. Cisco Annual Internet Report (2018–2023), 9 March 2020.
23. Help Net Security. Duration of Application DDoS Attacks Increasing, Some Go On For Days, June, 25, 2020.
24. Avishay, N., Kim, J. 2019 Global DDoS Threat Landscape Report, Imperva, 4 February 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

In 2019 the top attacked industries per number of attacks were[25]:



52% of all attacks lasted less than 15 minutes while 21% reached a duration of one hour. Longer DDoS attacks aim to cause permanent damage to the attacked infrastructures. An even worse scenario awaits for this cyberthreat in the future. **IoT devices and the 5G will increase** the number of devices connected to the internet, as well as the sophistication of DDoS attacks.

How to protect yourself against DDoS

Protecting yourself against DDoS mainly means being prepared to withstand this kind of attack at any time. To do so, you will need a scalable infrastructure and you will need to organize a response plan in case of attack. Do you have a plan for disaster recovery including a DDoS attack scenario? If you run a critical service that needs to be online 24/7, invest in a DDoS protection service. Ask your ISP how they respond to this cyberthreat and what protection level they offer. Test your defence and adjust it if necessary.

InterNetX DDoS Mitigation Service helps diffuse these attacks, ideally ensuring the continued operation of affected services or websites, while in any case reducing disruptions to a minimum.

DISCOVER DDOS PROTECTION AT INTERNETX

25. Ibid.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

07. Identity theft

Data is stolen **more often than the average internet user can imagine.** These are used to act on the part of someone who will never even know their identity was used for malicious purposes.

In the US identity theft cost Americans a total of about **$43 BILLION**[26] in 2020.

Nowadays, as we regularly enter our personal identifiable information (PII) on the internet, hackers are collecting them from international web servers. They can use these data to **act in the name of that person** for financial gain, but not exclusively. **Online impersonation** can be used, for example, to activate a SIM card and then use that number to register to specific services. Buying a gift card seems to be a very common action after identity theft[27]. This data might land on the dark web where they are organized and can be retrieved by hackers to better target an attack. We should not forget that identity theft occurs also when someone uses another person's identity to act in the name of that person on social networks, attributing statements to them.

How to protect yourself against identity theft

To avoid your sensitive data landing in the wrong hands, defend yourself with all conventional precautions of cybersecurity. Remain vigilant and do not fall for phishing emails or malware. Use strong passwords and be careful when surfing on public Wi-Fi. Opt for offline password managers rather than the ones offered by your browsers. For safer accounts, implement 2FA and do not share your personal information with unsolicited and unverified requests.

26. Buzzard, J., Kitten, T. 2021 Identity Fraud Study: Shifting Angles, Javelin, 23 March 2021.
27. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Identity Theft, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

08. Data breach

Today companies store a large amount of data, a mix of personal and sensitive information that needs to be properly protected. This is easier said than done. **Even a single "small" misconfiguration can lead to an exposure of the database.**

By 2024, business losses due to cybercrime data breaches will exceed **$5 TRILLION**[28]. The most exposed types of data are emails (70%) and passwords (64%)[29].

A data breach occurs when information is accessed without the necessary authorization of the owner for an unauthorized copy, disclosure, modification, loss of access, or deletion.

These actions can be accidental, but when carried out intentionally, they become espionage, theft, dissemination, compromise, voluntary encryption or destruction.

Usually, these data are then used for malicious actions. 71% of data breaches have financial goals[30]. The most critical part is that **companies and organizations are quite often not aware of data leakage** and information can be exposed to hackers for a long time.

In 2020, on average, organizations identified the data breach after **228** days and they needed **80** days to contain it[31].

28. Jupiter Research. Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024, 27 August 2019.
29. Risk Based Security, Inc. 2019 MidYear QuickView Data Breach Report (PDF), August 2019.
30. Verizon. 2019 Data Breach Investigations Report, see note 7.
31. IBM. Cost of a Data Breach Report 2020, accessed: 15 June 2021.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

How you can protect yourself against a data breach

Since data breach is the outcome of other cyberthreats, you should apply a general cybersecurity shield. Train everyone involved, from end-users to IT staff, and make sure they use strong passwords and safe password management practices.

Encrypt all communications and pay attention to the security of sensitive and personal data. Investing in detection and alerting tools will help to prevent data breaches.

09. Insider threat

Cyberthreats do not only come from outside of the company.

According to analysts, data breaches will increase by **8%** in 2021 and a third (33%) originates internally[33].

Employees are 85% more likely to leak files as almost half of them do not assess how effectively their technologies mitigate insider threats[34] and organizations do not have clear and strong guidelines. The increasing number of people working from home due to COVID-19 has strengthened this threat.

Today, computers and all internet-connected devices have become subject to a large number of possible

33. Shey, H. Predictions 2021: The Path To A New Normal Demands Increased Cybersecurity Resilience, Forrester, 26 October 2020.
34. Code42. 2021 Data Exposure Report, accessed: 15 June 2021.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

attacks from other companies or competitors who want to steal data or important resources. Specifically, the insider threat is a threat that comes from (former) employees, contractors, business partners, and other figures interested in stealing your sensitive data, attacking your computer systems or committing fraud[35]. There are different scenarios connected to an insider threat. Employees might, whether consciously or unconsciously, become pawns manipulated by hackers. Collaborators might work in a company for the sole purpose of stealing sensitive data which is then passed on to other companies. Hackers could also act on their own for different purposes, mostly for financial gain.

How you can protect yourself against insider threat

Having direct measures aimed at protecting your company from insider threats is not easy and probably unachievable. Monitoring people's behavior is not enough. You should train employees to adopt a mindset focused on data security. Starting from here, you can monitor specific areas and prevent possible threats and critical roles inside your company. Only a limited number of users should have access to sensitive data. All in all, it is important to have a strong and safe digital environment to prevent malicious and harmful actions and monitor activities, files, and emails with an alert system for abnormal behavior.

35. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Insider Threat, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

10. Botnets

A botnet is made up of **several internet-connected devices that are infected**, usually by malware. Under the control of cybercriminals operating in a peer-to-peer mode (P2P) or from a Command & Control center (C2), it is possible to **infiltrate systems and infrastructures by exploiting every possible vulnerability** to evade detection tools with malware or trojans.

In the first part of 2021, the gTLD .com was the domain extension associated with the most command-and-control (C&C) botnets. The new gTLDs .top and .xyz have a long history of abuse and continue to rank at the top of most abused top-level domains[36].

This malicious technique is used to carry out different types of scams and cyberattacks, mostly on a large scale through DDoS. Computing and automation have given a great boost to this technique and cyber attackers can operate more efficiently. The main goal of a botnet is in fact to infect as many devices as possible. Their resources and computing powers get exploited through automated processes the users are not aware of, thus finding themselves involved in an integral part of a network of remotely controlled bots. The zombie device is now instructed by the botmaster to convey the download of other types of malware, recruit other bots or launch other malicious activities. Botnets can allow the simultaneous action of hundreds of thousands of devices to perform e.g. DDoS attacks on web servers, targeting a website with anomalous traffic, overloading and blocking the services, distributing malicious software (adware, spyware, ransomware, etc. for a wide range of illicit actions and data breach), but also to mine Bitcoin using the computing power of zombie computers. Spamming appears to be the main means used for this purpose[37].

36. Spamhaus Malware. Spamhaus Botnet Threat Update: Q1 2021, 15 April 2021.
37. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Botnets, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

How you can protect yourself against botnets

The best defense strategy against this threat is to raise the protective walls around your network and all potential access points, such as a strong configuration network and firewalls. Users fall into this category as well; this is why it is very important to train them about cybersecurity.
Use tools that block connections to IP addresses related to botnet activities or check the origin of the traffic, such as reCAPTCHA.
Two-factor authentication can assure a double layer of protection and prevent botnet attacks.

11. Physical attacks

The IT infrastructure that makes your business run relies on physical systems. These are more delicate than you might think. You simply need to snip a fiber-optic cable to disrupt operations. Having devices that promise strong integrity is very important in today's world, in which we save data and rely on them. From IoT to smart homes, intelligent buildings or smart wearables, we need to make sure data can guarantee safety and **we need to create a new set of physical security measures.**
This number explains the why quite accurately:

54% of data breaches across all sectors included a physical attack as the main method[38].

Within the scenario of the Internet of Everything (IoE), which will create the next generation of internet, experts are starting to merge the idea of physical protection

38. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Physical manipulation/damage/theft/ loss, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

and cybersecurity. In a physical attack, the criminal has access to the physical asset and infrastructure through force, stealth, bypassing or disabling access controls and can then manipulate or damage the system and its data.

How you can protect yourself against physical attacks

Physical attacks can be critical, above all for SMEs that cannot afford security personnel or physical infrastructure. Train your team about how to keep your company environment safe and use tools like smart locks or smart keys. Be sure to implement a security plan for entry points like doors and windows. Alarm systems and surveillance cameras remain essential assets. They can also provide important forensic evidence. Take out insurance policies to cover damage, theft and losses both for physical and cybersecurity attacks. Only assign access rights to relevant individuals in your company. Rely on professional Colocation solutions.

DISCOVER COLOCATION SOLUTIONS AT INTERNETX

12. Information leakage

Information leakage occurs when **sensitive data is shown to unauthorized parties.** This is often due to a data breach, usually caused by someone inside the organization or a vulnerability in the organizational process. Information often gets leaked in very banal ways, due to the wrong application or server configurations where sensitive information gets disclosed in HTML comments, in the source code or

even in plain sight.

As of May 2021, the CAM4 case remains the biggest data breach with 10.88 billion records including sensitive information such as full names and email addresses[39].

14% of all incidents in the financial sectors in 2019 concerned data disclosures[40].

How you can protect yourself against information leakages

The first piece of advice is to only store data on safe assets. Identify sensitive data and apply controls and/or encryption and secure gateways. Use strong security protocols and test all your configurations and settings. To do this, you can employ tools that scan targeting vulnerability and data loss.

13. Ransomware

In 2021, businesses will fall victim to a ransomware attack every **11 SECONDS**[41].

Ransomware has grown to become **one of the main cybersecurity threats over the past few years**, and yet, these attacks keep increasing.

The number of attacks is high because ransomware is a **relatively easy-to-launch task for cybercriminals and the returns are**

39. Tunggal A. T. The 56 Biggest Data Breaches, UpGuard, 14 May 2021.
40. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Information Leakage, 20 October 2020.
41. Morgan S. Global Ransomware Damage Costs Predicted To Reach $20 Billion By 2021, Cybercrime Magazine, 21 October 2019.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

high[42]. According to estimates, in 2021 **the global ransomware damage costs is expected to hit $20 billion**[43], with services, education and government being the most targeted industries in 2020[44]. Ransomware can block both computers and mobile devices but also encrypts single electronic files. When this happens, the users can no longer access their files and data, unless they pay a ransom. So when the actor threat succeeds, the victim of a ransomware attack will always suffer an economic and/or data loss. Be careful, paying the ransom is not a guarantee of getting your data back!

In fact, in 2020, only **26%** of ransomware victims got their data back by paying the ransom[45].

Companies that paid the ransom eventually spent up to twice as much to restore business data. Added to this comes image damage the company reputation suffers if the information is made public[46]. So once again, it is highly recommended to never pay if you fall victim to a ransomware attack.

How you can protect yourself against ransomware

Effective countermeasures against ransomware must be adopted in a very short time by all companies by investing and working on a dual approach: staff training and innovative technology tools. Ransomware infection usually comes by email. It is therefore important to identify the messages containing malicious attachments or links. Never click on emails that look like spam or unfamiliar websites and do not open untrusted attachments. Hackers could also try to gain personal data by calling, texting or emailing. Do not disclose data without checking the authenticity of the asker. If you fall victim to ransomware, unfortunately

42. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 - Ransomware, 20 October 2020.
43. Morgan, S. Global Ransomware Damage Costs Predicted To Reach $20 Billion By 2021, see note 41.
44. Blackfrog. The State of Ransomware in 2021, 1 May 2021.
45. Sophos. The State of Ransomware 2020 (PDF), May 2020.
46. Ibid.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

in most cases, there is little you can do unless you have backed up or installed suitable security measures. From a technical point of view, this means installing security software tools aimed at identifying and mitigating the consequences of the attack. You will need to define a solution to safely back up your data in case of an emergency. You could also try to decrypt the infected computers with decryption software. For example "No More Ransom" offers 59 decryption tools for some 91 ransomware families.

These are the 10 most dangerous ransomware of the last years!

14. Cyberespionage

Cyberespionage is **the new frontier of cybercrime**, also as a consequence of the digital transformation that is affecting society and the entire production chain. With cyberespionage, we refer to **a set of activities designed to search for confidential information on a given system.** It is used to steal passwords, emails, projects, plans or any kind of secrets, usually from business competitors or **rivals to obtain military, political or economic advantages.**

Espionage attacks are carried out manually by humans or by malware. The latter usually affects large companies and it is classified as "industrial espionage". The "conventional" theft of personal information is giving **more space to the misappropriation of intellectual assets.** The theft of trade and government secrets is a highly profitable business. Still today, 38% of espionage actions are connected with nation states[47].

47. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Cyber Espionage, 20 October 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

During WWI and WWII, espionage was used as a weapon during the conflict. But it was during the Cold War that a particularly great work of espionage was implemented by the Soviets, who managed to get hold of the documentation of the American nuclear laboratories[48]. However, cyberespionage gained much wider popularity with the rise of the internet in the 90s.

Cyberespionage operations are carried out using spear-phishing as a vector of infection. A whopping **63% of cyberespionage incidents involve phishing[50].** In comparison with other cyberviolations, although cyberespionage is not the biggest threat and represents 10-26% of the cyberattacks, **it is more invasive and aggressive than others[50].**

A concrete **Managed Detection and Response (MDR) strategy** that includes, for example, Security Information and Event Management (SIEM) technologies, threat intelligence, user and entity behavior analysis (UEBA), threat search capabilities as well as integrations with technologies endpoint detection and response (EDR) and antifraud can reveal indicators of compromise on the network and the endpoints.

In addition to the countermeasures already mentioned to protect against phishing, a safety rule that always needs to be applied is to never open attachments of emails from unknown senders. It's important to keep not only your antivirus software updated, but also the operating system and all other programs by installing the patches released by the manufacturers as soon as available.

48. U.S. Department of Energy. Espionage and The Manhattan Project, accessed: 15 June 2021.
49. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2020 - Cyber Espionage, see note 48.
50. Verizon. Cyber-Espionage Report 2020, 2020.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

How you can you protect yourself against cyberespionage

Organizations can apply some best practices to defend themselves and recover from such attacks. As usual, the employees are the first line of defense. This is why everyone must undertake regular cybersecurity training. Social engineering and phishing is a common method used by cyberspies to gain access to sensitive systems. Strengthening your perimeter security can mitigate the threat.

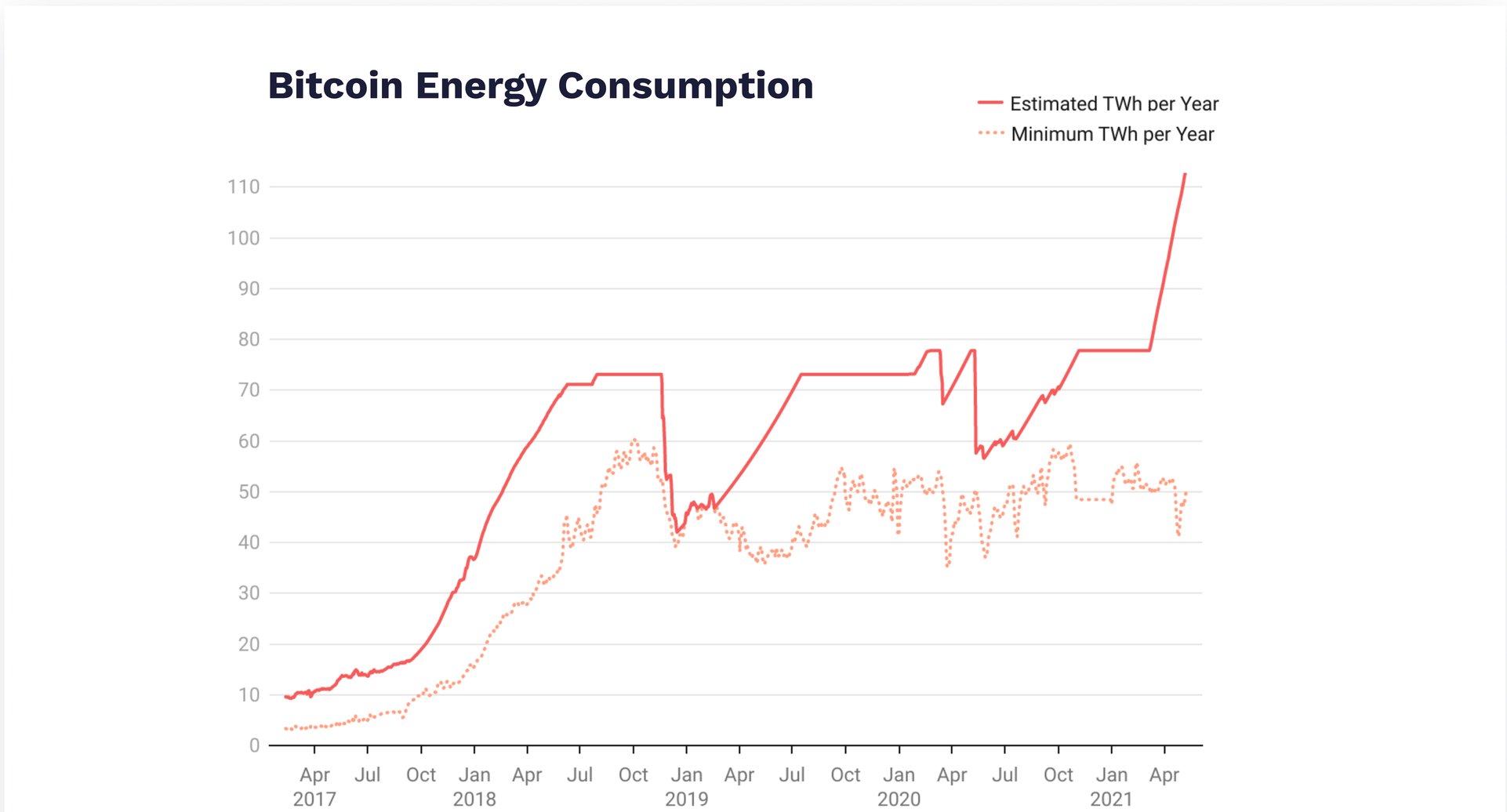
15. Cryptojacking

Cryptocurrency investors have found their new El Dorado. The functioning of these new forms of digital value is based on the principle of **cryptography.** To generate cryptocurrencies, **you need a process called mining**, which transforms the computing resources of a computer into cryptocurrencies. The rising number of cryptocurrencies available on the market requires even more computing power than ever before. And of course, this activity needs electricity.

In May 2021, Bitcoin energy consumption was estimated at almost **110 TWH PER YEAR**, comparable to the power consumption of the Netherlands.[51]

51. Digiconomist. Bitcoin Energy Consumption Index, accessed: 15 June 2021.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT



BitcoinEnergyConsumption.com

Among the miners, there are criminal hackers as well, who use malicious cryptomining techniques by exploiting the computing power of computers or mobile devices of unsuspecting users. **In fact, anyone with a computer can generate cryptocurrencies.** This threat can compromise websites and all types of devices, causing enormous economic damage, especially to companies.

Cryptojacking attacks can be carried out through various methods. Not surprisingly, phishing is widely used for this. The victim is persuaded to click on a link of a malicious email that leads to a web page where the cryptomining code was installed. Instead, "drive-by cryptomining" provides the integration of malicious JavaScript code hidden in a web page. Anyone who visits the page is infected and will immediately start generating cryptocurrencies.

Mobile devices with an Android operating system are not exempt. Most cryptojacking attacks on Android devices occur through the use of malicious apps that hide a trojan. In many cases, the exploitation of

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

smartphone resources is so intense that it causes an overload of the processor with consequent overheating and damage to both the battery and the smartphone itself.

All in all, mobile devices tend to have less processing power to offer as desktop computers and servers. As they are not that lucrative for the hackers, they are therefore less at risk.

How you can protect yourself against cryptojacking

Cryptojacking was designed to remain 100% hidden without damaging the compromised machine. To carry out a cryptojacking attack, the attackers can use various methods. One of the most popular is very similar to the one used to spread conventional malware. Through massive phishing campaigns, the potential victim is persuaded to click on a malicious link in an email and the cryptomining code is installed and activated on the device. Therefore, ad-blocking and anti-cryptomining extensions on the browsers can be an effective means of prevention. Nowadays, endpoint protection or antivirus software often offers cryptomining detection as an integrated tool in their suite. For example, Microsoft Defender for Endpoint applies machine learning to telemetry signals to detect this threat[52].

52. Selvaraj, K. Defending against cryptojacking with Microsoft Defender for Endpoint and Intel TDT, 26 April 2021.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

Do not underestimate cybersecurity: Raise your defence.

Most people tend to think that cyberattacks only come through sophisticated network hacking. This assumption can cause a lot of damage as you might lower your defense in the daily tasks you perform on the internet.

Most of the underestimated cyberattacks fall into the category of the so-called Social Engineering techniques: CEO frauds, spoofing (falsification of sender's data to deceive the victim) or attacks falling under the Business Email Compromise types and various account hijacking techniques with malicious attachments. Keep your eyes open and also watch out on social platforms, messaging apps and mailboxes. Too often we handle these applications without paying enough attention and without any prevention.

How you can protect your organization

Cyberattacks are becoming more sophisticated, targeted, widespread and increasingly going undetected. Although the efforts to contrast cyberthreats are growing, many small and medium-sized businesses fail to protect themselves sufficiently. The first factor for digital security is increasing the threshold of personal awareness around cybersecurity. Offering training to your staff is a great first step towards prevention. You can also adopt platforms based on artificial intelligence algorithms that are capable of filtering most threats after an appropriate learning period. In this steady and unstoppable shift to digital, businesses must stay nimble and place significant focus on preventing all kinds of cyberthreats. Increase your security and protect your organization.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

References.

- Avishay, Nadav, Kim, Johnathan. 2019 Global DDoS Threat Landscape Report, 4 February 2020.
- Blackfrog, The State of Ransomware in 2021, 1 May 2021.
- BuiltWith. CMS Usage Distribution on the Entire Internet, accessed: 15 June 2021.
- Buzzard, John, Kitten, Tracy. 2021 Identity Fraud Study: Shifting Angles, Javelin, 23 March 2021.
- Cisco. Cisco Annual Internet Report (2018–2023), 9 March 2020.
- Code42. 2021 Data Exposure Report, accessed: 15 June 2021.
- Contu, Ruggero et al. Forecast Analysis: Information Security, Worldwide, Gartner, 14 September 2018.
- Cvetićanin, Nikolina. What's On The Other Side Of Inbox - 20 Statistics For 2021, DataProt, 11 February 2021.
- Digiconomist. Bitcoin Energy Consumption Index, accessed:15 June 2021.
- Egan, Gretel. State of the Phish 2020, (PDF), Proofpoint, 23 January 2020.
- European Commission. What is a Data Breach And What Do We Have To Do in Case of a Data Breach?, accessed: 15 June 2021.
- European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020, 20 October 2020.
- Fruhlinger, Josh. Top Cybersecurity Facts, Figures and Statistics, CSO, 9 March 2020.
- Help Net Security. Duration of Application DDoS Attacks Increasing, Some Go On For Days, 25 June 2020.
- IBM, Cost of a Data Breach Report 2020, accessed: 15 June 2021.
- Imperva. Web Application Security, accessed: 15 June 2021.
- Jupiter Research. Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024, 27 August 2019.
- Morgen, Steve. Cybercrime to Cost the World $10.5 Trillion Annually by 2020, Cybersecurity Ventures, 12 November 2020.
- Morgan Steve. Global Ransomware Damage Costs Predicted To Reach $20 Billion By 2021, Cybercrime Magazine, 21 October 2019.

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

- O'Donoghue, Cynthia, et al. Coronavirus is Now Possibly The Largest-ever Security Threat - Here's How We may Be Able To Tackle It, Reed Smith, 24 March 2020.
- Risk Based Security, Inc. 2019 MidYear QuickView Data Breach Report (PDF), August 2019.
- Shey, Heide. Predictions 2021: The Path To A New Normal Demands Increased Cybersecurity Resilience, Forrester, 26 October 2020.
- Spamhaus Malware, Spamhaus Botnet Threat Update: Q1 2021, 15 April 2021.
- Selvaraj, Karthik. Defending against cryptojacking with Microsoft Defender for Endpoint and Intel TDT, 26 April 2021.v
- SonicWall. 2020 SonicWall Cyber Threat Report, 4 February 2020
- Sophos, The State of Ransomware 2020 (PDF), May 2020.
- Symanovich, Steve. Coronavirus Phishing Emails: How To Protect against COVID-19 scams, Norton, 5 March 2020.
- Symantec. Internet Security Threat Report, March 2018.
- Tunggal Abi Tyas. The 56 Biggest Data Breaches, UpGuard, 14 May 2021.
- U.S. Department of Energy. Espionage and The Manhattan Project, accessed: 15 June 2021.
- Verizon. 2019 Data Breach Investigations Report (PDF), accessed: 15 June 2021.
- Verizon. Cyber-Espionage Report 2020, 2020.
- Walter, Jenna. COVID-19 news: FBI Reports 300% Increase in Reported Cybercrimes, IMC Grupo, 2 May 2020.

Image credits.

- Cover image: Rawpixel on envato elements

INTRO
15 THREATS
CONCLUSION
REFERENCES
ABOUT

No warranty.

Dieses E-Book wurde von InterNetX GmbH mit größter Sorgfalt mit den zum Zeitpunkt der Herausgabe verfügbaren und aktuellsten Informationen erstellt. Alle Informationen entsprechen dem Stand der Technik und werden ohne Gewähr für ihre Richtigkeit und Vollständigkeit zur Verfügung gestellt. Die hier enthaltenen Informationen können ohne vorherige Ankündigung geändert werden und sind allgemeiner Art; daher sollten sie nicht für spezifische Zwecke verwendet werden. InterNetX übernimmt keine Haftung für Fehler oder Auslassungen in den hier bereitgestellten Informationen.

About.

InterNetX

With more than 4 million domains under management, InterNetX is one of the leading providers of white-label hosting and domain products. InterNetX provides Internet Service Providers, telecommunications companies and agencies with domains, shared and dedicated hosting products, security solutions and network connections. InterNetX also directly offers TLS/SSL and S/MIME products from leading certificate authorities.



Simone Catania specializes in B2B Tech Content Marketing. As Global Content & Communications Manager, Simone is the main author of InterNetX blog where we published our interview series “It’s all about domains”. Together with our creative team, he empowers and educates users about IT and internet-related topics.

InterNetX GmbH
Johanna-Dachs-Str. 55
93055 Regensburg
Germany
Phone +49 941 59559-0
Fax +49 941 59559-55
email: info@internetx.com
www.internetx.com

Follow us:

Subscribe to our newsletter:
www.internetx.com/internetxpress

InterNetX