Student: Predrag Stipanovic

NOROFF, Aug 2019 ONLINE

THE FINANCIAL IMPACT OF MALWARE

Contents

List of Pictures

List of Tables

List of Abbreviations

AVS	Anti-Virus Software
BSoD	Blue Screen of Death
CIA	Confidentiality, Integrity, Availability
CSIRT	Computer Security Incident Response Team
DC/BC	Disaster Recovery/Business Cognitivity
DLS	Data Los Prevention
DoS/DDoS	Denial of Service/ Distributed Denial of Service
FBI	Federal Bureau of Investigations
HTTP/HTML	Hypertext Transfer Protocol/Hypertext Markup Language
ICR	Internet Chat Relay
IoT	Internet of Things
IPS/IDS	Intrusion Prevention System/Intrusion Detection System
IT	Information Technologies
Malware	Malicious software
NCFTA	National Cyber-Forensics & Training Alliance
NDCA	National Defence Cyber Alliance
OS	Operative system
SP	Security Policy
SSH	Secure Shell
TCP / IP	Transmission Control Protocol / Internet Protocol
TLS / SSL	Transport Layer Security / Secure Socket Layer
WWW	World Wide Web

Key Words

- Availability
- Awareness
- Confidentiality
- Cyber threat
- Cybercrime
- Information security
- Integrity
- Intrusion detection
- IT Security
- Malicious actor
- Malware
- Obfuscation
- Software Security
- Threat actor
- Virus

Abstract

The rapid development of malware in recent years is a significant information security threat and the leading cause of the worldwide spread of cybercrime. The main reason for that is a lack of knowledge, malware threats understanding, and mechanisms used to prevent and detect the cyber threat. The main contribution of this document is a step toward explaining malware's impact, especially the financial impact of malicious software. This document will give a basic malware introduction by explaining and giving examples of why malware is a challenge. The document will further explain the criminal aspect and financial gains of malicious software.

This paper contribution is a step toward explaining factors aggravating the spread of malware and cybercriminal markets as well.

The document will look at direct/indirect costs for consumers and businesses and light a term such as businesses as criminals in the cybersecurity aspect.

Picture 1. (Bradymartz, 2021) Malware

In the end, this paper will try to give some answers to why companies worldwide should have ready a cyber security response plan.

Introduction

It is not easy to believe today that low-level code can still run-on machines, avoid detection and, in the end, cause some severe harm to the device. Governments at the global scale, businesses and societies worldwide suffer from the same challenge. They do not adequately defend and lose control of their environment in the war with cyber security threats.

The impact of malware is enormous and hits every part of modern society. Malware can sent emails users did not write, can infect the computers and networks, giving an attacker control of the system and resources. Some forms of malware are just annoying, and they drain computer resources and slow down devices. The other ones are more dangerous, more sophisticated and can cause some severe damage to the whole IT infrastructure.

This document will find answers to many essential questions about malware financial impact on businesses worldwide, discuss factors that aggravating the spread of malware and what are malware costs. It will answer why companies should have a cyber security response plan ready.

Impacts of malware are significant, severe, and long-lasting and especially in today's world where most of us have and carry at least one computing device connected to a global network that allows the impact of malware on a bigger scale.

This paper will also get light on businesses as criminals and vast cybercriminal markets.

According to *Bitdefender,* just ransomware attacks, a type of malware, was increased 485% in 2020 on a global scale. Total global ransomware costs estimate at 20 billion US dollars per Cybersecurity venture. Ransomware attacks rising and were 77% of actual attacks in the first quarter of 2021, with an average ransom payment of 220,298 US dollars.

Nobody guarantees that the ransomware payment will result in stolen data will be returned/undistributed. It can be risky to pay the ransom because of the financial and compliance risks such as “Know Your Customer” (KYC), “Anti-Money Laundering” (AML), and “Combatting Financing of Terrorism” (CFT) lows.

Societies and governments must transfer the risk, or companies could have increased financial risk in the future ransomware attack.

Nowadays, there are just two types of companies globally, companies that have been cyber-attacked and those that have not yet.

Main part

In this part, the document will try to find some answers and explanations in eleven chapters about the financial aspects of malware, and the financial impact malware attacks have on businesses worldwide. It is essential to give some introduction and examples of why malware is such a vast challenge. Further will explain the criminal aspect and financial gains of malware software attacks. Chapter four will look at factors that aggravating the spread of malware, and chapter five discuss the cybercriminal markets. Of course, the spread of malware does not have a local impact. It has a global and comprehensive impact on everyone's life.

The document will explain how malware threat spreads globally and will look at costs, both direct and indirect, but also cost for businesses and consumers. In the end, the paper will discuss businesses as criminals and try to explain why companies should have a cyber security response plan.

Chapter 1.

Introduction of Malware: Basic introduction

Application software runs on top of computer system software. That kind of software helps us to use the computer for a different purpose.

Application software or software built/programmed to cause damage to a computer, or any other electronic device, user or system are called malicious software or *Malware*.

Malware payload can be delivered in many different ways, but principally there are just two ways, with automated installation and manual installation.

The malware story begins in the early 1980s, and then, most malware software was just kid pranks and was annoying for users until the late 1990s. The virus creators were often teenagers that did not understand the consequences of such behaviour.

In the early 2000s, virus software creators and cybercriminals tried to use their talents for illegal activities. The Internet use and widespread of easily accessible information, as everyone’s tools, give some advantages for the businesses, societies, and banks to use it for transactions and commerce.

That gives a chance also to the criminal-minded software developers, and today`s amount of release of malware software is more than an entire valid software release.

There are many various kinds of malware software, and the title malware software includes viruses, trojan horses, worms, rootkits, spywares, keyloggers and many more. *(A definition of malware, 2021).*

There are differences between all virus types, and to understand them, it is practical to split them into groups:

Malware can be categorised and classified.

- Classification of malware software:

1. User mode malware
2. Kernel-mode malware

- Categorisation of malware software:

1. Virus,
2. Worm,
3. Trojan,
4. Backdoor

1.1 Virus (Vital Information Resource Under Siege)

It is easy to say that viruses are the standard type of malware software. Viruses work like they attach malicious code to the clean code and wait for a user or an automated process to execute the virus. Like any other non-computer virus, malware can spread widely and quickly, causing damage, corrupting files, and locking down the users. Viruses often have executable files.

A virus is such a type of malware software that, once is activated, will duplicate/replicate itself, inserting its code from one folder to another. The virus will spread fast and will infect a whole system.

The aim is to get financial and personal data and information, but also, sending spam or locking down the systems.

The virus has three vital components, concealer, payload, and replicator. *(Strawbridge, 2021).*

Virus vital components:

Concealer's job is to make the virus appear stealthy and make it available to install itself in secrecy. The payload component allowed the virus to carry another virus, and the replicator replicated the virus further.

The life cycle of the virus has six stages:

1. Origination,

2. Transmission,

3. Triggering,

4. Infection,

5. Identification and

6. Removal.

Picture 2. (Bradymartz, 2021) What is a virus

1.2 Worms

Starting from the first infected PC, they found their way through the network, connecting machines to continue the worm infection. Worms can infect the whole network of devices very easily.

Worm as malicious software is similar to the virus, it replicates itself on the system, but it does not spread to other software or programs. Once on the system, the worm quietly infects the computer without the user`s knowledge.

It can duplicate itself thousands of times, takes the resources from the system and damaging the device.

So, a worm is a self-replicating computer program and comprises of following components.

1. Scanner,
2. Penetration tool,
3. Installer,
4. Payload and
5. Discovery tool.

Picture 3. (Consultia, 2021) What is a worm

1.3 Spyware

Spyware is a modern plague designed to spy on user's activities on the computer. It is hiding from a user in the background and collects information without the user knowledge. Spyware collects all sorts of data, passwords, credit card numbers, browsing activity and much more.

It is a kind of malicious software that installs itself on a device. The first-ever known spyware software was known as "The Elf Bowling" programme, which was actually the game but acted as "Trojan" for one stealth programme that sends gathered data to the game`s creator.

Picture 4. (Avira, 2021) Spyware

1.4 Trojans

This type of malware software hides or presents itself as legitimate software. Acts discreetly and can breach all security by creating backdoors and give some advantages to other malware software's to act. Trojans are kind of malicious software that serves a malicious purpose.

It can be a game, free software update or anti-virus program. It tricks the user, and the goal is to install itself on the computer.

After installation, the Trojan software works quietly in the background and steals data, sensitive information, installs backdoor and take some harmful actions. Trojan consists of payload, concealer, and wrapper. *(Different Types of Malicious Software, 2019).*

Picture 5. (Kaspersky, 2021) Trojan virus

1.5 Ransomware

Scareware is also known as ransomware and comes with a heavy price. Ransomware can and will lock down a whole network or a single user until the user pays the ransom. Targets are often the most prominent organisations in the world.

Ransomware encrypts users data and often blocks access. The access unlocks when the victim pays the ransom demand. The payload comes after the user clicks on an email or with opening a malicious attachment.

Picture 6. (Kaspersky, 2021) Ransomware

1.6 Adware

Adware malicious software type is the least dangerous and will once download show advertisements on the user's computer. Adware are not created to steal data or personal information but can be highly annoying and frustrating.

The ads can be small banners or pop-up windows that can not be closed down.

Picture 7. (Varutra, 2021) Adware

1.7 Botnet

A bot is a device. A botnet is a system or network of infected devices. Botnet aim is to infect with malicious software and to do something harmful to the user and working computer.

A cyber attacker controls botnet devices, and they coordinate to infect as many computers as possible. Botnets perform DDoS attacks, send spam messages, or conduct phishing campaigns. *(What is a Botnet and How Can You Protect Your Computer?, n.d.).*

Picture 8. (Telesoft-technologies, 2021) Botnet

- Malware software can be collected and divided into smaller parties by the methods they operate:

1.8 Worms and viruses as the infectious threat

The keyword here is that this is the group of harmful malwares, project to diffuse with no the beneficiary`s knowledge. Computer owner spreads unconsciously the virus that already is infected the computer. The virus needs someone to deed before the virus can apply/spread.

Computer worms are, on the other hand, different because they do not need computer users to apply/spread out. Worms can spread without user action. *(A definition of malware, 2021).*

1.9 Trojans and Rootkits as the mask threat

Rootkits and Trojans are in the same group of malware software because they both look for to carry on strike on computer system.

Trojan horses are a type of malicious software that pretends to be a legitimate application or software. After a download, the user thinks that it is a benign application, and instead of it, ends with a malware-infected computer.

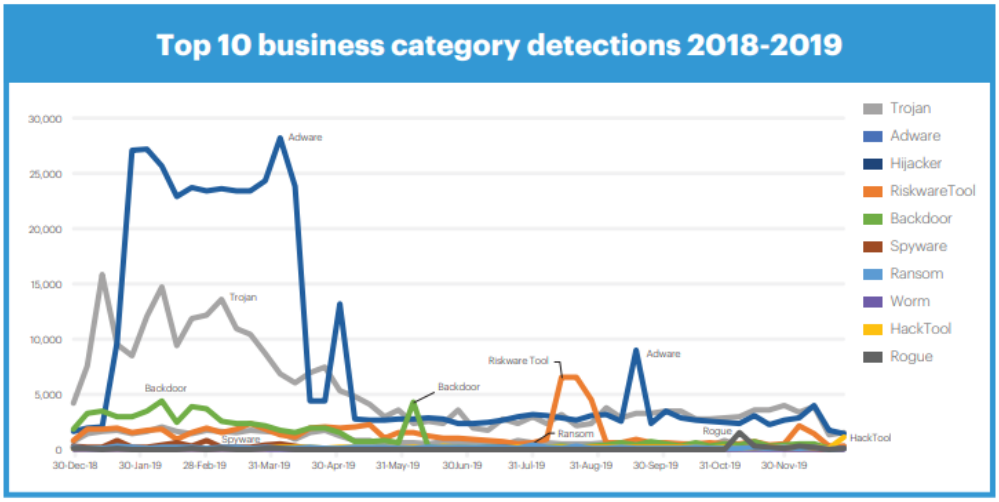
Rootkits do not work in the same way. They do not have harmful software; they are masking techniques for malware. Virus software developers developed the rootkit, which is to be undetected by AV detection and removal software.

Today there are AV programs that include very efficient rootkit removal implementation.

1.10 Spyware and keyloggers as the financial threat

Keyloggers and spyware are malware software mainly used for attacks like phishing, social engineering, and identity theft. They are designed to steal money from unknown users, banks, and businesses.

Security report from Jan 2021 with statistics for 2020 reports that USA malware attacks costs US businesses more than $29,1 million, and analysts predicted that malware security spending would reach a trillion-dollar mark. *(Tahir, 2018).*



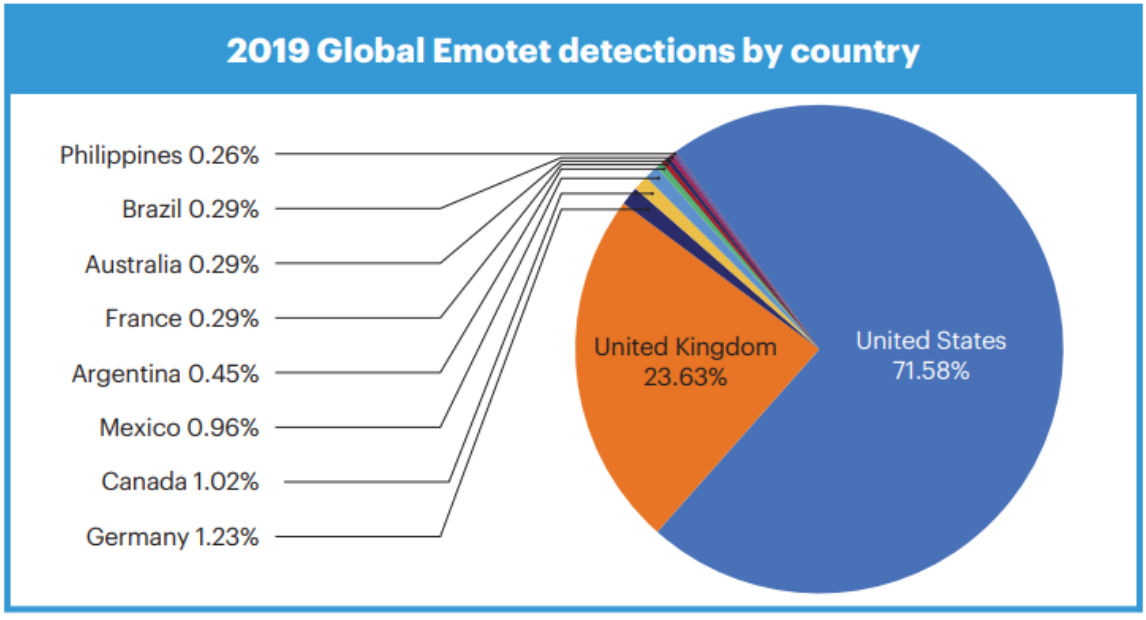
Picture 9. (Malwarebytes, 2021) Business threat categories by Malwarebytes

Top 10 global business categories 2018-2019

	Category	2018	2019	% Change
1	Adware	771,006	4,337,987	463%
2	Trojan	3,745,473	2,809,198	-25%
3	RiskwareTool	514,020	780,154	52%
4	Backdoor	591,903	672,495	14%
5	Hijacker	2,259,644	470,878	-79%
6	Spyware	246,156	110,805	-55%
7	Hacktool	31,835	103,102	224%
8	Ransom	101,624	95,523	-6%
9	Rogue	61,195	49,504	-19%
10	Worm	113,149	44,552	-61%

Picture 10. (Malwarebytes, 2021) Business threat categories ranking by Malwarebytes

On the picture under, we can see the global emoted detection by country.

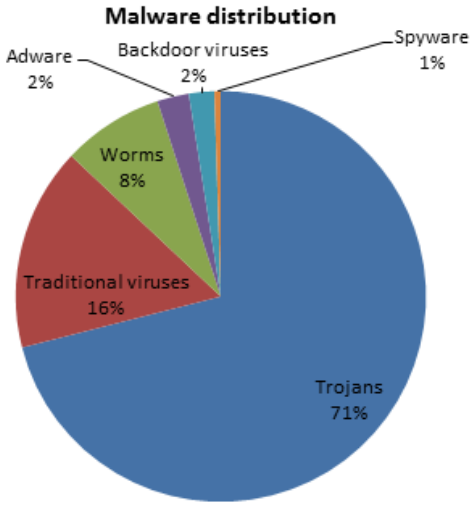


Picture 11. (Malwarebytes, 2021) Top ten countries ranking by Malwarebytes

Are there any methods to isolate computers and protect them from infections caused by malware software?

There are several steps or actions to take to prevent computers and other devices from infections:

1. To install Anti-virus software,
2. Regularly software update,
3. Download or purchase applications from trusted sources,
4. Do not click/open links that are suspicious and do not download from untrusted sources,
5. Install Firewall,
6. Back up data scheduled.



Picture 12. (Malwarebytes, 2021) Malware distribution

Chapter 2.
The problem of Malware: Explaining and giving examples to why malware may because a problem

Picture 13. (Consoltech, 2021) Malware may because a problem

As this document already writes, malicious software or shortly malware is any program/software designed with only one purpose – to harm the computer and data on it.

The question is, can malware software do some severe harm?

Malicious software works in many different ways; various types of malwares have additional capabilities.

This chapter will answer why malware may because a problem and give some examples with explanations.

1. Malware software can steal sensitive information, can steal a password, delete some files and make devices inoperable,
2. Malware will, after installation on a specific device, consume the computer`s memory. Malware software often replicates themselves and fill up hard drive, and there is no

more available storage for legitimate software. The user will end with an inoperable device that cannot carry on business.

3. Malware software can restrict access to files on the device. Particular types of malwares can damage or delete programs or data. Ransomware malware software holds data files hostage and waits for ransom money.
4. Malware spreads throughout the computer network. Worm as malware type is a disruptive one. After the worm contaminate the device, it will replicate and will metastasize through the whole network.
   Many of companies have all computers on a one single network, and worms can replicate themselves. Worms can damage not just one computer but the whole company.
5. Malware software can disrupt daily operations. A familiar thing for all malware types is that they will affect normal business operations. Adware malicious software especially hits business productivity. Once installed on the device, it enables constant popups. It is even able to redirect users search results to another. In such conditions, it is hard to enjoy the functionality of the computer.

There are some common symptoms of a malware infections influence:

1. First is a “SLOW COMPUTER”, some types of malwares can and will notably slowing down OS performance, programs and software.
2. The second one is “LACK OF STORAGE”, malware will use up all the storage space on the device, leaving little room for legitimate programs and data. The result is then a slow or not functioning computer.
3. The third one will be “CRASHING OR FREEZING”, it is a typical case that malware software can cause regular computer crashes, but it is essential to say that some technical problems can also cause that. Malware can even cause the BSoD or Blue Screen of Death.
4. The fourth one could be “POP-UPS” and “UNWANTED PROGRAMS”, It is irritating to see some constant pop-ups or some unfamiliar programs or toolbars that pop up on the screen.
5. Finally, is “SPAM”. The common thing is that spam software sends messages by itself.

Most hacker attacks use malware software at some point. Commonly, cybercriminals send phishing emails with no attachments and no links to click, and after gains, trust can send a malicious attachment.

What is interested here is intended behind, some cybercriminals use malware to make money, prevent businesses from running to steal confidential data or information, or just for fun.

The five most popular malware attacks in the last five years were:

2.1 2016, Petya ransomware

Petya is blocking the entire Windows computer`s OS, which is unlike most ransomware. It results in that the user must pay a ransom to release it. Petrya and its new and more destructive variants costs were 10 billion USD since 2016.

Petya`s victims were airports, companies (Oil and shipping), banks all over the world.

2.2 2017, WannaCry ransomware

It is one of the worst ransomware attacks in history. WannaCry was introduced via phishing e-mails in 2017. WannaCry exploits vulnerabilities in windows. About 200.000 users worldwide were hit by WannaCry ransomware.

Most vulnerable were hospitals, large companies, universities. This kind of ransomware hit FedEx, Telefonica, Nisan, Renault. The total costs were estimated to be about 4 billion USD.

2.3 2018, Emotet trojan

In 2018, the US Department of Homeland Security defined Emotet Trojan as the most destructive and most dangerous malware software. Emotet is widely used in financial information theft, most in bank logins and cryptocurrencies.

The way Emotet spreads is by malicious e-mails like spam or phishing campaigns. Just in two cases (Chilean Bank Consorcio and the city of Allentown), costs were estimated to be 3 million USD.

2.4 2019, LockerGoga ransomware

LockerGoga hit in 2019 large corporations all over the world. Hydro and Altran Technologies were hit by ransomware. It cost millions of dollars in damage. Infections involve phishing scams, malicious e-mails, and credentials theft.

LockerGoga considers very dangerously because malware software blocks complete access to the user’s system.

2.5 2020, CovidLock

Criminals have found a new and original way to gain profit in 2020. Fear related to COVID-19, Coronavirus have been exploited widely by cybercriminals. CovidLock ransomware software is one example. CovidLock infects users via malicious files that promise to give some more information about the disease. Android systems were hit by CovidLock ransomware, and it costs 100 USD per device to unlock.

❖ Relations between malware software and data breaches:

Malware software infections directly lead to a data breach. The data breach compromises security to the unexpected or illegal demolition, loss, alteration, unaccredited expose of, or access to protected data-essentially anything that affects its confidentiality integrity and availability. *(Data breaches 2021).*

The latest statistics show that 43% of businesses identified cyber security breaches or assault in 2020.

What can be done and how to prevent Malware infections?

2.6 Steps to be done to minimise the risk of malware threats:

- First of all, to install anti-malware software: A/V or A/M software/programs are an excellent tool to have to identify and remove any types of malware software. Regularly check with some of the A/M programs is a perfect start to improve and increase the security of the device/network.
- Another thing is that every business, society, company should have regular employee security training because the most significant challenge every business has in the war on cyber security field is its employees. To increase information security awareness, companies should have regular cyber security exercises in their workplace. Like cyber October, that is a typical month of the year to practice cybersecurity.
- Users should be aware of clicking on unfamiliar links and unknown pop-ups. Some pop-ups can look hasty, and they frequently bring malicious software installed onto the computer. Open only files from trusted sources that are expected, check URL and then click on the any links. *(What Happens If Your Computer Is Infected by Malware? - Consolidated Technologies, Inc., 2019).*
- It is crucial to have the systems updated. The number of new malicious software threats created every day is nearly a million. It is essential in such circumstances to have the system up to date.
- Implementation of network security is also essential for protecting information from cybercriminals. This kind of service can be provided in-house or through an outside trusted assistance.

Chapter 3.
Criminal use of malware: Explaining the criminal aspect and financial gains

3.1 The criminal aspect-intro:

In the criminal aspect, malicious software is the most practical way to perform unauthorized access to cybercriminals and their criminal activities. They are going to gain an advantage of reliance on digital communication systems and the Internet.

A review of the history of malware software, anti-malware reports and predictions shows continuous growth over the years. An increase in the number of attacks is significant, but significant is also growth in malware sophistication over the last years. That is something that should be considered and analysed closer. In such circumstances, traditional malware detection appears insufficient and cannot tackle increasingly sophisticated malware software.

Hence, the malware caused damages have been dramatically increased. Today, it is widely spread. Every country in the world uses an enormous amount of money and other resources to prevent, detect and disable malware attacks, but also to take away cybercriminals that are behind those attacks. In the United States exists many agencies that try to fight with increased cyber security threats, such as the FBI (Federal Bureau of Investigation), NDCA (National Defence Cyber Alliance), NCFTA (National Cyber-Forensics & Training Alliance) and others.

There are differences between traditional crime and cybercrime, but there are also many similarities. Both types of crimes involve target identifying, surveillance and psychological profiling. However, the most significant difference is that cybercriminals are remote to the scene of the crime. The criminal actors in one cybercrime can reside on different continents and commit the crime without ever actually meet.

Today, data has become more valuable than money is. Today, bank robbers do not need a gun or getaway car. Accessing bank data gives cybercriminals access to the funds. Criminals have sophisticated techniques and service providers, high-tech expertise to take advantage of targeted users. *(Alazab et al., 2012).*

3.2 Malware – The criminal aspect

Cybercriminals use malware for many reasons, and the most important reasons are listed below:

1. Identity theft by tricking a target into providing personal data,
2. Stealing financial and credit card data,
3. Take complete control over several computers to launch DDoS attacks,
4. Infecting computers and use them as bitcoin and other cryptocurrencies mining devices.

In 2021, when it speaks about malware, ransomware is the most famous malware attack with devastating consequences. A recent report has found that 84% of US organisations reported phishing or ransomware security incidents last year. *(Brooks, 2021).*

Criminal financial gains exploded in the last years. It is measurable with ransomware malware attacks. In 2021 the *"State of ransomware 2020 blog"* with data collected up to 01. September 2021. Claim that the damage caused by ransomware expects to hit $6 trillion (6000,000,000,000). *(The State of Ransomware in 2021 | BlackFog, 2021).*

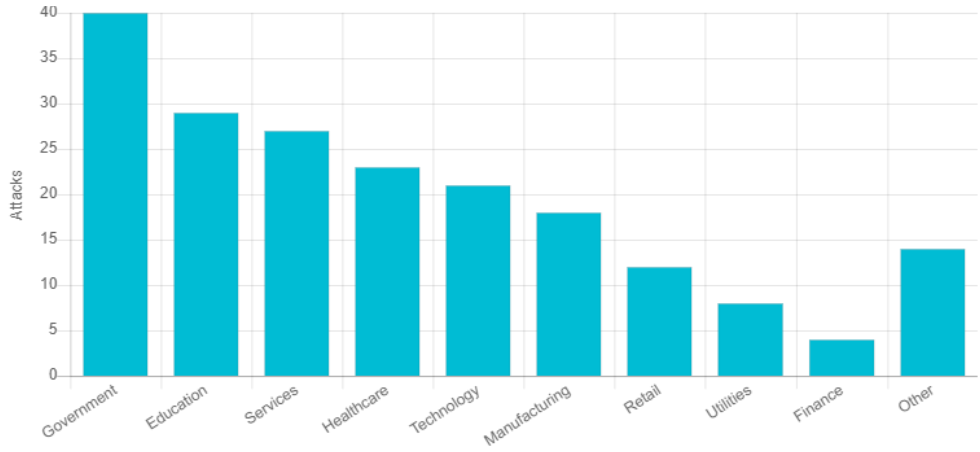
The damage caused in 2015 was $3 trillion. This document will try to give some overview in the pictures and tables under.

3.3 Malware attacks globally by industry, country, and month in 2020 and 2021:

The picture below shows ransomware attacks globally by industry.

No.	INDUSTRY	No. Attacks
1.	Government	40
2.	Education	29
3.	Services	27
4.	Healthcare	23
5.	Technology	21
6.	Manufacturing	18
7.	Retail	12
8.	Utilities	8
9.	Finance	4
10.	Other	14

Table 1. (Student, 2021) Ransomware attacks by industry up to September 2021

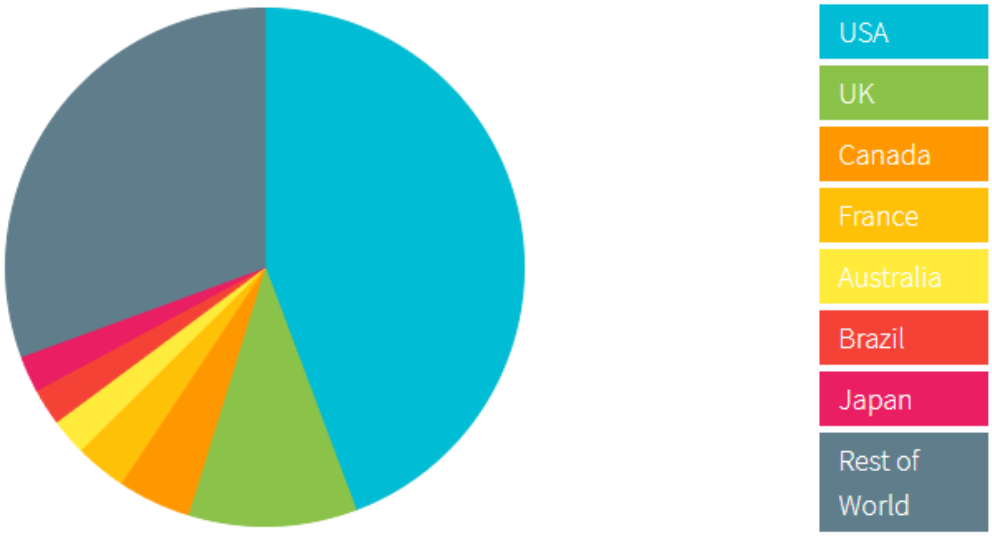


Picture 14. (Blackfog, 2021) Ransomware attacks by industry up to September 2021

The picture and table below show ransomware attacks globally by country.

No.	COUNTRY	No. Attacks
1.	USA	97
2.	UK	23
3.	Canada	10
4.	France	7
5.	Australia	5
6.	Brasil	5
7.	Japan	5
8.	Rest of the world	67

Table 2. (Student, 2021) Ransomware attacks by country up to September 2021

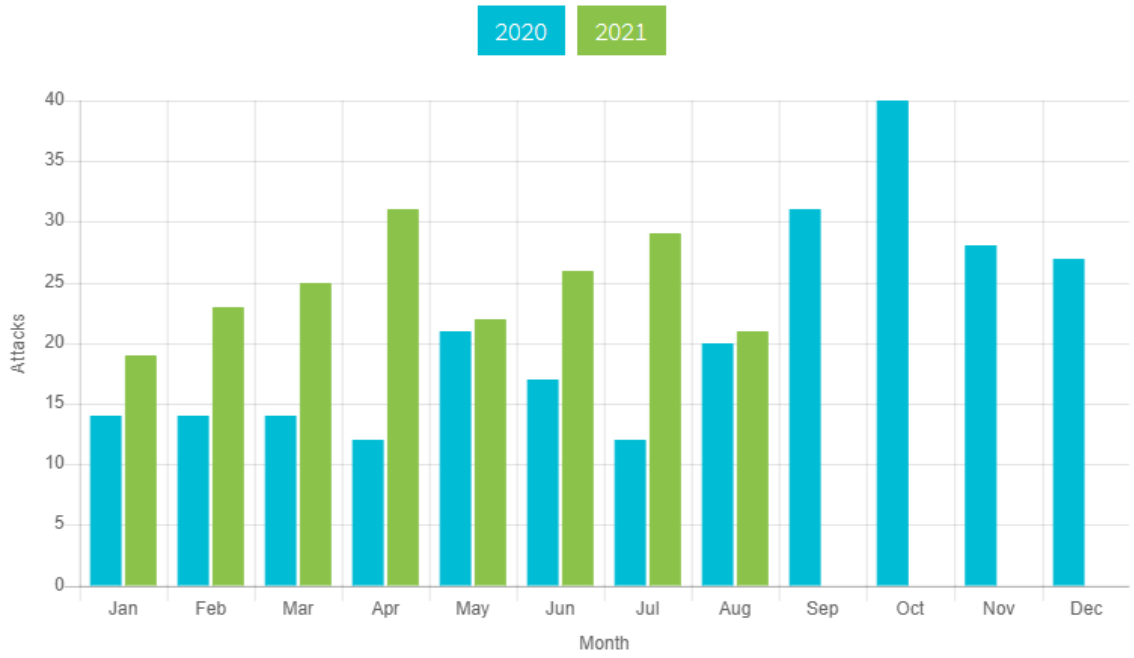


Picture 15. (Blackfog, 2021) Ransomware attacks by country up to September 2021

The picture below shows ransomware attacks globally by month in 2020 and 2021.

	Month	No. Attacks	
		2020	2021
1.	Januar	14	19
2.	February	14	23
3.	March	14	25
4.	April	12	31
5.	May	21	22
6.	Juni	17	26
7.	July	12	29
8.	August	20	21
9.	September	31	-
10.	Oktober	40	-
11.	November	28	-
12.	December	27	-

Table 3. (Student, 2021) Ransomware attacks by month up to September 2021



Picture 16. (Blackfog, 2021) Ransomware attacks by month up to September 2021

Chapter 4.
Factors aggravating the spread of malware

4.1 Malware aggravating factors:

The sophistication of malware and its versatility are potent tools combined with the growing number of Internet users and declining storage costs are a couple of aggravating factors. Another factor is the widespread availability of malware tools and the increasing gap between end-user awareness and sophistication of systems and applications.

Increased use of internet communications magnifies the challenge and increase the opportunities to attack information systems.

Shopping, banking, file taxing, working and access to pieces of information for social networking increase the range of activities online. All these activities are so-called “victim base”, and that “base” increases every day. The growth of online users ensures cybercriminals with a more extensive “victim base”. *(Bauer and Van Eeten, 2008).*

Enlargement of broadband access and connections gets more users that take primacy of ever-on Internet attach. Wi-Fi hotspots at home, while travelling, and in public locations with unrestricted access contribute to increasing problems generated by malware software. Widespread availability allows cybercriminals connectivity in public places, and further complicate finding cyber attackers.

Technological vulnerabilities are also worth mentioning here. Newer sorts and types of software and hardware carries more complexity and are combined with vulnerabilities that can be utilize. These effects could be and will increase by user ignorance to simple software updates tasks. *(Bauer and Van Eeten, 2008).*

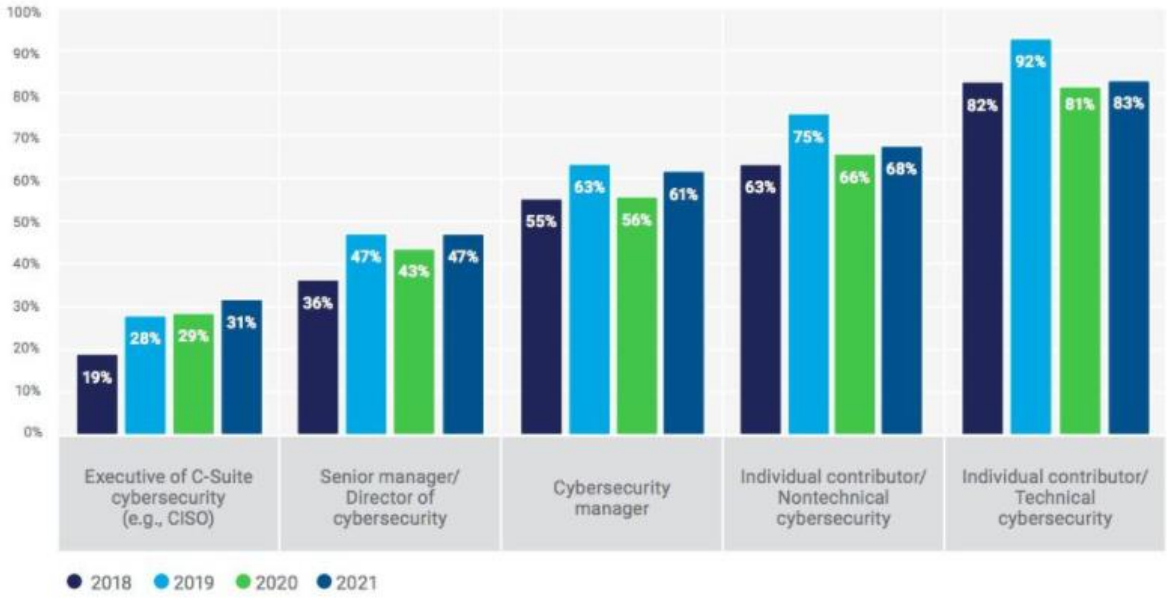
It is an ever-developing task, thanks to a push-and-pull game amongst cybercriminals and IT security professionals. Surprisingly, today over 60% of organisations have understaffed cybersecurity teams. Today, when we know that malware attacks coming from well-educated IT criminals.

Cybercriminals, despite numerous anti-malware measures, do not give up quickly, especially not if there is money to be picked up in such illegal activities. Cybercriminals attack new and underutilised vulnerabilities as the easiest way to gain access to data.

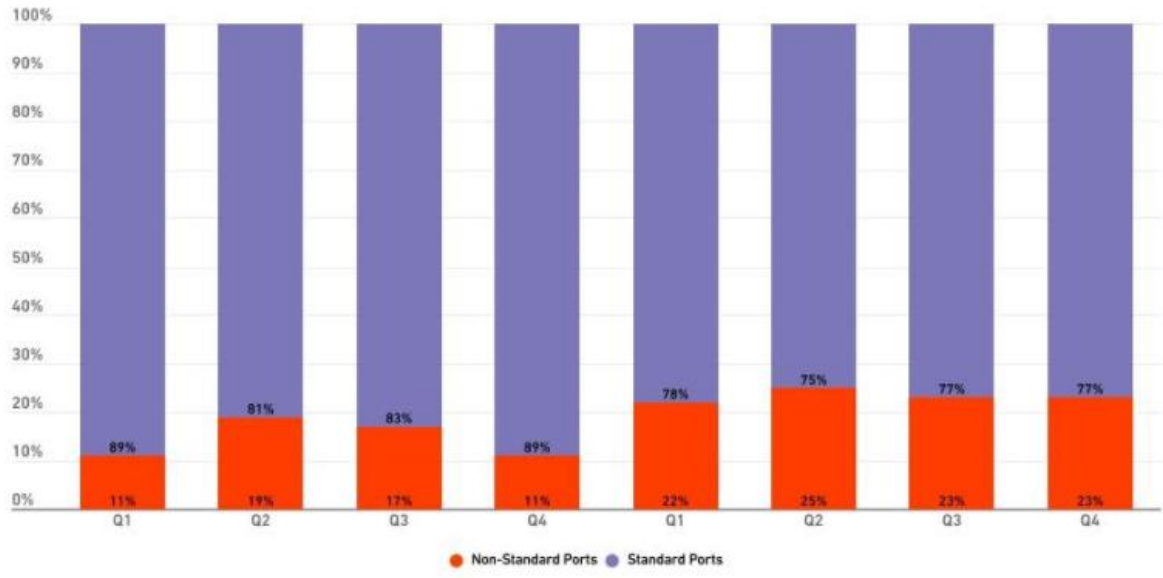
4.2 Some interesting facts are:

- Employees with infected machines spreading malware software more broadly,
- Business disrupting ransomware attacks are on the rise,
- Organisations worldwide report the most significant number of ransomware attacks,
- Over 60% of organisations have understaffed cybersecurity teams,

- There are some types of malware software on the decline,
- Traditional malware attack taking the hit,
- Phishing sites will be very trendy in years ahead,
- New malware variants decreasing year after year,
- Malware attacks on non-standard ports reached the top in 2019 and 2020,
- As cryptocurrencies rebounded, so did cryptojacking.



Picture 17. (ISACA, 2021) Unfilled positions reporting for 2018-2021



Picture 18. (SonicWall, 2021) 2019-2020 Global malware attacks on standard and non-standard ports

Chapter 5.
The cybercriminal markets

The Cybercriminal market, like any other market in the world, also is driven by profit. In the cybercriminal aspect, profit can be financial but also can be discontinuing some production line for any reasons, doing some damage for fun, but can be politically motivated too.

This chapter considers just money driven cybercriminal market.

5.1 Top ten security threats in 2021

- Phishing scams
- Cloud jacking
- Network perimeter and endpoint security
- Mobile Malware
- 5G to Wi-Fi security vulnerabilities
- IoT-devices vulnerability
- Deepfakes
- Highly developed ransomware attacks
- Insider threats
- API vulnerabilities and breaches

5.2 Cybercrime as a Service. How it works.

The Cybercriminal market gives many ways to earn money. With technology becoming widespread, traditional offline crimes tend to shift into online spaces. Cybercriminals include both buyers and sellers. They gather to perform transactions of data.

Products divide into three broad categories:

1) Stolen data:
   a) Stolen credit card data,
   b) Stolen bank accounts,
   c) Online payment accounts,
   d) Other personal credentials (IDs, passwords)

2) Cybercriminal tools:
   a) Malicious software,
   b) Hacking tools,
   c) Botnets,
   d) Phishing kits,

3) Cybercriminal services:
    a) Cash-out services,
    b) Consulting services

The research shows that cybercriminal sellers' way to do criminal business is to advertise products on the different web forums and Internet Chat Relay (ICR). The buyer, on the other hand, posts advertisements for wanted services. There are online criminal markets that use functionality with a moderator. With moderators in use increases trust among buyers and sellers. Moderators, after unsuccessful criminal business transactions, can remove those sellers/buyers who are not trustworthy or will do scams to others in the criminal society. *(R.Lee, 2020).*

Sellers, on some platforms, offer multiple contacts to be able to negotiate both deals and the prices. Both buyers and sellers complete transactions by use of communication methods that provide them privacy. Communication channels are often private messaging apps or direct messaging features.

Money exchange is done by using several well-known methods. Established trust in buyers/sellers relationship is crucial. After a transaction is done, buyers often leave feedback that can be positive or negative. Those who deliver risk behaviour in such transactions are banned.

5.3 Product pricing and confirmation of effectiveness

Product pricing for cybercrime as a service varies. Nevertheless, often resemble pricing strategies as used in legal services or production. All stolen data does not have the same level of desirability, quantity, and quality. Desirability, quantity, and quality of data are factors that determine the total cost of service. The higher product rates give higher product fees.

Another factor in forming a price is the total amount of time and expertise needed to make the product or service. Constant growing demand gives another way for getting prices done by competition and selling to the highest bidder.

Product or service that is selling in the cybercriminal market must have confirmation of effectiveness. The seller creates malicious software and advertises it on the underground market, such as "Dark web" with malware capabilities. It can be done directly or indirectly through an advertiser. This way of communication provides "less technical" buyers to purchase preassembled products.

Buyers er offered to buy "bulletproof" products or services that guaranties their privacy from low enforcements detection. So even if the attack is spotted, the attacker's identity remains hidden.

Buyers and sellers are all over the world, and they purchase in different currencies. The mediator can hire a person that can convert e-currencies into wanted fiat currencies.

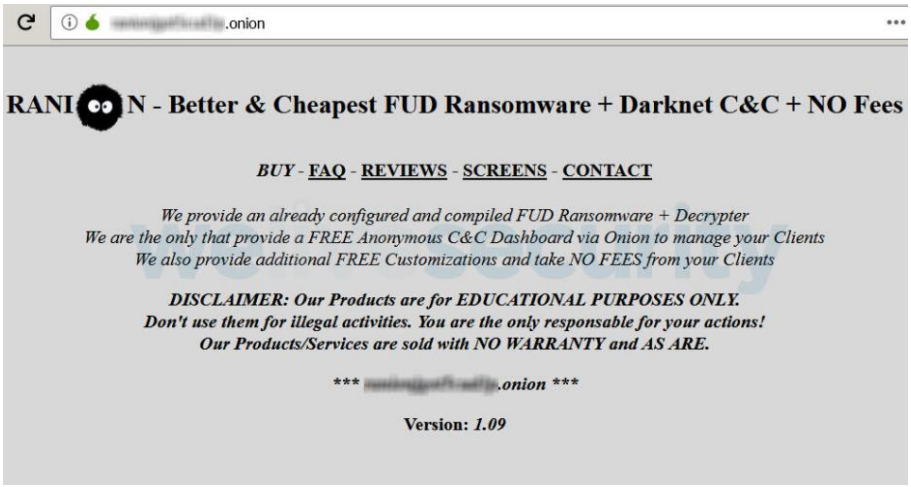
5.4 Cybercriminal product examples

There are many products and services today on the cybercriminal market, but to mention some:

- Fraud as a Service (FaaS),
- Malware as a Service (MaaS),
- Ransomware as a Service (RaaS),
- Attack as a Service (AaaS).

Pictures under shows examples of cybercriminal products. Ransomware as a service, renting infrastructure for DDoS attacks and selling PayPal and credit cards accounts.

Example 1: Ranion ransomware with possible subscriptions plans.



Picture 19. (WeLiveSecurity, 2021) Example 1. Ransomware like Ranion is available on the dark web

-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	12
Price	120 USD	490 USD	900 USD	1900 USD

Picture 20. (WeLiveSecurity, 2021) Example 1. Subscription plans offered for Ranion on the dark web

Example 2: Renting the power of compromised computers with infrastructure and compromised networks for spam emails sending DDoS attack launching.

Picture 21. (WeLiveSecurity, 2021) Example 2. Cybercriminal offering of infrastructure to run DDoS attacks

Example 3: Selling PayPal and credit card accounts.

Internal UID	Balance	Account type	Card	Country	Our Price	Add to cart
BGKGQFTL	2.023 USD	Premier	Yes (confirmed)	United States	$ 212	LOCKED
KUYATDLH	684 USD	Premier	Yes (confirmed)	United States	$ 78	LOCKED
QTEKVNUB	2.028 EUR	Personal	Yes (confirmed)	Italy	$ 253	Buy this!
HFQZEKOF	1.816 USD	Personal	No confirmed card	United States	$ 181	Buy this!
LUTBIKFX	1.738 USD	Premier	Yes (confirmed)	United States	$ 184	Buy this!
SCRZUPBI	761 USD	Personal	No confirmed card	United States	$ 75	LOCKED
WTPNRDPE	2.006 USD	Personal	Yes (confirmed)	United States	$ 211	Buy this!
BAGRXBON	803 USD	Premier	Yes (confirmed)	United States	$ 90	Buy this!
UNQXNCNM	2.038 USD	Personal	Yes (confirmed)	United States	$ 214	Buy this!
BGQWVWQP	707 EUR	Premier	Yes (confirmed)	France	$ 95	Buy this!
BXDALQYE	1.910 USD	Personal	Yes (confirmed)	United States	$ 201	Buy this!
CRVOGTUA	922 USD	Personal	Yes (confirmed)	United States	$ 102	Buy this!
YJYNMYSP	1.802 EUR	Personal	No confirmed card	France	$ 215	Buy this!
CQMOXGUB	1.506 USD	Personal	Yes (confirmed)	United States	$ 161	Buy this!
FJPDAECS	1.504 EUR	Premier	Yes (confirmed)	Germany	$ 191	Buy this!
QAMHTFEI	1.565 EUR	Personal	No confirmed card	France	$ 187	Buy this!
YTXQPZSL	747 USD	Personal	Yes (confirmed)	United States	$ 85	Buy this!
VUQTTWOV	1.065 USD	Premier	Yes (confirmed)	United States	$ 117	Buy this!
EARVCBWO	798 EUR	Personal	Yes (confirmed)	Spain	$ 106	Buy this!
XJXYGVCR	1.131 USD	Premier	Yes (confirmed)	United States	$ 123	Buy this!
VPRBJAMC	1.912 USD	Premier	Yes (confirmed)	United States	$ 201	Buy this!

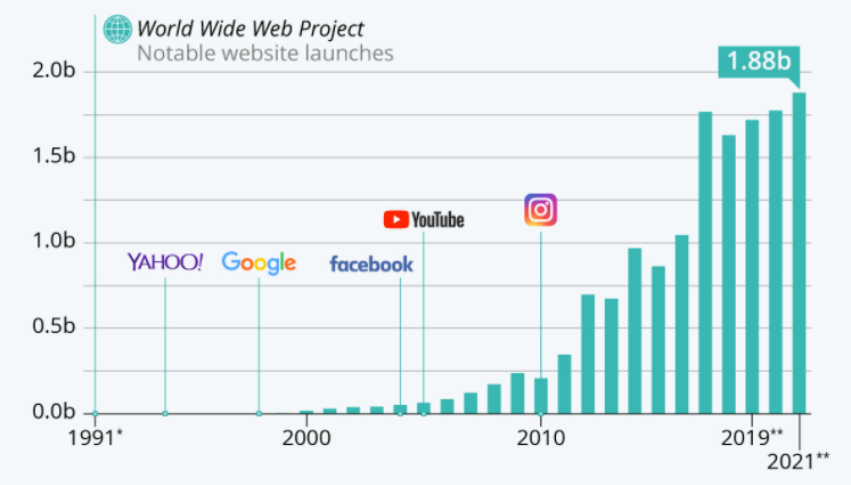
Picture 22. (WeLiveSecurity, 2021) Example 3. Cybercriminal selling PayPal and credit card accounts

Chapter 6.
The global spread of malware

Malicious cyber activities are a threat to public safety, national and economic security in every country in the world.

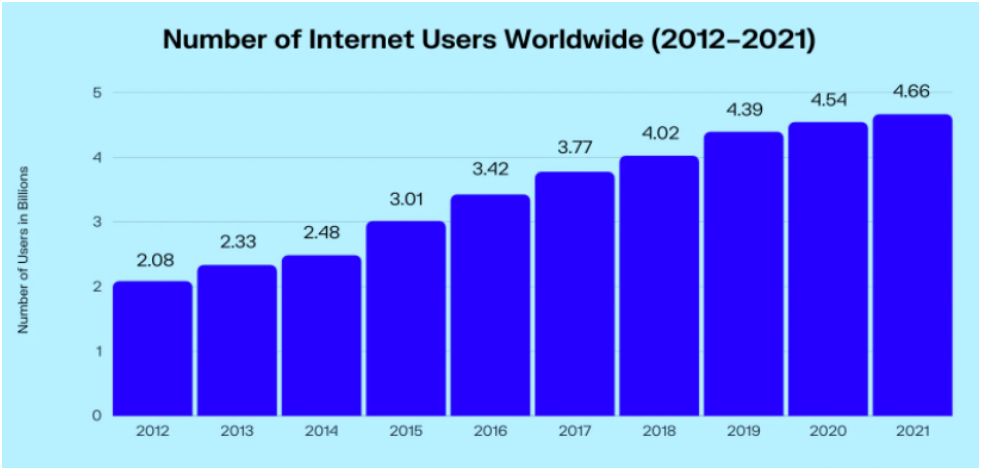
This chapter aims to understand the propagation mechanisms of the global spread of malware and the human impact. The paper already said that the widely used WWW (World Wide Web) in online banking, e-commerce, worldwide business activities in everyday lives helps people in many ways. However, it also helps cybercriminals to use it for their illegal activities.

Today, there are 1,88 billion websites worldwide.



Picture 23. (Statista, 2021) How many websites are out there in 2021

The number of Internet users has exceeded 4,66 billion users.



Picture 24. (Oberlo, 2021) Number of Internet users Worldwide 2012 - 2021

According to malware statistics, in 2021, it is expected:

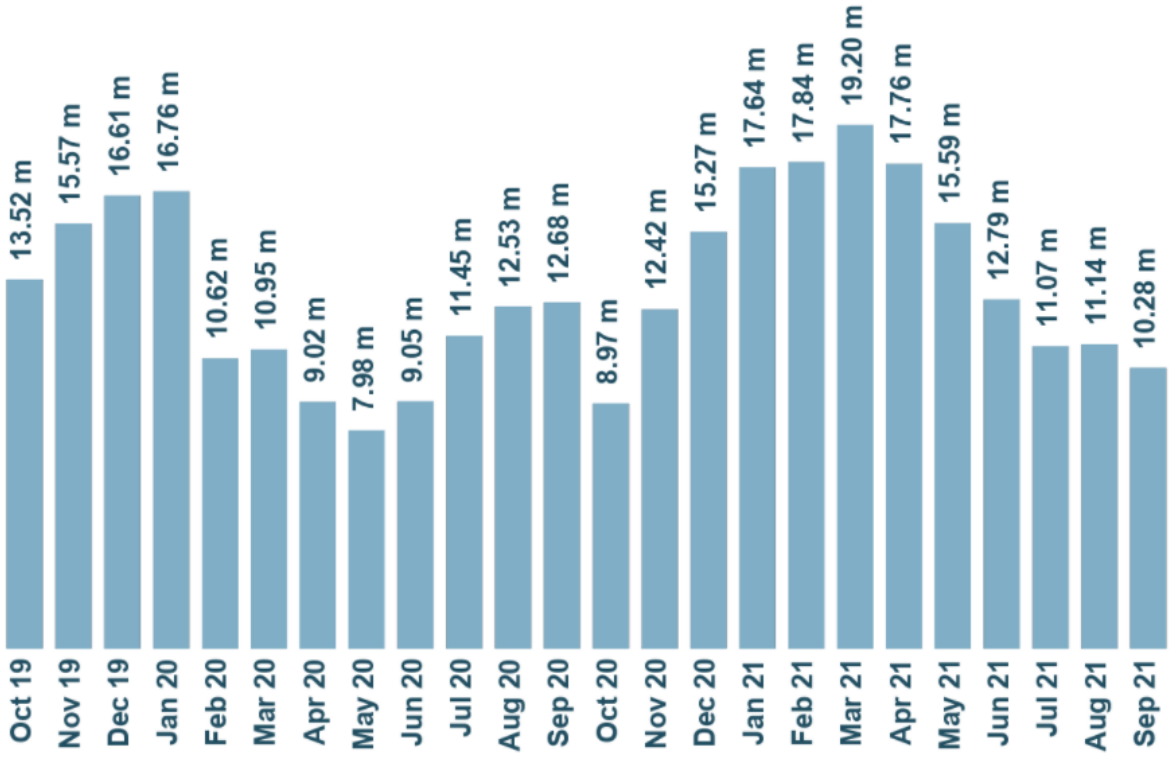
- Sites infected by malware will continue to fall out but will likely decrease in volume,
- Cyber-attacks will aim large companies/enterprises with malware to get large payments,
- The ransomware payoff sum will continue to rise,
- Formjacking will grow in the future too,
- The crypto-jacking threat will increase.

The recent trend is that the quantity of cyberattacks have tendency to boost in the last quarter in most years, and it is correlated with the phenomenon of "Black-Friday" and Christmas holiday shopping. *(Cook, 2021).*

As ever, cybercriminals go for easily exploited vulnerabilities in a company`s systems. The tactics tend not to change. Tactics change when efforts become unprofitable.

Just to mention, there is a danger that comes from state-sponsored malware attacks, which are not profit-driven but politically motivated. *(Cook, 2021).*

Most of the cybercriminals are motivated further to develop new and more sophisticated types of malware software:

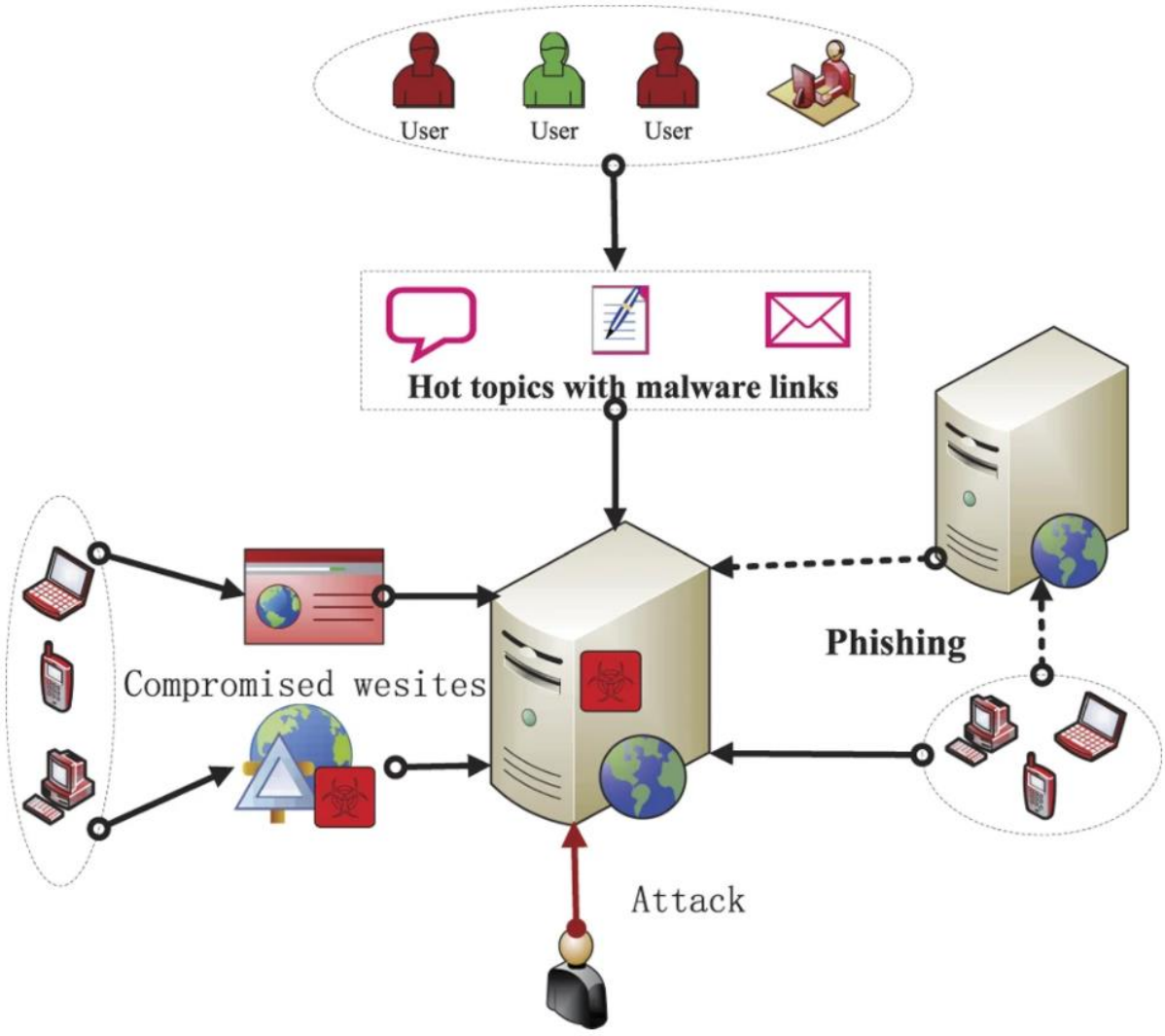


Picture 25. (AV-TEST, 2021) Number of new malware by month in 2019, 2020 and 2021

Web-based malware software is trendy for cybercriminals to attack users without searching for new vulnerabilities. Those can be spread in the form of hyperlinks by short

messages or spam emails. As the social networks use grows exponentially, the attackers more often use social networks to distribute malware. For example, Facebook was the top application used for mobile devices. On the other side, financial purposes motivate attackers to use websites.

Cybercriminals are trying hard to develop mathematical models of malware spread, like deterministic epidemic models. Some earlier models had compartmental approaches like SIS, SIR and SIRS models.



Picture 26. (Liu and Zhong, 2017) Malware spread modelling

Chapter 7.
Direct/indirect cost

This chapter aims to explain what direct and indirect malware attack costs are. Those kinds of costs are not easy to estimate. There are two main types of malware attack costs, the direct and indirect costs connected to malware impact.

Many public and private organizations, societies and business sectors have tried to count and get the direct and indirect costs of malware. This paper will differentiate in chapters 8. and 9. between business and consumer costs to make evaluating easier. *(M.Bauer and J.G. van Eeten, 2008)*.

7.1 What are direct costs?

Direct costs are businesses out of pocket expenses for cleaning up after a ransomware attack, repairing damaged networks and elements, but not just in money. There are also other costs and consequences. There are also costs and losses suffered by infrastructure, users and operations affected by the attack. *(Lis and Mendel, 2019).*

Direct costs calculation includes loss of services, loss of time, loss in equipment, loss in production, personal information losses and others such as:

- ✓ Ongoing recruiting,
- ✓ Operational disruption that includes replacement or upgrading of damaged equipment but also reserve parts,
- ✓ Organisation and business continuity plan,
- ✓ Agreements included IT security service,
- ✓ Security information and event management, access control procedures,
- ✓ Disruption of business income,
- ✓ Additional insurance charges,
- ✓ Losses in intellectual property,
- ✓ Costs of recovery process,
- ✓ Risk assessment costs,
- ✓ Damage to trade name costs,
- ✓ Los of customer relationships/contacts,
- ✓ Loss of life/health,
- ✓ Loses from disruption to internal sites and webpages,
- ✓ IT specialists and external contractors for bringing back all systems to full functionality,
- ✓ Legal complaints and privacy violation issues,
- ✓ Security product licence fees

7.2 What are indirect costs?

Indirect costs are more connected to the economic concept of negative external impact and are third party consequences. Third parties are not directly victims of the attack, and they are not responsible for support. *(Lis and Mendel, 2019).*

- ✓ A decline in future revenues,
- ✓ Insurance,
- ✓ Market breakdown due to attack may also strike cyber security stipulations, which have a consequent economical influence,
- ✓ Attack related government activities,
- ✓ Productivity losses,
- ✓ Privacy trauma and privacy preservation in the future,
- ✓ The recovery process,
- ✓ Increased cyber-security investments (installing additional cyber security technologies and procedures/policies),
- ✓ Hiring cyber-security experts and adding externals audits,
- ✓ Reduced foreign investing in the region which had experienced cyber-attack,
- ✓ Losses in stock market. *(Lis and Mendel, 2019).*

Chapter 8.
The cost for businesses

Malware attacks and ransomware especially continues to be a high-priority cyber threat in 2021, even more than in previous years. As everyone knows, the pandemic COVID-19 made 2020 a successful year for ransomware attacks. Mostly in increased volume. 27% of all ransomware attacks get paid in 2020. The average payment was $1,1 million per demand.

8.1 Remote work vulnerabilities

70% of organizations expect at least a third of remote workers will remain remote in the next year and a half.

Remote working introduced new risks, and 73% of high-level executives are concerned that the distributed workforce has introduced new vulnerabilities and increased exposures.

8.2 Data leak trend

It is not a new trend, but it has become common in the years behind. Before the “data leak trend”, if the victim does not pay, the victim does not get data back, and that is it. In the last years, the “data leak trend” has become more often used and explored. Cybercriminals pressuring the victim to pay the ransom. If the victim does not pay, all the sensitive data gathered during the cyber-attack become published and will do additional damage.

8.3 The Cost for businesses

Cyber attach attacks and all the harm they create can be very expensive to societies, organisations and businesses. As this paper mention in chapter 7. there are operational costs, downtime costs, reputational loss costs and other costs. In a study published by Sophos, the average ransomware attack costs are $732,520 for those organisations that did not pay the ransom money and $1,448,458 for those organisations that paid. This number includes total costs, including initial ransom demand and all downtime and operational costs caused by ransomware. *(Wu,2021).*

Every business is different, and risk tolerance is different for two different businesses. It is cost-effective to pay the ransom, and it is up to every business to estimate the risks and choose the best way to act. Even if one business is not attacked directly, it can be affected through collateral damage resulting from an attack on a vendor or business partner. When it occurs, businesses should be ready to soften or mitigate the risk. If businesses can mitigate the risk and limit an attack ability to spread, the result could be a less costly response. *(Wu,2021).*

As this chapter shows, the costs of a cyberattack can represent millions in damages, both direct and indirect costs. If businesses want to reduce or minimise the costs of a cyberattack, businesses must rely on their technology and experts in cybersecurity and save businesses the suffering of a long and expensive cyber-attack.

Chapter 9.
The cost for consumers

When it comes to cyber-attacks and the effects of one cyberattack, it is expected that all of us think about the consequences that it has on organisations, society, or businesses.

It is rarely written about the impact on consumers. What about consumer purchasing behaviour or brand loyalty. How does one cyberattack affect consumer trust in one organisation?

70% of asked consumers think that businesses or organisations are not doing enough to secure consumers' personal information. Despite wide-ranging and more frequent data privacy regulations such as the (GDPR) General Data Protection Regulation, organisations continue to experience cyberattacks that result in data breaches with massive private information data loss. *(Fair, 2020).*

Hospitals and healthcare have been attractive targets for cybercriminals, exposing personal data and banking information to healthcare records. Just one cyber-attack on the "Mariott" hotel resulted exposed the personal information details of 500 million hotel guests. *(Fair, 2020).*

Organisations need a different approach to defend their IT systems and customers from the consequences of possible cyber-attacks.

From the consumer's angle of view, many competitive organisations can offer the same service, and it is easy to lose consumers trust due to cyber security incidents.

Research indicates that 58% of consumers would keep away from doing dealership with organisations with a cyber breach experienced in the last years. Consumers today are well informed, and they know what consequences connected with one cyber breach are. Information about it will be crucial in a decision-making process in which the organisation will have consumers trustworthiness.

Those findings indicate that organisations and businesses must act quickly and do something about data and information security.

In today high-speed economy and even faster bank services, a single disruption or failed transaction can have and will have consequences for businesses or organisations. The consumers will decide to change their service providers.

Today`s businesses are aware that they cannot afford to lose the customers trust, especially today when three of four consumers think that data security is the responsibility of companies.

Picture 27. (Deloitte research, 2015) Consumers trust thresholds

Chapter 10.
Businesses as criminals? Businesses trying to get the upper hand by hacking opponents

10.1 Businesses as criminals

This chapter will find the answer to a question, do businesses act like criminals? Does business competitors hire cybercriminals to take down their opponents?

Small businesses are a highly targeted group, and it is essential to take information security very seriously. It is expected that large companies hack small businesses, not the opposite.

It is not a new thing that big corporations hire cybercriminals to hack competition. One of the first-ever known cases happened in 2005 when an entrepreneur and a hacker were arrested for hacking a business competitor.

In 2016, a ransomware gang reported that a “Fortune 550” company hired them to sabotage its competition. Year after, in 2017, one letter came to be published and accused “Uber” of the number of cyberattacks on its business competitors.

It was a long journey from a kid in the hoody breaking into accounts and businesses for the fun frame to full-scale cybercriminals as they are today. Cybercriminals today consists of teams, groups, nations, are male and female, backed up by corporations, politicians and even governments.

Businesses of all sorts have been hacked today, and the number of hacked businesses grows exponentially. The total number of attacks is higher because businesses do not report them.

The most sensitive are small businesses. They are either under-protected or have no protection at all. It is not clear why small businesses do not pay attention to information security. It is because of lack of funding, lack of insight or both. Without proper protection, they become easy prey to larger businesses.

The fact is that 43% of small businesses are targeted for a cyberattack, but only 14% are prepared. Less competition to big businesses means more business for them.

In the pandemic year, many small businesses vanished and those who survived struggles. Cybersecurity is not high on the list when the company is struggling with surviving. Last year employees were primarily worked from home, remote or in “hybrid” mode.

Cybercriminals take the chance and successfully gain access to networks via emails. Small businesses have less cybersecurity protection, and that makes them targets. It is essential to mention that most home networks have little to no protection beyond antivirus programs and easy guessing or no passwords.

Today is it possible to hire a hacker to perform a DDoS attack for $30-400 per day, and this is nothing compared to the costs for the targeted business. *(Kaspersky, Criminal Benefits, 2017).*

The damage made by a cybercriminal who denies service to customers for instance, on “Black Friday” sales day, would cost a business a lot of money and credibility and even ruin the whole business. It is easy to see opportunities for competition if such of cyber-attack occurs.

However, the story does not end here.

10.2 Countries and governments all over the world as criminals

As businesses do cyberattacks on their opponents and competition, governments do it to other countries also. One political party try to hack another, and further competitors hack their competition as well. There are many reasons why, such as, prevent nuclear war, protect the country`s citizens and further.

Knowing the enemy gives a strategic advantage, but this is the research for some other time.

10.3 Businesses trying to get the upper hand by hacking opponents - prevention

Small businesses especially, but also businesses as general need to cover three basic pillars in C-I-A to guard their businesses and investments.

Confidentiality of business-sensitive information and assets, Integrity of data stored and transferred, and of course, Availability of all resources within the business are crucial.

If the business cannot afford a cybersecurity expert as an employee, there is an option to hire a qualified cyber or IT consultant to guide the business in information security terms and prevent stealing the company's crucial assets or prevent Denial of Service.

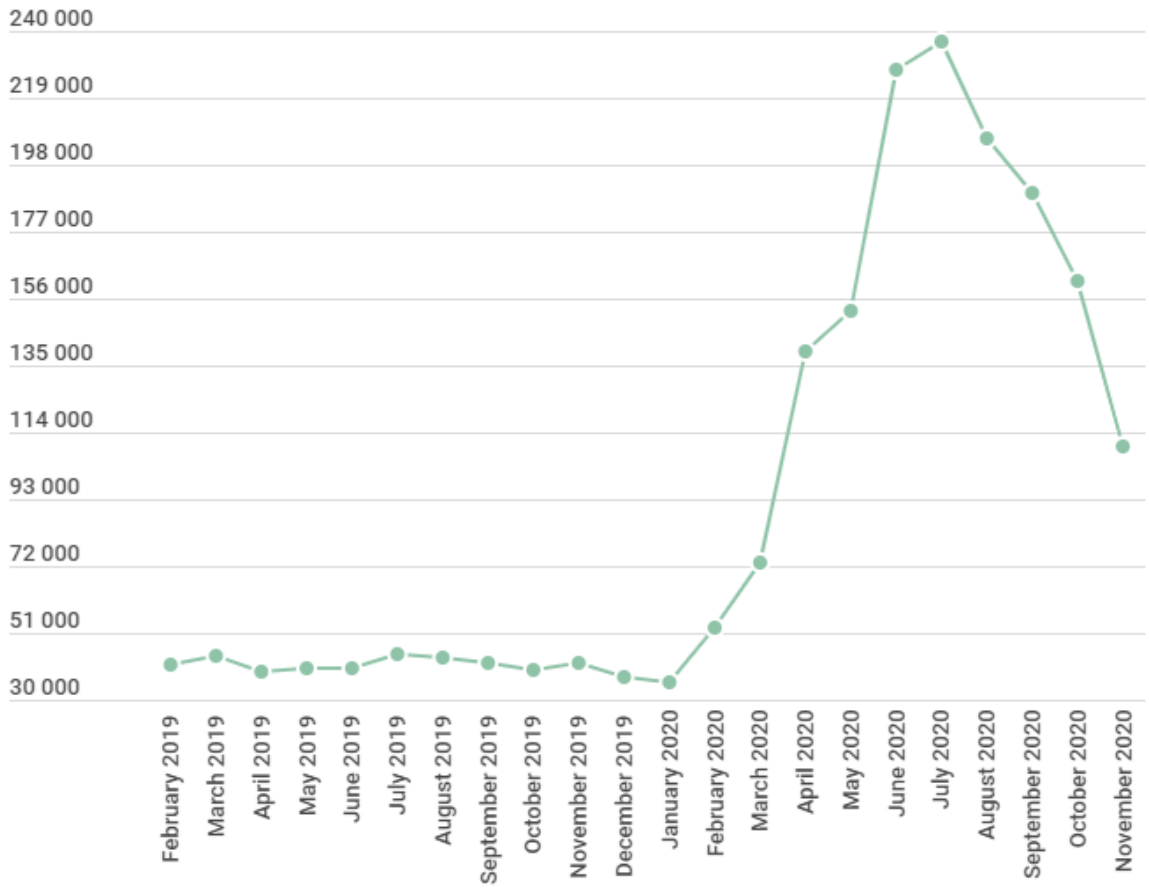
Chapter 11.
Why companies should have a response plan

11.1 Key events of 2020

Before diving into the question of why companies should have a response plan, look at the consequences and challenges pandemic COVID-19 bring in 2020.

Companies globally become less secure because of the deployment of remote work solutions. There are companies, businesses and public organisations that do not have even laptops to provide to their users/employees. Companies then must buy whatever is available on the market, even if computers do not match with the security standards of the company.

This solution kept businesses running, but those poorly configured computers had to connect to remote systems. Lack of training, default computer configurations for remote work left vulnerabilities and made all sorts of attacks, including ransomware, possible. *(Cyberthreats to financial organisations in 2021, 2021).*



Picture 28. (Cyberthreats to financial organisations in last the three years, 2021)

11.2 What is incident response

It is a process that gives organisations a chance to:

1. identify,
2. prioritise,
3. contain and
4. eradicate cyberattacks

The plan`s goal is to ensure that organisation is aware of a cyber security incident, to act quickly to stop the attack, minimise damage and prevent similar incidents in the future.

11.3 What is a cyber security response plan?

A cyber security incident response plan has, according to several sources, sometimes 6, 7 or 8 phases, but all of them include the following phases:

1. Preparation,
2. Identification,
3. Containment,
4. Eradication,
5. Recovery,
6. Lessons learned

Picture 29. (CyberCPR, 2021) Key stages of incident response SANS vs NIST

11.3.1 Preparation,

To review an organisational SP (Security Policy), perform a risk assessment, identify assets, define focus on selected critical security incidents and most essential to building a (CSIRT) Computer Security Incident Response Team. *(Incident Response SANS: The 6 Steps in Depth, 2021).*

Critical elements in this phase are Policy, Response plan or strategy, Communication, Documentation, Team, Access control, Training and Tools.

11.3.2 Identification,

How to monitor all IT systems and detect deviations from normal behaviour and operations and how to decide if those deviations represent actual cyber security incidents. If it does mean an incident, collect additional evidence and document everything.

Critical elements in this phase are Setting up monitoring, Analyzing events, Identifying the incident, Notifying CSIRT members, Documenting everything and Threat prevention and detection capabilities.

11.3.3 Containment,

The most crucial action is to isolate the network under attack and perform containment temporarily. Then focus on long term containment that allows all systems to be used in production (involves fixes and solutions temporarily). Containment allows rebuilding a new and clean system.

Critical elements in this phase are System backup, short and long-term containment.

11.3.4 Eradication,

Process of removing malware from all systems that have been affected, recognize the root cause of the cyber-attack and pick up some actions and try to hinder alike attacks in the future.

Critical elements in this phase are ReImaging, Preventing the root cause, Applying the basic security best practices, Scan for malware.

11.3.5 Recovery,

Recovery means bringing all systems back online very carefully to prevent future additional attacks. All IT systems are tested, verified, and monitored in this phase. This phase brings all systems back to regular activity.

Critical elements in this phase are Defining the date and time to restore operations, Test and Verifying, Monitoring, Do everything to prevent another cyber incident.

11.3.6 Lessons learned,

Perform retrospective of the incident, prepare documentation, and investigate the incident. It is crucial to understand what happened and improve security.

Critical elements in this phase are Completing documentations, Publishing an incident report, Identify ways to improve CSIRT performance, Establish a benchmark for comparison and lessons learned meetings.

11.4 Cyber security response plan and why companies need one?

If one or another organisation or company has not been threatened or attacked yet, it will be. Organisations that have experienced cyber-attacks are familiar with the chaos that follows the cyber-attack. Losing data or functionality is scary. Insufficient incident response cannot handle the cyberattack. Only a good incident response plan offers a course of action and detailed incident response to stop, contain and have control of the incident quickly.

11.5 Cyber security response plan frequently testing

As the years of experience shows us, incidents and cybercriminal are rising at a tremendous rate. It is crucial to have a cyber security incident response plan in place. Targeted attacks on organisations are significantly increasing.

Unfortunately, nowadays, it is not enough just to have a response plan in place. It is essential to test and apply a Security Response Plan through the organisation. The primary reason some organisations with response plan still fail to respond effectively is that organisation has never or not frequently enough tested their security response plan across the organisation.

With a Cyber Security Response Plan frequently testing, it is possible to check for loopholes and upgrade and evolve the response plan. It is crucial to do a test and upgrade the Security Response Plan and avoid known vulnerabilities.

Testing the security response plan allows organisations to make adequate investments in human and technological resources and processes.

Conclusion

Advanced malicious software represents a severe threat to the computer systems owned by companies, society and in private. This paper shows that the consequences of malware attacks can be severe and can ruin a company with direct and indirect costs. As long as there are financial gains in the malware industry, society will face malware threats and negative consequences of malware attacks.

Signature-based antivirus software can detect/neutralize only malware software that is known, registered and have already caused damage.

Cybercriminals are more sophisticated and more innovative. We can in the future expect new and more advanced varieties of malware threats that are going to be more challenging for malware detection and analysis. Today exists two methods of malware analysis: *static* that examine the malware without running the code, and dynamic, which involve examination with code running.

Machine learning technologies that are in use today are not adequate to handle challenges. These must be changed so that their potential can handle future more advanced and more sophisticated malware software.

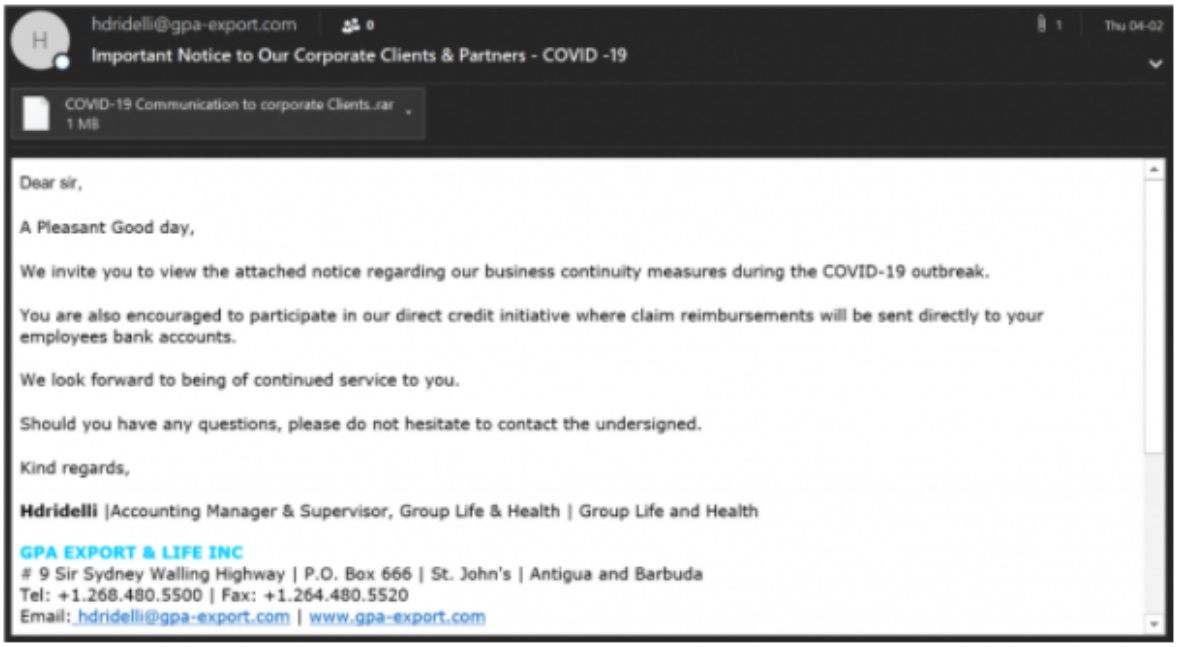
In the future, malware trends can be expected to increase the use of encryption. Improved machine learning techniques allow malware creators to create thousands of new malware versions daily. With the internet of things (IoT) that becomes widespread, every device connected to a global network become vulnerable to compromise for a money. Human error will remain the weak link, and cybercriminals will continue to take advantage of that weakness.

Malware has many different ways to spread, but that does not mean that it cannot be stopped by learning how to do it and be prepared for it when it comes with a response plan ready.

Having a response plan is crucial for a quick and efficient response when malware attacks occur.

Springhill Medical Center was in the middle of a ransomware attack in July 2019, when a woman was in the delivery room. Computers were disabled in every room, and a real-time tracker could not locate medical stuff. Patient health records were inaccessible. In the labor and delivery unit, medical staff were cut off from equipment that monitors fetal heartbreaks. All of this results in the death of a newborn.

As long as machines are unable to recognize the malware threat, make sure not to click on something like this in the future:



Picture 30. (Scam and phishing, 2021)

References

1. *2015. Symantec. [image] Available at: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf> [Accessed 4 October 2021].*
2. *2021. [image] Available at: <https://blog.360totalsecurity.com/en/what-is-virus/> [Accessed 24 August 2021].*
3. *2021. [image] Available at: <https://consoltech.com/blog/what-happens-if-your-computer-is-infected-by-malware/> [Accessed 1 September 2021].*
4. *2021. [image] Available at: <https://eu.usatoday.com/story/tech/columnist/komando/2017/04/14/how-tell-if-you-phone-or-tablet-has-a-virus/100332572/> [Accessed 24 August 2021].*
5. *2021. [image] Available at: <https://threatpost.com/mcafee-covid-rpowershell-malware-surge/165382/> [Accessed 24 August 2021].*
6. *2021. [image] Available at: <https://www.bullguard.com/community/blog/april-2014/what-is-spyware-and-how-to-remove-it> [Accessed 24 August 2021].*
7. *2021. [image] Available at: <https://www.bullguard.com/nb-no/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx> [Accessed 23 August 2021].*
8. *2021. [image] Available at: <https://www.kaspersky.no/resource-center/threats/trojans> [Accessed 24 August 2021].*
9. *2021. [image] Available at: <https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report.pdf> [Accessed 30 August 2021].*
10. *2021. [image] Available at: <https://www.varutra.com/adware-new-age-weapon/> [Accessed 24 August 2021].*
11. *2021. [image] Available at: <https://www.welivesecurity.com/2018/06/13/us-report-highlights-battle-botnets/> [Accessed 24 August 2021].*
12. *2021. Avira. [image] Available at: <https://www.avira.com/en/blog/no-more-secrets-everything-you-need-to-know-about-spyware> [Accessed 13 September 2021].*
13. *2021. Blackfog. [image] Available at: <https://www.blackfog.com/the-state-of-ransomware-in-2021/> [Accessed 9 September 2021].*
14. *2021. blog.360.360totalsecurity. [image] Available at: <https://blog.360totalsecurity.com/en/what-is-virus/> [Accessed 13 September 2021].*
15. *2021. Bradymartz. [image] Available at: <https://www.bradymartz.com/news/fileless-malware-poses-new-threat-to-computer-users/> [Accessed 13 September 2021].*
16. *2021. Consoltech. [image] Available at: <https://consoltech.com/blog/what-happens-if-your-computer-is-infected-by-malware/> [Accessed 13 September 2021].*
17. *2021. Kaspersky. [image] Available at: <https://www.kaspersky.no/resource-center/threats/trojans> [Accessed 13 September 2021].*

18. *2021. Malwarebytes. [image] Available at: <https://www.malwarebytes.com/resource/2020-state-of-malware-report> [Accessed 13 September 2021].*
19. *2021. Ransomware. [image] Available at: <https://www.kaspersky.no/resource-center/threats/ransomware> [Accessed 13 September 2021].*
20. *2021. Scam and phishing. [image] Available at: <https://securelist.com/the-story-of-the-year-remote-work/99720/> [Accessed 22 September 2021].*
21. *2021. Telesoft-technologies.com. [image] Available at: <https://www.telesoft-technologies.com/blog/the-rise-of-the-botnet/> [Accessed 13 September 2021].*
22. *2021. Varutra. [image] Available at: <https://www.varutra.com/adware-new-age-weapon/> [Accessed 13 September 2021].*
23. *Alazab, M. et al., 2012. Cybercrime: The case of obfuscated malware. Institute for Computer Sciences, Social Informatics and Telecomm Engineering, pp.204–211.*
24. *Anon, 2016. Cybercrime. FBI. Available at: https://www.fbi.gov/investigate/cyber [Accessed September 7, 2021].*
25. *Anon, 2021. Home. The National Cyber-Forensics and Training Alliance. Available at: https://www.ncfta.net/ [Accessed September 7, 2021].*
26. *Armstrong, M., 2021. Infographic: How Many Websites Are There?. [online] Statista Infographics. Available at: <https://www.statista.com/chart/19058/number-of-websites-online/> [Accessed 29 September 2021].*
27. *Av-test.org. 2021. Malware Statistics & Trends Report | AV-TEST. [online] Available at: <https://www.av-test.org/en/statistics/malware/> [Accessed 29 September 2021].*
28. *Bauer, J. and Van Eeten, M., 2021. Financial Aspects of Network Security: Malware/Spam. [online] Itu.int. Available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf> [Accessed 13 September 2021].*
29. *BlackFog. 2021. The State of Ransomware in 2021 | BlackFog. [online] Available at: <https://www.blackfog.com/the-state-of-ransomware-in-2021/> [Accessed 9 September 2021].*
30. *Brooks, C., 2021. Ransomware on a Rampage; a New Wake-Up Call. [online] Forbes. Available at: <https://www.forbes.com/sites/chuckbrooks/2021/08/21/ransomware-on-a-rampage-a-new-wake-up-call/?sh=2c19014c2e81> [Accessed 9 September 2021].*
31. *Bullguard.com. 2021. A definition of malware. [online] Available at: <https://www.bullguard.com/nb-no/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx> [Accessed 23 August 2021].*
32. *Bullguard.com. 2021. A definition of malware. [online] Available at: <https://www.bullguard.com/nb-no/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx> [Accessed 2 October 2021].*
33. *Comodo News For Enterprise Security. 2019. What is Malicious Software? | Different Types of Malicious Software. [online] Available at: <https://enterprise.comodo.com/blog/what-is-malicious-software/> [Accessed 3 October 2021].*
34. *Cook, S., 2021. MalwareStatistics in 2021: Frequency, impact, cost and more. [online] Comparitech. Available at: <https://www.comparitech.com/antivirus/malware-statistics-facts/> [Accessed 17 September 2021].*

35. *CyberCPR. 2021. Six steps to defending business with Incident Response - CyberCPR. [online] Available at: <https://www.cybercpr.com/6-steps-to-defending-your-business-with-incident-response/> [Accessed 22 September 2021].*
36. *Data breaches. IT Governance. Available at: https://www.itgovernance.co.uk/data-breaches [Accessed September 2, 2021].*
37. *Fair, A., 2020. Consumers Sound Off: Impact of Ransomware on Purchasing Behavior and Brand Loyalty. [online] Info.arcserve.com. Available at: <https://info.arcserve.com/blog/consumers-sound-off-the-impact-of-ransomware-on-purchasing-behavior-and-brand-loyalty> [Accessed 4 October 2021].*
38. *High-Tech crime. Europol. Available at: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime [Accessed September 7, 2021].*
39. *ISACA. 2021. Advancing IT, Audit, Governance, Risk, Privacy & Cybersecurity | ISACA. [online] Available at: <https://www.isaca.org/> [Accessed 17 September 2021].*
40. *Lis, P. and Mendel, J., 2019. Cyberattacks on Critical Infrastructure: Economic Perspective. Economics and Business Review, 5(2), pp.24-47.*
41. *Liu, W. and Zhong, S., 2017. Web malware spread modelling and optimal control strategies. Scientific Reports, [online] 7(1), p.3. Available at: <https://www.nature.com/articles/srep42308>.*
42. *M.Bauer, J. and J.G. van Eeten, M., 2008. Study on theFinancial Aspects of Network Security: Malware and Spam. [online] Itu.int. Available at: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf> [Accessed 16 September 2021].*
43. *Oberlo.com. 2021. Many People Use the Internet in 2021? [Mar 2021 Update]. [online] Available at: <https://www.oberlo.com/statistics/how-many-people-use-internet> [Accessed 29 September 2021].*
44. *R.Lee, J., 2020. Online Cybercrime Markets and Cybercrime as a Service. Michigan State University, [online] pp.2,3. Available at: <https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Lee_Cybercrime_as_Service.PDF> [Accessed 23 September 2021].*
45. *Securelist.com. 2021. Cyberthreats to financial organisations in 2021. [online] Available at: <https://securelist.com/cyberthreats-to-financial-organizations-in-2021/99591/> [Accessed 22 September 2021].*
46. *SonicWall. 2021. Next-Gen Firewalls & Cybersecurity Solutions - SonicWall. [online] Available at: <https://www.sonicwall.com/> [Accessed 17 September 2021].*
47. *Strawbridge, G., 2021. Malware And How To Prevent Against. [online] MetaCompliance. Available at: <https://www.metacompliance.com/blog/what-is-malware-and-how-to-prevent-against-it/> [Accessed 24 August 2021].*
48. *Tahir, R., 2018. Malware and Malware Detection Techniques. International Journal of Education and Management, 8(2), pp.20-30.*
49. *WeLiveSecurity, 2021. Cybercrime black markets: Dark web services and their prices. [image] Available at: <https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/> [Accessed 23 September 2021].*
50. *What is a Botnet and How Can You Protect Your Computer?. n.d. What is a Botnet and How Can You Protect Your Computer?. [online] Available at: <https://www.avg.com/en/signal/what-is-botnet> [Accessed 3 October 2021].*

51. *Wu, J., 2021. The Cost of Malware & its Impact on Business | Nettitude. [online] Blog.nettitude.com. Available at: <https://blog.nettitude.com/malware-costs-business-impact> [Accessed 2 October 2021].*
52. *www.kaspersky.com. 2017. Criminal Benefits: Profit Margin of a DDoS Attack Can Reach 95%. [online] Available at: <https://www.kaspersky.com/about/press-releases/2017_criminal-benefits> [Accessed 1 October 2021].*
53. Lis, P. and Mendel, J., 2019. Cyberattacks on Critical Infrastructure: an Economic Perspective. *Economics and Business Review*, [online] 5(2), pp.24-47. Available at: <https://sciendo.com/downloadpdf/journals/ebrpl/5/2/article-p24.pdf> [Accessed 6 October 2021].
54. Consolidated Technologies, Inc. 2019. *What Happens If Your Computer Is Infected by Malware? - Consolidated Technologies, Inc.*. [online] Available at: <https://consoltech.com/blog/what-happens-if-your-computer-is-infected-by-malware/> [Accessed 6 October 2021].
55. Cynet. 2021. *Incident Response SANS: The 6 Steps in Depth*. [online] Available at: <https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/> [Accessed 6 October 2021].
56. Cook, S., 2021. *Malware Statistics in 2021: Frequency, impact, cost & more*. [online] Comparitech. Available at: <https://www.comparitech.com/antivirus/malware-statistics-facts/> [Accessed 7 October 2021].