1. Table of Contents

2. List of figures

3. List of tables

SP1

PROJECT	SP1
TOPIC CODE	Project-10- The financial impact of malware
STUDENT NAME	Muhammad Irfan
SP1 TOPIC / PROJECT NAME	Project 10 - The financial impact of malware
DATE	

4. Introduction

Malware nowadays is not a strange phenomenon. Technology is advancing rapidly and devices are connecting to the internet increasingly and evolving. Technology to hack and attack is also advancing at the same pace. The chances of any organization experience an attack and pay the prices is increased with exploitations and malware. Malware attack damages can be very costly to organizations.

Malicious code is a term that includes viruses, worms, trojans, and other dangerous tools hackers use to make big companies lose a lot of money. Microsoft defines malware as, " Malware is a phrase that refers to any software that is meant to harm data systems, such as computers and servers.”. (Defining malware: Microsoft, 2021). It's critical to have a firm grasp of what malware is, how it is constructed, and its impacts on computers. What damages can it cause to computers? This will be discussed in detail further down in the main part.

Criminals nowadays are not working like old days. They don’t rob banks. Instead, they use malware to attack banks, companies, businesses, etc online. It gives cybercriminals much better security against cops, and in a single instance, they can rob millions of dollars. Cybercriminals can attack computer systems from anywhere with any computer. The only thing that a computer must have, is an internet connection. This flexibility makes it more attractive for criminals to follow this path.

Bigger question is why malwares are spreading? Why criminals are focusing on that side of cyber-attacks. What are the benefits and dangers it bears for criminals if they follow that part? Malware is the real cancer of the internet. If companies and private persons don’t take remedies to control malware it can wreak havoc on them. It can cause so many damages that companies can lose whole companies. Malware is designed to cripple businesses. It can turn off everything in a minute of activation (depending on malware). We all have read stories about different ransomware attacks on businesses in the past few years which caused a very messy problem for companies, It locked companies out of business for days, weeks, or in some cases forever. Ransomware is the most devastating part of malware. Ransomware is a family member that you don’t want to invite on Christmas.

It will be discussed how malware cost different businesses. What kind of losses does it bear to businesses? The cost of malware attacks is not limited to the immediate stop of business. There is a big part that is connected to direct cost. A direct cost is a price that companies have to pay to produce any product or service. Indirect expenses are incurred, such as operating costs, loss of sales from downtime, and recovery solutions may increase costs. A company might lose loyal clients' goodwill and confidence.

It will be expensive for consumers to have data in a company that gets hacked. The user can lose its identity in case of a data breach. In case it’s a bank one can lose all of its finances plus identity. It has happened that account holders lost different cryptocurrencies when crypto exchanges got hacked. It will be examined in detail how these attacks on business impact end-users. This impacts also business in the long run. The end-user loses trust in the company.

It has been evidenced by recent events; malware programmers are writing more sophisticated malware that could even affect the biggest of companies that follow very strong security policies.

Nowadays cybercriminals have started their businesses. They also provide MaaS (malware as a service). Different businesses(legit) have started to hack competitions to get the upper hand. This way they can get access to what their opponents are up to and what they can do to make their products better. Ideas like the next big thing. If one steals an idea from a company, one can launch the next big thing long before the original author. This way can companies get the upper hand in the market.

Nowadays companies take cybersecurity very seriously. This led to many companies have a response plan in case of attack. But still, many companies have not come far with cybersecurity. That’s why it’s still a young child. There are still many companies to plan for a good response plan. It will be discussed in the main part why a response plan is important in detail.

5. Main part

Malware is any software that is designed to harm or damage computers, servers, client machines, network devices, etc. Malware has many types, some do have the ability to spread themselves over the network and remain undetectable. It’s malware that can cause changes or damages to the systems for malicious intents.

There are many types of malwares and they are constantly changing. Money is often the main motive, in some cases, it can be data theft for other gains, spying can also be another motive. Statista.com claims "In 2020, there were a total of almost 1001 million data violations in the United States. Simultaneously, data exposures affected roughly 155.8 million persons.

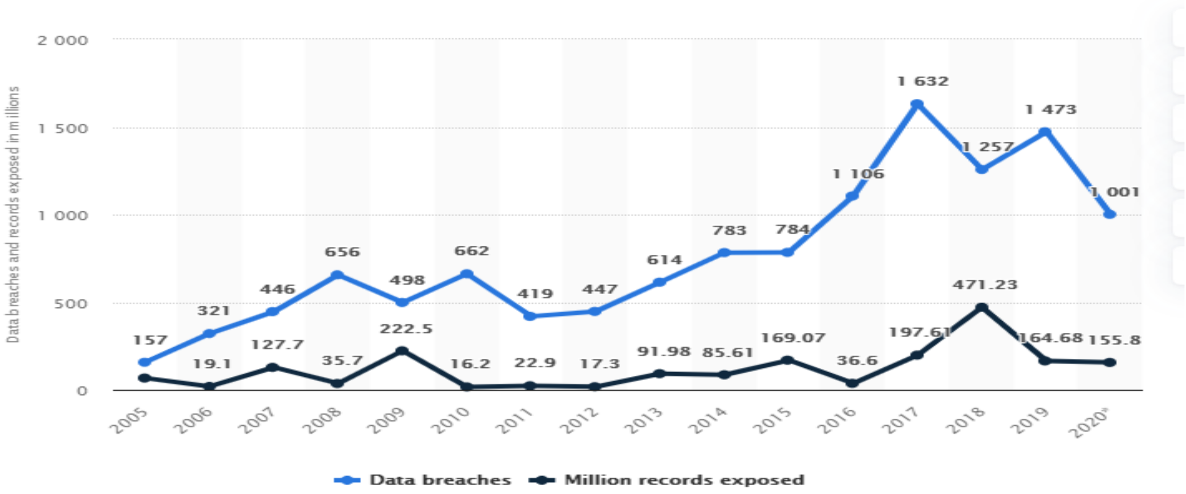


FIGURE 1(U.S. DATA BREACHES AND EXPOSED RECORDS 2020 | STATISTA, 2021)

- Definition
  - The NIST SP 800-53 defines malware as a non-authenticated software or firmware that affects the information system's confidentiality, integrity, or availability. An infectious virus, worm, Trojan horse, or other organism that has infected its host. Malicious code samples can be found in spyware and some adware programs. (malware - Glossary | CSRC, 2021)
- Types of malwares
  - Virus

According to Goodrich and Tamassia in their book Introduction to computer security "A computer virus is a piece of software that can repeat itself by altering other files or programs to introduce code that can copy itself again."

A virus is a piece of computer code that copies itself with another program, this code enforces the program to copy itself and implement code into other programs. The virus usually performs harmful actions like destroying data. Computer viruses are developed to constantly replicate your information and programs, computer viruses infect your data, modify the functioning of the system, and sometimes stop them from operating.

Some viruses in the computer can damage the machine with applications removed, files deleted, or the hard disks reformatted. Others just reproduce themselves by putting so great amount of load on the internet that computers cannot carry out online activities. Even if computer infections are not so destructive, their performance might be damaged and it's so slow that it often crashes.

Signs of a computer virus

According to Norton Security, there are few very common signs one can see if the computer is infected by a virus.

1. Computers performance gets slow down.
2. Pop-ups and spams.
3. It changes the homepage to some random spam page.
4. Unknown programs start at startup.
5. Spam e-mails are sent from your email address.
6. It causes system to crash

How to avoid Viruses.

1. Never open an unexpected email.

2. Use antivirus.
3. Always update the operating system.
4. Avoid pirated softwares
5. Implement a good backup plan

- Trojan horses

A Trojan is a kind of malware that characterizes as a valuable software while actually doing a harmful action, such as launching a keylogger program in the background. (Goodrich and Tamassia, 2014)

The Trojan horse is a famous wooden horse used by greeks during the Trojan war. They use this horse to enter the city of Troy.
Trojan horses are designed to be legit software to not be detected from antivirus and system take it as a normal program. Trojan doesn't reproduce. It is designed to masquerades a program that user wants to install and tricks user to activating it so it can do damages and spread.

Hackers starts trojan horse attack to steal user information, destroy personal data and programs on the hard drives. A trojan horse is a bit different from virus as the Trojan can patch itself to non-executable files, such as image, audio files. Normal delivery method for trojans is through mails, or comes patched with pirated software's. (Networkingsphere, 2019)

FIGURE 2 (MALWARETIPS, 2021)

How to avoid Trojan Horse

1. Avoid software from a not-trusted source.
2. Avoid an attachment or file from an unknown sender.
3. Always up to date system.
4. Install antivirus.

- Rootkit

  A rootkit, according to CNSSI 4009-2015, is a set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's actions and allow the attacker to keep root-level access to the host through covert ways.

  A rootkit is a set of software tools that provide remote and monitoring access to a computer or other system by a hostile actor. Rootkits open a hidden door on target computers to placed or exploit the system to perform additional network security attacks on malwared systems such as viruses, ransomware, keyloggers, or other forms of malware. Try to remain unnoticed by rootkits. This software is also suitable for legitimate purposes, such as providing remote access to end-user assistance. (Rosencrance, 2018)

  The malicious parties use legitimate software to hide the rootkit inside. When a user clicks that to install legitimate software so does the rootkit program also gets installed. It lies low until a hacker activates it. Rootkits are preinstally equiped with such harmful tools as password stealers, keyloggers, antivirus disablers, etc (DDoS).

  A rootkit objectives:

  - Avoid detection (Donovan, 2016)
  - Steal information (Donovan, 2016)

  Rootkit categorization

  Here are a few top rootkits types that can cause serious damages to enterprises

  - **Kernel-mode rootkit**

    This makes changes to the computer operating system kernel. It often disguises as device drivers and loadable modules; due to this it gets unlimited access without any restrictions.

    Some well-known kernel-mode rootkits are Adore, FU, Knark, Da IOS and Rkit. (Donovan, 2016)
  - **Boot kits**

    Rootkit that runs in kernel mode. During computer startup, The boot master (MBR), VBR or boot section is infected. This is a master record boot (MBR). When the kernel has loaded, the malware loader stays in protected mode, allowing it to disrupt it. (Donovan, 2016)

    Bootkits like Olmasco, Rovnix, and Stoned Bootkit are well-known.. (Donovan, 2016)
  - **Virtual rootkit**

    A virtual machine-based rootkit (VMBR) is a rootkit that operates as a virtual machine underneath the current operating system. A VMBR might go unnoticed in this manner unless specific technologies are employed to detect it. (AVG signal team, 2020)
  - **Firmware Rootkit**

    It creates a virus image in hardware such as a router, network card, hard drives, or UEFI (Unified Extensible Firmware Interface) and BIOS (Basic Input/Output System) by using devices or platforms firmware (Unified Extensible Firmware Interface). It's difficult to notice this way. (Donovan, 2016)

- Worm

  NIST SP 800-28 defines a worm is an auto-reproducing software which spreads to another computer system across the network, without a host application or human participation.

  The most dangerous form of malware is a worm, which reproduces and infects each machine that comes into contact with it. It has the ability to launch a devastating strike in a short amount of time. It causes harm in the same way as a virus does, but it does it without the need of any software. It can collect valuable information and create a back door by exploiting flaws in security software. A worm consumes a significant amount of system resources, causing a server or computer to fail or slow down.

Here are few famous worm attacks

1. **The Morris Worm, 1988**
   Robert Morris, a PhD student at Cornell University at the time, created one of the earliest computer worms in 1988. The payload of this worm was not harmful. Instead, it just replicated itself and disseminated over the internet. The primary issue with this worm was that it was intended to duplicate itself on a different machine, even if it was previously infected. It would examine the target machine to determine whether it had previously been infected, but it would ignore a "yes" response in one out of every seven checks and infect the computer nonetheless. (Goodrich and Tamassia, 2014)
   The 1/7 chance of reinfection became a significant issue. A DOS (denial of service) assault was launched on compromised machines. Morris virus was found on 10% of PCs. Damages in the tens of millions of dollars were incurred as a result of the incident. The first person convicted under the Computer Fraud and Abuse Act of 1986 was Robert Morris. (Goodrich and Tamassia, 2014)

2. **ILOVEYOU, worm, 2000**
   On and after May 5, 2000, the computer worm ILOVEYOU, also known as Love Bug or Love Letter for You, infected over 10 million Windows PCs. It spread by emails with the title "ILOVEYOU" and the payload "LOVE-LETTER-FOR-YOU.txt.VBS." When users opened the attachment, the Visual Basic script started running.

   According to estimates, the virus affected 45 million PCs. ILOVEYOU is also regarded as one of the first malware assaults that employ social engineering. It was a self-replicating worm that exploited the victims' email account to distribute spam. (Gatefy, 2021)
   Damages were estimated to be between $5.5 and $8.7 billion. (Catalogs.com staff, 2019)

3. **MyDoom, worm, 2004**
   W32 is the other name for Mydoom. Novarg, Mimail.R, and Shimgapi (MyDoom@mm, Novarg, Mimail.R, and Shimgapi) are some of the programs that can help you
   The MyDoom worm made headlines in 2004 when it attempted to attack big technological companies including Google and Microsoft.
   Emails helped spread the word. It was used as a backdoor for remote control and DDoS assaults. Millions were lost as a result of the incident. (Gatefy, 2021)
4. **Stuxnet, worm, 2010**
   In 2010, the Stuxnet computer virus was deployed in a political strike against Iran's nuclear program. It took use of a number of zero-day vulnerabilities in Windows. This worm does not require an internet connection to infect a computer; instead, it may be spread via USB devices. (Gatefy, 2021)

- Spyware

  Spyware is a type of software that tracks users' activities without their permission or knowledge, according to ENISA. Keylogging, activity tracking, data collecting, and other types of data theft are examples of espionage activities. Spyware is often distributed via a Trojan horse or by exploiting software flaws. (ENISA, n.d.)

Spyware is one of the most common threats. It infects devices easily and it is very hard to detect spyware. It's a threat to everyone who uses computers as they can easily steal personal information.

Common ways one can get infected with spyware are:

- Accepting a popup window without reading it. (NortonLifeLock, 2019)
- Using untrusted softwares. (NortonLifeLock, 2019)
- Downloading unexpected mail attachments. (NortonLifeLock, 2019)
- Pirating media. (NortonLifeLock, 2019)

Common signs of spyware on any computer.

It should not be easy to find spyware. It's made stealthy, deceptive, and hard to find. Here are some clues to look after to find spyware. (NortonLifeLock, 2019)

- The device crashes. (NortonLifeLock, 2019)
- The hard drive runs out of disk space. (NortonLifeLock, 2019)
- Pop ups when device connects to internet. (NortonLifeLock, 2019)

Common types of Spyware

There are many types of spyware. Each works in a different way to attack, but aim is often to spy on the user of that specific computer and steal information.

- Browser hijack
  It is a program that controls a web browser and shows unwanted advertisements. This doesn’t need any permissions to operate. Its because it creates shortcuts in favourite folder of browser.
- Keylogger
  Keyloggers are created to monitor computer activites by recording keystrokes, email activity, websites accessed, credentials details and personal search history. (Managed Solution, 2020)
- Banking Trojans
  It obtains credential information from financial institutions; it modifies transactions content or web sites for malicious intents and for that it tries to take advantage of vulnerable browser security.

- Adware

According to Malwarebytes Adware is a software designed to send advertisements on computers.

Adware ads are created as a pop-up or in certain circumstances as a "not closable window." Anti-adware software has been the attention of several businesses. Anti-adware software, both free and commercial versions, abound on the market. Extensions for web browsers are now available. On browser extensions, there is a long list of adblockers. These adblockers assist in the blocking of annoying ads.

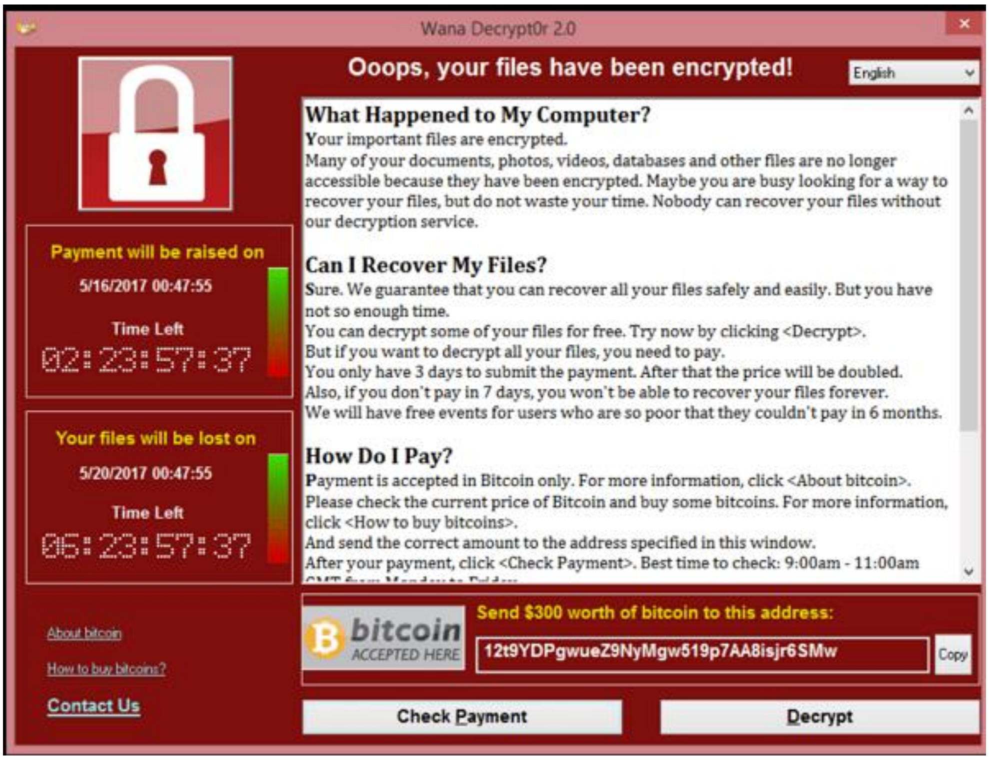
Signs of having adware on the computer.

1. Crashing of web-browser.
2. both MAC and PC installs softwares without owner consent.
3. PC performance slows down, same goes with web browser.
4. Default homepage of web browser changes without owner consent.
5. The unexpected advertisements.
6. Commonly visited pages doesn’t appears same as before.

- Ransomware

According to ENISA, “Ransomware refers to a type of malware (such as viruses, Trojans, and so on) that infects users' computer systems and manipulates it so that the victim is unable to use it or the information contained on it (partially or completely),” according to ENISA. In general, the victims receive a challenging message soon after and to persuade the victim to pay the money in order to regain full access to the victim's systems and archives." (ENISA, n.d.)

A very common and known sign of ransomware attack is that computer system data becomes encrypted and appears a ransom note on a computer screen.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

FIGURE 3 WANNACRY RANSOM NOTE

A list of known Ransomware attacks

1. **CryptoLocker, ransomware, 2013**

   This malware has a long and illustrious history. It gained notoriety in 2013 for having a very big encryption key, making it extremely tough for professionals to work with. It cost over $3 million in damages and infected over 200,000 machines. This malware targeted the Microsoft Windows operating system. It was mostly disseminated via e-mail. The ransomware was linked to a PDF file, making it harder to comprehend. Users were unaware that they were infecting themselves with malware. (Gatefy, 2021)

2. **Petya, ransomware, 2016**

Petya was different from other ransomwares in that it locked the user out of the whole operating system. This article concentrated on the Windows operating system. Paying a ransom was the only way to get the operating system open. Since its debut in 2016, this ransomware has been projected to cost approximately $10 billion. This virus attacked banks, airports, the oil sector, shipping firms, and many others. (Gatefy, 2021)

3. **WannaCry, ransomware, 2017**

   This is one of the most well-known ransomwares, having infected hospitals, universities, and big corporations all over the world, including FedEx, Telefonica, Nissan, and Renault. WannaCry infected over 200,000 computers around the world. In 2017, it all started with a phishing email. To target Windows systems, this malware used a zero-day vulnerability. This virus cost the whole globe about USD 4 billion.
   (Gatefy, 2021)

4. **LockerGoga, ransomware, 2019**

   In Norway, LockerGoga became well-known. Norsk Hydro 2019 was one of the companies affected, but it wasn't the only one. Many big businesses, like Hydro and Altran Technologies, were affected. Hydro alone lost USD 74 million, as did many others who lost millions as a result of the virus. It began by infecting people via email and phishing schemes. It acts similarly to the Petya ransomware in that it prevents full access to the machine. (Gatefy, 2021)

- Logic Bomb

According to Goodrich and Tamassia in their book “Introduction to computer security”

A logic bomb is a computer program that is intentionally inserted in a system and triggers off a destructive function when a certain situation is fulfilled. (Goodrich and Tamassia, 2014)

Logic bomb is a mischievous code injected surreptitiously into the operational network. It remains inactive unless a certain set of circumstances is met. A logic bomb is triggered when that condition is met. By altering data, erasing files, or wiping hard drives, the system is destroyed. (Logic Bomb | Avast, n.d.)

If a programmer is ever fired from the company, they may conceal code that starts deleting files (such as a salary database). This is a textbook example of a logic bomb. This code deletes the whole database if a certain condition is met. And it causes the firm to lose both money and data.
The time bomb is called a logical bomb that sets off on a certain time and date. Typically, this sort of attack occurs when an employee becomes dissatisfied and seeks retaliation for whatever reason.

Examples of Logic bombs

At the Siemens Corporation, a well-known logic bomb occurred. One of Siemens' offices received software from a contract employee named David Tinley. With over a decade, he worked for Siemens as a trusted advisor, offering spreadsheet software to monitor equipment. Tinley snuck a logic bomb into one of the spreadsheets. Every time the coded logical state is satisfied, the program breaks in and Tinley is called in to correct it. Tinley's curriculum was two years long. Tinley was able to meet to fix the problem, and following another crash, he gave the password to the software to Siemens' IT team, and the logic bomb was eventually discovered. (Logic Bomb | Avast, n.d.)

Another example of a real-life bomb assault against Omega Engineering Company. On the server for the Omega Engineering production business, A logic bomb was activated on July 31, 1996, causing millions of dollars in damage and forcing the company to lay off many of its employees. After the inquiry officials determined that Tim Lloyd's server manager was responsible for the entire attack. They located a few backup disks at the flat in Tim Lloyd's, but they were deleted. (Goodrich and Tamassia, 2014)

A logic bomb's may be designed to:

1. Gather sensitive data.
2. Delete files.
3. Wipe hard drives.
4. Siphon off funds.
5. Corrupt data.

Defences against insider attacks

Defences against such attack are not easy to defend against as it comes from a trusted employee(programmer) who is not to be trusted. But Defences against such attacks or not impossible.

According to Goodrich and Tamassia, in their book "Introduction to computer security" companies can take measures to avoid insider threats.

1. A single point of failure(spof) leads to disaster. It should be avoided.
2. Use a code walkthrough. Each programmer should present their code to another programmer, line by line so that they can help each other. In such a scenario it's impossible to implement a backdoor or logic bomb without that other programmer noticing it.
3. Archiving and reporting tools should be used. These kinds of tools have the ability to uncovering or documenting insider attacks.
4. Authority and permissions should be limited. It should be implemented least privilege principles.
5. Critical systems should be under higher watch, security and in locker rooms with limited access.
6. Employee's behaviour should be monitored. Companies should have plans to watch out for disgruntled employees.
7. Software installations should be controlled. Only reliable software's should be installed and used.

- The remote access Trojan (RAT)

A remote access trojan (RAT) is a form of malware that uses the back door to gain administrative access to a target machine. Malware like this is frequently introduced through pirated software or email attachments. Once a machine has been hacked, an attacker can use it to spread RATs to other computers, forming botnets. (TechTarget Contributor, n.d.)

According to Cisco RATs are a nasty malware. This type of malware makes possible for intruders to gain remote access of compromised machine, and can be used to perform malicious activities like monitoring users through keyloggers and other spywares. Infected device can be used to infect other devices, impersonate the victim, deleting, downloading data or altering files in the system.

A remote administration tool (RAT) gives criminals administrative authority over the targeted computer, allowing them to do anything they want:

1. accumulating data from the system
2. steal usernames and passwords.
3. Log keystrokes.
4. This makes possible for intruders to get hold on personal and financial information like credit cards information, bank information etc.
5. Virus and malware distribution
6. Disk formatting
7. Recording audio, video and screen recording,
8. Delete, download or modify files and system of files

One of the better-known examples of a RAT was the Back Orifice rootkit. A hacking group called Dead Cow's Cult set up Back Orifice to reveal Microsoft's Windows operating systems' security vulnerabilities. (TechTarget Contributor, n.d.)

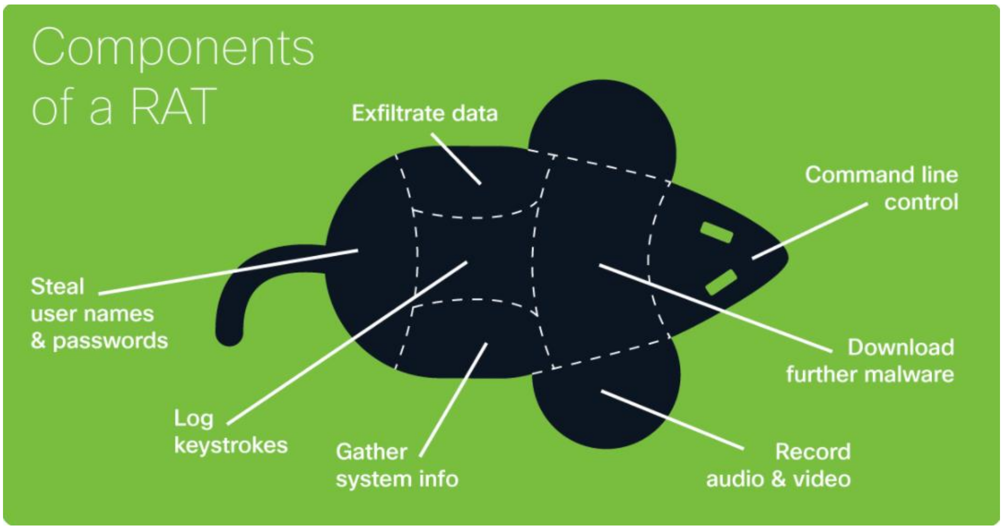


FIGURE 4(NAHORNEY, 2019)

How to detect and catch a RAT

RATs can't be detected easily. Often, they do not appear in listings of applications or tasks that run. The activities they perform frequently resemble those of reputable programmes.

1. To guard against RATs, a robust endpoint protection program is essential. (Nahorney, 2019)
2. It's also crucial to keep an eye on network traffic for any illegal activities. (Nahorney, 2019)
3. Many RAT's encrypt traffic, and you may keep traffic monitoring. Encrypted Communications Analytics provide a clear overview of hazards in encrypted traffic, without decryption utilizing machine learning and network analytics. (Nahorney, 2019)
4. 4. It is essential for many RATs to be able to connect to host domains. It might take a long time to block known malicious sites to halt a RAT in its path. (Nahorney, 2019)
5. If an attacker obtains login credentials, multi-factor authentication technologies can prohibit them from logging into a system. (Nahorney, 2019)
6. A solid email security solution, as well as a strong network perimeter, will aid in the complete blocking of RATs. (Nahorney, 2019)
7. In the case of a RAT gaining network access and trying to rob important information, a DLP (Data Loss Prevention) online security apparatus can be used to assist. (Nahorney, 2019)

- Bots/Botnet

It is desired to control massive networks of hacked computers, utilizing them as nodes in a spam operation or stealing information from their owners, because criminal businesses are engaged in unlawful operations on a large scale. Botnets are the term for such a network. (Goodrich and Tamassia, 2014)

A botnet is a group of bots-containing computers. A bot is malevolent software, which receives a master's commands. The term bot originates from the ancient Internet Relay Chat chat service (IRC), where users may build so-called "bots" that can keep channels alive, provide amusing on-demand lines, etc. The earliest botnets were constructed as IRC bots directly. A system is infected with either a worm that installs the bot or via a browser-weakness visit to a malicious site. (ENISA, n.d.)

Botnets are one of the most serious dangers to the internet, according to ENISA. When bot malware is installed on a computer, it has the same level of access to the system's resources as the machine's owner. Bots may then read and write files, run programs, intercept keystrokes, gain access to the camera, and send e-mails, among other things.

How Botnets are installed and Controlled

Botnets rely exclusively on a command-and-control system. When bot software is installed on a victim's host through a worm, Trojan, or other malware package, the infected system, known as a zombie, reaches out to a central control server for orders. This manner, owners of bots may give orders at whim that influence possibly millions of machines without having to control each zombie individually. (Goodrich and Tamassia, 2014)

Botnet uses

Once built, the botnet owner can engage in criminal behaviour. On a far larger scale, botnets can gather credit card details, bank account credentials, and other sensitive information. Some botnets send out millions of spam e-mails. Due to the massive total bandwidth under the control of a single individual or organization, certain botnets have been utilized to carry out distributed denial of service assaults (DDoS).

Most notable Botnets attacks

1. **Earth-Link Spammer – 2000**
   The first botnet to receive widespread attention was this one. Khan K. Smith constructed it. The botnet sent over 1.25 million phishing emails disguised as official website communication. This botnet's primary goal was to collect sensitive information such as credit card details or to infect victims' machines with malware. Smith could have made $3 million if he worked hard enough. However, for exploiting Earthlink's network for this spam operation, he was sued for $25 million. (White Ops, 2018)
2. **Storm – 2007**
   Storm is widely regarded as one of the first peer-to-peer botnets. This was the first botnet that several servers operated. This botnet was used in a number of DDoS assaults since it had a large number of infected machines under its control, allowing it to produce a flawless DDoS attack. There were between 250000 and 1 million infected machines in the network. (White Ops, 2018)
3. **Cutwail – 2007**
   It turned out to be a spam mail botnet. In 2009, it was responsible for 46.5 percent of all spam sent throughout the world. Due to the impossibility of removing 1.5 million compromised computers, the cutwail is still accessible for rent. Many law enforcement organizations, including the FBI and Europol, attempted to take down Cutwail in 2014 but were unsuccessful. (White Ops, 2018)

4. **Grum – 2008**
   In 2009, Grum could also send 39.9 billion e-mails every day, it became famous for specializing in pharmaceutical spam. (White Ops, 2018)
5. **Mariposa --- 2008**
   Mariposa was a botnet that originated in Spain and was able to steal millions of dollars from innocent clients by collecting credit card information and login credentials to their consumer finance accounts. It took over 10 million devices using malvertising, or the use of digital adverts to distribute malware, making it the second-largest botnet ever uncovered. (White Ops, 2018)
6. **Mirai – 2016**
   On the east coast of the United States, the Mirai botnet was responsible for a major DDoS attack that rendered much of the internet unavailable. Mirai was important, though, because it was the first major IoT-infected botnet. The worm infected approximately 600,000 machines at its height. A group of university students created the botnet, aiming for a competitive advantage in Minecraft. (White Ops, 2018)

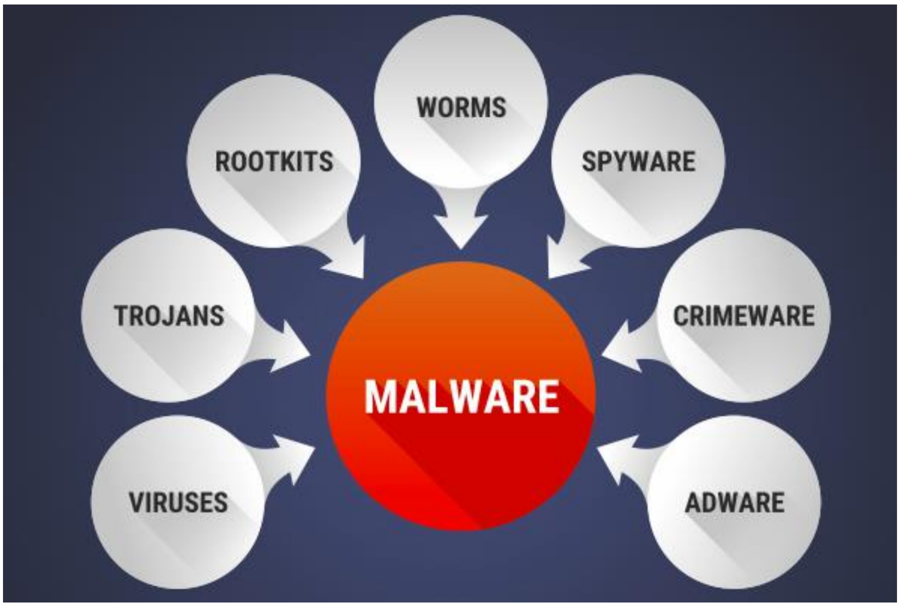


FIGURE 5 (WHAT IS MALWARE & HOW TO DETECT MALWARE, 2019)

- ## Problems of malware

A malware can cause many problems for computers and networks. Hackers use it to access unauthorized computers, steal passwords, destroy information and inactivate machines. A malware-infected computer may give corporations and private users a serious problem. Malware is available in numerous kinds, and each sort of malware's impacts can vary considerably. Malware may interrupt corporate activities in many ways, from daily operations to private data robbing to major reputational harm. The most prevalent assaults on companies range from data robbery to ransom data encryption.

Damages caused by malware are different in the home network and a corporate network. Malware compromises the security infrastructure of a network/system in a corporate network, causing a slew of security concerns for organizations. The following are a handful of the most significant effects of malware on businesses:

- Disrupts and Disables Services:

It undermines an organisation's network and stops business operations in the worst case and mild case it just disrupts business operations. It is very depending on what kind of malware attack happened to a business. If it was a ransomware attack, it can cripple a business and stops everything in business. But a simple Trojan attack can cause big data leakage or data theft.

- Identity and personal information will be retrieved:

This kind of attack is very common on a home network, but it can also hit businesses. This happens in many ways. A malicious code can be activated remotely, through e-mails or downloads. A malicious software runs in the background and tries to collect sensitive information (bank details, passwords, user names, account details, etc)

- Completely Breakdowns the Entire Enterprise Network Infrastructure:

This will be a cocktail of attacks in which a ransomware attack happens at the same time as some other attacks.

- Malware can control all apps running on your device:

Malware is famous for that. Once downloaded on a target computer, it will try to take control of the machine. Its highly depending on which type of malware, some do control machine which can be noticed by a user, others are very stealthy, stealthy malware are like cockroaches, they sit on the side and wait for darkness.

- Access Sensitive Information:

This is often the target of Attackers (hackers). Sensitive information is often very expensive. It can cause businesses millions in a loss. This will have a negative impact on market business operations.

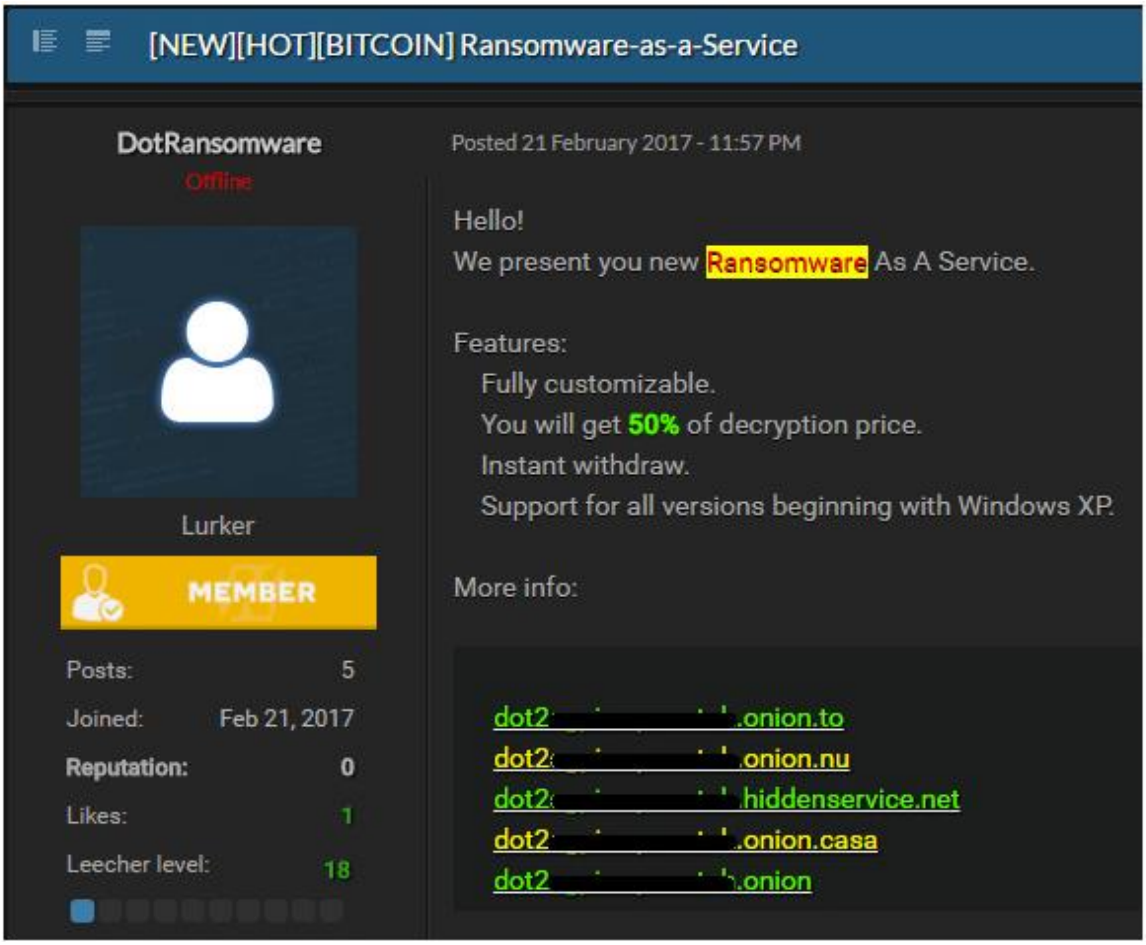
- Send Spam mails

A malware installed on company servers can use corporates mail servers to send malicious e-mails on the company's behalf. This makes those mails legitimate for other parties and in this way a simple attack can get much bigger and dangerous for many other partners of that particular company. In the long run, this can cause much bigger financial damages to the company.

Some of the famous attacks in the past few years show us what is the biggest problem with malware is. They are the gateway to all the problems. One single wrong click can cause a company millions of dollars and for a private user can cause a stolen identity which leads to a bigger problem for that specific person.

- ## Criminal use of malware

If you consider cybercriminals as a company, they need to earn money and be efficient. They are unlawful criminals, but they are also businesses and like any business they need to have a beneficial business. Previously, criminal activity was carried out in person, which was an increased risk, decreased reward method. Criminals discovered that online crime had a minimal chance of being detected and could be spread to countless millions with a few mouse clicks. Among the most powerful weapons in this arsenal is malware. A single piece of malware like ransomware or a trojan bank may cost from 100 to 500 dollars anywhere and infect millions of people. Cybercriminals have turned every product into a service, much like our modern technology industry has done. Many varieties of malware are available as a service, which means criminals don't have to manufacture or distribute it themselves. A snapshot of FLUX ransomware-as-a-service is shown below (RAAS) (Why cybercriminals love malware, n.d.)



[NEW][HOT][BITCOIN] Ransomware-as-a-Service

DotRansomware
Offline

Lurker

MEMBER

Posts: 5
Joined: Feb 21, 2017
Reputation: 0
Likes: 1
Leecher level: 18

Posted 21 February 2017 - 11:57 PM

Hello!
We present you new Ransomware As A Service.

Features:
Fully customizable.
You will get 50% of decryption price.
Instant withdraw.
Support for all versions beginning with Windows XP.

More info:

dot2[redacted].onion.to
dot2[redacted].onion.nu
dot2[redacted].hiddenservice.net
dot2[redacted].onion.casa
dot2[redacted].onion

FIGURE 6 (RANSOMWARE AS A SERVICE (RAAS) | THE BUSINESS OF RANSOMWARE, 2020)

The main motive behind any cyber crime is always financial gains. The cybercriminal can do anything to meet that target. We will look into some of ways of how they exactly get financial benefits.

- Ransomware

  Ransomware is the number one risk to people and has dominated the news in the last several months. This is a type of malicious software that can restrict users or businesses from accessing their computer systems, data, or servers until they pay a ransom to the cybercriminal. This has been number one method used by cybercriminals to get hold on user's computer which leads to ransom and often targets of this type of attacks are big businesses. (sophos, n.d.)

- Product sales

  Despite the fact that this is an old hoax, fraudsters continue to set up a business offering unbelievable offers in order to get payment information. Others do, in fact, deliver phony goods to unwary customers. This way they use stolen credentials to get financial gains. (sophos, n.d.)

- Pay click fraud.

  After getting into a user's computer, criminals can install malware that deceives Internet traffic. The victim's inputs are redirected to the offenders' websites for advertising. Cybercrooks earn from ad networks by directing traffic to their customers' advertisements. (sophos, n.d.)

- Banking malware

  Cybercriminals are motivated by money. Capturing login information to gain access to online banking institutions has spawned an entire business. Modern banking has come a long way from simple key-logging software that captures identities and data. Trojans can capture screen and collect SMS messages as user check in. Hundreds of millions of dollars have been stolen as a result of this approach. (sophos, n.d.)

- MaaS (Malware as a Service) business model

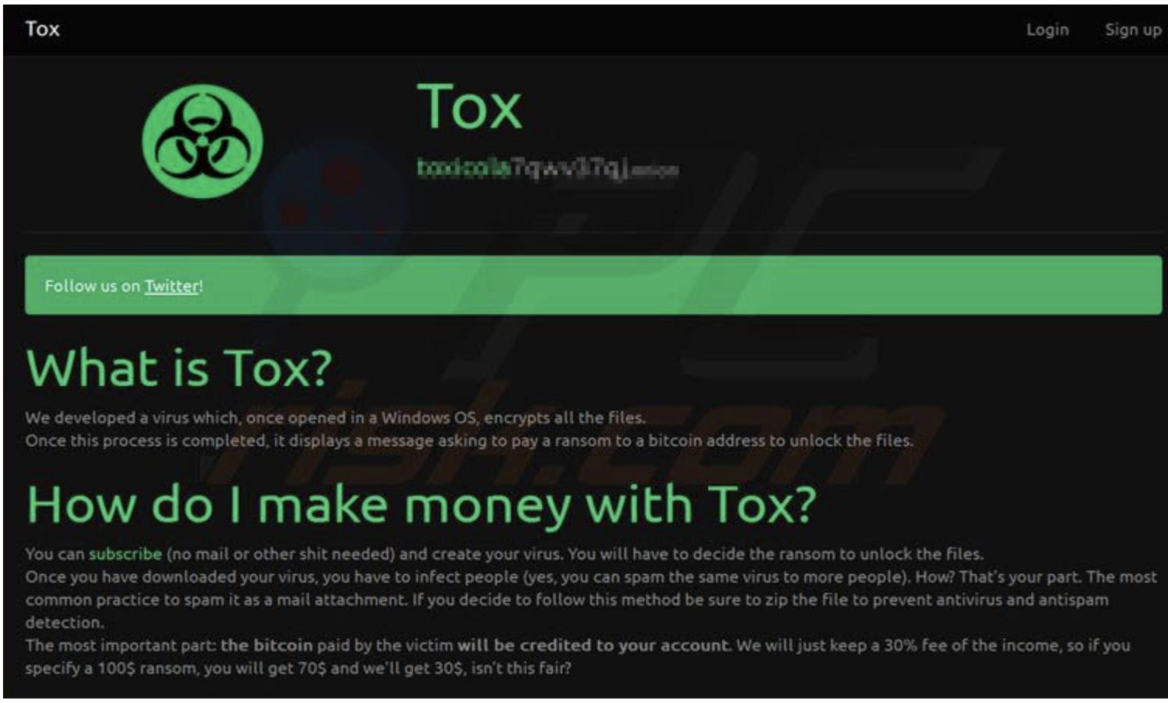
As long as people desire to conduct cybercrime, there will be those eager to help them do so. However, there are some extra profit centres as a result of this. It seems, the criminal must still deploy their program after purchasing it. After they've purchased the malicious programs, they may discover that they require more functionality or services. Upsells and customer service, in other words. Malware-as-a-Service gives cybercriminals everything they need to get started and poses a danger to modern businesses in two ways. First, as malware writers seek to differentiate themselves from their competitors, Malware-as-a-Service creates a need for making it the easily available, easy-to-use harmful applications. As a result, malware threats have become far more accessible and sophisticated. Secondly, the quantity of individual threats is significantly increasing with malware as a service by empowering individuals who would not otherwise be able to build harmful programs on their own. This basically gives everyone the ability to launch cyberattacks. This is next level of earning; malware creator never comes into picture and, sells and earns money without risking getting caught. (Laing, 2018)

- Stealing login details

The objective is to persuade users to communicate spam from someone that they know or trust. Criminals apply social engineering methods for real brands to gain usernames and passwords for value-added websites such as PayPal, the banks, Yahoo, and other web services. Phishing E-mail leverages a user's ignorance about hacking and data infringements. This leads to either financial gains on the spot or they use your credentials from that website and sell it on dark web. (sophos, n.d.)

- Social media spam

Spammers are having a difficult time with normal spamming methods. With time, spam detection improved, and users become more adept at identifying phony names. Instead, criminals have turned to using social media to propagate fake websites—users are statistically more likely to open the link if it originates from either a friend or relative. Which leads to that concerned party downloads malware of some sort on their pc and from that point and onward user loses confidential information to hackers. (sophos, n.d.)



Follow us on Twitter!

What is Tox?

We developed a virus which, once opened in a Windows OS, encrypts all the files.
Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.

How do I make money with Tox?

You can subscribe (no mail or other shit needed) and create your virus. You will have to decide the ransom to unlock the files.
Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more people). How? That's your part. The most common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to prevent antivirus and antispam detection.
The most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will just keep a 30% fee of the income, so if you specify a 100$ ransom, you will get 70$ and we'll get 30$, isn't this fair?

FIGURE 7(RANSOMWARE AS A SERVICE (RAAS) | THE BUSINESS OF RANSOMWARE, 2020)

- ## Why malware spreading aggressively

There are several variables that contribute to the propagation of malware. Vandals, swindlers, blackmailers, and other criminals are among the ones who want malware production. While the vast majority of harmful programs are created with the intent of making money illegally, the motivations for developing malware can range from pranks and activism to cyber theft, espionage, financial gain, being first in creation by stealing others' ideas, making the competitors seem bad, and MaaS (malware as a service).

Malicious persons will, sooner or later, find a method to abuse nearly any discovery or new technology in order to inflict harm or make income. As the lawful use of computers, mobile devices, and the Internet has increased, so have the chances for unscrupulous individuals to profit from the creation of destructive computer viruses, worms, Trojans, and other types of malwares. Many of these virus authors were formerly pranksters looking for a way to pass the time and get notoriety. Though this is still true for some, the overwhelming majority of people who create malware do so for purely illegal purposes, such as erasing data, acquiring personal and sensitive information, reconnaissance, and a number of other illegal activities. Cybercriminals make a lot of money by creating malware, and they profit from your mistakes. Malware authors may be found all around the world, with many of them having ties to corporate and government entities. Malware development, on the other hand, thrives in areas where cybercrime laws aren't enforced and there are limited possibilities for technically capable individuals. (Kaspersky, n.d.)

Even virus writers are moving to a cloud-based commercial model. Rather of making a one-time profit by selling a security exploit, malicious software writers are instead offering malware as a cloud-based service. Experts believe that this means that cybercriminals benefit every time one pays to use or hire one of their products. (Palmer, 2016)

Cybercriminals follow in the footsteps of major companies, taking more than a few pages from the books of large technological enterprises. They are now concentrating on building solutions that are incredibly simple to use and accessible from any location in terms of deployment. To put it another way, malware has moved to the cloud. (Laing, 2018)

Here are some of reasons why malwares spreading like wild fire.

- ### Understaffed Cybersecuirty teams

In its State of Cybersecurity report for 2021, ISACA found that 61 percent of cybersecurity specialists believe their organization's cybersecurity team is understaffed. Understaffing in organizations, such as business and government, can put a burden on current employees and raise the danger of malware attacks. (Cook, 2021)
About half of respondents (47%) stated they "had somewhat" understaffed, while 14% said they "had a large amount" of underemployed people. A further 34% said their company is “appropriately” staffed, while only 4% said they are “somewhat” or “significantly” overstaffed. (Cook, 2021)
Year after year, there is an increase in the need for labor. Jobs in the cybersecurity business continue to go vacant, from C-suite executives to technical and contributor positions, as demand outpaces the amount of people with the necessary capabilities. (Cook, 2021)

- ### Ransomware and IoT attacks increasing

IoT devices are growing and many have considerably less malware security than devices with more prevalent operating systems. In 2020, SonicWall discovered malware was down 43%, while ransomware was up 62% while IoT malware experienced a 66% rise with a total of 56,9 million IoT assaults. (Cook, 2021)

- Encrypted malware attacks

Malware assaults are being sent through SSL/TSL traffic by an increasing number of threat actors. Because encrypted channels make identification and mitigation more difficult, the malware packages in question have a greater success rate. In 2019, SonicWall detected 3.7 million malware assaults of this type, up 27 percent from the previous year. (Cook, 2021)

- Formjacking, Uprising problem

Symantec also noticed a spike in "formjacking," that BrightTALK named the "innovative threat of 2019." Formjacking occurs when cybercriminals inject malicious Javascript into a website's code, allowing it to "skim" financial data from payment forms. Security investigators are comparing this to ATM skimmers connecting ATM machines with the card reader and siphoning information via a credit card magnetic strip. In 2018, Symantec discovered an average of 4,800 websites per month that were infected with formjacking malware. In the same year, the security firm stopped 3.7 million formjacking assaults, indicating the rising problem. Prior to 2018, there is little data on formjacking to depend on, indicating the rapid rise of this malware attack vector. In total, it appears that hackers have shifted their strategy away from convincing online users to download malware directly from compromised web pages and toward other malware distribution techniques. Even formjacking, a type of malware, does not require the user to download a file. Hackers tend to favor more distinct tactics these days. (Cook, 2021)

- Ransomware payment demands increased

One of the primary reasons why hackers prefer ransomware over other common viruses and malware is the payoff. Payments for ransomware have already surpassed $1 billion per year, making it far more profitable than traditional malware. Ransomware has become so profitable that hackers have increased the sums they want in ransom payments. In the first quarter of 2019, the criminals' asking price for ransomware eradication jumped by 93%, according to Beazley. (Cook, 2021)

• Direct and indirect cost

▪ Direct cost:

It is a cost that relates to direct expenses caused by a malware attack. Examples of these costs include settlement costs, investigation, drops in share value, notification to those impacted, potentiallitigation sales and operational disruption, financial theft, legal costs, regulatory fines, public relationscosts, credit monitoring, and reimbursement costs.

.

▪ Indirect cost:

Because there is no direct monetary outlay associated with indirect expenses, they are naturally more difficult to quantify. According to the 2016 Ponemon Cost of Data Breach research, these costs account for 66% of the cost of a cyberattack. loss of customers and market share, Downtime, Loss of reputation, loss of clients, declines in productivity and profit, hiring experts’ expenses and data loss, and insurance and reputation costs are examples of indirect costs. (sitelock, 2017)

Type of Direct and indirect cost

Direct cost	**Indirect cost**
Settlement cost i.e. ransom payment	Data loss
Revenue loss due to the stop of production and sales.	Downtime because of attack
Paying the Incident Response Costs	Reputation loss
Damages to trade name	loss of customer trust and talentedemployees
The recovery process takes time and it cost also a lot.	Collateral Damages like legal costs due to indictments from unhappy clients.
Cost of lost productivity	Stock market losses due to mistrust from investors.

TABLE 1 DIRECT AND INDIRECT COSTS

• True Cost of Malware for a business

After defining the direct and indirect cost of malware. It's not so difficult to see which costs more for businesses. A direct cost is an expense incurred as a result of a malware attack. While the indirect cost isnot directly related to the attack, it is realized as a result of the malware's effects. Several factors play role in this manner.

It is indeed important to note that direct losses aren't always an accurate reflection of a company's overall financial impact. For starters, these estimates do not include the cost of precautions. Organizations invest a broad range of sums on data protection, The costs of different indirect measures such as security awareness training for employees, work or labor expenditures for malware research in order to disinfect infected systems are not covered by direct costs. (ITU, 2008)

Some of the financial impacts of a malware attack for businesses:

- The Ransom

  To begin with, professionals think that paying the ransom is not a good idea. Paying a ransom helps thecyber-criminal business, and numerous cases demonstrate that firms that have paid have seen an increase in ransom demands. Almost all of the retrieved data was corrupted by cryptography, or they never received a response from the attackers. So,stop bleeding, stick to the incident management strategy, and begin securely recovering corporate data. (Juul, n.d.)

- Legal expenses

A data breach might result in sanctions in several sectors. Clients may seek direct compensation, and/ora firm may face serious financial difficulties. Furthermore, even if the firm processes personal or sensitive data per the EU's GDPR legislation, the company must always notify clients of a data breach assoon as possible. Because of this legal difficulty, the Danish Centre for Cybersecurity has begun warningabout a rising trend of cyber-criminals threatening to reveal stolen data if it is sensitive, such as health, financial, or other personal information. (Juul, n.d.)

- Downtime

Even if a firm can restore all of its data from backup and refuses to pay the ransom, business disruptionlosses due to downtime are unavoidable. For many businesses, the cost of downtime is measured in minutes rather than hours. The entire operation is paralyzed when systems are down, and the firm is unable to service clients, sell or create items, and so on. Downtime has a significant financial impact onbusinesses due to wasted opportunities, production constraints, and service disruptions, among other things. (Juul, n.d.)

- Data loss

Aside from the time it takes to recover data and the expense of downtime, a ransomware attack also poses the danger of losing some data entirely. Even if businesses can restore data from backups, there isa chance that not all files were properly or completely backed up. (Juul, n.d.)

- Collateral damages

When a firm is struck by malware, it must determine how the assault occurred. How did cyber-criminalsget their hands on a company's data? Is there any evidence of a data breach? A firm must ensure that the underlying reason for cyber-criminals is no longer feasible. However, there is still the danger that a business could have stolen some credentials, other security measures leaked, which would lead to the use of information during other forms of attack or a future malware assault, even after the issue is resolved and gates are shut down. Hackers interchange this type of information and interact in a sophisticated and well-organized manner. (Juul, n.d.)

- Brand name

Data can be recovered, but a tarnished reputation is difficult to repair. Although brand reputation is difficult to assess, a business may expect a negative impact on its brand following a ransomware attack, which will almost certainly result in financial losses. No matter how quickly and efficiently the ransomware situation was addressed, the harm to a company's brand is difficult to prevent. "The public"comprises "not just consumers, but also employees, investors, and other stakeholders," it's vital to remember. (Juul, n.d.)

- Labor cost

With the monetary cost of downtime, there is also the personal cost to consider. IT staff are unable to function within their normal scope while attempting to restore company servers. The same may be saidfor the majority of other personnel who rely on database access. As a result, there is a congestion of tasks across the business. Furthermore, extra specialist help or consultation may be required to tackle data issues prior, during, and after the downtime is resolved. (Juul, n.d.)

Some examples of true cost of malware for companies.

Ransomware Attack on Norsk Hydro 2019

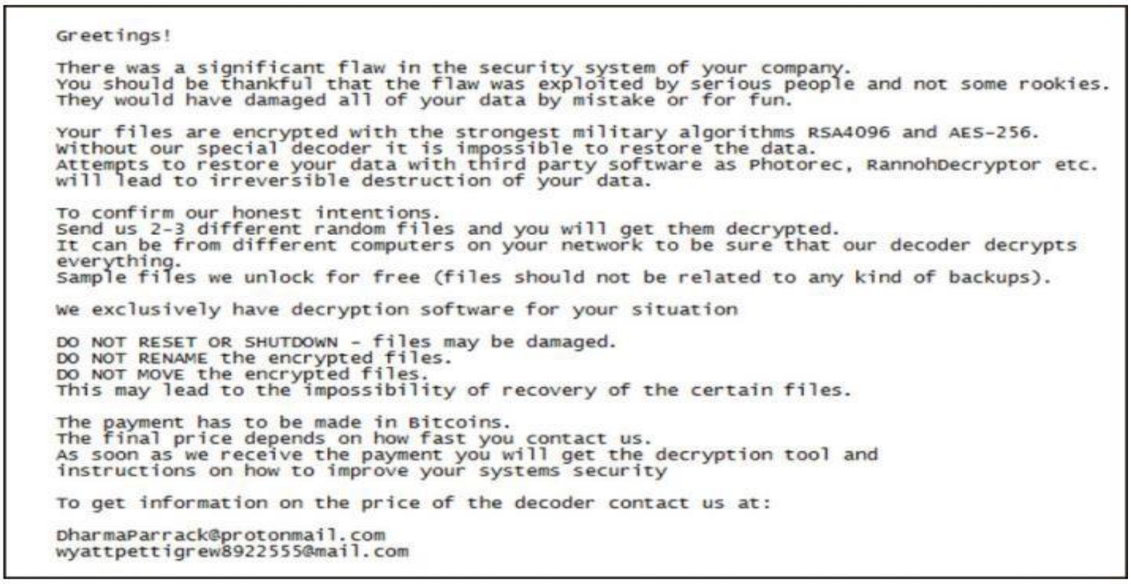
Norsk Hydro was the victim of a large-scale cyber-attack on March 19, 2019. (Ransomware attack). The attack impacted the whole worldwide company, with Extruded Solutions facing the most substantial operational and financial problems. (Cyber-attack on Hydro, 2020)

Norsk Hydro stated on Facebook that the malware that encrypts the data is a new variety known as LockerGoga. However, instead of paying the hackers the required ransom, the organization has decided to restore data using backups. LockerGoga is the malware that has been blamed for preventing access to data servers. (Goud, 2019)

The attack impacted directly all Norsk Hydro personnel in 40 countries worldwide, resulting inthe inaccessibility of files on thousands of servers and PCs. It cost Norsk hydro around $71 million. (Briggs, 2019)

Hackers gained access to Norsk Hydro using a spam email sent by a trusted customer that was unwittingly opened by an employee. The hacker was able to infiltrate IT infrastructure and secretly plant a virus as a result of that email. (Briggs, 2019)

Norsk Hydro was able to recover from the LockerGoga ransomware because they had a solid backup policy in place and had backed up everything. They simply recovered their data without having to pay any monetary compensation to the hackers.



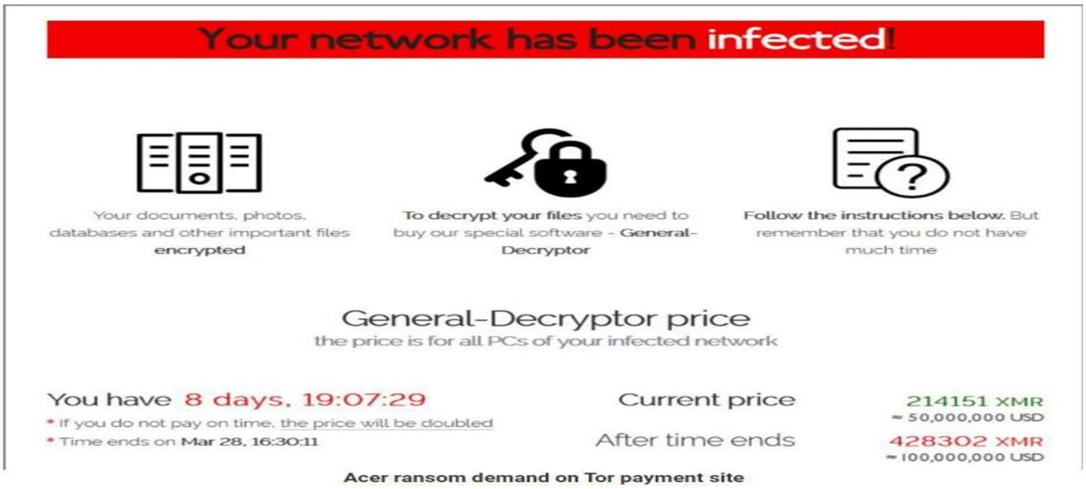
```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

FIGURE 8 (SECURITY, 2019)

Computer giant Acer ransomware Attack 2021

On March 18, 2021, A member of the ransomware cybergang REvil insinuated to have obtained sensitive data from Acer, a Taiwanese computer manufacturer, as well as an undisclosed range of encrypted devices, The data breach and ransomware assault have been linked to Microsoft Exchange flaws, according to security company Advanced

Intel. For the first time on March 5, 2021, Advanced Intel discovered that one of Acer's Ms Exchange servers had been compromised. REvil has requested a fifty-million-dollar payment in exchange for "a decryptor, abug report, and the deletion of stolen data." if the ransom is paid and that if it is not paid by the deadline, the ransom will double to $100 million. (Abrams, 2021)



Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 8 days, 19:07:29

* If you do not pay on time, the price will be doubled

* Time ends on **Mar 28, 16:30:11**

Current price 214151 XMR ≈ 50,000,000 USD

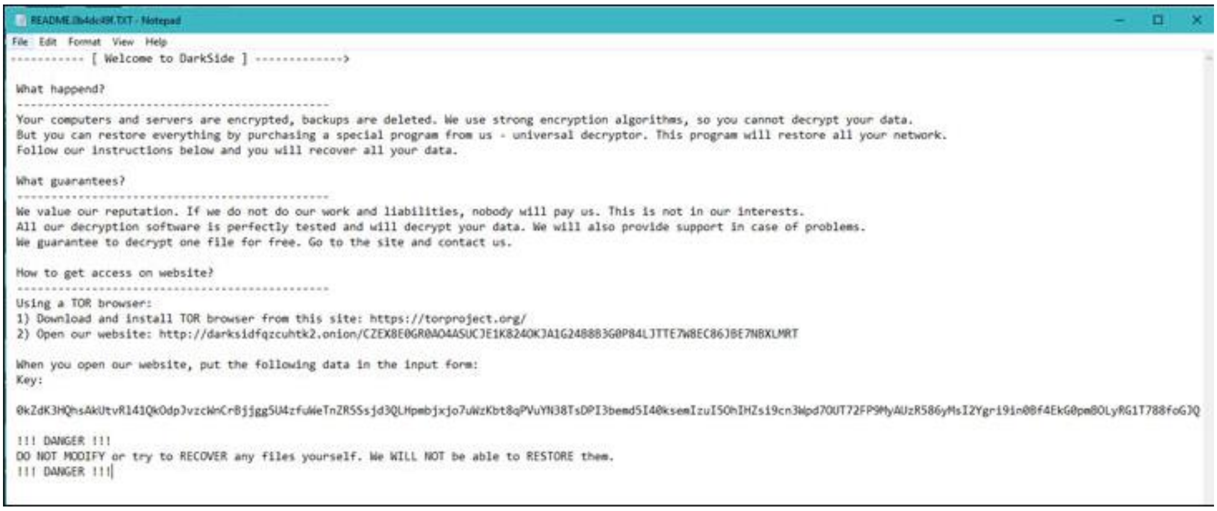
After time ends 428302 XMR ≈ 100,000,000 USD

Acer ransom demand on Tor payment site

FIGURE 9 RANSOMWARE NOTE (ABRAMS, 2021)

- Colonial Pipeline Ransomware Attack 2021

The Colonial pipeline is the largest refined product pipeline in the United States, a 5,500-mile (8,852 kilometers) infrastructure that delivers 100 million gallons of refined goods from Houston, Texas to New York Harbour got attacked by ransomware attack. (Lakshmanan, 2021) The Colonial Pipeline, according to Bloomberg, paid the demanded ransom (75 bitcoins, or roughly $5 million) within hours of the incident. Colonial Pipeline was subsequently provided a software application by the hacker to repair their network, however, it ran slowly. (Bloomberg,2021)



```
----------- [ Welcome to DarkSide ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

What guarantees?
----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
----------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion/CZEX8E0GR0AO4ASUCJE1K824OKJA1G24B8B3G0P84LJTTE7W8EC86JBE7NBXLMRT

When you open our website, put the following data in the input form:
Key:

0kZdK3HQhsAkUtvR141QkOdpJvzcWnCrBjjgg5U4zfuWeTnZR5Ssjd3QLHpmbjxjo7uWzKbt8qPVuYN38TsDPI3bemd5I40ksemIzuI5OhIHZsi9cn3Wpd7OUT72FP9MyAUzR586yMsI2Ygri9in0Bf4EkG0pm8OLyRG1T788foGJQ

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

FIGURE 10(LAKSHMANAN, 2021)

Norsk hydro didn't pay ransom money they had backup of everything but it still cost them about71 million dollars in recovery. Hackers got into Norsk Hydro by a spam mail that was unknowingly opened by an employee from a trusted customer. Acer got attacked by ransomware cybergang REvil with a ransom demand of about $50 million. Colonial Pipeline paid75 bitcoins ($5 million) to hacker group DarkSide just to save time and money. Financial losses with malware attacks can be so big that companies are forced to inforced top-notch security.

Many companies do have very high cyber security but they still get hacked with zero-dayvulnerabilities.

Businesses should consider all of these factors when assessing the potential risk posed by ransomware attacks: payout, downtime, reputational harm, data loss, and more. After considering all of these factors, it's an excellent suggestion to look for a reliable endpoint solution that can give maximum ransomware protection while also complementing it with suitable backup systems and business continuity measures. It's also a good idea to get some cyber insurance to help mitigate the danger even further.

• Impacts of malware attack on consumers

Despite the abundant evidence that malware may do significant harm to customers, estimating the losses caused by malware is considerably more difficult. Such charges are made up of several components. As a result of identity theft or other unlawful activities, they might inflict immediate hardware and software damage, as well as financial and other damages. Despite the fact that the range of estimates differs, the general picture that emerges is quite consistent. (ITU, 2008)

Despite the fact that cyber-attacks at any stage can be devastating, most people lack the necessary skills to rapidly recover from a cyber-attack. A company may be more secured and is highly unlikely to go bankrupt as a result of a single assault. (ecpi university, n.d.)

PC World found that the typical ransomware payment is $1,077. This might be a blip on a company's radar. Individuals may be forced to choose between losing the whole of their earning and become bankrupt. Sometimes malicious hackers aren't out to raise profits; instead, they want to cause mayhem. Because many programs and networks become linked, hackers will have a better chance than before infiltrating several account and causing chaos on someone's private affairs merely for fun. (ecpi university, n.d.)

Yahoo, the world's largest internet company, had 3 billion email accounts hacked in 2013. As a consequence, thieves got access to sensitive consumer information in the biggest data breach in history. (Vuleta, 2021)

• Killing the competition

Acquisitions by hostile forces are not a new occurrence. They're neither beautiful nor ethical, but they're perfectly legal. The CEOs of Apple, Facebook, Google, and Amazon testified before a legislative anti-trust committee in July 2020 to defend their companies' use of anti-competitive tactics to prevent a fair market from having too much market power. (R. Christos, 2020)

Both Compulife and NAAIP create life insurance premiums for insurance brokers, thus they are direct competitors in the business. NAAIP recruited a hacker to steal trade secrets from Compulife Software, according to a court decision in 2020. " They hired a hacker called Natal who, it is unquestionable, acquired Compulife's data that later they used in their own program, according to the court documents." Judge Hall said in his decision. (Sussman, 2020)

Today's hackers are made up of teams, groups, and nations, are both male and female, and are supported by companies, politicians, and governments. It is a massive industry worth billions of dollars every year. Groups are available for hiring for both ethical and unethical hacking. (R. Christos, 2020) Organizations with a lot of money don't only stay afloat, they also profit from other people's misfortunes. Less competition equals more business for them, and it's very probable that they take advantage of this chance right away. This is enough reason to hire a hacker or team of hackers to take down competition, In long run its more beneficial, no competition means monopoly for them.

It's the same with hacking for hire. According to Kaspersky Labs, a hacker may be hired for as low as $7 for five minutes and as much as $30 for a day to execute a DDoS assault. The cost each day might range from $400 to more than $400 depending on the goal and level of protection. When compared to the victim's costs, this is a drop in the bucket. (R. Christos, 2020)

Consider how much big retailers like Elkjøp, Komplett, Power, and netonnet lose if they refused service to customers on Black Friday. It's simple to understand how such an attack may help a rival.

- ## A response plan is alfa omega

When an organization's reputation, income, and customer trust are on the line, it's vital that security issues and events are detected and responded to quickly.

Organizations must have an incident response plan (IRP) in place, regardless of how big or little the breach is, to reduce the possibility of becoming a victim of the present cyber-attack. (cipher, n.d.)

A data breach costs an average of $3.92 million (USD) according to the Ponemon Institute and IBM's 2019 Cost of a Data Breach Report. A data breach in the health-care industry now costs an average of $6.45 million USD. (isacybersecurity, 2020)

As a result of IRPs, a company's budget can be significantly reduced. As per a 2017 IBM study, organizations can save up to $1 million if they are able to contain cyber events within 30 days. It also allows businesses to fix vulnerabilities before they become a serious problem. The reputation of a company can be preserved if a problem is quickly resolved. (RSI Security, 2019)

Another major impact is that consumers would transfer their business elsewhere if they were personally harmed by a data leak, according to IDC. If a security breach is not addressed promptly, the firm may lose some or all of its customers. Customers will lose trust in the company if they have a data leak. It should be obvious by now that it may be a PR disaster for businesses. (RSI Security, 2019)

If the reaction phase is effective, these costs can be significantly reduced. If a company's security is breached, they must act fast. How much income does a business lose per minute when its website is down?   What happens if a firm misses a deadline for filing, reporting, or submission? Having a tried and true plan for what to do in the case of a crisis may help reduce the quantity of data lost, the scope of the damage, and the recovery time.

In addition, the IRP can enhance a company's trust with stakeholders. The fact that you have a solid strategy in place instills more trust in investors, clients, and employees. En outre, limiting the impact of a breach can help reduce the harm to a company's reputation. It may make a huge difference to clients or business partners if you take a professional approach to dealing with an incident, even if the worst happens. It is much better to communicate calmly and clearly (to the extent possible) with your clients about a breach than to keep quiet in such a situation.

It doesn't matter if IRPs aren't used in reality. Creating a feedback loop via the design and testing of their IRPs has proven beneficial to many consumers. A company's cybersecurity architecture may have vulnerabilities that may be corrected before an actual breach happens if it creates and tests intrusion scenarios and tests them. Tests such as these verify that virtual server backups are working effectively, that offsite backups are readable and recoverable, as well as that contact and license information is up to date. (isacybersecurity, 2020)

This is only the beginning. IRPs and preparation assist instill a culture of cybersecurity awareness in an organization. Every employee should be concerned about cybersecurity, just as everyone should be concerned about health and safety. Individuals will also become more conscious of their everyday activities and be better equipped to recognize prospective or emerging risks when they are involved in the appropriate handling of an incident response plan. Similarly, plan testing has same impact. (isacybersecurity, 2020)

As part of their regulatory and compliance obligations, many organizations require its members to develop and test incident and breach response plans. In order to comply with PCI DSS requirements for accepting online payments, for example, firms must develop a strategy and test it. On the basis of the company's replies, most cyber insurance underwriting questionnaires will alter premiums or even deny coverage. In most cases, incident response plans are mandated by law. (isacybersecurity, 2020)

A good reponse plan should includes

Introduction	• What is the purpose of the response plan, what are the beginning rules, and how do you use it? • Outlines the contents and area of usage.
How to use the IRP	• Defining the various levels of incident response and escalation areas • Description of how to utilize the document in each step of the procedure
Event handling	• Event categories, classification rules, and proposed actions
Incident topology	• Lists the types of incidents • Data assets that have been impacted
War room and incident-response team	• A team in charge of incident response • Rights and duties of working groups that are part of the war-room
Response plan	• There are plans in place for each sort of incident. • strategies for each sort of information asset • Checklists of important procedures, activities, and alerts that should be initiated in the case of a cyberattack, organized by incident and asset type.
The post-incident protocol	• Procedures for post-incident learning and codification, as well as documentation: ✓ Keeping track of event information and responses ✓ collecting incident response lessons ✓ updating strategy to enhance future responses

TABLE 2(BAILEY, BRANDLEY AND KAPLAN, U.D.)

6. conclusion

Technology has advanced rapidly in the last few years. Which leads to possibilites of companies becoming more vulnerable. Its not strange that same thing has happened with hacking and cyber crimintality. It also increase in the same speed.

It has been discussed in detail what malware is, different types of malwares i.e viruses, worms, trojans. It more rewarding for criminals to steal on the internet compared to outdated stealing and robbing methods. Hackers doesn't need much to perfom a attack on any computer from anywhere in the world. Cyber security is still a young child its not fully developed and there are a lot of area that can be misused. Its has been discussed why malware is used in cyber attacks. Why criminals follow that path. What benefits they get. Cybercriminals may be at risk, but it's much easier to evade detection than to catch someone on the internet.

Cybercriminals have proven many times they can do anything from behind a computer screen. There has been mentioned few well known cases, norsk hydro got hacked, acer faced a data breach led to losing schematics of apple upcoming products, and a very famous oil suppling company "The Colonial pipeline " got hacked which led to many problems for company. The colonial pipeline choosed to pay 75bitcoin to a get universal enrcryptor from hackers. There are companies that have very good response plan and they tries not to motivate hackers to attack them again like Norskhydro, Norskhydro got hacked they didn't pay ransom money. Instead they restored their systems from backup, but it still costed them 71million dollar in recovery. The fact that malware programmers are creating increasingly complex software that may damage even the largest organizations with highly strict security measures is evident in recent attacks on many big companies.

Its clear that the cost of malware attacks is not limited to the immediate stop of business. A malware attack bears indirect cost for businesses like operating costs, loss of sales from downtime, and recovery solutions. A company might lose loyal clients' goodwill and confidence. In many cases consumers loses trust on companies. The consumers often think having data in a hacked company leads more problems for them. This leads to losing customers. Its much easier for a company to recover from data breach then a user(consumer). If a consumer loses his/her identity, it can be devistating for concering party. That one issue can cause a chain reaction that leads to bankruptcy.

The ligit businesses have also started hacking competitions to take upper hand in some cases and in other cases to lead small business to bankruptcy. This at the end benefits big businesses. No competition means monopoly in the market.

Advancement in technology led to many benefits for companies but it does also carry some problems. To deal with that part, companies do need a good response plan. A good response plan does explains what should a company do in case they get attacked. Employees will have a far better understanding of what to do in the event of an attack if they have a response plan. Consumers tend to have more faith in firms that have a response plan. Its clear that a good IRP carries many benefits for companies.

Businesses should consider all of these factors when assessing the potential risk posed by ransomware attacks: payout, downtime, reputational harm, data loss, and more. After considerig all of these factors, it's a good idea to look for a reliable endpoint solution that can give maximum ransomware protection while also complementing it with suitable backup systems and business continuity measures. It's also a good idea to get some cyber insurance to help mitigate the danger even further.

7. References:

- Docs.microsoft.com. 2021. Defining Malware: microsoft. [online] Available at: <https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN> [Accessed 5 May 2021].
- Csrc.nist.gov. 2021. malware - Glossary | CSRC. [online] Available at: <https://csrc.nist.gov/glossary/term/malware> [Accessed 5 May 2021].
- 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 5 May 2021].
- Networking Sphere. 2019. What Is Malware & How to Detect Malware?. [online] Available at: <https://www.networkingsphere.com/2019/08/What-is-malware.html> [Accessed 9 May 2021].

- Rosencrance, L., 2018. What is a rootkit? - Definition from WhatIs.com. [online] SearchSecurity. Available at: <https://searchsecurity.techtarget.com/definition/rootkit> [Accessed 9 May 2021].
- Blogs, M., 2021. How to remove malware from Windows (Virus Removal Guide). [online] MalwareTips Blogs. Available at: <https://malwaretips.com/blogs/malware-removal-guide-for-windows/> [Accessed 9 May 2021].
- Networkingsphere, 2019. What Is Malware & How to Detect Malware?. [online] Networking Sphere. Available at: <https://www.networkingsphere.com/2019/08/What-is-malware.html> [Accessed 9 May 2021].
- Goodrich, M. and Tamassia, R., 2014. Introduction to computer security. Harlow: Pearson, pp.173-220.
- Donovan, F., 2016. Top 5 Rootkit Threats and How to Root Them out. [online] eSecurityPlanet. Available at: <https://www.esecurityplanet.com/networks/rootkit-threats/#:~:text=These%20rootkits%20avoid%20detection%20by,Adore%2C%20Rkit%20and%20Da%20IOS.> [Accessed 9 May 2021].
- AVG signal team, 2020. Everything You Need to Know About Rootkits and How to Protect Yourself. [online] Everything You Need to Know About Rootkits and How to Protect Yourself. Available at: <https://www.avg.com/en/signal/what-is-rootkit#:~:text=A%20virtual%20machine%2Dbased%20rootkit,Round%20and%20round%20it%20goes.> [Accessed 9 May 2021].
- Norton security, 2019. What is a computer worm and how does it work?. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html> [Accessed 9 May 2021].
- Gatefy, 2021. 11 real and famous cases of malware attacks - Gatefy. [online] Gatefy. Available at: <https://gatefy.com/blog/real-and-famous-cases-malware-attacks/#:~:text=created%20in%202007.-,9.,and%20%E2%80%9CMail%20Delivery%20System%E2%80%9D.> [Accessed 9 May 2021].
- Catalogs.com staff, 2019. Top 10 worst computer viruses. [online] Lb.catalogs.com. Available at: <https://lb.catalogs.com/library/top-10-worst-computer-viruses/> [Accessed 9 May 2021].
- ENISA, n.d. [online] Enisa.europa.eu. Available at: <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware> [Accessed 9 May 2021].
- RFC 4949, 2007. [online] Rfc-editor.org. Available at: <https://www.rfc-editor.org/rfc/rfc4949.txt> [Accessed 9 May 2021].
- NortonLifeLock, 2019. What is spyware? And how to remove it. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html#:~:text=Spyware%20is%20unwanted%20software%20that,computer%2C%20often%20without%20your%20knowledge.> [Accessed 12 May 2021].
- Managed Solution, 2020. The Common Types of Spyware & How to Detect Them. [online] Managed Solution. Available at: <https://www.managedsolution.com/4-common-types-of-spyware-and-how-to-detect-them/> [Accessed 12 May 2021].
- Cisa.gov. n.d. Ransomware | CISA. [online] Available at: <https://www.cisa.gov/ransomware> [Accessed 12 May 2021].
- Enisa, n.d. [online] Enisa.europa.eu. Available at: <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware> [Accessed 12 May 2021].
- Csrc.nist.gov. n.d. logic bomb - Glossary | CSRC. [online] Available at: <https://csrc.nist.gov/glossary/term/logic_bomb> [Accessed 12 May 2021].
- Enisa, n.d. Botnets. [online] Enisa.europa.eu. Available at: <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets> [Accessed 12 May 2021].
- What Is a Logic Bomb? How to Prevent Logic Bomb Attacks. n.d. Logic Bomb | Avast. [online] Available at: <https://www.avast.com/c-what-is-a-logic-bomb> [Accessed 12 May 2021].
- Goodrich, M. and Tamassia, R., 2014. *Introduction to computer security*. Harlow: Pearson, pp.173-220.
- TechTarget Contributor, n.d. What is RAT (remote access Trojan)? - Definition from WhatIs.com. [online] SearchSecurity. Available at: <https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan#:~:text=A%20remote%20access%20Trojan%20(RAT,sent%20as%20an%20email%20attac

hment.&text=Monitoring%20user%20behavior%20through%20keyloggers%20or%20other%20spyware.> [Accessed 19 May 2021].

- Nahorney, B., 2019. Remote Access Trojans - Cisco Blogs. [online] Cisco Blogs. Available at: <https://blogs.cisco.com/security/remote-access-trojans> [Accessed 19 May 2021].
- White Ops, 2018. White Ops | 9 of History's Notable Botnet attacks. [online] Humansecurity.com. Available at: <https://www.humansecurity.com/blog/9-of-the-most-notable-botnets> [Accessed 19 May 2021].
- Fitzsimmons, S., 2021. Biggest Cyber Attacks of 2020. [online] Blog.tbicom.com. Available at: <https://blog.tbicom.com/biggest-cyber-attacks-of-2020> [Accessed 5 May 2021].
- Mehrotra, K., 2021. Bloomberg - Are you a robot?. [online] Bloomberg.com. Available at: <https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta> [Accessed 5 May 2021].
- Briggs, B., 2019. Hackers hit Norsk Hydro with ransomware.. [online] Transform. Available at: <https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/> [Accessed 9 May 2021].
- Abrams, L., 2021. Computer giant Acer hit by $50 million ransomware attack. [online] BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/> [Accessed 20 May 2021].
- Lakshmanan, R., 2021. Ransomware Cyber Attack Forced the Largest U.S. Fuel Pipeline to Shut Down. [online] The Hacker News. Available at: <https://thehackernews.com/2021/05/ransomware-cyber-attack-forced-largest.html> [Accessed 20 May 2021].
- bloomberg, 2021. Bloomberg - Are you a robot?. [online] Bloomberg.com. Available at: <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom> [Accessed 20 May 2021].
- Abrams, L., 2021. Computer giant Acer hit by $50 million ransomware attack. [online] BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/> [Accessed 20 May 2021].
- Professional cyber risk management combined with insurance. n.d. Why cybercriminals love malware. [online] Available at: <https://www.amplifyintelligence.com/malware/> [Accessed 20 May 2021].
- zvelo. 2020. Ransomware-as-a-Service (RaaS) | The Business of Ransomware. [online] Available at: <https://zvelo.com/raas-RAAS/> [Accessed 20 May 2021].
- sophos, n.d. *The Money Behind the Malware*. [online] Sophos. Available at: <https://www.sophos.com/en-us/security-news-trends/security-trends/money-behind-malware-threats.aspx#:~:text=Pay%2Dper%2Dclick%20fraud%3A,traffic%20to%20their%20customers'%20ads.> [Accessed 20 June 2021].
- Laing, B., 2018. *Malware-as-a-Service: The 9-to-5 of Organized Cybercrime*. [online] Lastline. Available at: <https://www.lastline.com/blog/malware-as-a-service-the-9-to-5-of-organized-cybercrime/> [Accessed 20 June 2021].
- Kaspersky, n.d. *Who Creates Malware?*. [online] www.kaspersky.com. Available at: <https://www.kaspersky.com/resource-center/threats/who-creates-malware> [Accessed 21 June 2021].
- Palmer, D., 2016. *Criminals in the cloud: How malware-as-a-service is becoming the tool of choice for crooks | ZDNet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/criminals-in-the-cloud-how-malware-as-a-service-is-becoming-the-tool-of-choice-for-crooks/> [Accessed 21 June 2021].
- Laing, B., 2018. *Malware-as-a-Service: The 9-to-5 of Organized Cybercrime*. [online] Lastline. Available at: <https://www.lastline.com/blog/malware-as-a-service-the-9-to-5-of-organized-cybercrime/> [Accessed 21 June 2021].
- sitelock, 2017. The Ballooning Cost of Cybercrime. [online] The SiteLock Blog. Available at: <https://www.sitelock.com/blog/the-ballooning-cost-of-cybercrime/> [Accessed 28 June 2021].
- Cook, S., 2021. Malware statistics and facts for 2021. [online] Comparitech.com. Available at: <https://www.comparitech.com/antivirus/malware-statistics-facts/> [Accessed 25 June 2021].
- ITU, 2008. ITU Study on the Financial Aspects of Network Security: Malware and spam. [online]

Itu.int. Available at: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financialaspects-of-malware-and-spam.pdf> [Accessed 30 June 2021]

- ecpi university, n.d. How Cyber Attacks Affect Individuals and How You can Help Keep them Safe. [online] Ecpi.edu. Available at: <https://www.ecpi.edu/blog/how-cyber-attacks-affect-individuals-and-how-you-can-help-keep-them-safe> [Accessed 3 August 2021].
- Vuleta, B., 2021. *44 Must-Know Malware Statistics to Take Seriously in 2021*. [online] Legaljobs.io. Available at: <https://legaljobs.io/blog/malware-statistics/> [Accessed 3 August 2021].
- R. Christos, K., 2020. *Big Business Hired Hackers to Destroy Competition: Is Your SMB At Risk?*. [online] Linkedin.com. Available at: <https://www.linkedin.com/pulse/big-business-hired-hackers-destroy-competition-your-smb-kim-christos/> [Accessed 3 August 2021].
- Sussman, B., 2020. *Company Hires Hacker for Corporate Espionage*. [online] Secureworld.io. Available at: <https://www.secureworld.io/industry-news/company-hires-a-hacker-for-corporate-espionage> [Accessed 3 August 2021].
- cipher, n.d. 3 Reasons Why You Need an Incident Response Plan - Cipher. [online] Cipher. Available at: <https://cipher.com/blog/3-reasons-why-you-need-an-incident-response-plan/#:~:text=A%20thorough%20incident%20response%20process,a%20potential%20loss%20of%20revenue.&text=The%20faster%20your%20organization%20can,a%20potential%20loss%20in%20revenue.> [Accessed 4 August 2021].
- RSI Security, 2019. *The Importance of an Incident Response Plan | RSI Security*. [online] RSI Security. Available at: <https://blog.rsisecurity.com/the-importance-of-an-incident-response-plan/> [Accessed 5 August 2021].
- isacybersecurity, 2020. *Why You Need an Incident Response Plan*. [online] isacybersecurity. Available at: <https://www.isacybersecurity.com/why-you-need-an-incident-response-plan/> [Accessed 5 August 2021].
- Bailey, T., Brandley, J. and Kaplan, J., n.d. How good is your cyberincident-response plan?. [online] https://www.mckinsey.com/. Available at: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-good-is-your-cyberincident-response-plan> [Accessed 6 August 2021].