Ransom Virus

Information Security Project

By : Fatima Riyadh

The supervisor : Dr Rajaa

2021/12/19

Definition of

Injury

Types of viruses

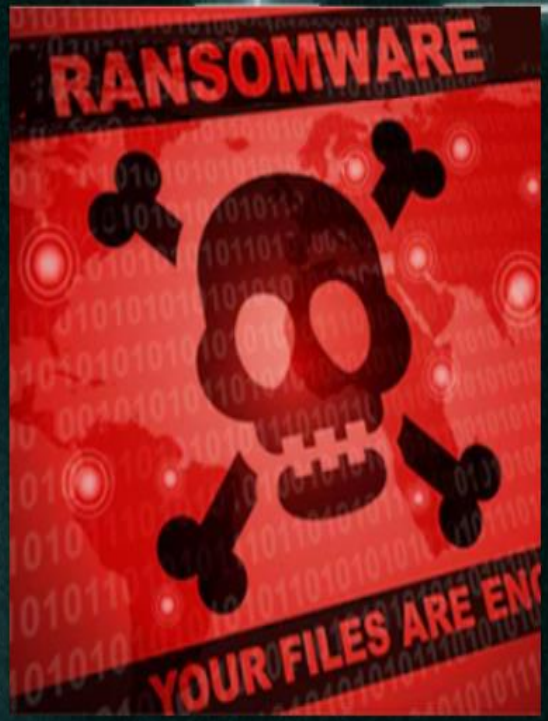
recovery

Protection

Examples

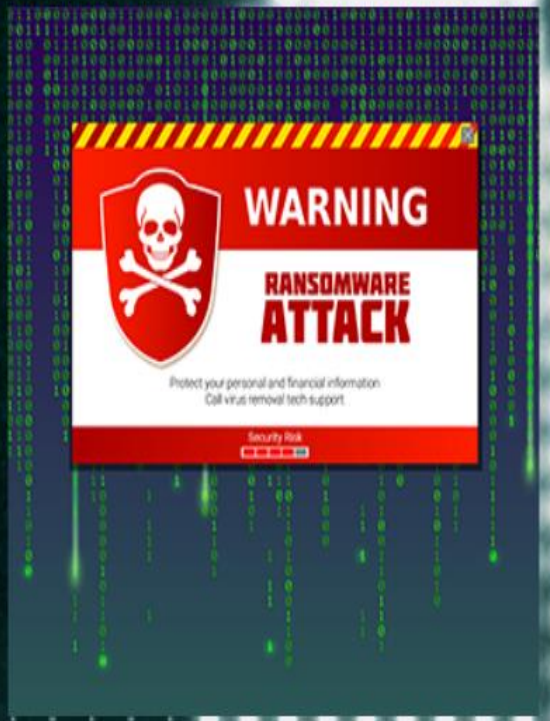
Virus Definition

It is a type of virus that infects the computer and encrypts all computer data and prevents the user from accessing it and shows a message asking the user to pay an amount of money and the payment is mostly in digital currencies so that it is not tracked. This type of virus began to appear in the early eighties in Russia specifically And soon it spread all over the world and infects all devices, even mobile phones



virus Infection

One of the most common ways that devices are infected is by sending an e-mail known as social engineering messages that delude the victim that it is a message from the authorities to investigate or a message from someone he knows contains a link, PDF, Word file, or image containing viruses. Once the file is opened, viruses will enter the device and encrypt the data and show a message asking the user to pay the ransom within a specified time.



Types of viruses

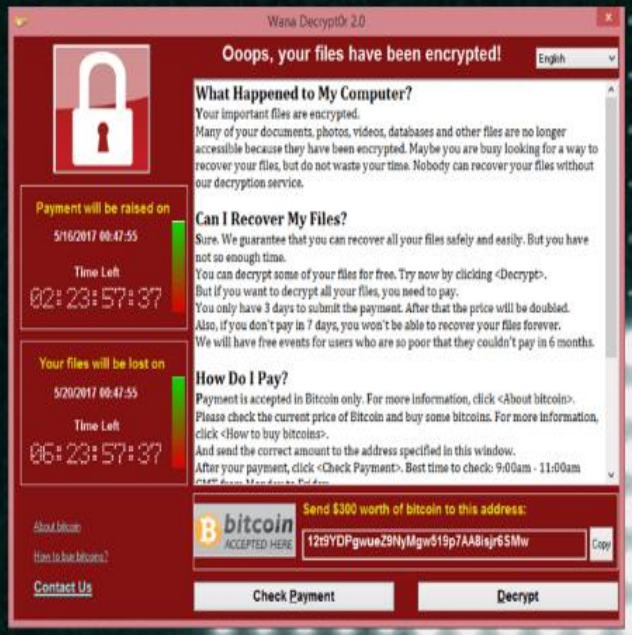
1-Jigsaw: is a particularly dangerous ransomware. It encrypts your files and then starts deleting them systematically until the ransom is paid. It will delete one or more files every hour for 72 hours. Once 72 hours have passed, all files that have been encrypted will be deleted.

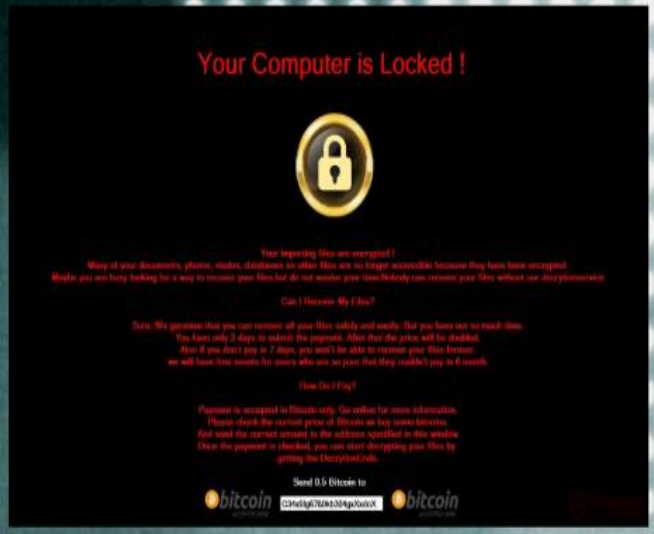
2-Scareware : It is also a disguised virus, as it reaches your device in the form of an anti-virus program or cleans the device, claiming that there are some risks that threaten the device and then starts asking for money in exchange for solving it, and its damages range from the appearance of a large number of annoying messages to the complete shutdown of the device in exchange for payment ransom

3-Doxware :This type of virus uses a different method for obtaining the ransom, whereby the user threatens to publish his stolen data online in case of non-payment, which of course includes photos, sensitive data and various media.

4-WinLocker :This type of virus does not encrypt files, but rather blocks access to the infected device from the ground up and paralyzes the entire system, and when the device is opened, a message appears only asking the victim to pay the amount.

5-Mac Ransomware :This type of virus targets devices that use the Mac operating system and began spreading in 2016, also known as KeRanger, and it may infect the device in several forms and through different applications





Recovery

1- it is very important not to obey the victim and pay the ransom, because this will lead to re-exploitation in the future, or perhaps the attacker will not crack the codes.

2- Download any anti-virus program that will delete the virus from the device, but in this case the files will remain encrypted and can be decrypted through the nomoreransom website, by placing one of the encrypted files, and it will search for the type of encryption with which the data was encrypted and decrypt it.

4- It is possible that this program does not contain the encryption key with which your data was encrypted. In this case, what you have to do is format the computer, but this will delete your files completely

5- It is possible to communicate with a security expert in order to try to decrypt the code, as it is possible that the malware programmer has made a mistake, and there is a gap that enables him to find the key and thus decryption.

Virus protection

1- Always update the operating system
2 -Do not download any files from suspicious websites
3 -Do not open any message from unknown mail
4 -Not to publish personal, computer or network information on websites
5 -Make sure to change the password periodically, and it must be a strong password
6 -Always make backup copies of important files
7 -Close computer programs that we don't need
8 -If it is necessary to open the links, they can be opened by opening an emulator for the operating system provided by Teachradar, which provides an emulator for the operating system. We can open the sent link and once the emulator is closed, the link will also be closed
9-Some companies whose employees work remotely using the VPN system so that employees can enter the company's system and also will prevent any unauthorized entry from outside the company, such as Earthlink company.

Stories

1- Ransomware attack on Communications & Power Industries
It was revealed in March that California-based CPI, a major electronics manufacturer, had been attacked by a ransomware.
The company manufactures components for military hardware and equipment, and the US Department of Defense is among its customers. The ransomware attack occurred when a domain administrator at the company opened a malicious link that triggered file-encrypting malware. Since thousands of computers on the network were on that same undivided domain, this ransomware quickly spread to every office in the company, even to backups on the corporate headquarters!
The company reportedly paid $500,000 in response to this attack, and the type of ransomware used in the attack is unknown
2. Manchester United Football Club made headlines when it was revealed that it had been exposed to a cyber attack, which the club then confirmed was a ransomware attack, and the club revealed that although the attack was of a complex level, they had comprehensive protocols and procedures in place for such events. , meaning that they were prepared and able to maintain their cyber defenses that identified the attack and shut down the affected systems to contain the damage and protect the data

3- In the United Kingdom, a medical center was attacked. That medical center was conducting early medical experiments on drugs and vaccines, and after the center refused to pay the ransom, the group published the personal data of thousands of former patients, and the media quoted the director of the center, "Malcolm Boyce" as saying that he preferred to leave work to pay the ransom.
4- Michigan State University was infected with ransomware The attackers stated in their demands that the university has one week to pay the ransom in exchange for decrypting the encrypted files, otherwise the attackers will leak personal and banking data of the group's students on the dark web. The university chose not to acquiesce and pay the ransom, and they said they made this decision on the advice of a large law firm