

Ransomware

A BRIEF DEFINITION
FRAZER GRAHAM

Table of Contents

Introduction:	2
What is Ransomware?	2
How does Ransomware operate?	3
Payment:	3
What can be done to prevent Ransomware?	3
Case Study:	4
Conclusion:	5
Bibliography	6

Introduction:

This document should give the reader a basic understanding of the following: what Ransomware is, how it operates, and what can be done if your PC (Personal Computer) is infected by Ransomware.

In addition, some additional principles will be highlighted such as encryption, how an attack is executed, and the potential damage ransomware can cause if successful.

What is Ransomware?

Ransomware defined by the Oxford dictionary is, "A type of malicious software designed to block access to a computer system until a sum of money is paid." [1]

From the above, this means that ransomware is code with malicious intent in order to extort money from the victim. This can be done by preventing the user from accessing their files. One method used to prevent the user accessing their files is encryption.

Encryption defined by the Oxford dictionary is, "Convert information or data into a code, especially to prevent unauthorized access." [2]

This means documents, media files, and other applications would be encrypted by the malware. This would then prevent authorisation/access to these files by the user. These files can be accessed if the key which encrypted the files can be obtained. This would allow the decryption of these files. However, this would require payment as per the examples below.



Figure no.1 [3]

How does Ransomware operate?

Ransomware requires the use of voluntary action by the user. This could be in the forms of downloading documents over the internet. Opening a link from a suspect email. Running programs sent over the internet.

Once installed on the PC, the malware goes into a term known as hibernation. In which, the malware will not reveal itself to the user. This will then make it more difficult for the user to determine when and where they have picked up the malware. [3]

Once shown, ransomware can be of two types. One in which the virus will encrypt the user's files. Another, type is a screen lock. This would then prevent the user from accessing any files or using the computer at all.

Some ransomware programs have been designed to search local area networks. This is to find all possible back-ups of a file. By encrypting all copies of files and backups this would then force the user into paying the fee for those documents. [9]

Payment:

It is advised to avoid paying the malware the payment fee to unlock your files/screen. This is because there is no guarantee that those who created the virus will send the decryption key. [4]

This means, despite paying the ransom the files will remain encrypted. Therefore, you would still have no access to the files but the people who created the files would still have your money.

What can be done to prevent Ransomware?

There are several techniques that can be used to prevent Ransomware. One of which is education. This is to train staff within the company to prevent them from opening random attachments within emails or prevent them from downloading documents from the internet. This would then prevent malware from infecting the PC.

Another technique is to use an anti-virus. This would then flag the malware and will give an opportunity to remove the malware before it activates.

Within industry, admin access should only be granted to those who require it for their role. This would then prevent unnecessary downloading of documents. This again prevents the possibility of a PC becoming infected from malware.

Keeping the IT up to date. This is to ensure that no bug within the code can be exploited. By keeping up to date this prevents the attackers using known exploitations within the previous code. This could then make it more challenging for the malware to infect the PC.

Finally, by using a suitable backup method. This could be in the form of using cloud-based files and using external hard drives that are not connected to the network. It is important that the hard drives are not connected as this reduces the chances of the malware spreading to all the files. However, this is not guaranteed.

For example, during a periodic back up process you could transfer the malware to the hard drives. This would then infect the files on those hard drives thus infecting the backup files. [9]

Case Study:

On 20th May 2017, the NHS was subject to a ransomware in which costed them £92 Million. [5] This is due to 19000 appointments to be cancelled, with a further £72 Million being spent on IT repairs.

This shows that large businesses and infrastructure can also be infected. Therefore, it is important to know the possible effects of malware.

Some key names linked to ransomware are Cryptolocker and PETYA:



Fig no.2 [6]



Fig no.3 [7]

Cryptowall:

Cryptowall is another form of malware which encrypts data.

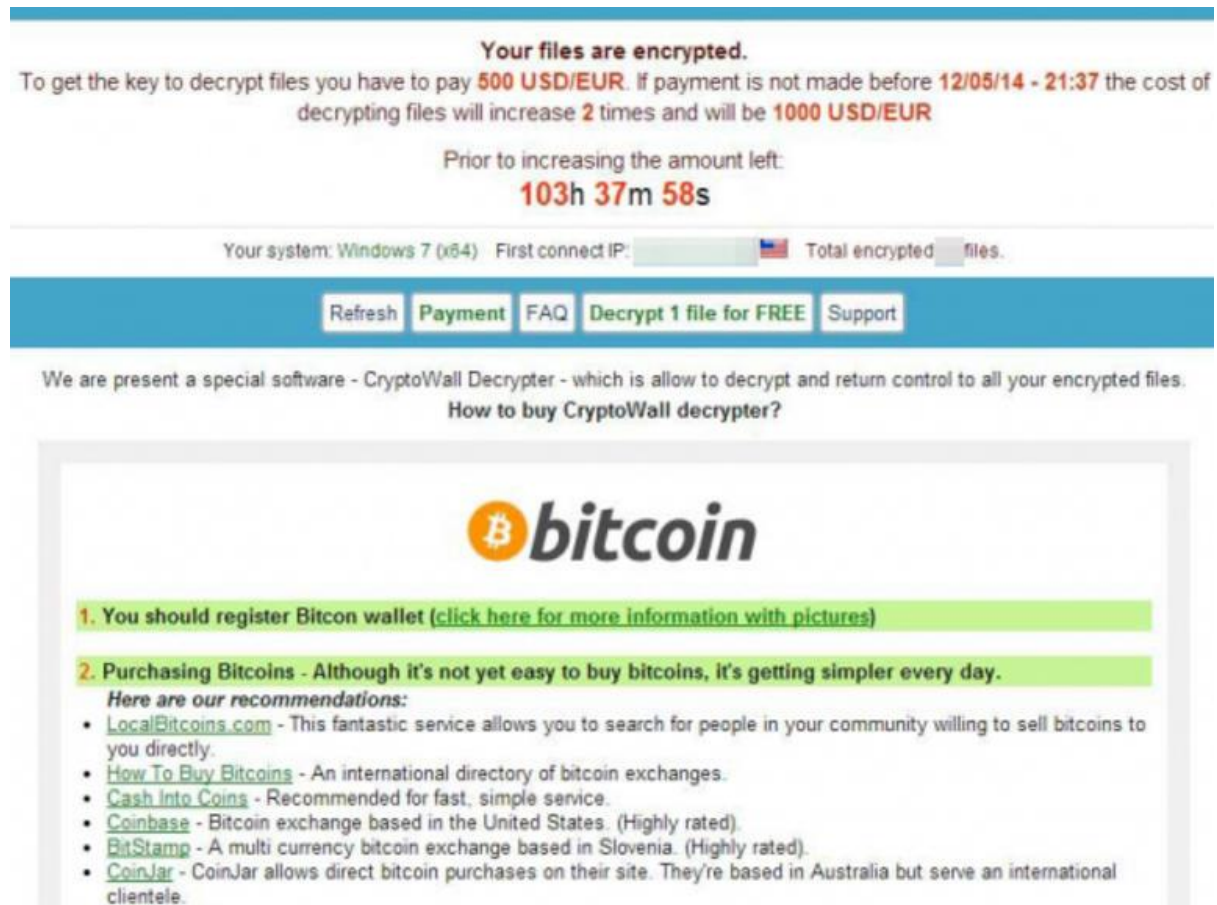


Fig no.4 [8]

Suppose that a suspicious email was received and opened by an employee. This could lead to the installation of Cryptowall. This malware would then disguise itself with the Operating System (OS) such as Windows [8].

It starts to infect the computer by making copies of the original files within the PC. This includes all other computers that are on the same network in addition to any cloud-based servers and backup hard drives. The malware would then encrypt each copy of file, before finally deleting the original and leaving the encrypted file in its place. [8]

When you attempt to open your files a notification such as Fig No.4 will appear. This would then be demanding ransom for your files. In return, the program will hopefully decrypt your files. Payment is a risky business, as it is not guaranteed that if you pay the ransom you will receive the files back.

Overall, it is important to implement security measure to prevent malware from infecting networks you install. This could be by using suitable back-ups. Using firewalls or only allowing specific employees with to have access to downloading files. Finally, another method is to educate the threat such as Ransomware to make people aware of the threats from the internet.

Conclusion:

Ransomware is a dangerous virus; however, steps can be taken to prevent the virus. These actions could be as simple as checking the content being downloaded/opened, keeping software up to date, and having a sufficient anti-virus.

If the PC is infected by ransomware the PC may be either screen locked. In which the user cannot do anything, or the files may be encrypted. Either method would require some payment in order to unlock the PC.

Payment could be considered to unlock the infected files. However, it should be noted that the receiver of the payment does not need to give you the key.

References

- [1] "Lexico," [Online]. Available: <https://www.lexico.com/en/definition/ransomware>. [Accessed 14 11 2019].
- [2] "Lexico," [Online]. Available: <https://www.lexico.com/en/definition/encrypt>. [Accessed 14 11 2019].
- [3] "G DATA," [Online]. Available: <https://www.gdatasoftware.com/guidebook/what-actually-is-ransomware>. [Accessed 14 11 2019].
- [4] "frsecure," [Online]. Available: <https://frsecure.com/blog/why-you-shouldnt-pay-ransomware-attackers/>. [Accessed 15 11 2019].
- [5] C. Graham, "The Telegraph," 20 5 2017. [Online]. Available: <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>. [Accessed 14 11 2019].
- [6] "Bleeping Computer," [Online]. Available: <https://www.bleepingcomputer.com/virus-removal/locker-ransomware-information>. [Accessed 15 11 2019].
- [7] "MalwareBytes," [Online]. Available: <https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/>. [Accessed 15 11 2019].
- [8] Vigo Jesus [Online]. Available: <https://www.techrepublic.com/article/cryptowall-what-it-is-and-how-to-protect-your-systems/> [Accessed 24 11 2019]
- [9] D. Winder, "Ransomware," *PC Pro*, pp. 107, 2016. Available: <https://search.proquest.com/docview/1797553615?accountid=130472>.