

An Evaluation on Ransomware Prevention Methods and Techniques

Assessing the previous and current methods used to prevent ransomware. What is working and what isn't. Demonstrating how ransomware has bypassed these prevention methods.

Patrick Collins

CMP320: Ethical Hacking 3

BSc (Hons) Ethical Hacking

2021/22

Abstract

Ransomware is a type of malware that's aim is to extort money from the victim. This extortion is done by either encrypting important and personal data on a computer system or locking the user out of their system and then demanding payment for the restoration. If the ransom is not paid in time either the encrypted data gets deleted permanently or uploaded online publicly for all to view. The main aim of this evaluation is to give the reader a clear understanding of the threat ransomware poses and the steps being taken to mitigate it.

The researcher used malware analysis environments with Windows Operating Systems XP SP3 and 10 Home and a live ransomware sample (WannaCry) to test these prevention methods and techniques using anti-ransomware software such as Windows Security. The researcher successfully demonstrated the prevention methods created against ransomware and how effective they are today. All aims of the evaluation were met demonstrating that we are moving in the right direction to combat this type of malware.

If the researcher were to continue the evaluation, he would test prevention methods against locker ransomware such as Reveton, as only crypto ransomware was researched in this evaluation, conduct an in-depth analysis on how ransomware spreads between systems and set up a home network environment to analyse the anti-ransomware software. Finally, as only the Windows Operating System was researched in this evaluation it would be beneficial to check the prevention methods and techniques in Linux-based Operating Systems.

Contents

1	Introduction	1
1.1	Ransomware 101	1
1.2	Types of Ransomware	2
1.3	Aims.....	2
2	Methodology.....	3
3	Research.....	4
3.1	The first ransomware attack	4
3.2	Notable Ransomware & Attacks	4
3.2.1	Locky	4
3.2.2	WannaCry.....	5
3.2.3	Conti.....	5
3.2.4	Reveton	6
3.3	Prevention methods and techniques.....	6
3.3.1	Backup.....	6
3.3.2	Software updates and patches	6
3.3.3	Securing email communications	6
3.3.4	Not paying the ransom	7
3.3.5	Anti-Ransomware software.	7
3.3.6	Online decryption tools.....	7
4	Procedure and Results	8
4.1	Overview of Procedure	8
4.2	Windows XP SP3 Environment.....	8
4.2.1	Without Protection	8
4.2.2	With protection.....	11
4.3	Windows 10 Home Environment.....	12
4.3.1	Without Protection	12
4.3.2	With Protection.....	14
5	Discussion.....	18
5.1	Direction Ransomware Is Going In.....	18
5.2	General Discussion.....	18
5.3	Countermeasures To Ransomware.....	19

5.4	Future Work	20
	References	21
	Appendices.....	24
	Appendix A – Windows XP SP3	24
	Appendix B – Windows 10 Home.....	25
	Appendix C – WannaCry Demonstration	27

1 INTRODUCTION

1.1 RANSOMWARE 101

Ransomware is a type of malware that's aim is to extort money from the victim. This extortion is done by either encrypting important and personal data on a computer system or locking the user out of their system. The cryptographic algorithms to encrypt the data is usually a combination of RSA (Rivest–Shamir–Adleman) and AES (Advanced Encryption Standard).

Ransomware using RSA encrypts the data with a public key and ransom a private key which decrypts the data (R.L. Rivest, 1978). To decrypt this data without a key would take an impossible amount of time. Due to how long it would take to decrypt the data, it is a bulletproof method to extort money out of the victim. To get the data back requires the victim to pay, with the attacker's payment choice usually being cryptocurrency bitcoin. This method of payment is used to try and hide the identity of the attacker holding their data for ransom which makes it difficult to track down exactly who is behind the attack.

This type of malware isn't kind to who gets targeted either. It could range from a regular computer user to a major corporation. Even worse, critical infrastructure has fell victim before. The colonial pipeline in the U.S, which is a major oil supplier, was targeted with a ransomware attack on May 7th, 2020, by Darkside Ransomware which crippled the fuel supply nationwide. The company decided to pay a massive 75 bitcoin (which is equivalent to \$5 Million (Wilkie, 2021)) ransom in order to restore their infrastructure and provide fuel back to millions of Americans (Kerner, 2022). Amazingly, U.S law enforcement were able to recover \$2.3 Million from the bitcoin payment (Wilkie & Macias, 2021). Hospitals are also a heavily affected area from ransomware. In 2017 the NHS in the U.K fell victim to the WannaCry ransomware which crippled the health service nationwide (BBC News, 2017; BBC News, 2017).

Most ransomware has a deadline to pay. If the ransom is not paid within this time either the encrypted data gets deleted permanently or uploaded online publicly for all to view. This can be a deadly situation for an organisation if their customer data is up for ransom. However, there is no guarantee that the attackers will decrypt the data once the ransom is paid.

Figure 1 on the next page is a bar graph showing the annual number of ransomware attacks worldwide from 2016 to 2020 (Johnson, 2021). It's clear from this graph that ransomware is still a prominent threat to this day and attacks are only increasing exponentially.

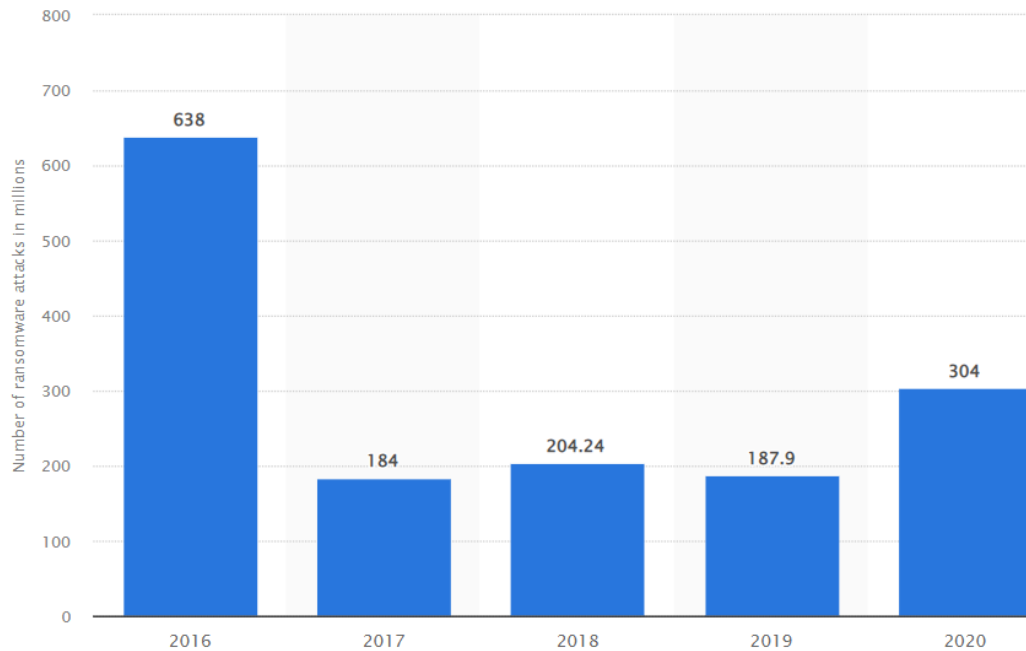


Figure 1: Johnson, J 2021, Number of ransomware attacks per year 2016-2020.

1.2 TYPES OF RANSOMWARE

As mentioned previously there are two main types of ransomware. They are:

- **Crypto Ransomware** – Encrypts important data with a cryptographic algorithm and ransoms the key/tool to decrypt the data. Payment is asked by attackers in Bitcoin (WannaCry), MoneyPak (Reveton), PaySafeCard, Ukash or even a prepaid card (Baker, 2022).
- **Locker Ransomware** – Entirely locks the user out of their machine with a pop-up screen and peripherals no longer work. Files and applications become inaccessible until the ransom is displayed, with a countdown timer to pay (Baker, 2022). As the aim is just to block access to the machine, data will most likely not be encrypted.

1.3 AIMS

The main aim of this evaluation is to give the reader a clear understanding of the threat ransomware poses and the steps being taken to mitigate it. The researcher hopes to achieve this by following several sub aims:

- demonstrating ransomware previously used in attacks.
- demonstrate previous attempts to prevent ransomware in old Operating Systems.
- demonstrate current ransomware prevention methods in modern Operating Systems.

2 METHODOLOGY

The tools and software the researcher will use for the evaluation is as follows.

Table 1 - Malware Analysis Environments

Operating System	Version	Reasoning
Microsoft Windows XP VM	Windows XP SP3	Simulate the security of a very outdated operating system still mostly used to this day against a ransomware attack. Updating to latest version to patch the exploit “EternalBlue” to see if it helps secure the operating system. (Microsoft, n.d.)
Microsoft Windows 10 Home VM	10.0.19042 Build 19042	Simulate up to date prevention measures implemented into modern operating systems.

Table 2 - Ransomware Sample

Ransomware	File Name	Reasoning
WannaCry	Ransomware.WannaCry.zip	WannaCry will be the live ransomware sample used in the evaluation - Obtained from TheZoo (tisf, 2021).

Table 3 - Anti-Ransomware Software

Software	Reasoning	Reference
ZoneAlarm – trial version	Test the prevention methods against crypto ransomware in modern operating systems (WannaCry).	(ZoneAlarm, 2022)
Microsoft Defender/Security	Test the improvements from windows XP to Windows 10/11.	(denisebmsft, chrisda, v-mathavale, RatulaC, & Ashok-Lobo, 2022)
Windows XP Security Update (KB4012598)	To test if the update released to Windows XP is sufficient to prevent the ransomware attack.	(Microsoft, 2017) (Heath, 2017)

3 RESEARCH

3.1 THE FIRST RANSOMWARE ATTACK

The first case of ransomware occurred back in 1989 with the AIDS Trojan (see figure 2). This was a malicious software which was spread through floppy disks. Once inserted into the computer, it would lay dormant until the user turned on the computer for the 90th time. Upon booting up the system for the 90th time the malware encrypted system files and displayed a ransom note demanding payment to unlock them (Waddell, 2016).

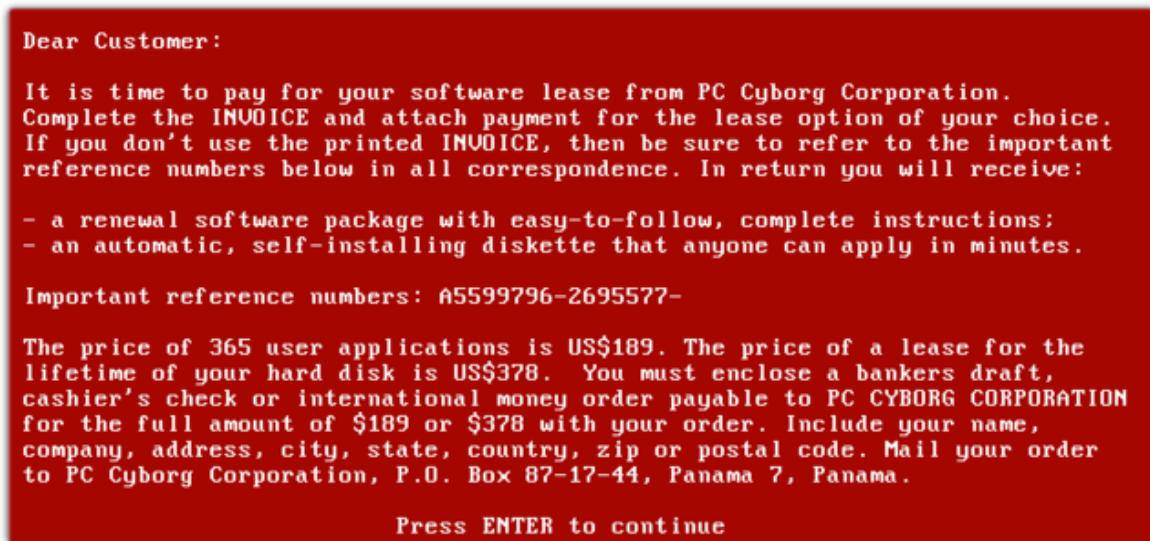


Figure 2: By Joseph L. Popp, AIDS Information Trojan author (Popp 2019).

This is how ransomware still operates today. Encrypting files, displaying a ransom note and demanding a payment. The method of ransomware hasn't really changed over the decades but is still a major threat even today.

3.2 NOTABLE RANSOMWARE & ATTACKS

3.2.1 Locky

This type of crypto ransomware is spread through email communications and social engineering methods like phishing. Important files are encrypted and a ransom screen asking for payment to decrypt is displayed (see figure 3). Locky first appeared in 2016 and spread to many parts of the world in North America, Europe, and Asia (Avast n.d). A hospital in Los Angeles fell victim to this ransomware and paid out \$17,000 to get their systems restored. Despite law enforcement helping with the attack the hospital chose to pay as it would have been the fastest way to recover from the attack and restore their critical infrastructure (Brewster 2016).

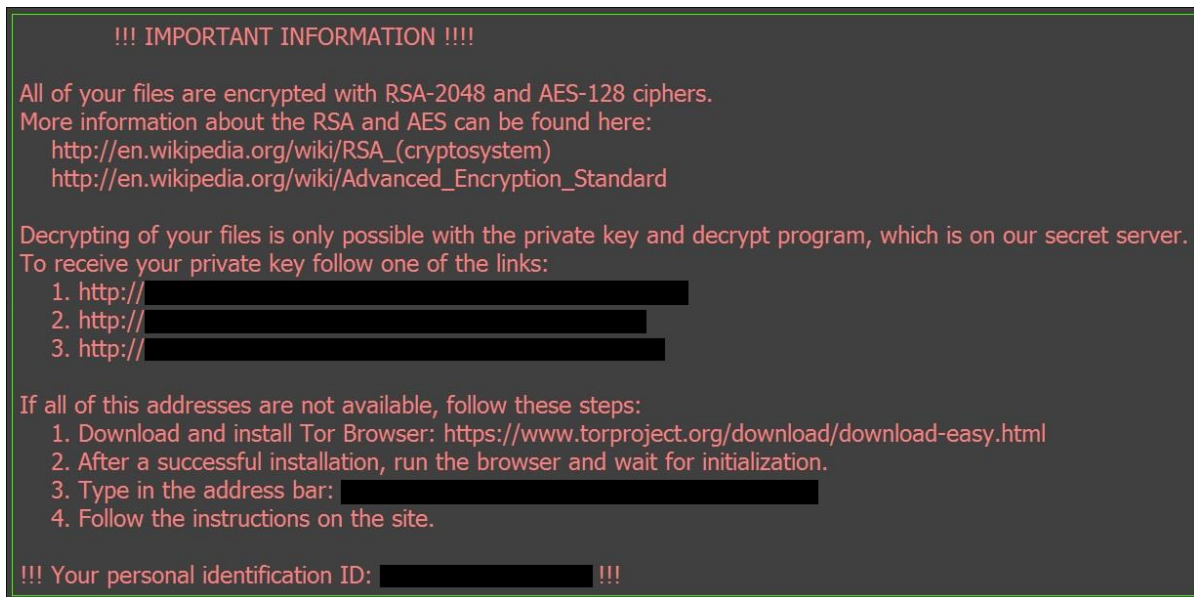


Figure 3: Avast n.d., Locky Ransomware.

3.2.2 WannaCry

One of the most notable type of ransomware is WannaCry. In May 2017, this new type of crypto ransomware devastated computers worldwide. Systems running the Windows Operating System without the most recent updates and patches were susceptible to the EternalBlue exploit which is how WannaCry was spread. This exploit was traced back to NSA when this tool was leaked (avast n.d.). The NSA notified Microsoft about the exploit and a patch for MS17-010 was released for all Windows Operating Systems, even Windows XP. However, users weren't forced to update their system with this patch which ultimately caused WannaCry to spread as rapidly as it did shortly after the exploit was known publicly.

3.2.3 Conti

A more recent strain first appearing in 2020 is the Conti Crypto Ransomware. This ransomware is linked with Russian cybercriminals. Acting as a ransomware as a service, criminals pay to use Conti and the data that's found by the attackers is publicly displayed on their extortion site (Yaakobi 2022). It encrypts every file it discovers and deems important and creates a ransom note in a text file. This ransomware attempts to spread to other systems on the network using SMB port 445 (Yaakobi 2022). However, the Conti operation has now been shut down by the cybercriminals dispersing into smaller groups (Abrams 2022).

One major attack from Conti was the attack on the Health Services Executive (HSE) in Ireland. Like the NHS, on 14th May 2021 a ransomware attack completely crippled the Irish health service nationwide (pwc 2021). The situation was so critical that the Irish Defense Forces were needed to recover from the attack and reset all affected systems.

However, shortly after the decryption key was given by the attacker without payment. Possibly due to the significant damage the attack was having. It was only on the 21st of September that the HSE had restored the majority of their systems. Attacks like the one against the HSE displays the real threat ransomware poses.

3.2.4 Reveton

Also known as FBI MoneyPak, this strain is a Locker Ransomware and dates back to 2012 which aims to impersonate law enforcement to convince the victim to pay the ransom (FBI, 2012). Once infected, the ransom screen appears acting as the FBI demanding payment in MoneyPak currency, which is a different payment method from previous ransomware discussed. The advice for victims of Reveton was to not pay and contact a computer professional to attempt malware removal (FBI, 2012).

3.3 PREVENTION METHODS AND TECHNIQUES

As discussed, the various types of ransomware all target and spread differently. Some steps can be taken to prevent becoming a victim of a ransomware attack, or if you become one methods to restore your system.

3.3.1 Backup

The first measure against ransomware and how it functioned was to make a backup of the data it would eventually encrypt. This data could be backed up to a cloud provider such as OneDrive or to an external hard drive. However, it's very important that the storage medium used to back up the data cannot be accessed by the system. This is to prevent the ransomware from spreading to the back up and encrypting those files as well. The victim can simply restore their system with the backed-up data, wiping the ransomware in the process like it was never there. Although, this is not addressing the threat of ransomware but just providing an effective measure against it.

3.3.2 Software updates and patches

The main method that ransomware spreads nowadays is through vulnerable software by using exploits within them. If the system hasn't updated to the latest version that blocks these exploits, then the ransomware will be able to spread and infect. Keeping all software updated on the system will protect the system and prevent ransomware spreading to the system this method.

3.3.3 Securing email communications

Some ransomware's main means of infecting is through phishing. If the victim downloads the malware, then the system and network become infected. It only would take one user out of a whole organisation for the attack to happen. Due to this it's important to have good email security in place. Good security would be checking the files being sent around the network through email and blocking suspicious emails/files to stop the user from falling victim.

If the email communications are secure, then ransomware using this method to spread will be prevented. There are many companies already providing this service ready to be deployed.

3.3.4 Not paying the ransom

If someone has fallen victim to ransomware, they are now being advised to not pay the ransom demand. The hope for not paying the ransom is it will deter the attacker in future attacks as there is no incentive for them now (Baker, 2022). The victim of ransomware is at a disadvantage with their data encrypted. It's not preventing the attack, just the commercial incentive for attackers. However, many continue to ignore this and pay in the hopes to get their data back. This is not a prevention method and does not target the issue of ransomware. This is simply the victim accepting that they have been hit with ransomware which is not suitable advice for a victim when their data is lost. Advising critical infrastructure such as hospitals not to pay as a prevention is simply not possible as ineffective, as risk to life is occurring during a ransomware attack on their systems.

3.3.5 Anti-Ransomware software.

As mentioned in the methodology there is now anti-ransomware software that aims to prevent ransomware on the system. The researcher will test how effective this prevention method is in the evaluation. However, older operating systems such as Windows XP SP3 are not widely supported with anti-ransomware software.

3.3.6 Online decryption tools

Once a ransomware attack has occurred the type of ransomware that has infected the system may have a decryption tool already available. A great project called "No More Ransom (NMR)" by Europol's European Cybercrime centre aims to provide decryption tools for the most common ransomware (Europol, 2021; nomoreransom, n.d.). The tools provided are made by various security companies. NMR is run by the Netherlands police and McAfee. The decryption tool will recover the encrypted data by decrypting the data with the decryption key.

4 PROCEDURE AND RESULTS

4.1 OVERVIEW OF PROCEDURE

The evaluation will be split into two parts. Part one investigating WannaCry on Windows XP SP3 and Part two investigating the difference in prevention methods on Windows 10 Home.

4.2 WINDOWS XP SP3 ENVIRONMENT

4.2.1 Without Protection

To begin with the evaluation the researcher created the XP environment and got it set up with the necessary tools and software. Figure 4 below shows the environment set up on Windows XP. As seen, the .zip file “Ransomware.WannaCry.zip” contains the live ransomware sample WannaCry. The “windowsxp-...” .exe file is the security patch given to windows XP after the WannaCry attack occurred. For this section no security update installed and no anti-virus protection enabled (as the operating system is no longer being supported by Microsoft).

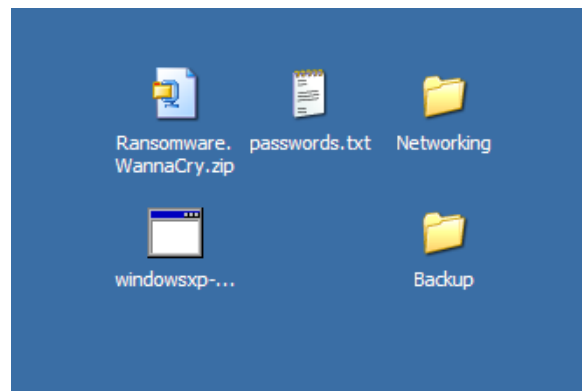


Figure 4: Windows XP environment set up

After unzipping the ransomware sample the executable file was now on the system. The filename is shown in figure 5.

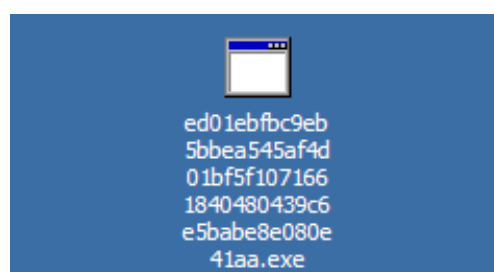


Figure 5: WannaCry executable file

The researcher ran the executable file and files on the system immediately began encrypting. See Appendix A, figure 1 which shows the WannaCry files created and the desktop files encrypted.

After executing the ransomware, the ransomware note and its decryptor appeared (see figure 6). At this stage the operating system has failed preventing the ransomware attack on the machine. To recover the files decryption is needed.

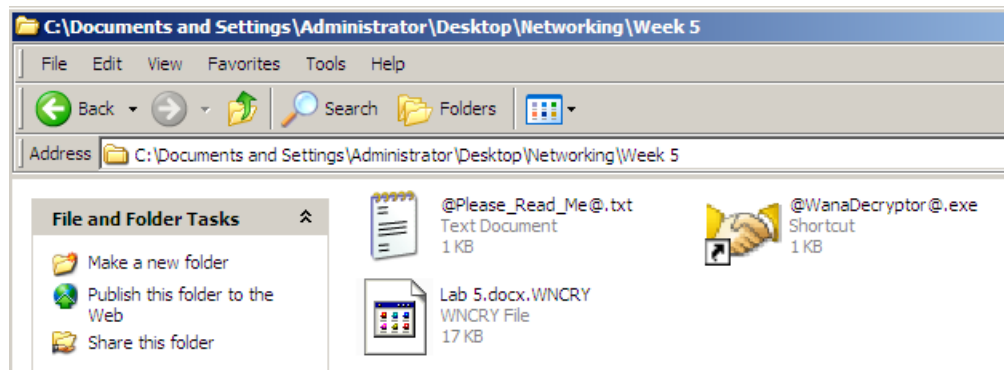


Figure 6: Ransomware note and WannaCry decryptor.

Appendix C, figure 1 is the ransomware note which gives information on what exactly has happened to the victim. As expected, the attackers require payment to their bitcoin address to decrypt the files. You can see the attackers guarantee "we guarantee that you can decrypt all your files" if the victim pays. As mentioned previously, there is no guarantee you will recover the files by paying.

After running the "@WannaDecryptor @.exe" executable the victim is greeted with the window shown in figure 7 on the next page. This is how the cybercriminals would get payment from the malware by posting their bitcoin address for victims to send their money to. The timer is defunct in this live malware scenario however it would be running in a real ransomware attack. It's clear the aim of ransomware is to instill fear into the victim by the malware design and time urgency.

Once WannaCry is executed the background image of the system changes as well with instructions to take. This can be seen in Appendix C, figure 2 & 3. Changing the background image also lets the victim understand the malware has full control over the system.



Figure 7: WannaCry Decryptor payment window.

If the victim attempts to ignore the ransomware and open their files the system will be unable to open the file as demonstrated by figure 8.

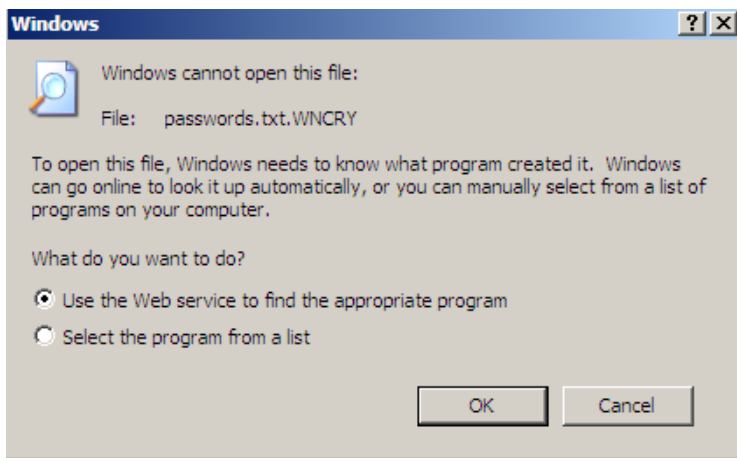


Figure 8: Unable to open text file due to encryption.

Furthermore, if the victim attempts to decrypt the files without paying an error will appear demanding payment (see Appendix C, figure 4). Also, it's clear from the supporting languages that this ransomware was intended to spread globally from the beginning of its campaign (see Appendix C, figure 5).

From the evaluation the researcher has conducted in this section it's clear Windows XP SP3 is unable to prevent a ransomware attack. The WannaCry ransomware was able to be executed with no resistance from the operating system.

4.2.2 With protection

Before continuing with this section the researcher reverted the Windows XP SP3 virtual machine to a snapshot before the ransomware was installed and executed (see figure 9).

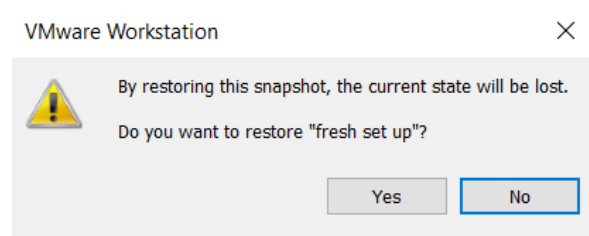


Figure 9: Reverting to old snapshot before ransomware executed

The objective for this section is to install the patch update for Windows XP against the exploit that WannaCry used. The researcher ran the patch executable called "windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe". Figures 10&11 below shows the installation wizard for the security update.

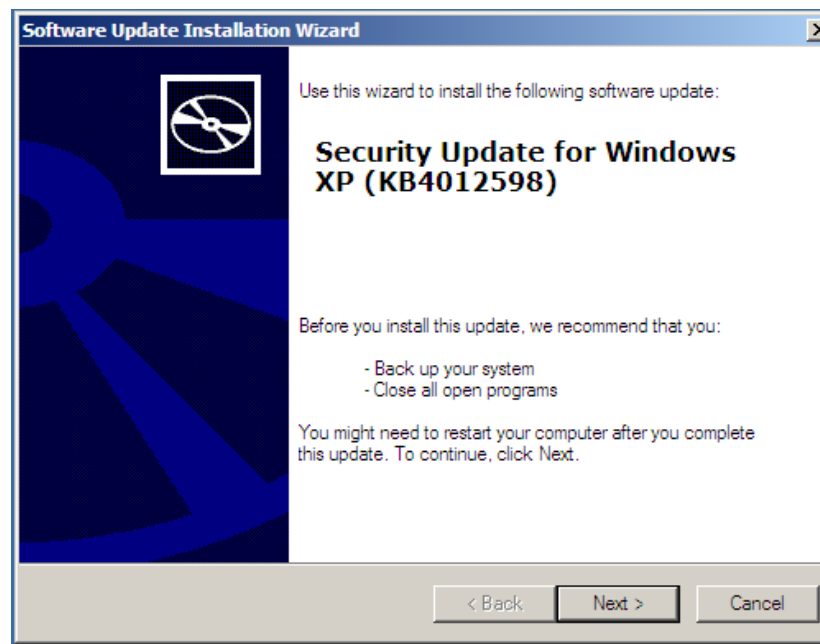


Figure 10: Windows Security Update installation wizard.

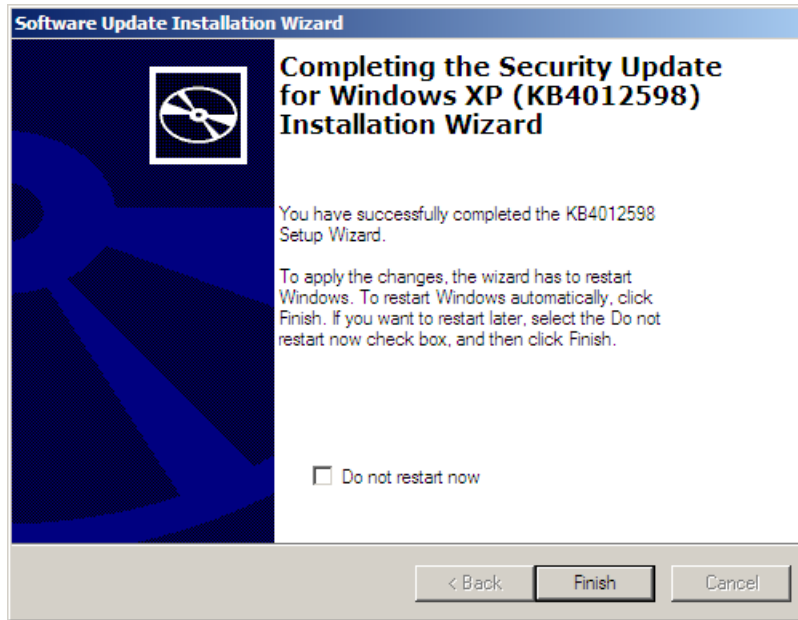


Figure 11: Installation of security update complete.

The researcher restarted Windows XP and attempted to run the WannaCry with the security patch now installed. However, despite patching the exploit the ransomware still successfully executed (see Appendix C, figure 6). The security patch seems to not prevent ransomware from executing on the system. Instead the update will stop the spread of the “EternalBlue” exploit to other machines (Microsoft, n.d.). Having demonstrated the previous attempt to prevent ransomware in Windows XP SP3 a sub aim has been met.

4.3 WINDOWS 10 HOME ENVIRONMENT

4.3.1 Without Protection

To define “without protection” in this section, it is what the Windows 10 base operating system is able to prevent without any additional security added on or enabled. For example, with no Ransomware Protection feature or anti-ransomware software. Meaning just testing the Windows Defender/Windows Security within Windows 10.

To begin with the evaluation the researcher created the Windows 10 Home environment and got it set up with the necessary tools and software. Appendix B, figures 1&2 show the environment set up on Windows 10. Like shown previously, the .zip file “Ransomware.WannaCry.zip” contains the live ransomware sample WannaCry. The “ZaarSetup” executable is the anti-ransomware software.

The researcher ensured that Windows Security was up to date and the latest update to windows 10 was installed (see figure 12 on the next page). After this the researcher was ready to evaluate the prevention measures against ransomware.

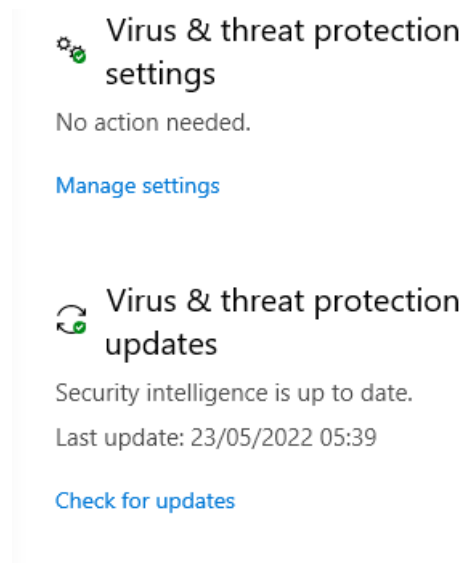


Figure 12: Windows Security up to date.

The researcher executed the WannaCry ransomware and the malware was immediately discovered and quarantined by Microsoft Defender Antivirus (see Figures 13&14). This was a brilliant result. The ransomware didn't even get to executing at all, no files were created like seen previously in Appendix A, figure 1.



Figure 13: Notification of Ransomware found by Windows Security.

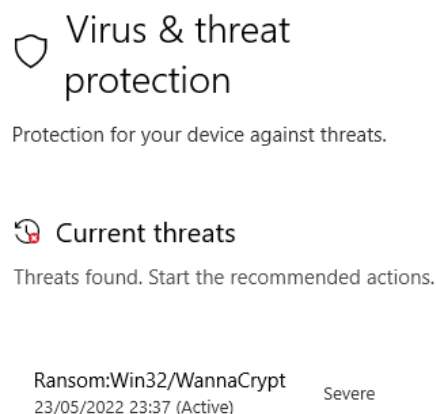


Figure 14: Threat identified as WannaCrypt.

The researcher attempted to run the ransomware anyway to see the reaction, even though the warning was in place by Windows Security. The action was blocked with a pop-up window explaining that the file contains a virus or potentially unwanted software (see figure 15). Another brilliant response to malware in the modern operating system. Windows Security then permanently removed WannaCry from the system as seen in figure 16.

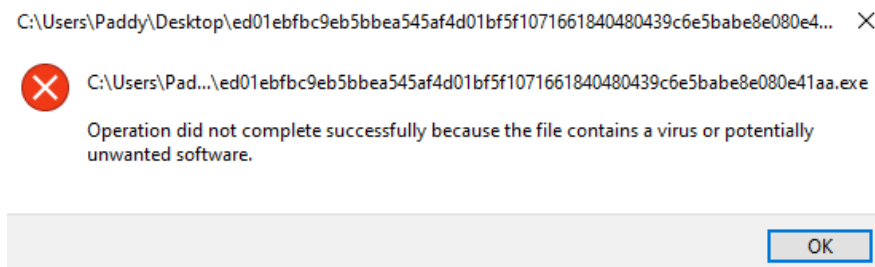


Figure 15: Pop up message explaining file is malicious.

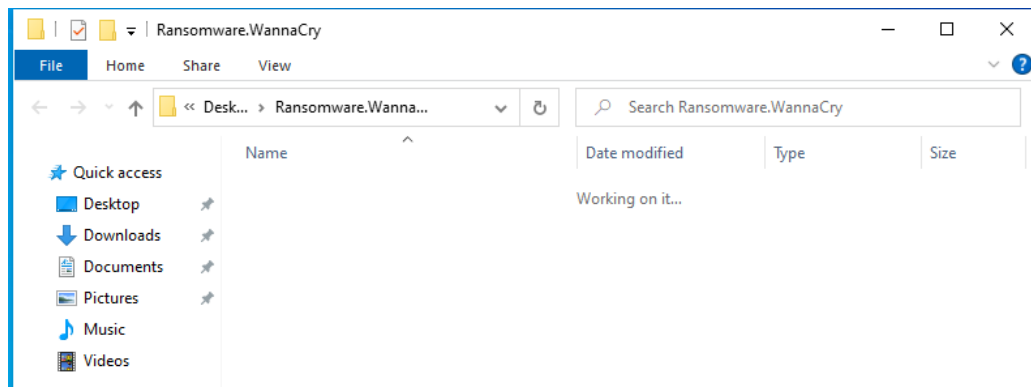


Figure 16: WannaCry executable removed from the system.

From the evaluation the researcher conducted, Windows Security in Windows 10 Home is sufficient enough to detect and stop ransomware.

4.3.2 With Protection

Ransomware Protection

In 2021 they added a Ransomware Protection feature to Windows Security with a Windows Update release. The researcher enabled this feature as seen by figure 17. This works by setting certain directories to prevent unauthorised changes.

Ransomware protection

Protect your files against threats such as ransomware and see how to restore files in case of an attack.

Controlled folder access

Protect files, folders and memory areas on your device from unauthorised changes by unfriendly apps.

 On

[Block history](#)

[Protected folders](#)

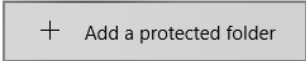
[Allow an app through controlled folder access](#)

Figure 17: Ransomware Protection enabled in Windows 10 Home.

As the WannaCry ransomware sample was saved on the Desktop, the researcher modified the protected folders to include the Desktop directory (see figure 18).

Protected folders

Windows system folders are protected by default.
You can also add additional protected folders.

 + Add a protected folder

Desktop
C:\Users\Paddy\Desktop

Documents
C:\Users\Paddy\Documents

Documents
C:\Users\Public\Documents

Pictures
C:\Users\Paddy\Pictures

Pictures
C:\Users\Public\Pictures

Videos
C:\Users\Public\Videos

Figure 18: Desktop directory added to protected folders.

Finally, to ensure only ransomware protection was being evaluated the researcher allowed WannaCry through Windows Security as demonstrated by figure 19. Allowing the ransomware so as to not be blocked by Windows Security would be a close match to the environment of the Windows XP SP3 system.

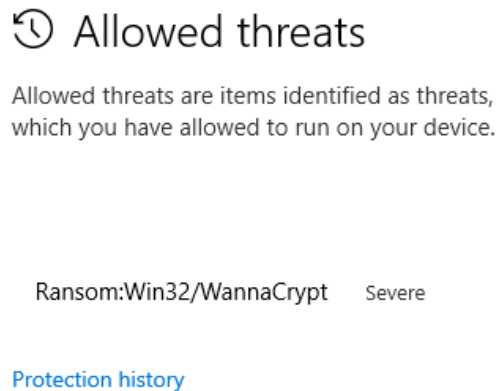


Figure 19: WannaCry threat allowed on Windows 10 Home.

Once the set up was completed the researcher executed the ransomware on the Desktop. Ransomware Protection successfully detected the ransomware attempting to make changes to the Desktop directory by adding the WannaCry files and encrypting files on the system (see figure 20).

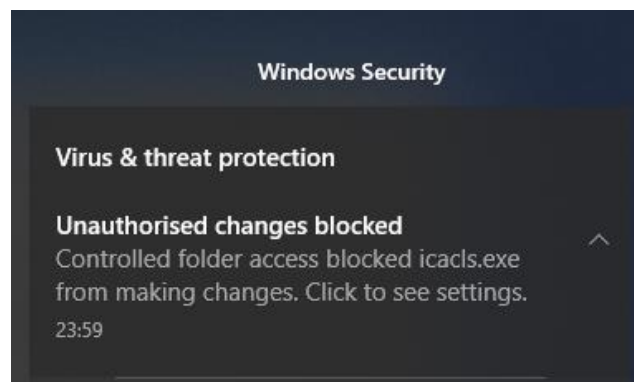


Figure 20: Ransomware Protection detected unauthorised changes.

After successfully detecting the ransomware, the malware was blocked. The protection history in Ransomware Protection can be seen in Appendix B, figure 3. From the evaluation of the researcher Ransomware Protection in Windows Security is a successful prevention method for ransomware.

Anti-Ransomware Software

Unknown to the researcher, the specific type of anti-ransomware defined in the methodology (ZoneAlarm) of this evaluation required internet access (see figure 21 on the next page).

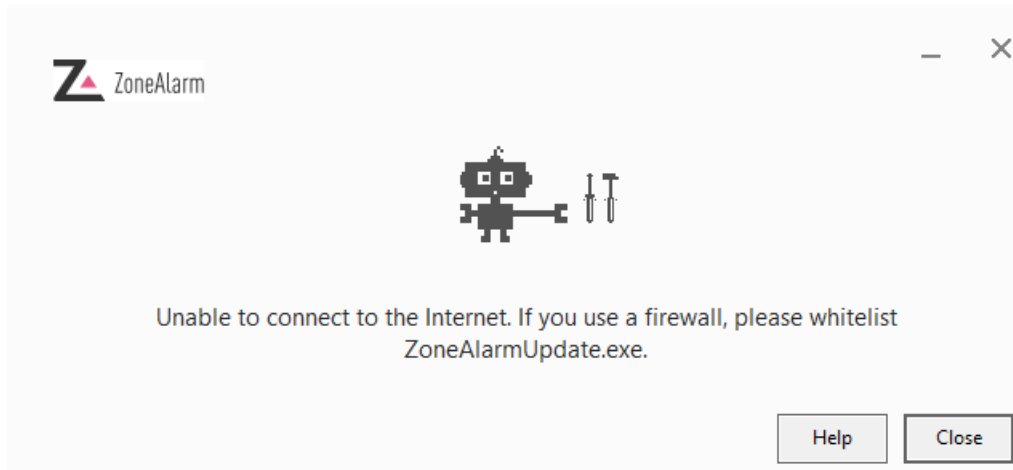


Figure 21: Anti-Ransomware software (ZoneAlarm) requiring internet access.

Therefore, for the sake of security the researcher did not want to risk the ransomware sample escaping from the malware analysis lab through the network. Unfortunately, anti-ransomware software could not be evaluated by the researcher. However, from this evaluation it's clear that modern operating systems have enough prevention methods to combat ransomware and third-party software is not necessary. The researcher has successfully demonstrated current ransomware prevention methods in modern operating systems meeting another sub aim of this evaluation.

5 DISCUSSION

5.1 DIRECTION RANSOMWARE IS GOING IN

The United States have recently declared ransomware as terrorism - *“The U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack and mounting damage caused by cyber criminals, a senior department official told Reuters.”* - (Reuters, 2021).

Due to this announcement attempts were made to make ransomware payments illegal, however were unsuccessful and many companies and individuals continue to pay the ransom (OFAC, 2021). If an individual or company pays for the decryption key in hopes to recover their data, they are breaking the law and in the eyes of the U.S, helping aid terrorism. There were also many discussions last year on if the ransom should be paid and if enforcing not paying would be an effective countermeasure (BBC, 2021).

Furthermore, regulating cryptocurrency was actually a discussion in hopes to deter ransomware (euronews, 2021). Undeniably, this is an overkill method to prevent criminals making money from ransomware. Legitimate users of cryptocurrency would suffer, and it's likely the criminals will just use the other payment methods mentioned.

Ransomware as a service (Raas) is a new method cybercriminals are using to make money from ransomware (Baker, Kurt, 2022). This service enables the cybercriminal to get paid for their malware by providing it to the attackers. The attackers also pay a service fee per successful ransom. Having multiple attackers from various locations around the world using a service like this makes it difficult to prevent the operation. If one attacker is caught, the ransomware service is still active out there being used and maintained by other cybercriminals.

5.2 GENERAL DISCUSSION

The researcher has successfully demonstrated the prevention methods created against ransomware and how effective they are today. All aims of the evaluation were met demonstrating that we are moving in the right direction to combat this type of malware. With lots of existing solutions available for users to protect themselves it makes the attackers role much more difficult. It's clear over the years protection against ransomware within operating systems has improved greatly. Having security implemented at a base level such as the operating system helps protect non-technical users as well.

5.3 COUNTERMEASURES TO RANSOMWARE

Alongside the prevention methods implemented into newer operating systems and software available, there are general countermeasures against ransomware every organisation and individual are advised to take.

Backup Data

So far, the only foolproof method against ransomware is to have a backup of all important files created regularly. In the case of a ransomware attack, a simple backup restore and the ransomware is wiped clean like it never happened. A hassle to be continuously doing, but an effective method.

Update Software

Any software running on a system must be kept up to date with the latest patch. Vulnerabilities present in old versions of the software will become ineffective due to the patch sent out by the software developers. The most critical software to keep up to date is the operating system, as this will be a target for attackers creating the malicious software using flaws and vulnerabilities in the operating system (As seen by WannaCry with Eternalblue exploit against the NHS).

Ensure Anti-Virus Is Enabled

If using a modern Windows-based Operating System ensure that Windows Security is enabled and that all virus definitions are kept up to date. For further protection you can enable Ransomware Protection as seen in this evaluation. While not necessary installing a third-party anti-ransomware software will help protect the system even further by checking files downloading for ransomware.

Incident Response Plan

If all else fails and you end up being the victim of a ransomware attack organizations need to have a plan to respond. Some good points for consideration, as provided by NCSC (NCSC, 2021), in your response plan:

Think about how you will respond to the ransom demand from an attacker and the threat it poses to your organisation. The attacker may threaten publishing this data if the ransom is not paid. This will have negative backlash in the media if word gets out that your organisation has fell victim to a ransomware attack, so you will need to be prepared for this outcome too. Furthermore, know your legal obligations if you fall victim to an attack about reporting the incident to regulators. You should also take time to understand how approach it.

Incident Management Plan

Alongside a good incident response plan is a good incident management plan. This plan helps define the roles of the staff within the organisation and prioritising data recovery. Think about how long it would take to restore systems in the case of a ransomware attack and the procedure for restoring from backup. Finally, plan for the case that you may have to operate critical business operations if none of the systems or services are able to be used. (NCSC, 2021).

5.4 FUTURE WORK

If the researcher were to continue the evaluation, he would test prevention methods against Locker Ransomware such as Reveton, as only Crypto Ransomware was researched in this evaluation. Furthermore, a more in-depth analysis on how ransomware spreads between systems could be an area of focus to extend the project research and understanding of the subject area.

A home network environment with a custom broadband internet connection could help analyse the anti-ransomware software used in the evaluation. The researcher would feel more comfortable and confident to run the ransomware if the network and internet was securely locked down. A paid anti-ransomware version would also be better to test than a trial version.

Finally, as only the Windows Operating System was researched in this evaluation it would be beneficial to check the prevention methods and techniques in Linux-based Operating Systems.

REFERENCES

For URLs, Blogs:

Rivest, R, Shamir, A and Adleman, L, February 1st, 1978, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, People.csail.mit.edu, viewed 17 May, 2022, <<https://people.csail.mit.edu/rivest/Rsapaper.pdf>>.

Joe Tidy 2021, Ransomware: Should paying hacker ransoms be illegal?, BBC News, viewed 17 May, 2022, <<https://www.bbc.co.uk/news/technology-57173096>>.

Kerner, S 2022, Colonial Pipeline hack explained: Everything you need to know, *WhatIs.com*, viewed 17 May, 2022, <<https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>>.

Wilkie, C 2021, Colonial Pipeline paid \$5 million ransom one day after cyberattack, CEO tells Senate, *www.cnbc.com*, viewed 17 May, 2022, <<https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html>>.

Wilkie, C & Macias, A 2021, U.S. recovers \$2.3 million in bitcoin paid in the Colonial Pipeline ransom, *cnbc.com*, viewed 17 May, 2022, <<https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html>>.

BBC News 2017, NHS cyber-attack: GPs and hospitals hit by ransomware, *BBC News*, viewed 17 May, 2022, <<https://www.bbc.co.uk/news/health-39899646>>.

BBC News 2017, NHS 'could have prevented' WannaCry ransomware attack, *BBC News*, viewed 17 May, 2022, <<https://www.bbc.co.uk/news/technology-41753022>>.

Johnson, J 2021, Number of ransomware attacks per year 2020 | Statista, *Statista*, viewed 17 May, 2022, <<https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/>>.

Baker, K 2022, What is Ransomware? - CrowdStrike, *crowdstrike.com*, viewed 17 May, 2022, <<https://www.crowdstrike.com/cybersecurity-101/ransomware/>>.

Rueters 2021, Exclusive: U.S. to give ransomware hacks similar priority as terrorism | Reuters, *Rueters*, viewed 17 May, 2022, <<https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/>>.

OFAC, 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, p . 3, ,viewed 17 May, 2022, <https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf>.

euronews 2021, EU will make Bitcoin traceable and ban anonymous crypto wallets in anti-money laundering drive, *euronews*, viewed 21 May, 2022, <<https://www.euronews.com/next/2021/07/21/eu-will-make-bitcoin-traceable-and-ban-anonymous-crypto-wallets-in-anti-money-laundering-d>>.

tisf 2021, theZoo/malware/Binaries at master · ytisf/theZoo, *GitHub*, viewed 18 May, 2022, <<https://github.com/ytisf/theZoo/tree/master/malware/Binaries>>.

ZoneAlarm 2022, ZoneAlarm Anti-Ransomware, ZonemAlarm, viewed 18 May, 2022, <<https://www.zonealarm.com/anti-ransomware>>.

denisebmsft, chrisda, v-mathavale, RatulaC and Ashok-Lobo 2022, Microsoft Defender Antivirus in Windows, *Docs.microsoft.com*, viewed 18 May, 2022, <<https://docs.microsoft.com/en-gb/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide>>.

Microsoft 2017, Microsoft Update Catalog, *Catalog.update.microsoft.com*, viewed 18 May, 2022, <<https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>>.

Heath, N 2017, New Windows XP patch: Microsoft issues extraordinary fix to protect PCs against next WannaCry, *TechRepublic*, viewed 18 May, 2022, <<https://www.techrepublic.com/article/new-windows-xp-patch-microsoft-issues-extraordinary-fix-to-protect-pcs-against-next-wannacry/>>.

Waddell, K 2016, The Computer Virus That Haunted Early AIDS Researchers, *The Atlantic*, viewed 19 May, 2022, <<https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/>>.

Avast n.d., What is Locky Ransomware?, *avast.com*, viewed 19 May, 2022, <<https://www.avast.com/c-locky>>.

Brewster, T 2016, As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up \$17,000 In Bitcoin, *Forbes*, viewed 19 May, 2022, <<https://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/?sh=78e6f4a6408f>>.

Europol 2021, No More Ransom – do you need help unlocking your digital life? | Europol, *Europol*, viewed 19 May, 2022, <<https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life>>.

nomoreransom n.d, Decryption Tools | The No More Ransom Project, *nomoreransom.org*, viewed 19 May, 2022, <<https://www.nomoreransom.org/en/decryption-tools.html>>.

avast n.d., What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?, *avast.com*, viewed 19 May, 2022, <<https://www.avast.com/c-eternalblue>>.

Yaakobi, O 2022, Conti Ransomware - How it Works and 4 Ways to Protect Yourself, *Datto.com*, viewed 19 May, 2022, <<https://www.datto.com/uk/blog/conti-ransomware-how-it-works-and-4-ways-to-protect-yourself>>.

pwc 2021, Conti cyber attack on the HSE, viewed 19 May, 2022, <<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>>.

FBI 2012, FBI, This Week: Reveton Ransomware, [podcast], viewed 19 May 2022, <<https://www.fbi.gov/audio-repository/news-podcasts-thisweek-reveton-ransomware/view>>.

Abrams, L 2022, Conti ransomware shuts down operation, rebrands into smaller units, *BleepingComputer*, viewed 20 May, 2022,

<<https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/>>.

Microsoft n.d., How to verify that MS17-010 is installed, *Support.microsoft.com*, viewed 20 May, 2022, <<https://support.microsoft.com/en-us/topic/how-to-verify-that-ms17-010-is-installed-f55d3f13-7a9c-688c-260b-477d0ec9f2c8>>.

NCSC 2021, Mitigating malware and ransomware attacks, *ncsc.gov.uk*, viewed 21 May, 2022, <<https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>>.

Baker, Kurt 2022, Ransomware as a Service (RaaS) Explained | CrowdStrike, *crowdstrike.com*, viewed 22 May, 2022, <<https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>>.

For Images:

Popp, J 2019, Part of AIDS DOS trojan horse payload, <[https://en.wikipedia.org/wiki/AIDS_\(Trojan_horse\)#/media/File:AIDS_DOS_Trojan.png](https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)#/media/File:AIDS_DOS_Trojan.png)>.

Avast n.d., Locky Ransomware, <<https://www.avast.com/c-locky>>.

APPENDICES

APPENDIX A – WINDOWS XP SP3

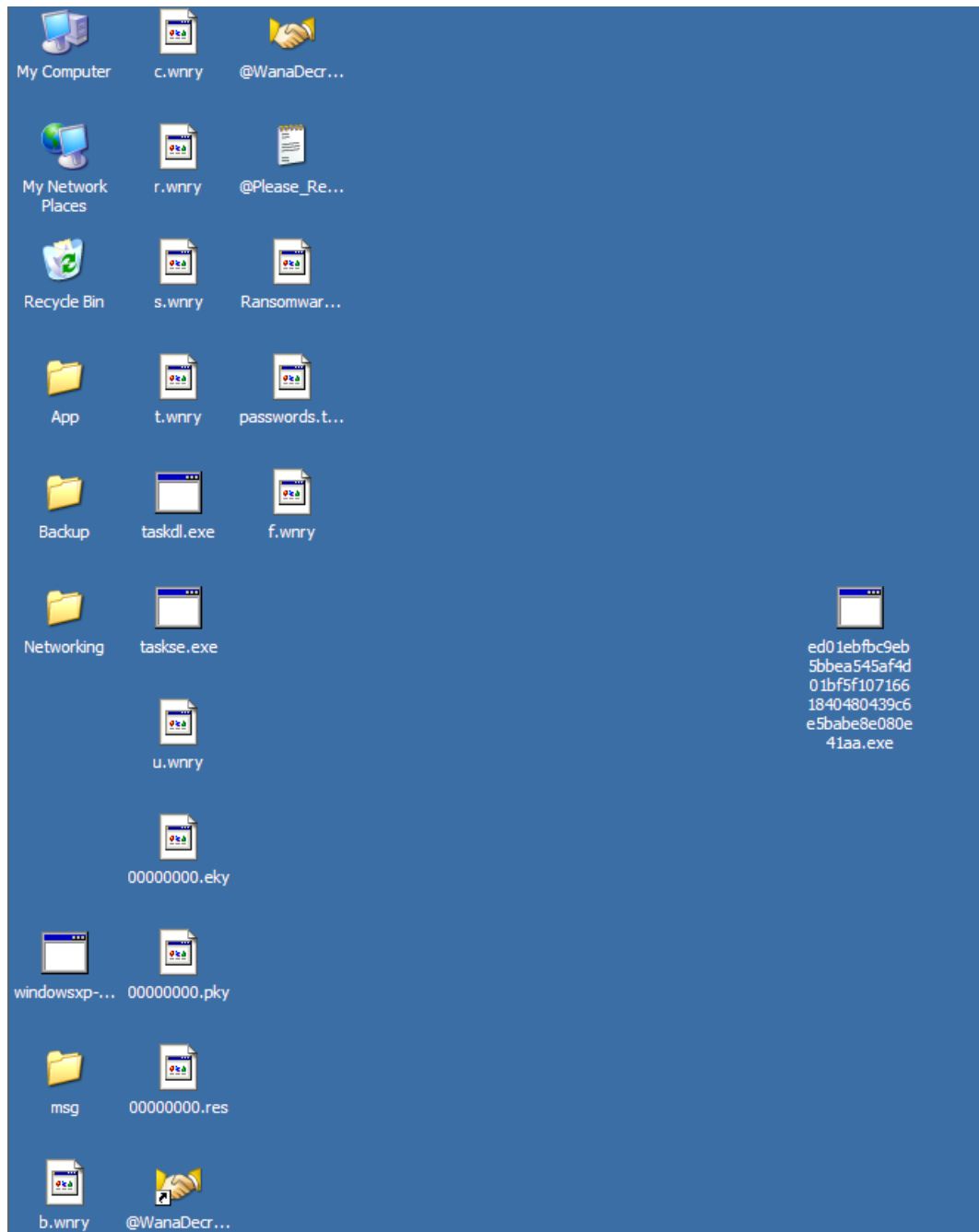


Figure 1: WannaCry executed – files now encrypted.

APPENDIX B – WINDOWS 10 HOME

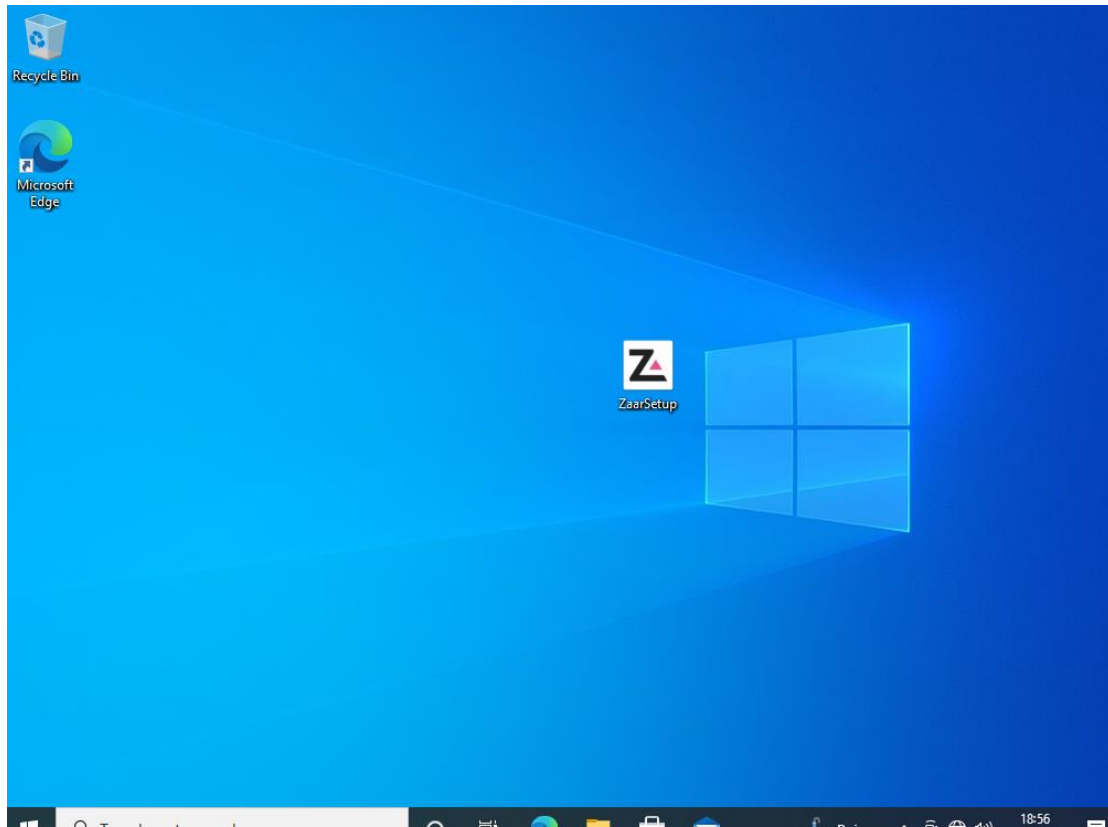


Figure 1: Windows 10 Home environment set up.

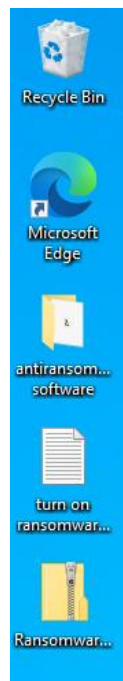




Figure 2: WannaCry ransomware added


Protection history

View the latest protection actions and recommendations from Windows Security.

Filtered by: Blocked folder access

Filters 

 Protected folder access blocked Low 
23/05/2022 23:59

 Your administrator has blocked this action.

App or process blocked: ed01ebfbc9eb5bbea54
5af4d01bf5f107166184
0480439c6e5babe8e08
0e41aa.exe

Protected folder: %desktopdirectory%\Ransomware.WannaCry\

Blocked by: Controlled folder access

You can allow apps to access your protected folders, but you should only allow apps that you trust.

[Controlled folder access settings](#)


Actions 

Figure 3: Ransomware Protection history. WannaCry blocked.

APPENDIX C – WANNACRY DEMONSTRATION

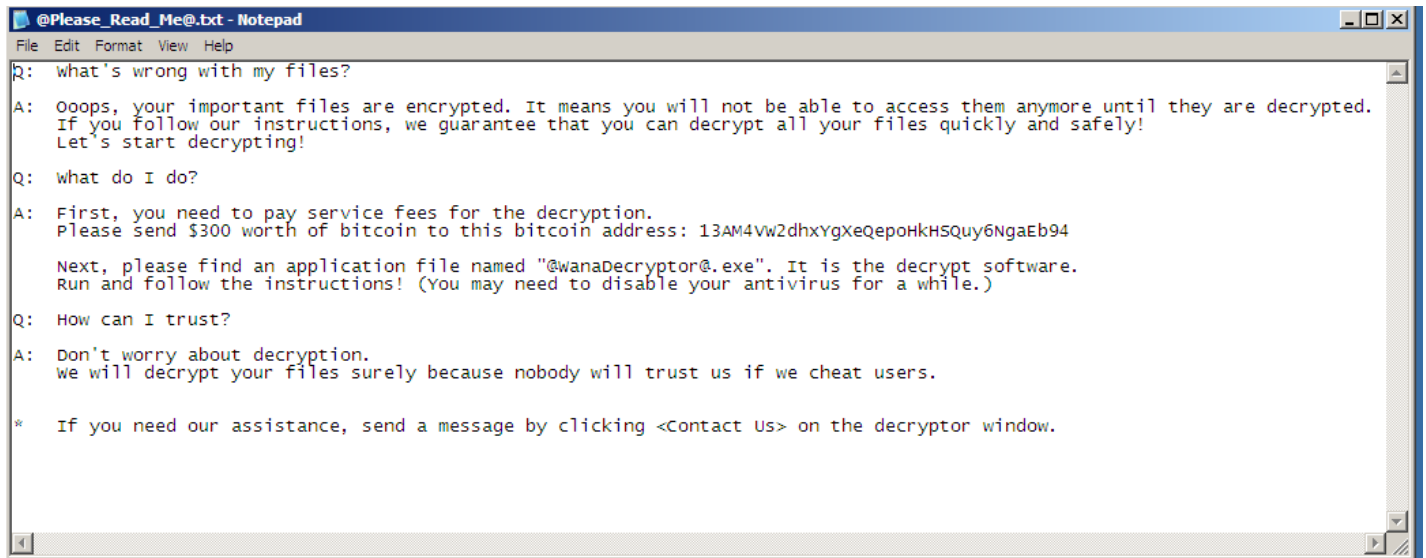


Figure 1: Ransomware note from WannaCry.



Figure 2: WannaCry payment window with background image changed.

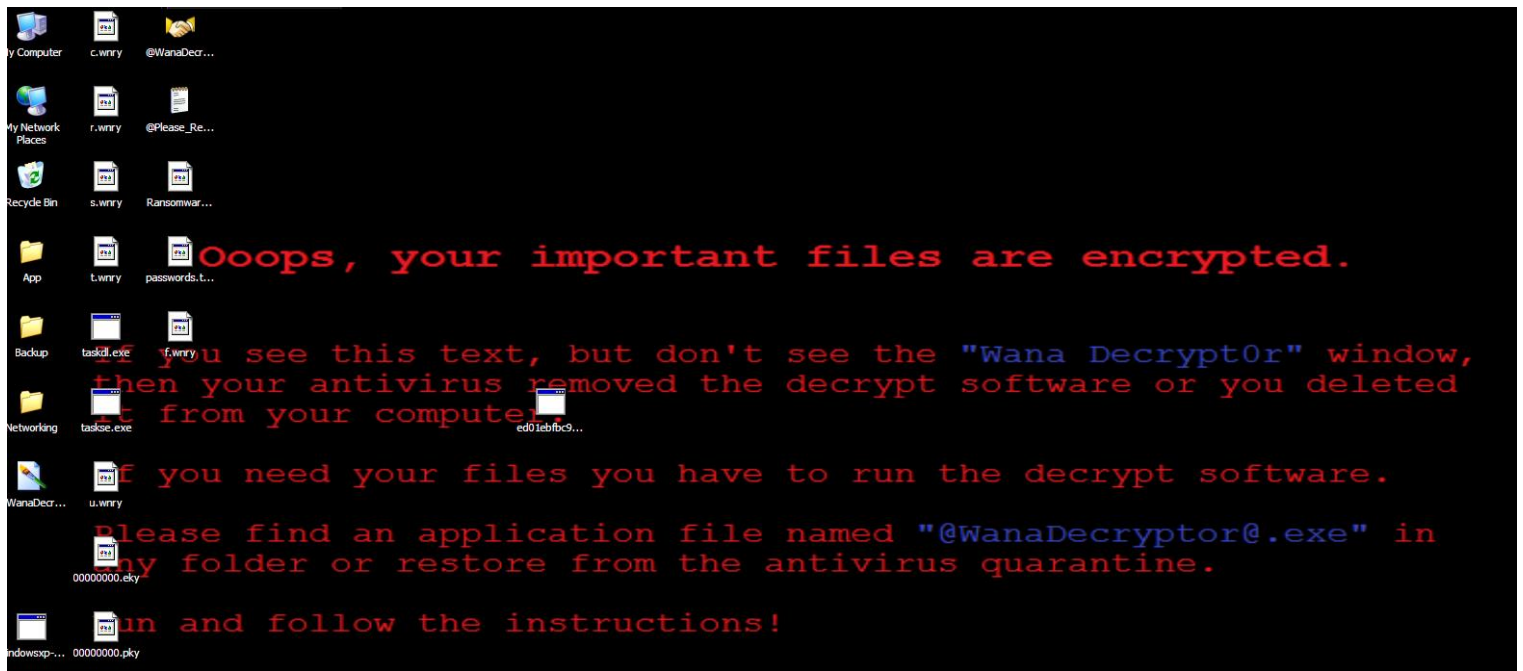


Figure 3: Background of Windows XP changed to ransomware note.

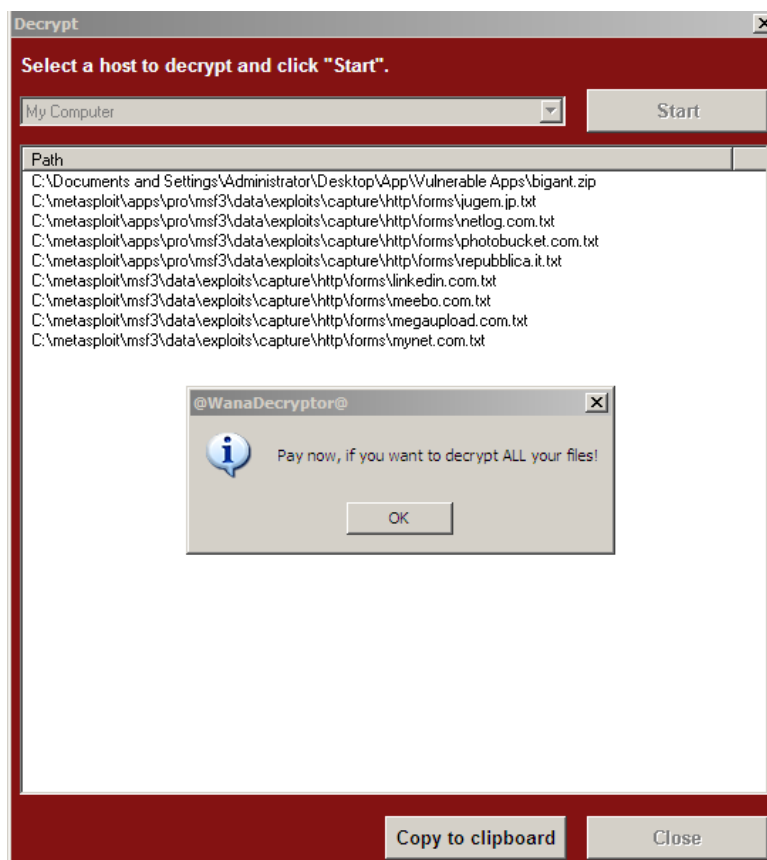


Figure 4: Attempt to decrypt blocked.



Figure 5: Language support for WannaCry Ransomware.



Figure 6: Ransomware executed after windows patch installed.