Abertay University

Anti-Virus Effectiveness Against Ransomware

Sam Heney – 1700469@abertay.ac.uk

Introduction to Security – CMP110

BSc Ethical Hacking Year 1

2017/18

.

Abstract

The aim of this paper is to test how effective various anti-virus and anti-malware software is against ransomware, particularly while the anti-viruses are offline. Ransomware is a very prevalent and relevant threat, so it would be useful to find out which software provides a consistently effective protection against it.

To test the effectiveness of the anti-viruses, a virtual environment running windows 7 (SP1) was set up. It was ensured that the machine was isolated and not connected to the internet. A few dummy “Important” files were created and then the anti-virus was installed. Finally the ransomware was deployed. The effectiveness of the anti-virus was then recorded and the virtualbox was reset.

This test was repeated fourteen times to have each iteration of malware against anti-virus tested. Two ransomware samples were used (Wannacry and Cerber) and six Anti-viruses were tested. There were two extra tests with no anti-viruses to ensure that both samples of malware fully functioned. The results were recorded, organised and compared.

The tested anti-viruses tended to be very effective against the ransomware. Wannacry was prevented far more effectively across the board than Cerber was. The least effective anti-viruses tested were Panda and Norton. The most effective was tied between Avast, Bitdefender, MalwareBytes and Kaspersky who were the only four that managed to completely prevent both attacks.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

The idea of malware extortion has been around for a while, but the techniques that involve cryptography and are far more difficult to prevent have only recently been implemented. Cryptographic Ransomware has now begun to be used maliciously on a massive scale with the number of different strains being discovered increasing exponentially and the number of reported cases also increasing. [1]

Ransomware is a form of malware that blocks access to a user's files until a ransom is paid to the attacker. By this definition, access to the files could be blocked using any means imaginable. The concept was refined however by Young and Yung of Columbia University and they first presented their new version, named cryptoviral extortion, in 1996 at the IEEE Security & Privacy conference. The attack followed a three step procedure: [2]

1. Attacker generates a key pair and the public key is coded into the malware. The malware is released.

2. For each new victim, the malware generates a random symmetric key and uses this to encrypt the user's data. The public key generated in step 1 is then used to encrypt the symmetric key. The malware then destroys all of the original unencryped data. It displays to the user instructions of payment and the asymmetric ciphertext. The victim then makes the payment and sends the asymmetric ciphertext to the attacker.

3. The attacker then decrypts the asymmetric ciphertext with their private key thus revealing the symmetric key that the victim needs. The attacker then, if payment has been received, sends the victim the symmetric key and the victim may use it to decrypt their data. The attack is complete.

This basic premise can be elaborated on. For example, the attacker's message may impersonate government services, making the victim more likely to trust the hacker. In some cases, the ransomware is designed so poorly that even if the payment is processed, the files aren't decrypted. This was the case for the Wannacry worm, where the attackers had no way of confirming if a payment had actually been made or not. This indicated that the hackers didn't really intend to decrypt the files at all. [3]

One big problem with ransomware for the attackers is the form of payment, which used to be difficult to make untraceable. Initially payments methods such as wire transfer or pre-paid vouchers were used but now cryptocurrency presents a far easier alternative. Bitcoin solved the problem of trustless, nearly anonymous transactions over the internet but unfortunately this also solved those problems for ransomware attackers. Bitcoin is now used as the primary method of payment in most common ransomware attacks. [4]

A big case that happened recently was the Wannacry attack in 2017. This attack spread through several countries and affected many important services, namely the NHS. The malware targeted computers running Windows and demanded payment in Bitcoin. It used the EternalBlue exploit to gain access to computers, an exploit created by the NSA. [5]

This attack was covered heavily by the media, which resulted in a large public interest in computer security. This also prompted anti-virus companies to use ransomware protection heavily in their advertising, knowing that people would be scared of the threat.

Anti-virus creators have had to quickly adapt to this new wave of attacks. Many anti-virus programs now include ransomware defense within them. In most cases it is nearly impossible to revert an attack after it has already happened meaning that the protection that most anti-viruses offer is therefore usually preventative rather than retroactive. Of course, ideally businesses should be implementing their security systems before an attack happens, but this tends not to be the case.

1.2 Aim

The aim of this project is to test the capability of various anti-virus software to defend against ransomware with the anti-viruses on default settings and offline. The tests will be carried out in fair conditions. Several anti-virus softwares will be tested and each anti-virus will be tested against several different ransomware samples.

The results of the tests will be compared to find which anti-virus software is best at preventing ransomware attacks, and which ones are not. The results will probably be split into five results:

1. No files encrypted
2. No files encrypted and Ransomware payment screen displayed
3. Some files encrypted
4. Some files encrypted and Ransomware payment screen displayed
5. Files fully encrypted (Ransomware not prevented)

Through these tests it should be clear which anti-viruses are effective at defending against ransomware, and which are not. More information will be discussed, but that is a secondary aim.

2 PROCEDURE

2.1 PROCEDURE PART 1 – SETUP

Software Required:

- VirtualBox
- Copy of Windows 7
- The Anti-Viruses that should be tested
- The Malware samples used for testing

Optional Software:

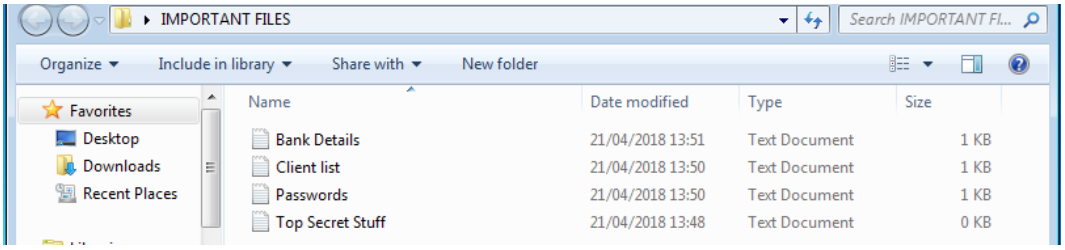
- Process Hacker 2
- HaoZip
- Firefox
- VirtualBox Guest additions

In order to test the malware in a safe environment VirtualBox was used to create an isolated virtual machine. The machine in this case was running windows 7 service pack 1, and was not connected to the internet. It is vital that the machine is completely isolated from any other machine as live malware may try and spread itself over the network. In this case the guest additions were added to the virtual machine, but when recreating this test their inclusion is optional. Not including them may lead to better testing and more security, but in this case they were included for efficiency of testing.

Now the virtual computer was prepared to be attacked. Fake "Important Files" were placed in the computer (to bait the encryption) and then some useful tools were installed. In this case, Process Hacker 2 was used to monitor processes more closely, and HaoZip was used to extract malware samples. Firefox was also installed as a web browser to replace internet explorer. Windows Defender should be disabled.

Finally, a snapshot of the operating system was taken using virtualbox, so that in the case of the anti-viruses failing and the ransomware infecting the PC, it could just be reset to an uninfected state. Also this means that each anti-virus has the exact same computer initially, making it a fairer test. Without this, the entire setup procedure would have to be executed for every new test.

Fig 2-1: Important Files



2.2 PROCEDURE PART 2 – TESTING

Now the anti-virus which is being tested needs to be installed. In this case, either the anti-virus was free or the free trial was used. The anti-virus installation files were downloaded from the internet on the host computer, then put into a "Transfer" folder. This folder was then activated as a read only folder for the virtual machine, and the files were put onto the virtual computer. The folder was then disconnected and deleted. The anti-virus is then installed. In order to make a fairer test the anti-virus was always left in it's default state.

The malware sample should now be activated. One of five things should happen:

1. No files encrypted
2. No files encrypted and Ransomware payment screen displayed
3. Some files encrypted
4. Some files encrypted and Ransomware payment screen displayed
5. Files fully encrypted (Ransomware not prevented)

Other events may occur, like the payment & decryption application being prevented from being executed, but these events are a useful way of categorising the effectiveness of the anti-virus. After the malware has finished executing, which of the five events occurred should be noted and the machine should be reset. This entire process should be repeated for each anti-virus and malware sample.

Fig 2-2: Wannacry Successful encryption

Fig 2-3: Encrytion prevented but Wannacry Readme left behind

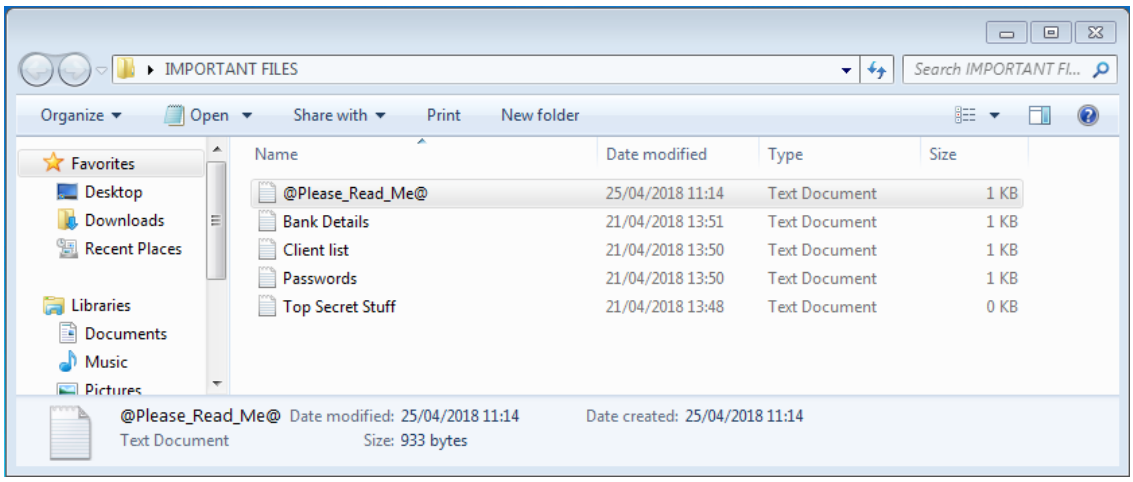
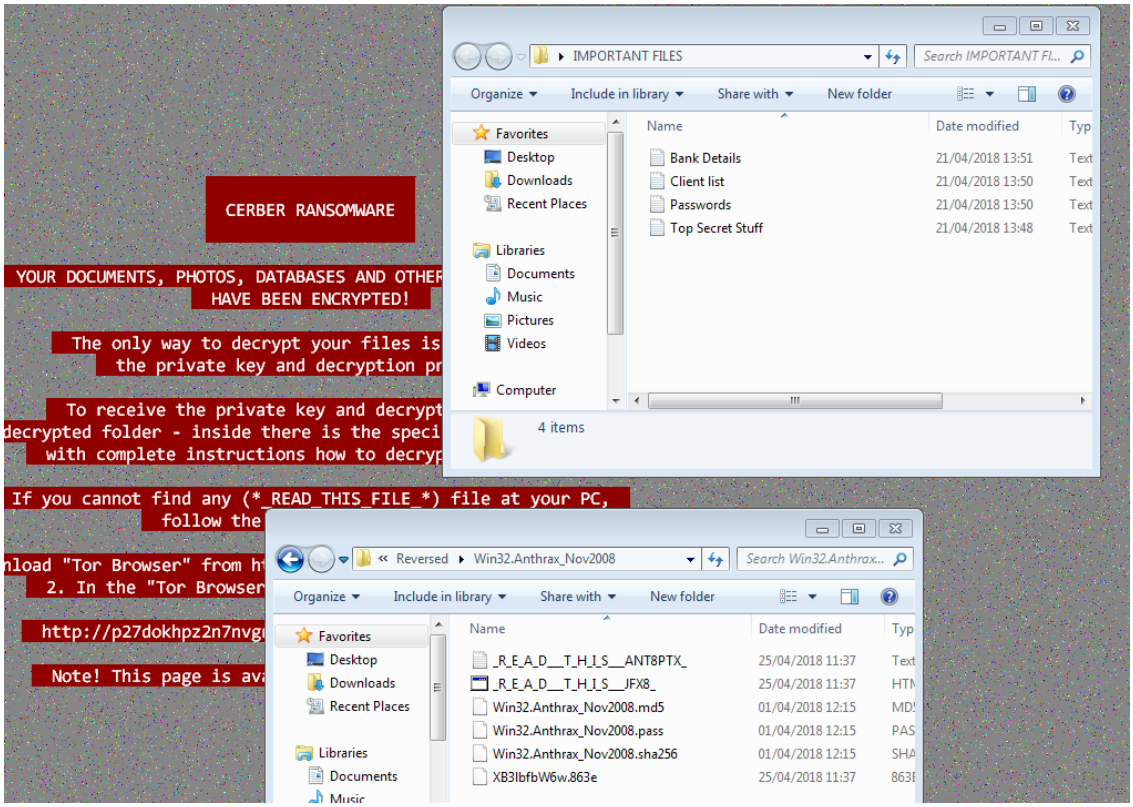


Fig 2-4: Some files encrypted by Cerber, ransomware payment screen displayed



3 RESULTS

Table Key:

1 = No files encrypted

2 = No files encrypted and Ransomware payment screen displayed

3 = Some files encrypted

4 = Some files encrypted and Ransomware payment screen displayed

5 = Files fully encrypted (Ransomware not prevented)

	Wannacry	Cerber
Avast	1	1
AVG	1	2
Bitdefender	1	1
Kaspersky	1	1
MalwareBytes	1	1
Norton	3	4
Panda	3	5

4 Discussion

4.1 General Discussion

The anti-viruses tested were mostly very impressive. The successful anti-viruses managed to take action immediately and effectively. Avast, Bitdefender, MalwareBytes and Kaspersky were particularly impressive as they, in both attacks, managed to immediately detect what was happening, halt the processes of the malware, and prevent any files from being encrypted. On restart of the machine there was also no trace of anything left behind.

It seemed strange that Panda and Norton were unable to cope with Cerber or Wannacry, especially considering that Wannacry has been so prevalent recently. Possibly it was because the anti-viruses were disconnected from the internet and therefore not connected to their databases of ransomware signatures.

Bitdefender was the most resource intensive succesful anti-virus, followed by Kaspersky, then Avast and finally MalwareBytes. This was tracked using process hacker. It would seem, therefore, that MalwareBytes was the most successful anti-virus, being completely effective at preventing the attacks while also being least resource intensive.

Bitdefender did however seem to have many features that could be useful to some people, so the most useful anti-virus really will depend on the particular user or use case. It could be that one user doesn't mind having less resources for more useful tools.

4.2 Conclusions

- MalwareBytes was the most effective in terms of Preventing the attacks while being least resource intensive.
- Bitdefender, Avast and Kaspersky were also fully effective, but slightly more resource intensive.
- AVG, Panda and Norton were not fully effective in preventing the attacks.
- Panda was the only anti-virus to fail in preventing Cerber from being completely successful.
- Norton and Panda were the only anti-viruses to fail in preventing Wannacry from activating.

4.3 FUTURE WORK

If this test were done again with more time and resources, a few improvements could be made:

- Testing with more malware samples. This would make the test more thorough and therefore more accurate.
- Testing with more Anti-viruses. This would make the test more useful.
- Using the full, paid versions of the anti-viruses. This may make no difference but it would be better to be closer to a real situation.
- Not using the virtualbox additions. This may let the malware know that it is on a virtual machine, but in this case it made dealing with the anti-virus installation and transferring the malware samples far more efficient.
- Testing on different operating systems. It would be interesting to expand the scope of the test to different versions of windows to see if the anti-viruses are any more or less effective.
- Testing online and offline. In this case all the tests were done offline for security reasons, but it would be more thorough to test online too. The anti-viruses would then have access to constantly updated databases of malware and would probably perform far better.

REFERENCES

[1] Ted Samson. 2013. *Update: McAfee: Cyber criminals using Android malware and ransomware the most*. [online] Available at: https://www.infoworld.com/article/2614854/security/update--mcafee--cyber-criminals-using-android-malware-and-ransomware-the-most.html. [Accessed 26 April 2018].

[2] Adam L. Young, Moti Yung. 2018. *Cryptovirology: The Birth, Neglect, and Explosion of Ransomware*. [online] Available at: https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext. [Accessed 26 April 2018].

[3] Michael Kan. 2017. *Paying the WannaCry ransom will probably get you nothing. Here's why.*. [online] Available at: https://www.pcworld.com/article/3196880/security/paying-the-wannacry-ransom-will-probably-get-you-nothing-heres-why.html. [Accessed 26 April 2018].

[4] Dan Goodin. 2018. *You're infected—if you want to see your data again, pay us $300 in Bitcoins*. [online] Available at: https://arstechnica.com/information-technology/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/. [Accessed 26 April 2018].

[5] Alex Hern. 2017. *NHS could have avoided WannaCry hack with 'basic IT security', says report*. [online] Available at: https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office. [Accessed 26 April 2018].