

Report on Malware
Cieran Hughes
Academic and Employability Skills
Applied Computing

Abstract

In this report there will be information on:

- Malware and Viruses. An overview of what is and how it works. Followed by a section on how to get infected.
- Ransomware. An over view of Ransomware. A section on what to do if you are infected.
- CryptoWall and Trojans. This section of writing will include specifics of the threat and what it does to the device it is on. The file types that the infection encrypts. Seeing if it is possible to decrypt the files that it encrypts without paying the ransom, and how to do this to the main device, an external storage it is connected too, and a Dropbox account that is mapped as a device letter.
- Prevention from all the threats talked about in the report.
- Payment, which will include whether you should pay the ransom, how to pay the ransom and why the attacker chose bitcoin as a way of collecting the payment.

Contents Page

1. Malware and Viruses.....	1
1.1 Overview	1
1.2 How To Get Infected	1
2. Ransomware	2
2.1 Overview	2
2.2 What To Do If Infected	2
3. CryptoWall Trojans.....	2
3.1 Specifics Of The Threat.....	2
3.2 File Types It Encrypts.....	2
3.3 Is It Possible To Decrypt The Infected Files.....	3
3.4 How To Find The Files That Are Encrypted	3
3.5 How To Restore Encrypted Files Without Paying	3
3.5.1 Personal Device	3
3.5.2 Dropbox	4
3.5.3 NAS Drives	4
4. Prevention	4
4.1 Backups.....	4
4.2 Antivirus Software	5
4.3 Updates and Patches	5
4.4 The Links.....	5
5. Decrypting Files When Paying	5
5.1 Overview of Bitcoin.....	5
5.2 Should you Pay	6
6. Conclusion	6
7. Appendices	7

7.1 Appendix 1	7
7.2 Appendix 2	8
8. Bibliography	9

1. Malware and Viruses

1.1 Overview

Malware is Malicious Software that is designed to cause damage to the network or standalone device that it is put on too [1]. There are many different types of Malware that exist and each one will do something slightly different to a system. These different types can range from collecting data to sell, corrupting data or changing data without you knowing.

1.2 How To Get Infected

There are many different ways to get infected. The first one is spam emails, on the email there will be a link and if this link is clicked on then it will cause you to download the executable code that will run on your computer. The email will convince you to open the link as it will falsely say what will happen if you do, and this normally will sound like something that you will want [2]. Linked to spam emails, some attackers can use social engineering in order to trick people to open the attachments [3] as the email will look to be from friends, big companies or family.

The second way to get infected is by using infected removable media. There is a special type of malware that works this way and it is called a Worm. This type of malware works by infecting any type of removable hardware like Flash Drives, External Software or SD Cards [2]. When the removable storage device is plugged in to your device it will start a AutoRun file that will download the Malware to your device without you knowing, causing the malicious file to run [4].

Some viruses can be bundled in with other software downloads from the internet, third-party website, or file shares over a network [2]. These will be downloaded and then they will run in the background.

2. Ransomware

2.1 Overview

Ransomware is malicious software that will encrypt user files that they created and then will ask for payment to decrypt the files [3]. There are different types of ransomware, some encrypt the C: directory after 90 reboots [5].

2.2 What To Do If Infected

When you get infected you will be asked to pay the ransom so that your data can be decrypted [3]. If you do pay this ransom, it is not certain that your data will actually be decrypted and the attacker might ask for more money, or target you again. So it is said by some major security companies to never pay the ransom [3].

3. CryptoWall Trojans

3.1 Specifics Of The Threat

CryptoWall is a type of ransomware that will encrypt files on the compromised user's computer, it is a trojan horse that will ask the user to pay for the files to be decrypted [6].

Once the malicious software is downloaded it will install the infection installer to your computer. Once this is all done it will scan your drive and find files to encrypt. This can spread to attached devices and even Dropbox mappings. Once it finds supported files it can encrypt, it will add the pathway to a text document in to specific file. This will be used to show the user what files are encrypted. Once it is finished encrypting all the data then it will delete all the Shadow Volumes on the computer as this could be a way of getting copies of the encrypted files. Now the files are fully encrypted it will open a notepad window, containing instructions on how your files can become decrypted, by paying for the decryption service [7].

3.2 File Types It Encrypts

When the CryptoWall is executing it will encrypt all files that the user creates. From word processing, data processing and presentations like .docx .txt .xlsx .wpd .pptx. It

will also encrypt all music, video and photo files like .mp3 .mp4 .mov .jpg .cr2. Also, it encrypts many more file types (see Appendix 1) [8]. It does this so that no matter what files you've been working on, you will lose them. This will make the pool of targets larger as all people will have important files encrypted.

3.3 Is It Possible To Decrypt The Infected Files

Encryption is the process of encoding the data in a file, making it unreadable and scrambles [9]. The encrypted data is paired with an encryption key, this key is the only way of decrypting the data, turning it in to readable data [9].

This means paying the ransom is the only way of decrypting the data as by paying you get the encryption key and can decrypt the files using the CryptoWall Decryption Service [7].

3.4 How To Find The Files That Are Encrypted

As said under the, "CryptoWall Trojans - Specifics Of The Threat" heading, the file destinations are saved, this makes the user able to find the files that are encrypted on their machine [7]. The destination of these encrypted files (see appendix 2) is used by some companies to find and export the files. This is part of the process of cleaning up the computer is the user is not to pay the ransom. [7]

3.5 How To Restore Encrypted Files Without Paying

3.5.1 Personal Device

There are some ways of attempting to restore the files that have been decrypted, but most of the ways rely on the user having a process in place in case of this attack happening [7].

The first method is resorting the files from a backup of the machine or file [7]. If the user of the machine take regular backups of the device then it is possible that they can restore the device to an older state when the files weren't encrypted. Or if the user alternatively take copies of the files and stores them off the machine then they

won't be effected. This means that they can just get that copy of the file and use it. The problem with this method is if the user doesn't do these backups then this isn't an option for them.

3.5.2 Dropbox

If you have your Dropbox account mapped on the infected device as a drive letter, then the CryptoWall infection will attempt to encrypt all the files on Dropbox [7].

Dropbox offer a service to restore the files encrypted the files for up to 30 days. You can revert the file back to an earlier version which wasn't encrypted [10]. The only problem with this is that you can only revert one file at a time back to an earlier version [7]. Meaning if you have a lot of files on Dropbox and they are all encrypted then it will take the user a long time to restore them all.

3.5.3 NAS Drives

Like having a Dropbox account mapped on your device as a drive letter, having a NAS drive or any external device mapped on your device as a drive letter, they will also be infected by a CryptoWall infection [7]. To prevent the CryptoWall infection, infecting the NAS drive it is recommended to turn the device off or disconnect it from the internet. This means that the infected device won't be able to connect to the NAS drive, therefore the CryptoWall infection won't encrypt the NAS drive.

4. Prevention

There are lots of ways of preventing CryptoWall attacks, some need to be done manually and some can be done automatically.

4.1 Backups

This technique of backing up you device or files can be done manually or automatically. You can either manually set the backups to run on the device or manually drag the files over on the an external source, the other way is setting software to automatically backup the device or update the new files [11].

4.2 Antivirus Software

Antivirus software can protect your device from all types of attacks when updated regularly [11]. It stops malware executables from running and prevents them from executing [11].

4.3 Updates and Patches

When a vulnerability is found by the hackers, they will use this to exploit many devices [11]. When this happens the company's that the vulnerability is found in will release a patch to update to the system to fix it. If you don't install these updates then the user is affectively leaving a back door open to the hacker to gain access and run the attacks. If you keep the operating system of the device and all the applications running on the machine up to date then you have more of a chance not being hacked [11].

4.4 The Links

Another way of preventing from being attacked by a CryptoWall Attack is not allowing any downloads from unknowns sources. These downloads can come from spam emails [11]. When clicking on a link in a spam email a malicious downloads will commence. This could be the executable file for the CryptoWall Attack, or a way for the hacker to install the relevant software for the CryptoWall Attack to commence [11].

5. Decrypting Files When Paying

5.1 Overview of Bitcoin

Bitcoin is a peer-to-peer payment system, it can be sent to anyone in the world [12]. There is no government in charge of the currency and it is virtual [12], meaning that there is no physical representation of it.

Hackers use Bitcoin for its anonymity, you can convert your money to bitcoin, send money, and receive money without the need of using your name or any identity at all [13]. This makes it anonymous and untraceable because of the lack of identity,

therefore it is a hackers dream as they can receive untraceable funds for the crimes they commit [13].

5.2 Should you Pay

Most law enforcements discourage you from paying the ransom. The FBI said:

“Paying a ransom doesn’t guarantee an organization that it will get its data back - we’ve seen cases where organizations never got a decryption key after having paid the ransom.” [14]

As these are the types of people that hack and encrypt your files with no idea on how you are or how it will affect you, how do you know that they will give you the key once you’ve payed them, how do you know that they won’t just keep asking for more money.

6. Conclusion

To conclude, there are many ways of preventing from getting malware on your device, but they are all procedures you need to implement. It might feel like a waste of time doing these processes to prevent the attacks, but if one happens to you then you will be glad that you have put them in place.

7. Appendices

7.1 Appendix 1

.3dm	.c	.dgc	.iiq	.nsg	.pdf	.rwl	.txt
.3ds	.cdf	.djvu	.incpas	.nsh	.pef	.rwz	.vob
.3fr	.cdr	.dng	.indd	.nwb	.pem	.s3db	.wallet
.3g2	.cdr3	.doc	.java	.nx2	.pfx	.sas7bdat	.wb2
.3gp	.cdr4	.docm	.jpe	.nxi	.php	.say	.wmv
.3pr	.cdr5	.docx	.jpeg	.nyf	.pl	.sd0	.wpd
.7z	.cdr6	.dot	.jpg	.obj	.plus_muhd	.sda	.wps
.ab4	.cdrw	.dotx	.kc2	.ods	.plc	.sdf	.x11
.accdb	.cdx	.drf	.kdbx	.p7c	.pot	.sldm	.x3f
.accde	.ce2	.drw	.kdc	.r3d	.potm	.sldx	.xis
.accdr	.cer	.dtd	.key	.mov	.potx	.sql	.xla
.accdt	.cfp	.dwg	.kpdx	.flv	.ppam	.sqlite	.xlam
.ach	.cgm	.dxb	.lua	.wav	.pps	.sqlite3	.xlk
.acr	.cib	.dxf	.m	.dcs	.ppsm	.sqlitedb	.xlm
.act	.class	.dxg	.m4v	.cmt	.ppsx	.sr2	.xlr
.adb	.cls	.eml	.max	.ce1	.ppt	.srf	.xls
.agdl	.cpi	.eps	.mdb	.odb	.pptm	.srt	.xlsb
.ai	.cpp	.erbsql	.mdc	.odc	.pptx	.srw	.xlsm
.ait	.cr2	.erf	.mdf	.odf	.prf	.st4	.xlsx
.al	.craw	.exf	.mef	.odg	.ps	.st5	.xlt
.apj	.crt	.fdb	.mfw	.odm	.psafe3	.st6	.xltn
.arw	.crw	.ffd	.mmw	.odp	.psd	.st7	.xltx
.asf	.cs	.fff	.moneywell	.ads	.pspimage	.st8	.xlw
.asm	.csh	.fh	.mos	.odt	.ptx	.stc	.ycbcra
.asp	.csl	.fhd	.mp3	.oil	.py	.std	.yuv
.asx	.csv	.fla	.mp4	.orf	.qba	.sti	.zip
.avi	.dac	.flac	.mpg	.otg	.qbb	.stw	
.awg	.db	.fpx	.mrw	.oth	.qbm	.stx	
.back	.db_journal	.fxg	.myd	.otp	.qbr	.svg	
.backup	.db3	.gray	.nd	.ots	.qbw	.swf	
.backuppdb	.dbf	.grey	.ndd	.ott	.qbx	.sxc	
.bak	.dc2	.gry	.nef	.p12	.qby	.sxd	
.bank	.dcr	.h	.nk2	.p7b	.raf	.sxx	
.bay	.ddd	.hbk	.nop	.pages	.rar	.sxi	
.bdb	.ddoc	.hpp	.nrw	.pas	.rat	.sxm	
.bgt	.ddrw	.ibank	.ns2	.pat	.raw	.sxw	
.bik	.dds	.ibd	.ns3	.pcd	.rdb	.tex	
.bkp	.der	.ibz	.ns4	.pct	.rm	.tga	
.blend	.des	.idx	.nsd	.pdb	.rtf	.thm	
.bpw	.design	.iif	.nsf	.pdd	.rw2	.tlg	

7.2 Appendix 2

Format:

HKCU\Software\<unique computer id>\<random id>

Example:

HKCU\Software\03DA0C0D83CCC22DD0AAAD117\0113342BDEEEF.CryptoWall

8. Bibliography

- [1] B. Swain, "What are malware, viruses, Spyware, and cookies, and what differentiates them ?," Symantec, 25 June 2009. [Online]. Available: <https://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them>. [Accessed 22 November 2018].
- [2] "Microsoft Security," Microsoft, 09 October 2018. [Online]. Available: <https://support.microsoft.com/en-gb/help/4466968/windows-10-how-malware-can-infect-your-pc>. [Accessed 22 November 2018].
- [3] "Ransomware," Malwarebytes, [Online]. Available: <https://www.malwarebytes.com/ransomware/>. [Accessed 22 November 2018].
- [4] "Spreading Viruses on USB Thumb Drives," Ophtek, 30 January 2015. [Online]. Available: <https://www.ophtek.com/viruses-on-usb-thumb-drives/>. [Accessed 22 November 2018].
- [5] "Ransomware Blog," Malwarebytes, 13 December 2017. [Online]. Available: <https://blog.malwarebytes.com/threats/ransomware/>. [Accessed 22 November 2018].
- [6] L. O'Brien and J. Morparia, "Ransom.Cryptowall," Symantec, 19 June 2014. [Online]. Available: <https://www.symantec.com/security-center/writeup/2014-061923-2824-99>. [Accessed 22 November 2018].
- [7] "CryptoWall and HELP_DECRYPT Ransomware Information," BleepingComputer, 10 July 2014. [Online]. Available: <https://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information#CryptoWall>. [Accessed 22 November 2018].
- [8] Cyber Threat Alliance Founding Companies, "Analysis of the CryptoWall Version 3 Threat," October 2015. [Online]. Available: <https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf>. [Accessed 22 November 2018].

- [9] C. Mercer, "What is encryption?," 15 May 2018. [Online]. Available: <https://www.techworld.com/security/what-is-encryption-3659671/>. [Accessed 23 November 2018].
- [10] S. Brown, "How to Decrypt Dropbox Files Encrypted by Ransomware," intego, 6 October 2016. [Online]. Available: <https://www.intego.com/mac-security-blog/how-to-decrypt-dropbox-files-encrypted-by-ransomware/>. [Accessed 25 November 2018].
- [11] J. Petters, "The State of CryptoWall in 2018," Varonis, 6 January 2018. [Online]. Available: <https://www.varonis.com/blog/cryptowall/>. [Accessed 25 November 2018].
- [12] T. Mittal, "Bitcoin for beginners," YourStory, 28 November 2017. [Online]. Available: <https://yourstory.com/2017/11/bitcoin-beginners-guide/>. [Accessed 25 November 2018].
- [13] ECPIblog, "Why Do Hackers Use Bitcoin?," ECPI, [Online]. Available: <https://www.ecpi.edu/blog/why-do-hackers-use-bitcoin-and-other-cybersecurity-questions-answered>. [Accessed 25 November 2018].
- [14] A. Kujawa, "FBI announcement: paying the ransom is a bad idea," MalwareBytesLabs, 13 December 2017. [Online]. Available: <https://blog.malwarebytes.com/security-world/2016/05/fbi-announcement-paying-the-ransom-is-a-bad-idea/>. [Accessed 25 November 2018].