

Research, Referencing and Report Formatting on Ransomware



PRIFYSGOL CYMRU

Y Drindod Dewi Sant

UNIVERSITY OF WALES

Trinity Saint David

Siobhan Kelly Stephens

30/11/2018

Academic and Employability Skills

School of Applied Computing

University of Wales Trinity Saint David

Table of Contents

Abstract.....	3
1. Introduction	4
2. Methodology	4
2.1. What is Ransomware	5
2.2. How Ransomware Infects Devices	5
2.3. Case Study on the Cryptowall Trojan.....	6
2.4. Ransomware Effects on Business	6
2.5. Protecting Against Ransomware	7
3. Conclusion.....	8
4. References	8

Abstract

Ransomware is one of the biggest threats to internet users in present day. This report educates about malware and in particular, ransomware and how it can affect individuals and organisations. It discusses the recent CryptoWall attacks as a case study and offers recommendation on how to protect a system against a ransomware attack, and how to recover from an attack in a timely manner if one should occur, whilst mitigating against data loss.

1. Introduction

This aim of this report is to inform about the risks of malware, specifically ransomware, and to identify the ways in which to mitigate against it and recover from an attack should one occur.

Malware is a type of software that is written with the intent of causing damage to data or devices and can result in organisations ceasing to operate, loss of business and personal data and also loss of customer trust in a company, often with devastating effects [1]. Malware attacks are often seen in the news, with notable attacks including *WannaCry* in May 2017, which infected 230,000 computers across 150 countries, and Mirai, which targeted Netflix, Twitter and Reddit [2].

Ransomware is a form of Malware. Widespread use of the internet has provided a platform for the growth and spread of ransomware [3]. The principle of Ransomware is that it 'locks' a system or data by applying strong encryption and prevents the victim from accessing it unless a ransom is paid to the attacker [3]. Once the ransom is paid, the attacker promises to send the decryption key, however this often doesn't occur.

As many as 25 percent of businesses experienced more than 20 ransomware attacks in 2016, and Malwarebytes' Second Annual State of Ransomware Report, showed that of the 32 percent of companies hit by at least one malware attack in 2016, one fifth had to immediately cease operations [12].

A 4000 percent increase in crypto ransomware incidents plus a 113 percent increase in ransomware attacks was reported by Symantec [4], and more than 8.8 million systems were affected [5] in 2014 alone, proving that more must be done to protect systems against attack and to ensure the successful recovery of data.

2. Methodology

There are many types of malware used today other than ransomware, such types include:

Virus: Viruses spread throughout a host system and attach themselves to a legitimate executable file, which when opened by a user, may cause harm to data by corrupting or deleting files [6].

Trojans: These are disguised as legitimate software and are often used in conjunction with other malware in order to create *backdoors* to allow them and other hackers in [6].

Spyware: This is designed to capture a user's keystrokes, bank details, passwords and surfing habits [6].

Worms: These self-replicate across devices and networks by spreading to connected devices without interaction from a user.

2.1. What is Ransomware

Ransomware is a type of malicious software that encrypts data, such as personal files and system files. Ransomware prevents users from accessing them and threatens harm to the data unless payment is made. Ransomware was first seen in 1989 in the 'Aids Trojan' by Harvard-trained Joseph L. Popp, where approximately 20,000 copies of 'Aids Information' were sent out containing a program for a basic AIDS assessment. The program waited until the users had booted their PC a number of times until finally encrypting all system files and displaying a message demanding that the users pay a licence fee in return for the decryption key [7]. The fundamentals of this early case of ransomware are still used today.

2.2. How Ransomware Infects Devices

Ransomware can infect devices in many different ways, most commonly using social engineering. This is done by fooling users into believing they are downloading a legitimate program or opening an email from a reputable organisation, but instead an executable file containing the ransomware is downloaded and opened onto the system. Concurrently a pair of public and private keys are generated, with the public key being used to encrypt personal files, and the private key kept secret by the hacker. Subsequently files are encrypted throughout the system and a note is often displayed to the user, informing them that they have been a victim of a ransomware attack, and the steps they must take in

order to recover their data. This requires payment of varying amounts, likely increasing in amount after periods of time.

Other infection routes include *Malvertising*, where a user clicks on a paid illegitimate advertisement on a lawful website, which downloads the ransomware, or through security holes in out-of-date software, such as a web browser, where the ransomware is downloaded without the user's knowledge [7].

2.3. Case Study on the Cryptowall Trojan

CryptoWall can be dated back to September 2013, however became prominent in February 2014 [8]. According to the Cyber Threat Alliance, CryptoWall is one of the most lucrative and extensive ransomware movements affecting users of the Internet in present day [9], and in the 2015 report "The Internet Organized Crime Threat Assessment (IOCTA)", Europol considers ransomware as one of the key threats to the internet and its users [10].

CryptoWall differs from ordinary ransomware as it uses a very strong 2048-bit RSA encryption [11], which cannot be decrypted without the private key owned by the hacker, however the principles remain the same. According to Dell Secureworks Counter Threat Unit, "of nearly 625,000 infections, 1,683 victims (0.27%) paid the ransom, for a total take of \$1,101,900 over the course of six months" [8].

2.4. Ransomware Effects on Business

Ransomware attacks on businesses can be devastating if the business does not have measures in place to mitigate against them. According to Acutec, "54% of UK businesses have been victims of ransomware attacks, with 58% of those businesses paying the ransom. 60% of the attacks ask for more than \$1000 and 20% ask for more than \$10,000" [13]. Therefore, if a business decides to pay, they will suffer financially, despite the risks of not receiving the decryption key.

These attacks not only cause financial loss through demanding payment, but without suitable measures in place can cause significant down time, leading to loss of business, clients and therefore income, in fact 63% of businesses that became victims of attack said that it affected their clients and daily operations, plus 34% have not been able to recover files that are essential to the operation of the business [13], leaving them with further down time until recovery.

Other financial and legal impacts of a ransomware attack on a UK organisation if a data breach was to occur includes fines of up to 4% of annual global turnover or €20 million, from the Information Commissioner's Office due to the 2018 General Data Protection Regulation [14].

2.5. Protecting Against Ransomware

In order to protect your business against ransomware and to ensure effective and timely recovery of data and business operations if an attack did occur, the following measures are recommended.

1. Establish a robust backup and recovery plan. Regularly back up data with offline backup media. Backups made to locally connected, network-attached, or cloud-based storage are not sufficient as these can be penetrated and therefore encrypted by ransomware such as CryptoWall [8]. Backups must be regularly tested to ensure they are complete and are not corrupted.

The purpose of a robust backup and recovery strategy is so that in the case of an attack, data can be retrieved from a range of different secured sources and recovered in a timely manner.

2. Ensure sufficient security measures are put in place. Firewalls, anti-virus software and physical security such as locked doors, and disabled USB ports should be utilized, along with blocking all unnecessary websites and even attachments in emails. These security measures aim to mitigate the infection of malware via methods ranging from physical file

transfer from a USB drive, to accessing unlawful websites containing malware, and an unwitting employee opening a malware attachment in an email.

3. Staff training. Comprehensive staff training should be employed so that staff are made aware of the risks of such malware, plus how to protect against an infection and the steps involved in a successful recovery if such an infection should occur.

3. Conclusion

In conclusion, all individuals who access the internet should be concerned with the use of malware and should ensure they utilise measures to protect themselves and their data.

Organizations in particular have the most to lose, and so they should consider the points made above regarding protecting themselves and compare them to their current security practices, to ensure they are not one of the businesses who does not survive an attack.

4. References

- [1] "What is malware (malicious software)? - Definition from WhatIs.com." [Online]. Available: <https://searchsecurity.techtarget.com/definition/malware>. [Accessed: 21-Oct-2018].
- [2] "The 10 best (or should that be worst?) malware attacks | IT PRO." [Online]. Available: <https://www.itpro.co.uk/security/innovation-at-work/29577/the-10-best-or-should-that-be-worst-malware-attacks>. [Accessed: 21-Oct-2018].
- [3] R. S. Sajjan and V. R. Ghorpade, "Ransomware attacks: Radical menace for cloud computing," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 1640–1646.
- [4] K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall," *IEEE Netw.*, vol. 30, no. 6, pp. 14–20, Nov. 2016.
- [5] J. S. Aidan, H. K. Verma, and L. K. Awasthi, "Comprehensive Survey on Petya Ransomware Attack," in *2017 International Conference on Next Generation*

Computing and Information Systems (ICNGCIS), 2017, pp. 122–125.

- [6] Roger A Grimes, “8 types of malware and how to recognize them | CSO Online.” [Online]. Available: <https://www.csoonline.com/article/2615925/security/security-your-quick-guide-to-malware-types.html>. [Accessed: 21-Oct-2018].
- [7] “What is Ransomware: Guide to Protection and Removal | AVG.” [Online]. Available: <https://www.avg.com/en/signal/what-is-ransomware>. [Accessed: 21-Oct-2018].
- [8] Dell SecureWorks Counter Threat Unit™ Threat Intelligence, “CryptoWall Ransomware Threat Analysis | Secureworks,” 2014. [Online]. Available: <https://www.secureworks.com/research/cryptowall-ransomware>. [Accessed: 20-Oct-2018].
- [9] Cyber Threat Alliance, “Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat.”
- [10] Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2015,” 2015.
- [11] L. O’Brien and Jeet Morparia, “Ransom.Cryptowall | Symantec.” [Online]. Available: <https://www.symantec.com/security-center/writeup/2014-061923-2824-99>. [Accessed: 21-Oct-2018].
- [12] Claire Reilly, “Ransomware shuts down 1 in 5 small businesses after it hits - CNET.” [Online]. Available: <https://www.cnet.com/g00/news/malwarebytes-state-of-ransomware-shutting-down-1-in-5-affected-small-businesses/?i10c.ua=1&i10c.encReferrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8%3D&i10c.dv=11>. [Accessed: 04-Jan-2019].
- [13] “How Ransomware Affects Businesses.” [Online]. Available: <https://www.acutec.co.uk/blog/ransomware-affects-businesses>. [Accessed: 21-Oct-2018].
- [14] “GDPR Penalties and Fines | IT Governance UK.” [Online]. Available: <https://www.itgovernance.co.uk/dpa-and-gdpr-penalties>. [Accessed: 21-Oct-2018].