Ramsonware: Holding your Data Hostage

Erik Miranda Lopez, Seo Yeon Moon, Jong Hyuk Park
Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, 139-743, Republic of Korea
e-mail : erik.miranda.lopez@gmail.com, {moon.sy0621, jhpark1}@seoultech.ac.kr

Abstract

In the recent years ransomware has become one of the most popular malware used by criminals. This particular type of malware is notorious for locking users' data or systems and unscrambling it only after the victims pay a fee. With more and more individuals, companies and public agencies being targeted and the ransom being as high as $17,000, the need for countermeasures against this kind of malware is greater than ever. This paper explores how the malware infects and encrypts its victims. Then, it suggests mitigation techniques based on how the ransomware spreads, making special emphasis on countermeasures in order to protect end-users.

1. Introduction

Ransomware is increasing its popularity between cyber-criminals as more and more attacks are making headlines on mainstream media. Recent examples include Lincolnshire County Council (UK), which was blackmailed into paying $500, [1] and Tinseltown hospital (US), which paid $17,000 ransom to release their computer systems [2]. According to data gathered in 2014 by Dell's research team, estimates a single ransom-payment server collected up to $1.1 million in a six-month period [3]. Although most incidents may go unreported, the Australian government claims 72% of business experienced ransomware incidents in 2015 [4]. This increase of incidents and lucrative payments may well explain why ransomware is at its peak of popularity.

This paper describes how ransomware reaches its victims – it could either be by email attachment, payload or compromised website – and it also explains how the data is locked once the malware infects their systems. Once the attack vectors are understood, the paper recommends countermeasures to reduce the probability of getting infected and mitigations to reduce its impact.

2. Related Work

This section describes ransomware and explains how it works. It is essential to first understand the enemy in order to protect against it.

Ransomware: Ransomware is a type of malicious software or malware known for its data-kidnapping capabilities [5]. This kind of malware can either prevent users from using their systems or accessing their data and then blackmails them. It demands its victims to pay a ransom in order to remove the restriction. Although the infection may be removed with anti-malware tools, it is impossible to recover the locked files [6].

Ransomware is profitable for cyber-crooks because many victims decide to pay rather than face the shame of false accusations. Or simply because they urgently need their data back.

Spreading Method: Before ransomware denies access to the system, it needs first to reach its target. The malware can spread through various infection vectors:

Compromised/Malicious websites: Users might be tricked into downloading this threat from malicious or compromised sites [3]. The users may unwittingly download the ransomware or simply be under the impression of downloading another file.

Email attachments: Users may also be deceived into opening malicious attachments by using social engineering techniques [6]. These methods usually involve “act fast” subjects such as tax returns deadlines, fines or lawsuits and “bargain” sales. Sometimes the emails will simply try to exploit the receivers’ curiosity factor like the well-known ILOVEYOU virus. Hence, users feel compelled to open the attachment without considering the source.

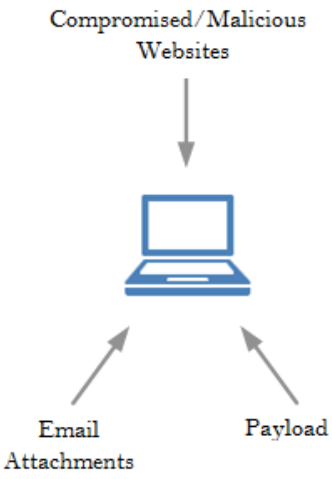
Payload: Ransomware can also arrive from an already concealed malware in the system [3]. The malware might be able to drop or download the ransomware with the aim of locking the system or data.

As soon as the ransomware is executed, it can either lock the whole system or encrypt certain files depending on its purpose [3]. If it locks the system, the ransomaware will prevent users from using their own system at all. In the second scenario, the ransomware will lock predetermined files such as .doc, .xls and .pdf [7]. The next section explains how this is achieved.

File Encryption: Most recent ransomware, such as Cryptolocker and Onion, use a combination of symmetric (same key to encrypt and decrypt) and asymmetric (one key to encrypt, one to decrypt) encryptions to lock victims' files or systems [7].

Acknowledgments

This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2015-H8501-15-1014) supervised by the IITP(Institute for Information & communications Technology Promotion)



(Figure 1) Infection Vectors

Briefly explained, once the ransomware is run, it generates a random symmetric key to encrypt predefined files like documents and pictures or critical files used by Windows. Then, it connects to randomly generated domains to download a public key of 1024 or 2048 bit [8] – recently 4098 bit keys have started to be used too. The ransomware uses this public key to encrypt the random symmetric key generated earlier, ensuring only the attacker, who's in possession of the private key, can access it [7]. The final result is either the whole system or files being completely inaccessible. Although it is possible to remove the malware with antivirus and similar tools, the data will be still unavailable [6]. At this stage is when the victims receive a ransom note demanding a payment and with instructions on how to unlock their systems or data.

Usually ransomware will ask the victims to purchase Bitcoin and transfer them to the malware writer. Once the transaction is complete, the victims should receive –though there's no guarantee - the private key needed to decrypt their data.

The use of asymmetric encryption makes it virtually impossible to decrypt the data using brute-force or similar techniques; therefore, it's mostly important to prevent the malware from reaching the system in the first place.

3. Proposed Countermeasures

Earlier the paper explained how the ransomware can reach its targets via email attachments, compromised websites or payload. Taking into account the malware's attack vectors, a variety of countermeasures are presented to prevent or mitigate the threat of ransomware.

This paper suggests two types of mitigation strategies; one is all about informing about the risks, for example, educating users about the threats and risks; the other one focuses on mitigating the risk, by putting countermeasures in place.

3.1. Inform about the risk

This section is all about educating users as they are the weakest link in any computer system:

Threat and Risk: Users – especially careless users – can pose a threat to their own system. Hence, educating them about ransomware and its risks shouldn't be overlooked. Aware users are more likely to take a pro-active approach to defend their systems.

Safe Internet Browsing: Users should be careful when browsing the internet; pop-ups, deceptive links and clickable graphics can lead to infections. Therefore users should avoid questionable sites and only download from trusted sources.

Email attachments: If a spam or phishing email goes undetected through the spam filters, avoiding opening attachments, particularly from senders you don't know or from emails you were not expecting, will greatly reduce the chances of being infected.

Don't pay up: Paying for the ransom will only make ransomware a highly profitable business model, thus contributing to more sophisticated attacks. Furthermore, there's no guarantee the victims will either get their data back or won't be targeted and blackmailed again in the future.

3.2. Mitigate the risk

Unprotected systems are like an open door for threats. This section proposes some countermeasures to reduce the likelihood and impact of ransomware infection based on its attack vectors.

Spam Prevention: As previously described, ransomware spreads via email exploiting social engineering techniques. Therefore, preventing spam from reaching end-users is one of the most important countermeasure solutions.

Anti-malware: Antivirus or similar security solutions should be turned on at all times. Additionally, their databases should also be kept up to date. This will help detecting infected downloads from compromised or malicious websites and stopping other malware that may open a back-door for the ransomware. Moreover, both commercial and open-source security software might have some sort of in-build anti-spam solution and they may also scan email attachments, thus greatly reducing the likelihood of infection. Unfortunately, some email-clients automatically download attachments, voiding anti-malware protection.

Software Updates: Ensure your operating system and software have the latest patches by performing regular updates. These fixes should reduce the flaws found on software and will reduce the attack vector thus reducing the ransomware chances of arriving as payload.

Hash Checks: Checking downloads using MD5, SHA1 or SHA256 to ensure the file hasn't been compromised or replaced. Despite download websites don't always provide hashes, it is a good idea to verity the integrity of the file.

Firewall: Both software and hardware firewalls monitor and analyse the traffic to identify and block unwanted connections. This can help blocking known-vulnerability exploits on applications and OS as well as malware connections.

Backup Management: Though backups won't stop the ransomware from getting onto the system, once disaster strikes, only a good functional backup may be the difference between losing and keeping all your critical data. Moreover, care needs to be taken as the malware could have been on the system before the lock-down and already been included on

the backups.

Bear in mind that a compromised system should never be trusted. Even if the restore causes a long downtime, it is preferable to restore the backup to a new, clean system.

3.3. Analysis

This section analyses the proposed countermeasures against the ransoware infection vectors:

<Table 1> Countermeasures vs. Ransomware Infection Vectors

	Compromised Website	**Email Attachment**	**Payload**
Spam Prevention	No	**Yes**	No
Anti-malware	**Yes**	No*	**Yes**
Software Updates	No	No	**Yes**
Hash Checks	**Yes**	No	No
Firewall	**Yes**	No	**Yes**

Anti-malware solutions not always include anti-spam protection. Also some mail-clients automatically download attachments, which may be already too late for the anti-malware to detect and stop the ransomware.

As the table demonstrates, there's no complete solution to effectively prevent ransomware from reaching the system. Therefore, a combination of multiple countermeasures is highly encouraged. Moreover, multiple countermeasures protecting against the same infection vector will greatly reduce the rate of false-negatives and the chances of being hit by this notorious malware.

4. Conclusion

This paper defined ransoware as a data-kidnapping malware that blackmails its victims after locking their data. The paper also described how the malware can spread by email, payload or compromised websites. In addition, it was explained how the malware encrypts its victims data using a combination of symmetric and asymmetric encryption techniques.

More importantly, the paper provided a variety of countermeasures to prevent and mitigate the ransomware: to prevent spread by email, the paper suggests the use of anti-spam technologies and also avoid opening attachments of not solicited emails; to prevent spread by malicious websites, check the hashes and keep the anti-virus always up-to-date; to prevent spread by payload, keep the OS and software with the latest fixes and patches. Moreover, the paper also recommended a good functional backup system and not falling for the blackmail as there's no guarantee the victims will get their data back.

Reference

[1] “Lincolnshire County Council 'will not paycyber ransom”, BBC News, 2016, Retrieved from: http://www.bbc.com/news/uk-england-lincolnshire-35453801

[2] “Los Angeles Hospital Pays Hackers $17,000 After Attack”, New York Times, 2016, Retrieved from: http://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html?_r=0

[3] Dell SecureWorks Counter Threat Unit Threat Intelligence, “CryptoWall Ransomware”, Dell, 2014

[4] Australian Government, “2015 Cyber Security Survey: Major Australian Businesses”, Australian Cyber Security Centre, 2015.

[5] Alexandre Gazet, “Comparative analysis of various ransomware virii”, Journal in computer virology, Springer, Vol 6, Issue 1, PP. 77-90, 2010.

[6] Kim Donghyun, Soh Wooyoung, Kim Seoksoo, “Design of Quantification Model for Prevent of Cryptolocker”, Indian Journal of Science and Technology, Vol 8, Issue 19, 2015

[7] Luo Xin, Liao Quin, “Awareness Education as the key to Ransomware Prevention”, Information Systems Security, Taylor & Francis, Vol 16, Issue 4, PP. 195-202, 2007.

[8] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, Engin Kirda, “Cutting the gordian knot: a look under the hood of ransomware attacks”, Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Vol 1, Issue 4, PP. 3-24, 2015.