

CryptoWall, Ransomware, security brief

1. Abstract

A brief overview on ransomware detailing common methods of attack, the effects of an attack and possible mitigation and recovery steps. Also a more detailed breakdown on the specifics of the ransomware CryptoWall.

2. Contents

1. Abstract
2. Contents
3. Introduction to ransomware
4. Ransomware in general
 1. Method of attack
 2. Effect of attack
 3. Mitigation and data recovery
5. CryptoWall
 1. Method of attack
 2. Effect of attack
 3. Mitigation and data recovery
6. References

3. Introduction to ransomware

Ransomware is a type of malware that blocks access to files and then requests a ransom if the victim wishes to regain access to those files. Ransomware uses many attack vectors varying from posing as attachments to exploiting system vulnerabilities through malicious websites to infect systems. It then typically proceeds to encrypt user files or restricts access to files and subsequently displays a ransom note demanding payment in exchange for access or the decryption key.

4. Ransomware in general

4.1 Method of attack

There are a few different ways that ransomware can infect computer systems. A common way is as a Trojan file attachment to an unsolicited email, such as a PDF or Word document. These attachments look like normal documents but when they are run they can easily infect the computer system.

Another method to deliver ransomware is Malspam, which is a method to trick users into clicking or downloading files that appear from a trusted source. Often these malicious websites appear very similar to genuine sites but with only minor differences, such as a typo in the url, using social engineering to deceive users.

Advertising can be exploited to redirect unsuspecting users to malicious websites that exploit a browser vulnerability to deliver the ransomware. These malicious websites scan and profile users in the background in order to find the most effective way of delivering the malware payload, often through a known software vulnerability [1].

4.2 Effect of attack

The effects of a ransomware attack can vary from popups to total data loss. Some ransomware will only attempt to scare the user into paying the ransom, either through popups or full screen windows that demand payment. Other more damaging variants will encrypt files to varying degrees, making data recovery difficult if not impossible without the decryption key [1].

4.3 Mitigation and data recovery

Having a robust and up to date backup strategy will help mitigate most if not all of the damage done by ransomware. If the files held at ransom are easily restored or backed up in another location then the ransomware can be removed through either a anti-malware security product or a full system re-install.

If a backup of the ransomed data is not available then specialized decryptors are available for some infections and scanning for infections using an anti-malware security product can help in some instances [1].

In the worst case scenario where no backup is available and no anti-malware product can restore access to files, paying the ransom is not recommended as suggested by the FBI [2]. They state that many organizations never get a decryption key and could embolden criminals to further develop and utilize this method for criminal gain.

5. **CryptoWall**

5.1 Method of attack

CryptoWall can target all version of windows [3] and can use many different infection methods. The most common attack vector being from a phishing email, which can use social engineering to encourage users to click a download link for the malware. The second most common method is to take advantage of known software vulnerabilities through exploits to directly infect systems. The final method being through malicious advertising to install the malware unbeknownst to the user [4].

5.2 Effect of attack

A CryptoWall attack is one of the more damaging forms of ransomware due to its improved and widespread encryption. The malware will initially install itself into a background windows task, meaning it cannot be removed easily through a system reboot.

Once running as a background task it will communicate with its base server to get an encryption key, then it will scan and encrypt any personal files it finds. The encryption algorithm used varies according to the version of the CryptoWall infection, the old versions preferring RSA-2048 whilst the newer versions use AES-256 encryption. These encryption methods are cryptographically strong and a brute force attempt to find the decryption key is infeasible due to the time to traverse all possible combinations. It will try to encrypt files on the local machine as well as files on any connected network devices. Newer version also encrypt files names, making data recovery even more difficult [3].

5.3 Mitigation and data recovery

Taking steps to target each of the common attack vectors can reduce to risk of initial infection. Utilizing real time scanning anti-malware security products that have protection in place against the exploits used by CryptoWall can mitigate from initial infections [5]. Educating users on possible phishing attempts and not clicking on links and attachments can also prevent initial infection. Using a local firewall can also halt a CryptoWall attack as the malware would be unable to connect to its base server to retrieve an encryption key to begin the attack. Updating and keeping systems up to date with current security patches can help mitigate known avenues for the malware to exploit. If an infection does occur then having a backup and restore strategy can render the attack useless as the data and system can be restored to a previous known good state.

Systems can also be set up with a minimal privilege model, so that in the event the malware does gain access it has insufficient privileges to execute the attack.

Again as recommended by the FBI, paying the ransom is not recommended as getting the decryption key is not guaranteed. [2][4][5]

References

- 1: , All about ransomware, <https://www.malwarebytes.com/ransomware/> [Accessed 18/06/2019]
- 2: , Incidents of Ransomware on the Rise, 2016 Apr <https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise> [Accessed 18/06/2019]
- 3: , CryptoWall and HELP_DECRYPT Ransomware Information Guide and FAQ, 2014 Jul <https://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information#cryptowall4> [Accessed 18/06/2019]
- 4: Jeff Petters, The State of CryptoWall in 2018, 2018 Jan <https://www.varonis.com/blog/cryptowall/> [Accessed 18/06/2019]
- 5: O'Brien Laura, Morparia Jeet, Ransom.Cryptowall, 2016 Sept <https://www.symantec.com/security-center/writeup/2014-061923-2824-99> [Accessed 18/06/2019]