Analyzing Ransomware Attacks and Exploring Methods of Prevention

Andres Perez with Advisor: Dr. Daehee Kim
California State University Stanislaus, Computer Science Department, Turlock, CA 95382

Abstract

Ransomware is one of the fastest growing and dangerous type of malware that has appeared in the last couple of years, as it has caused the most damage to industries and individuals alike. This attack has caused billions in damages, and new ransomware attacks are constantly being developed and released around the world. We explore how the malware operates in depth, and cover methods of protecting against it in hopes of creating long-standing solutions to this problem.

Introduction

Ransomware is a type of malware that infects a user by taking over their system and encrypting or locking them out of their data and demanding some kind of fee in return for access to said data. The attackers generally encrypt a system and hold the 'key' for ransom. Businesses and large corporations lose billions a year to these types of attacks, so It's important to understand how this attack works to understand how to prevent it.

Types of Ransomware

- Locker Ransomware – This type of ransomware locks the user from accessing their files, but doesn't use encryption, so it's easier to combat and files can still be accessible.
- Crypto Ransomware – Encrypts the user's files and hides the 'key' that decrypts information. Symmetric or Asymmetric encryption used, or both.
- Hybrid Ransomware - Combines elements of both locker and crypto type ransomware. Encrypts files and disables functionality of system. Uses similar encryption methods as the crypto type ransomware as well.

Five Steps of Infection

1) First the malware infects the host, generally through email phishing scams or exploit kits.
2) Files are installed on the host's computer undetected.
3) Malware deletes any backups on the system to eliminate any chance of recovery.
4) Malware encrypts all files very rapidly with varying extensions and attacker keeps key.

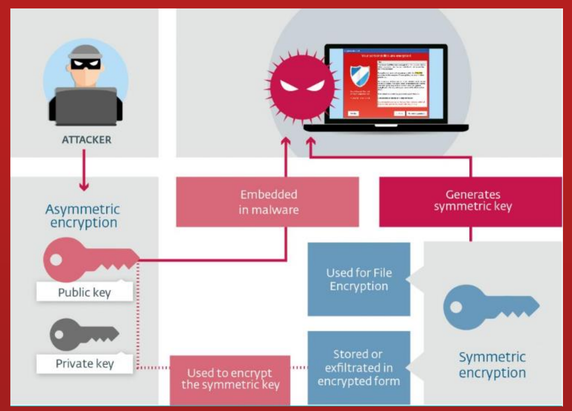

Figure 1. Using both asymmetric and symmetric encryption to lock data.

5) Malware disables system functionality, prompts user and demands money for stolen files.

Figure 2. WannaCry ransomware prompting user

Ransomware in the Real world

WannaCry:

- Attack launched May 2017
- Utilized exploit discovered by the NSA against Windows Operating System.
- Affected over 200000 computers across 150 countries.
- Propagates itself without human interaction to infect new hosts (worm).
- Caused an estimated billions of dollars in damage.

Figure 3. WannaCry's affect in different countries

Attack Prevention and Conclusion

There are no long-standing solutions to Ransomware attacks aside from paying the ransom. The only real way to combat these attacks is by preventing them. These methods include:

1. Make sure all devices are up to date
2. Make isolated backups
3. Be weary of links and attachments especially through email
4. Browser-side plugins and pop-up blocker enabled
5. If you become infected, make sure you disconnect immediately from any network, as it can spread.

References

1. Wira Zanoramy A. Zakaria, Mohd Faizal Abdollah, Othman Mohd, and Aswami Fadillah Mohd Ariffin. 2017. The Rise of Ransomware. Proceedings of the 2017 International Conference on Software and e-Business - ICSEB 2017(2017). DOI:http://dx.doi.org/10.1145/3178212.3178224
2. Abhijit Mohanta, Mounir Hahad, and Kumaraguru Velmurugan. 2018. *Preventing ransomware: understand, prevent, and remediate ransomware attacks*, Birmingham: Packt.
3. Cassius Puodzius. 2016. How encryption molded crypto-ransomware. (September 2016). Retrieved April 29, 2019 from https://www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware/
4. Anon. 2019. WannaCry ransomware attack. (April 2019). Retrieved April 29, 2019 from https://en.wikipedia.org/wiki/WannaCry_ransomware_attack