Theresa Nguyen

Investigation of Cryptology by Malware

Introduction

On October 3, 2017, Yahoo announced that every single account was affected by 2013 attack—3 billion accounts. Every day, billions of people use the Internet with the risk of exposing themselves to cyber-attacks. To defend from these attacks, cryptology is used to protect the user’s information. On the other side, cryptovirology is used to enter computer system. To define, cryptovirology is the study of cryptology to create malicious software. It is the use of cryptology in an offensive way to extort and steal information. Thus, the topic extends to kelptography, which is the study of taking information securely without user’s notice. This project will analyze these topics in depth and illustrate potential attacks. Furthermore, the project will demonstrate common protocols attackers use when gathering information.

Problem Area

As news of cyber security attacks increase each day, there is little understanding to what information an attacker targets for and why, especially for the average individual. What methods and protocols are they using to enter big businesses? How are attackers using mathematics to obtain information? If a student is learning cryptology, should they have skills in cryptovirology as well?

Initial Deliverable

Project will deliver information regarding the difference between cryptology and cryptovirology. Methods and protocols will be released as well, but not from the eyes of the defender but the attacker. This will include some code if found. If possible, some example code will be demonstrated live. Furthermore, the project may include methods of protection and possibly the attacker’s purpose if found.

Project Components

Possible code that can demonstrate what attackers use will be in Python. This project will also highlight the use of public keys and hardware encryption and decryption. This project will be mainly focused on research and delivering information.

Bibliography

“Cryptovirology.” Wikipedia, Wikimedia Foundation, 9 Sept. 2017, en.wikipedia.org/wiki/Cryptovirology.

Young, Adam, and Moti Yung. “Cryptovirology: Extortion-Based Security Threats and Countermeasures.” ResearchGate, ResearchGate, 13 Oct. 2013, [www.researchgate.net/publication/2301959\_Cryptovirology\_Extortion-Based\_Security\_Threats\_and\_Countermeasures](http://www.researchgate.net/publication/2301959_Cryptovirology_Extortion-Based_Security_Threats_and_Countermeasures).

Young, Adam. “Cryptovirology FAQ”. 20, Nov. 2004, https://download.adamas.ai/dlbase/ebooks/VX\_related/Malicious%20Cryptography%20Cryptovirology%20and%20Kleptography.pdf