

Constructing Malicious Ransomware In Python

Aidan Rubenstein ar2126@rit.edu Andrew Giannone atg5232@rit.edu

Evan Hirsh exh7928@rit.edu ■ ■ ■ Advisor: Dr. Rajendra K. Raj rkr@cs.rit.edu

Introduction

- Popularity of ransomware has increased drastically
- Responsible for some of the largest attacks and loss of capital globally by malware
- This study is motivated to build, test, and observe ransomware so that it can be better understood and mitigated

Ransomware

- Ransomware is a type of malware that renders users' files inaccessible by encrypting them with a key known only to the attacker.
- In most cases, a ransom in the form of cryptocurrency is demanded by the malicious actor, hence the term ransomware [1]
- In 2019, the average payment requested to release files from ransomware was \$84,116. This has been steadily increasing.
- the notable "WannaCry" ransomware affected businesses and users in over 150 countries and cost an estimated \$4 billion in financial losses [6]

WannaCry Ransomware

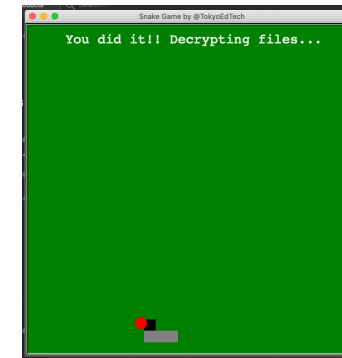


Our Program

- We built a simple ransomware in python using easily available resources, packaged into an executable, and targeting Windows machines.
- We do not want the executable to be used maliciously for actual ransomware purposes
- To solve this, it does not encrypt data by default, and asks consent from the user.

System Design

- Detects the home directory on Windows, and encrypts all files
- Decrypts the files only if the user scores 3 points in a game of snake
- Downloaded and executed via malicious VBA Office macro
- Utilizes the python cryptography library to implement AES
- Utilizes a modified open source snake game written in python



```
evan@evans-macbook ~/repos/evanextreme/CSCI455 master gametheory
Hello. Welcome to game theory.
THIS IS A MALWARE DESIGNED TO ENCRYPT YOUR WHOLE SYSTEM. Currently it is operating in SAFE MO
DE, which means nothing will be encrypted. If you would like to turn safe mode OFF, type TURN
OFF SAFE MODE and press ENTER. Otherwise, press [ENTER] TURN OFF SAFE MODE
YOU WILL LOSE EVERYTHING. PRESS [ENTER] IF YOU ARE OK WITH THIS
I don't believe you. Input the seventh word of the bee movie script below and press [ENTER] if
you understand this
Hint: "According to all known laws of aviation, there is no way that a bee should be able to f
ly"
The word is: aviation
```

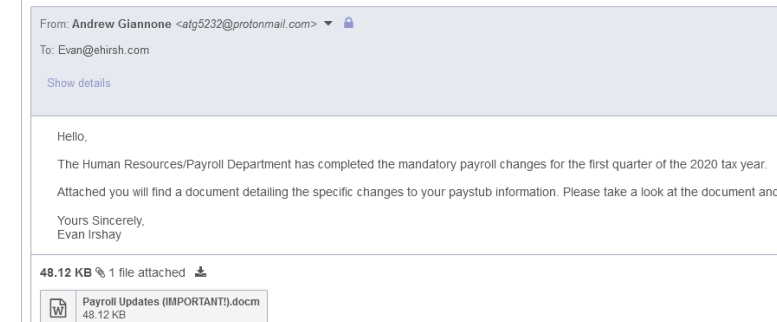
Implementation



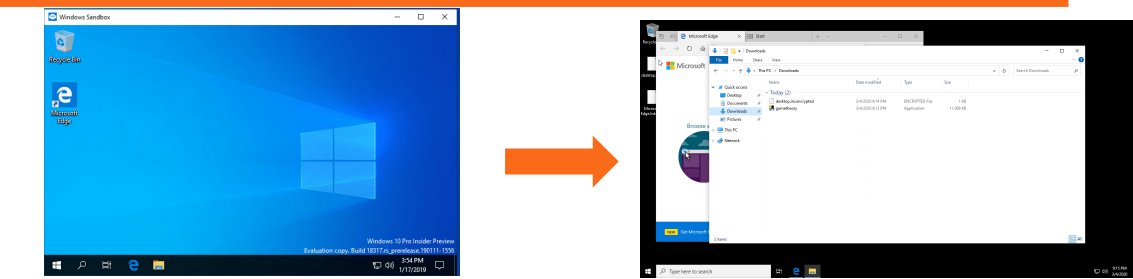
The Phish

- We created a phishing email which includes a word doc with a macro that downloads our ransomware exe
- Looks completely innocuous, can be sent from any compromised account
- Not flagged as spam

Important Payroll Information



Results



Before

After

- **Before:** A clean uncompromised Windows Sandbox environment.
- **After:** A fully encrypted user directory, compromising even the desktop images.

Future Work

Parallelizing Encryption

- Encryption / Decryption runs serially
- Each file can be edited using a thread in a map pool

Circumventing Security

- Our program and macro was detected by the system at multiple points. This can potentially be improved.
- Chrome, Edge, and Windows Defender all saw the EXE as malicious.
- Office parses macros and flags any that download/execute payloads

Summary

- We determined that a ransomware is easy to implement in most languages
- Modern copies of Windows by default does an excellent job of detecting ransomware, but older versions deployed in enterprises do not.
- To protect these systems, it is imperative that files are backed up routinely and securely in offside or cloud locations.

References

- U.S. Cybersecurity and Infrastructure Security Agency. 2019. Ransomware.(2019). <https://www.us-cert.gov/Ransomware>
- Kaspersky Lab. 2018. What are the different types of ransomware? (2018). <https://www.kaspersky.co.uk/resource-center/threats/ransomware-examples>