DECEIVING RANSOMWARE WITH ENDPOINT DECEPTION HAX

STUDENTS: Hunter Camfield, Lexie Chau, Wayne Lai, Michael Phenicie, Brendan Weibel

VERAMINE

Motivation

- Ransomware attacks are becoming more prevalent in the world.
- Some ransomwares are designed to avoid computers with certain configurations.
- With this project, we hope to find common configurations that these ransomwares check for and exploit them as a technique to obstruct ransomware encryption.
- We also wanted to find ways to expedite the testing process to allow for rapid testing in the future.

Requirements

- Our primary goal is to create a testbench that can be used to understand future ransomware.
- The testbench allows analysts to quickly create a testing environment and automate the testing process.
- The dynamic testbench receives a ransomware sample as input then provides efficacy score as output.
- The static testbench gives useful information about the binary file.

```
----------GetLocaleInfo----------
GetLocaleInfo at 411d50
GetLocaleInfo at 4140c0
GetLocaleInfo at 414fd8
GetLocaleInfo at 418f22
----------CreateFile----------
CreateFile at 4067a3
CreateFile at 411d50
CreateFile at 4140c0
CreateFile at 414fd8
CreateFile at 418f22
----------ReadFile----------
ReadFile at 414080
ReadFile at 4140c0
ReadFile at 414fd8
ReadFile at 418f22
----------WriteFile----------
WriteFile at 4124e2
WriteFile at 4140c0
WriteFile at 414fd8
WriteFile at 418f22
```

Methods

Our primary design was to have two main areas of research towards ransomware; static analysis and dynamic analysis.

Dynamic

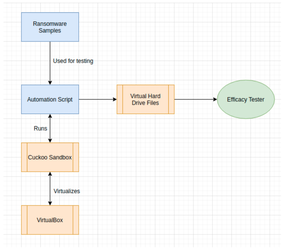
- Objective: install and automate a sandbox to which we could extract information about the ransomware to research its behavior.
- First researched the best sandboxing tools and determined the industry standard is Cuckoo Sandbox.
- Had difficulties installing Cuckoo Sandbox until Cindy Jenkins from UW Medicine Cybersecurity helped us.
- Once Cuckoo Sandbox was running, we wrote python scripts to automate the testbench environment.
- Used the Cuckoo API to automate inserting files into Cuckoo and storing the virtual machine image.
- Then installed and used Binwalk API to write a script to calculate the average entropy of file system which contributed to an efficacy metric.

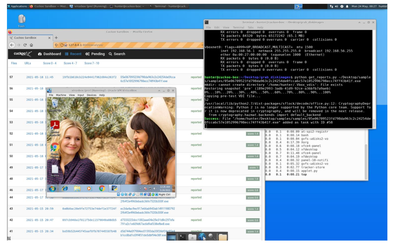
Static

- Objective: analyze the information that was collected either from ransomware samples or from the information given to them by the dynamic analysis team to further decrypt ransomware and find mitigation techniques.
- Gathered malware samples from sites like MalwareBazaar, any.run, etc.
- Loaded the sample into IDA Pro.
- We looked for exit conditions which signal potential exploits to abort the encryption process.
- After unsuccessful attempt at several Ryuk samples, we turned to Rapid 2.0, which checks Russian locale before running.
- Wrote script to tell locations of common ransomware calls to Window's API.

Automated Testing System

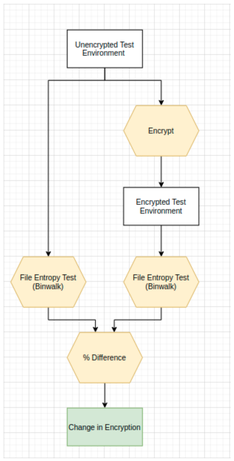
- Using software called Cuckoo Sandbox, which lets us run individual ransomware samples in a controlled environment, we could run ransomware one sample at a time.
- Our automated system then streamlines this process, making it easy to run many samples and get analytical information from each sample, and potentially find insights of a ransomware's interworking.
- The testing system also feeds virtual hard drive images to the efficacy testing system





Efficacy Testing

- Efficacy testing checks how effective our mitigation tactics are at stopping Ryuk from encrypting files.
- Our main decided method was to use file system entropy.
- Highly encrypted file systems should have higher entropy, non-encrypted files should have lower entropy.
- We automated checking the entropy of files before and after encryption to allow for quick analysis of ransomware samples and mitigation tactics.
- We can also use this system to check how effective a mitigation tactic was at stopping ransomware.

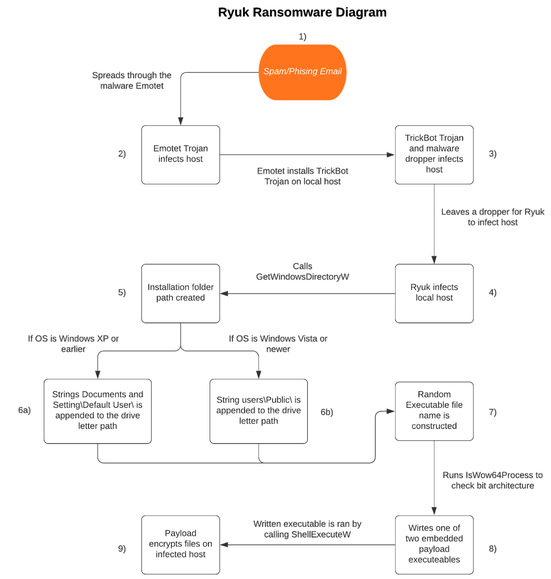


Results & Recommendations

- After analyzing many samples of the Ryuk ransomware, both dynamically and statically, our team was not able to stop ransomware from encrypting files.
- Our recommendations include focusing individual efforts on analyzing different ransomware that is impacting individuals and corporations, alike.
- It would be beneficial to analyze ransomware that is a derivative of the Ryuk family, too. Usually, many ransomwares that are within the same family are built off of one another. There potentially could be an exploit to stop a ransomware which could also give us better insight into stopping Ryuk from encrypting files.

Understanding Ryuk

- Ryuk is a popular ransomware family first discovered in 2019, meant for targeting specific corporations. It was well known for attacks on US hospitals, the LA Times, and several US local governments.
- Ryuk's origin is believed to be created by developers in Russia. Hence, our research was targeted at understanding if changing the DNS and locale would stop the ransomware
- We decided to focus on Ryuk as its ready availability, and wide array of known working samples are available to the public.
- Below is a flow chart in the different processes Ryuk completes in order to encrypt the files of a WIndow's machine:



Future Work, References

- Conduct further research into understanding how various types of ransomware work.
- Create scripts that can identify the unique type of ransomware
- Create executables for various operating systems that will stop ransomware from encrypting files.

Faculty: John Raiti, Payman Arabshahi
Industry Mentor: Johnathan Ness
Undergraduate Students: Hunter Camfield, Wayne Lai, Brenden Weibel, Lexie Chau, Michael Phenicie

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

ADVISOR: JOHNATHAN NESS, JOHN RAITI

SPONSOR: VERAMINE