Reverse Engineering Paper Assignment

CSC 4999 Directed Reading

Spring-2020 Semester

Danh Pham

Summary:

The author of this summary is Danh Pham, for the CSC 4999 Directed Reading class of Spring 2020. In this project, we will be summarizing the article, “The Static Analysis of WannaCry Ransomware.” In this article, the authors address the problem of the analyzing ransomware, WannaCry, which is essentially a ransomware, which encrypts the victim’s data until they pay money for the decryption key. The problem they address is significant because their analysis of WannaCry can help them understand ransomware and malware programs in general, which would help them solve or prevent new forms of malicious programs. The authors propose their solution through explaining malware and ransomware in general and use that information to analyze WannaCry. The authors explain how ransomware attack comes in sequential stages, such as deployment, installation, destruction, and command and control. They use this underlying principle to guide their analysis. For the Deployment phase, the researchers found out that they exploited the MS17-010 vulnerability to inject malicious binaries and drivers from an Eternal Blue Exploit and Double pulsar backdoor. From this, the installation phase consists of using the InternetOpenA and InternetOpenUrlA windows API with a defined URL kill-switch, which is propagated from the mssecsvx.exe and tasksche.exe. This is where the researchers found the kill-switch that stops the ransomware if it can connect to the defined URL. The Destruction phase consists of encrypting the victim’s file through the use of an RSA and AES encryption method. Finally, the command and control phase are the WanaDecyptor.exe program which tells the victim to send bitcoin to a certain address to decrypt their files. The major conclusions the author discloses is that analyzing malware is beneficial because students can identify common attack patterns and obtain a better understanding of how malicious code works. With this new-found understanding, they can create better malware defense systems with less vulnerabilities and potentially solve future malware cases.

Critique:

I think this research paper was very informative and well-done. A strength of this paper is that, it gave necessary background information for people that are not well-versed on how ransomware program works, and this definitely help my understanding of their research analysis. I liked how the researchers included figures with explanation of how each step worked in the ransomware process. A weakness of this paper is that it did not include downloadable resources that readers could reference to if they decided to follow along with the author’s analysis. I think an improvement they can make is by including these downloadable resources. Some open issues that the authors do not address are explanations of malware defensive programs, and how we could improve these programs to defend against these types of malware attacks. Additionally, the authors could have left general tips or guidelines on how to stop these types of attacks from propagating if a reader comes across one.

Synthesis:

One way in which this research work could be further developed is by creating a modified version of WannaCry.exe where the researchers could create a step by step comment notation inside the code for readers to mess around with. The authors could create a version where the virus is deactivated, however readers would have to fix the code through guided steps in the code comments. This would help readers learn how each step of the WannaCry ransomware virus works and learn about how the virus propagates and injects itself through a form of live demonstration. Currently, some form of this exists; However, there does not exist a thorough modified version with comments and commented out code which could help the learning process through fixing the ransomware chronologically. Another way, to develop this research work is by linking analysis to other ransomware and malware programs, which have step by step tutorials and explanation of how the program works. Consequentially, the researchers could create a compare and contrasting research article, which could potentially help readers understand how ransomware and malware work through the use of multiple case examples.

Reproducing the Case Study:

https://www.youtube.com/watch?v=eIilUca7Ic0&feature=youtu.be

Step 1: Load Wannacry.exe into Ghidra

Step 2: Analyze the executable with Decompile Parameter ID and WindowsPE x86 Propagate enabled

Step 3: Go into the entry function

We can find a call function of local6c into something_interesting

Step 4: Go into the renamed something_interesting function

From here, there is a strange_url variable that is equal to a URL string, and a InternetOpenA and InternetOpenUrlA API function.

Step 5: Define the type of InternetOpenA and InternetOpenUrlA as an HINTERNET, this is basically the WinINET handle API to get the functions to work

Explanation: The URL defined in the strange_url variable is basically the killswitch for WannaCry. If someone registers the domain defined strange_url, then the code can successfully connect to the URL. If this happens, the code does not execute; However, if the code can not connect, then it moves to the next function and executes the function FUN_00408090, therefore executing the malicious ransomware code.

References

[1] S. Hsiao and D. Kao, "The static analysis of WannaCry ransomware," *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon-si Gangwon-do, Korea (South), 2018, p 153-158