The Static Analysis of WannaCry Ransomware

Shou-Ching HSIAO[*], *Da-Yu KAO*[**]

*Haishan Precinct, New Taipei City Police Department, New Taipei City 220, Taiwan

**Department of Information Management, Central Police University, Taoyuan City 333, Taiwan

oliver84312@gmail.com, dayukao@gmail.com

***Abstract*—Hacking weapons come in handy for cyber criminals anytime. Ransomware has increased in popularity. Its creators are playing our fears. The rapid proliferation of ransomware attack indicates the growing tendency of ransomware-as-a-service (RaaS) and the integration of hacking weapons. This paper presents the static analysis of the infamous WannaCry ransomware, which is one of the most impacted and propagated malware in 2017. This international wave of cyber threats is reported to have struck over 150 countries worldwide. Through the static analysis, the details of WannaCry processes and functions are revealed. The anatomy of ransomware attack is discussed to dissect the multi-staged execution of Wannacry, including deployment, installation, destruction, and command-and-control. The WannaCry ransomware not only implements the strong encrypting algorithm and key structure, but also integrates the hacking weapons leaked by the Shadow Brokers. In this paper, the reverse engineering analysis is conducted to explore each chain of malware execution.**

***Keyword*—Cyber Threat, Ransomware, Static Analysis, Reverse Engineering, WannaCry**

Shou-Ching Hsiao is an information lieutenant at Haishan Precinct, New Taipei City Police Department, Taiwan. She is responsible for information system management, information security, and real-time video for security control. She can be reached at oliver84312@gmail.com.

Da-Yu Kao is an Associate Professor at Department of Information Management, Central Police University, Taiwan. With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.