Classification of Exploit-Kit Behaviors via Machine Learning Approach

Sukritta Harnmetta, Sudsanguan Ngamsuriyaroj

Faculty of Information and Communication Technology, Mahidol University, Nakornpathom, Thailand

sukritta.harn@gmail.com, sudsanguan.nga@mahidol.ac.th

***Abstract*— An Exploit-Kit (EK) is the cyber attacking tool which targets in finding vulnerabilities appeared on a web browser instance such as web-plugins, add-on instances usually installed in a web browser. Such instances may send some suitable malware payload through the vulnerabilities they found. This kind of such cyber-attack is known as the drive-by-download attack where malware downloading do not require any interaction from users. In addition, EK can do self-protection by imitating a benign website or responding to end-users with HTTP 404 error code whenever it encountered an unsupported target web browser. As a result, detecting EK requires a lot of effort. However, when an EK launches an attack, there are some patterns of interactions between a host and a victim. In this work, we obtain a set of data from www.malware-traffic-analysis.net and analyze those interactions in order to identify a set of features. We use such features to build a model for classifying interaction patterns of each EK type. Our experiments show that, with 5,743 network flows and 45 features, our model using Decision tree approach can classify EK traffic and EK type with accuracy of 97.74% and 97.11% respectively. In conclusion, our proposed work can help detect the behavior of EK with high accuracy.**

***Keyword*— Drive-by-Download, Exploit-Kit, Machine Learning, Network Analysis**

Sukritta Harnmetta received her B.Sc. degree in ICT from the Mahidol University, Thailand in 2014 and currently a Master student in Cybersecurity and Information Assurance program at Faculty of ICT. In 2015, she joined the cybersecurity team at G-Able Co., Ltd., as an internship student.

Sudsanguan Ngamsuriyaroj received her Ph.D. degree in Computer Science and Engineering from Pennsylvania State University, United States of America. Her research interests include network security, cloud security, IoT security and Parallel computing. Her research projects include IoT energy and healthcare applications especially for rehabilitation medicine.