Attack Tactic Labeling for Cyber Threat Hunting

SHENG-XIANG LIN, ZONG-JYUN LI, TZU-YANG CHEN, DONG-JIE WU

*Cybersecurity Technology Institute, Institute for Information Industry, Taiwan, R.O.C

leaflin@iii.org.tw, tomlee@iii.org.tw, tzuyangchen@iii.org.tw, dongjiewu@iii.org.twst-third.edu

***Abstract*—Recently, the cyber attack has become more complex and targeted, making traditional security defense mechanisms based on the "Indicator of Compromise" ineffective. Furthermore, fail to consider attack kill chain may lead to a high false-positive rate for attack detection. To trace hackers' behaviors and footprints, it is crucial to provide additional information such as attack tactics, techniques, and procedures in detecting attacks. In this study, we propose a mechanism for labeling attack tactics of network intrusion detection system (NIDS) rules on the basis of text mining and machine learning. The proposed approach can help security experts determine the current attack state and infer its purpose, making it possible to detect complex attacks (e.g., APT). Besides, we refer to the ATT&CK framework developed by MITRE (a leading organization in information security) to strengthen the reliability of labeling results. The experiment result shows that the accuracy of our proposed mechanism can effectively boost the performance of the labeling attack tactic. The experimental result shows that the F1 score of our approach is more than 90% and up to approximately 96%, which can effectively assist cyber security experts in tactic labeling and provides a solid base for further alert correlation. Moreover, we also compare our approach with one of the well-known TTP labeling tools, rcATT; the result shows that our approach's accuracy, precision, recall, and F1 score are all significantly better than rcATT.**

***Keyword*—Cyber threat hunting, Cyber kill chain, Tactic labeling, APT detection, Machine Learning, Malicious Traffic Detection**

Sheng-Xiang Lin received his M.S. degree in Department of Computer Science and Information Engineering from National Ilan University, Yilan, Taiwan, R.O.C. in 2019. He is currently an engineer in Cybersecurity Technology Institute, Institute for information industry, Taiwan, R.O.C. His research interests include forensic analysis, reverse engineer, penetration testing, and machine learning skills.

Zong-Jyun Li received his B.S. degree in Department of Computer Science and Information Engineering from National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C. in 2018. He is currently an engineer in Cybersecurity Technology Institute, Institute for information industry, Taiwan, R.O.C. His research interests include forensic, reversing, and red team skills.

Tzu-Yang Chen received his B.S. degree in Department of Computer Science and Information Engineering from National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C. in 2020. He is currently an engineer in Cybersecurity Technology Institute, Institute for information industry, Taiwan, R.O.C. His research interests include machine learning, data mining, deep learning and security.

Dong-Jie Wu received his M.S. degree in Department of Computer Science and Information Engineering from National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C. in 2012. He is currently a deputy director in Cybersecurity Technology Institute, Institute for information industry, Taiwan, R.O.C. His research interests include cyber threat hunting, incident response, penetration testing and machine learning.