Study on Systematic Ransomware Detection Techniques

Sun-Jin Lee*, Hye-Yeon Shim*, Yu-Rim Lee*, Tae-Rim Park*, So-Hyun Park†, Il-Gu Lee*†

* Department of Convergence Security Engineering, Sungshin University, South Korea

†Department of Future Convergence Technology Engineering, Sungshin University, South Korea

{20180935, 20180922, 20180940, 20180917, 220206035, iglee}@sungshin.ac.kr

***Abstract*—Cyberattacks have been progressed in the fields of Internet of Things, and artificial intelligence technologies using the advanced persistent threat (APT) method recently. The damage caused by ransomware is rapidly spreading among APT attacks, and the range of the damages of individuals, corporations, public institutions, and even governments are increasing. The seriousness of the problem has increased because ransomware has been evolving into an intelligent ransomware attack that spreads over the network to infect multiple users simultaneously. This study used open source endpoint detection and response tools to build and test a framework environment that enables systematic ransomware detection at the network and system level. Experimental results demonstrate that the use of EDR tools can quickly extract ransomware attack features and respond to attacks.**

Keyword— Ransomware, ransomware detection, endpoint detection and response (EDR), Google rapid response, osquery, Open Source hids SECurity (OSSEC), open-source EDR

Sun-Jin Lee is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin University, Seoul, Korea. Her current research interests are in the area of deep learning, Internet of Things, malware detection, voice security, image security, and video security.

Hye-Yeon Shim is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin University, Seoul, Korea. Her current research interests are in the area of artificial intelligence, deep learning, malware detection, and programming.

Yu-Rim Lee is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Un iversity, Seoul, Korea. Her current research interests are in the area of artificial intelligence, threat defense, malware detection, and I nternet of Things.

Tae-Rim Park is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin University, Seoul, Korea. Her current interests are in the areas of artificial intelligence, network security, malware detection, cloud co mputing, and Internet of Things.

So-Hyun Park received her B.S. degree in Convergence Security from Sungshin University, Seoul, Korea, in 2020. She joined Convergence Security Engineering Laboratory, Sungshin University, Seoul, Korea in 2020, where she is currently pursuing M.S. Her research interests include wireless networks and communications security, digital forensics, cyber security, Internet of Things (IoT) security, and voice recognition security.

Il-Gu Lee received his B.S. degree in electrical engineering from Sogang University, Seoul, Korea, at 2003, and his M.S. degree in t he Department of Information and Communications Engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, at 2005. He received his PhD degree in the Graduate School of Information Security in Computer Science & Engin eering Department from KAIST at 2016. He is a professor at the Department of Convergence Security Engineering, Sungshin Univer sity (SU), Seoul, Korea. Before joining SU in March 2017, he was with the Electronics and Telecommunications Research Institute (ETRI) as a senior researcher from 2005 to 2017, and served as a principal architect and a project leader for Newratek (KR) and Ne wracom (US) from 2014 to 2017. His current research interests are in the area of wireless/mobile networks with an emphasis on info rmation security, networks, wireless circuit and systems. He has authored/coauthored more than 55 technical papers in the areas of in formation security, wireless networks and communications, and holds about 160 patents. He is also an active participant of and contributor to the IEEE 8 02.11 WLAN standardization committee.