# Ransomware Detection Using Open-source Tools

Sun-Jin Lee, Hye-Yeon Shim, Yu-Rim Lee, Tae-Rim Park, Il-Gu Lee

*Department of Future Convergence Technology Engineering, Sungshin Women's University, South Korea*

**{220214013, 220214012, 220214014, 220214011, iglee}@sungshin.ac.kr**

***Abstract*— The recent development of new and variant malicious codes, and the increase in cyberattacks in the form of intelligent Advanced Persistent Threat (APT), has led to rapidly increasing levels of damage. In particular, in the case of ransomware, the damage per attack is large, because ransomware uses a network propagation method, by which each attack can infect multiple victims. As ransomware as a service (RaaS) has increased recently, even people without the capacity to develop malicious code have become able to attack via ransomware. In this study, we built and experimented with a framework that detects ransomware in network and system environments using open-source tools. This study showed through analysis and experiments that open-source tools can quickly identify and respond immediately to APT attacks.**

***Keyword*— Open-source, Endpoint Detection and Response (EDR), Google Rapid Response, Open-source HIDS SECurity (OSSEC), osquery, Ransomware Detection**

**Sun-Jin Lee** was born in Korea in 2000. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's 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** was born in Korea in 2000. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current research interests are in the area of artificial intelligence, deep learning, malware detection, and programming.

**Yu-Rim Lee** was born in Korea in 1999. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current research interests are in the area of artificial intelligence, threat defense, malware detection, and Internet of Things.

**Tae-Rim Park** was born in Korea in 1999. She is a student of the Integrated B.S./M.S. course in the Department of Convergence Security Engineering in Sungshin Women's University, Seoul, Korea. Her current interests are in the areas of artificial intelligence, network security, malware detection, cloud computing, and Internet of Things.

**Il-Gu Lee** was born in Korea in 1978. He received his PhD degree in the Graduate School of Information Security in Computer Science & Engineering Department from KAIST at 2016. He is a professor at the Department of Convergence Security Engineering, Sungshin Women's University, Seoul, Korea. His current research interests are in the area of wireless/mobile networks with an emphasis on information security, networks, and wireless systems