Cloud-based Android Botnet Malware Detection System

Suyash Jadhav*, Shobhit Dutia+, Kedarnath Calangutkar+, Tae Oh*+, Young Ho Kim**, Joeng Nyeo Kim**

**Dept. of Information Sciences and Technologies,*
^Dept. of Computing Security,
+Dept. of Computer Science
Rochester Institute of Technology,
152 Lomb Memorial Dr, Rochester, NY, USA

***Cyber Security System Research Dept., Electronics and Telecommunication Research Institute,*
218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, KOREA

ssj8127@rit.edu, , snd7555@rit.edu, krc9698@rit.edu, thoics@rit.edu, wtowto@etri.re.kr, jnkim@etri.re.kr

***Abstract*— Increased use of Android devices and its open source development framework has attracted many digital crime groups to use Android devices as one of the key attack surfaces. Due to the extensive connectivity and multiple sources of network connections, Android devices are most suitable to botnet based malware attacks. The research focuses on developing a cloud-based Android botnet malware detection system. A prototype of the proposed system is deployed which provides a runtime Android malware analysis. The paper explains architectural implementation of the developed system using a botnet detection learning dataset and multi-layered algorithm used to predict botnet family of a particular application.**

***Keywords*— Android botnet, Cloud-based malware detection, Vyatta, Android on VirtualBox, Android botnet family detection , and Android Sandbox.**

Suyash S. Jadhav born in Pune, INDIA on 31st March 1992. Holding Bachelor of Engineering in computer engineering form Pune University, India (2013); currently pursuing Master of Science in computing security at Rochester Institute of Technology.
He is currently working with Dell SecureWorks as a Security Analyst at Atlanta,USA.

Tae H. Oh received a B.S. degree in Electrical Engineering from Texas Tech University in 1990 and M.S. and Ph.D. degrees in Electrical Engineering from Southern Methodist University (SMU) in 1995 and 2001, respectively. He is Associate Professor of Information Sciences and Technology Department at Rochester Institute of Technology (RIT). His research focus has been in mobile computing, mobile device security, mobile ad hoc networks, and cyber security. He has over 20 years of experience in networking and telecommunication as an engineer and researcher for several telecom and defense companies before he joined RIT.

Youngho Kim received his MS and BS degree in Computer Science from Korea University, Korea, in 1999 and 2001 respectively. He was a visiting research scholar at Rochester Institute of Technology (RIT) in 2013 and 2014. Since 2002, He has been a senior member of engineering staff at the Electronics and Telecommunications Research Institute (ETRI). His research interests include operating system, embedded system and mobile device security.

Jeongnyeo Kim received her MS degree and Ph.D. in Computer Engineering from Chungnam National University, Korea, in 2000 and 2004, respectively. She studied at computer science from the University of California, Irvine, USA in 2005. Since 1988, she has been a principal member of engineering staff at the Electronics and Telecommunications Research Institute (ETRI), where she is currently working as a management director of the Cyber Security System Research Department. Her research interests include mobile security, secure operating system, network security and system security.