Comparative Analysis of Darknet Traffic Characteristics between Darknet Sensors

Falguni Gadhia [*, **], Jangwon Choi[**], Buseung Cho[**], Jungsuk Song[*, **]

*Korea University of Science & Technology, Daejeon, South Korea

**Department of Advanced KREONET Security Service, Korea Institute of Science and Technology Information, Daejeon, South Korea

gadhiafalguni@kisti.re.kr, jwchoi@kisti.re.kr, bscho@kisti.re.kr, song@kisti.re.kr

Abstract— **Today, Internet is incessantly attacked by wide variety of network-based threats. One of the ways to monitor or identify such prevailing threats is to monitor incoming traffic to unused network addresses popularly known as darknet and often also referred with various other names like network telescope or black hole. As, all the traffic arriving at darknet is mainly the result from malicious probing or misconfiguration in the network. It is expected that to have similar incoming traffic behaviour across different darknet sensors, however, various studies found it different. Various reason cited behind it is misconfiguration, certain kind of attack, difference in filtering parameter or system configuration itself. However, concrete reason beside this is still missing. In this regard, to get further understanding, in this study, we performed deeper comparative analysis between two darknet sensors (KISTI Darknet network) that are differently located but have similar filtering and system configuration. Comparative analysis considering total incoming packet, number of source host, targeting destination port and protocol revealed that there exists wide difference in incoming traffic characteristics between the darknet sensors. Moreover, for TCP and UDP comparison, UDP traffic showed more targeting behaviour to particular darknet block (difference in traffic characteristics between darknet sensors), in contrast to it, TCP traffic showed more scanning behaviour (similarity in traffic characteristics between darknet sensor).**

Keyword— **Darknet, network monitoring, network security, TCP, UDP**

Falguni Gadhia received her B.S degree in 2010 from Atmiya Institute of Technology and Science, India. She worked as an intern in Korea Institute of Science and Technology Information from Sept. 2011 to Aug. 2012. She is currently pursuing her master degree in grid and supercomputing from Korea University of Science and Technology. She is working as a master student in Department of Advanced KREONET Security Service, Korean Institute of Science and Technology Information from March 2013. Her research intersect include network monitoring, network and data management, network security.

Buseung Cho received his B.S, M.S and Ph.D. degree from Sungkyunkwan University, Korea in 2000, 2002, and 2012 respectively. He was a researcher in Institute for Advanced Engineering from Sept. 2002 to July 2005.He is working as a senior researcher in Korea Institure of Science and Technology Information(KISTI) from July 2005. Currently, he is a senior researcher and director of Dept. of Advanced KREONET Operation and Service. His research interest include international research retworking, future internet and future network operation, knowledge-based network configuration and fault management, optical network and network management and data modeling and standardization for plant. He is member of Technolgy Program Committee, International Conference on Nertworks (ICN), GLIF and GOLE Partnership, GLORIAD Partnership and APAN.

Jangwon Choi received his B.S. and M.S degrees in Electronic Engineering from Hongik University, Korea in 1996 and 1998, respectively. He received his Ph.D. degree in the Department of Computer Science and Engineering, Korea University, Korea in 2009. He is a principal researcher and director of Dept. of Advanced KREONET Security Service at Korea Institute of Science and Technology Information. His research interests include network, cloud computing, grid computing, network security, security issues on IoT, and cryptography theory

Jungsuk Song received his B.S. and M.S. degrees in Information and Telecommunication Engineering from Korea Aerospace University, Korea in 2003 and 2005, respectively. He received his Ph.D. degree in the Graduate School of Informatics, Kyoto University, Japan in 2009. He worked for NICT (National Institute of Information and Communications Technology), Tokyo, Japan, as an expert researcher from Apr. 2009 to Sep. 2010 and as a researcher from Oct. 2010 to Sep. 2011. He is currently a senior researcher at KISTI (Korea Institute of Science and Technology Information), Daejeon, Korea. His research interests include network security, data mining, machine learning, and security issues on IPv6, spam analysis, and cryptography theory.