APT attack response system through AM-HIDS

Seoung-Pyo Hong*, Chae-Ho Lim**, Hoon Jae Lee***

**Department of Ubiquitous IT, Dongseo University, Busan 47011 Republic of Korea*

***Bitscan INC, Seoul 04789 Republic of Korea*

****Division of computer engineering, Dongseo University, Busan 47011 Republic of Korea*

debiii@naver.com, skscogh@naver.com, hjlee@dongseo.ac.kr

In this paper, an effective Advanced Persistent Threat (APT) attack response system was proposed. Reference to the NIST Cyber Security Framework(CRF) was made to present the most cost-effective measures. It has developed a system that detects and responds to real-time AM-HIDS(Anti Malware Host Intrusion Detection System) that monitors abnormal change SW of PCs as a prevention of APT. It has proved that the best goverment-run security measures are possible to provide an excellent cost-effectiveness environment to prevent APT attacks.

***Keyword*—APT, AM-HIDS, Anti, Malicious, WhiteList**

Seoung-Pyo Hong
He received the B.S., degrees from Dept. of Computer Engineering, Dongseo University, South Korea, in 2020. Since 2020, he is currently a Master course in the Dep. of Computer Engineering, Dongseo University, South Korea. His research interests include Digital Forensic, Malicious Analysis, Computer Security

Chae-Ho Lim
He received the B.S degree in Computer Science and Engineering(CSE) from Hongik University in Korea 1996 and his received the M.S degree in CSE from Konkuk University in 1999 and his received the Ph.D degree in CSE from Hongik University in 2000, His resarch interests are in the security topic of Internet Security and Software Security and Risk Management

HoonJae Lee
He received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.