An implementation of log visualization system combined SCADA Honeypot

Jaehee Lee*, Jinhyeok Jeon**, Changyeob Lee***, Junbeom Lee****, Jaebin Cho*****

** Department of Information Security, Korea University, Seoul, Korea*

*** Department of Information Security, Sungkyunkwan University, Seoul, Korea*

**** Department of Computer Science and Engineering, Sogang University, Seoul, Korea*

*****Department of Information and Telecommunications Engineering, University of Suwon, Suwon, Korea*

******Department of Convergence Security, Kyonggi University, Suwon, Korea*

foodlook88@gmail.com, as26vl@gmail.com, howbest@ gmail.com, jb93lee@gmail.com, xxzchozxx@gmail.com

***(Pt9)Abstract*— Recently, the leading trend and the biggest issue in global security is cyber terror. In case of Korea, on December 2014, a nuclear power plants' network was hacked into and its blueprint and manual was leaked. The case was a big threat not only to national security but also to the finance of Korea Hydro & Nuclear Power Co., LTD. However, despite this situation, there is not enough information about or detailed explanation on cyber terror. Identifying the cyber terrorists who commit a cyber terror is the best way to defend against the attack. So far, we thought that we successfully defended an attack by blocking the cyber terrorist's IP in the network firewall. However, when a certain attack fails, the cyber terrorist usually tries to find another way to attack. Especially, in case of cyber terror, a cyber terrorist uses very technical ways to attack and hack into computer network exploiting the fact that human beings can easily make mistakes. To increase the security, we do a profiling on cyber terrorist's attack techniques beforehand and set up concrete measures to deal with the attacks. This paper proposes a measure to implement a system to profile cyber terrorists, attack techniques on SCADA system, and discuss the practicality of such system by reviewing the result from actual implementation.**

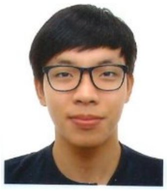
***(Pt9)Keyword*— Keywords-APT; Cyber Terror; APT; SCADA Security; SCADA Honeypot; SIEM**

Jaehee Lee working on a Master's Degree in the Department of Information Security at the Graduate school of Information security, Korea University. His Research interests are in the areas of risk management and malicious code analysis. He is researching SCADA Honeynet recently. He takes 'Best of the Best' education program in KITRI.

Jinhyeok Jeon working on a Master's Degree in the Department of Information Security, Sungkyunkwan University. His Research interests are in the areas of security log analysis. He is researching analyzing APT recently. He takes 'Best of the Best' education program in KITRI.

Changyeob Lee working on a Bachelor's Degree in the Department of Computer Science and Engineering, Sogang University. His Research interests are in the areas of log analysis and visualization. He is researching SIEM solution recently. He takes 'Best of the Best' education program in KITRI.

Junbeom Lee working on a Bachelor’s Degree in the Department of Information and Telecommunications Engineering, University of Suwon. His Research interests are in the areas of log analysis and visualization. He is researching log visualization recently. He takes ‘Best of the Best’ education program in KITRI.



Jaebin Cho working on a Bachelor’s Degree in the Department of Convergence Security, Kyonggi University. His Research interests are in the areas of log analysis and visualization. He is researching log analysis recently. He takes ‘Best of the Best’ education program in KITRI.