Analysis and Comparison of Honeypot Activities on Two ISP Networks

Devran Yener
Department of Computer Engineering
TOBB University of Economics & Technology
Ankara, Turkey
dyener@etu.edu.tr
ORCID: 0000-0003-2811-086

Tansel Özyer
Department of Computer Engineering
TOBB University of Economics & Technology
Turkey
ozyer@etu.edu.tr
ORCID: 0000-0002-2529-5533

Emin Kugu
Department of Software Engineering
TED University
Ankara, Turkey
emin.kugu@tedu.edu.tr
ORCID: 0000-0001-7829-8087

Abstract—While the enormous growth of cyberspace makes life easier, it also brings new challenges to overcome. The concept of the Internet of Things (IoT) is the main actor of this metamorphosis. They are spreading very quickly due to their advantages and cost-effective nature. These systems also cause risky situations by ignoring security requirements. By their nature, honeypots help us to understand and prevent malicious activities by the attackers. Although significant research has been completed by using honeypots, many of them have not evaluated the real-world scenarios, and some of them have covered only the cloud or a single network. Comparison between Internet Service Providers (ISPs) or cloud providers has been neglected. In our work, we try to fill this gap by positioning the Kippo honeypot behind two different ISP lines with some known IoT device credentials. We have collected Kippo logs for a fifteen-day period. The study shows us that all devices can be discovered by mass scan. Therefore, both ISP networks are at the same amount of risk from cyberattacks. Although there was no significant change in the number of attacks per day during the fifteen-day test period, it is quite high compared to previous studies. This comparison highlights the fact that protecting cyber assets is getting harder every year.

Keywords *— honeypot, kippo, internet service provider, internet of things, cyber security*