ISSN 0511-5728
The West Indian Journal of Engineering
Vol.43, No.2, January/February 2021, pp.23-30

Cybersecurity Threat Analysis for an Energy Rich, Small Island Developing State

Reshawn Ramjattan [a,Ψ], Darren Ramsook[b] and Patrick Hosein [c]

Department of Computing and Information Technology, Faculty of Science & Technology, The University of the West Indies, St. Augustine, Trinidad and Tobago, West Indies;

[a]Email: reshawn.ramjattan@gmail.com;
[b]Email: darrenramsook@outlook.com;
[c]Email: patrick.hosein@sta.uwi.edu

[Ψ] *Corresponding Author*

(Received 28 July 2020; Revised 16 December 2021; Accepted 02 February 2021)

Abstract: *With the ever-increasing use of the Internet by people of all walks of life and the storage of their personal and financial information, attacks on web sites have been rapidly growing. Unfortunately, many do not take sufficient precautions and some even significantly underestimate the potential threats and the associated costs of an intruder. In particular, Small Island States (SIDs) lack the resources to monitor and repel attacks, even those rich in energy and natural resources. We determine the level of threats and the source of such threats for educational and industrial web sites for one such country. We deployed a network honeypot with File Transfer Protocol (FTP), Secure Shell (SSH), Hypertext Transfer Protocol (HTTP) and Industrial Control System (ICS) on a fake educational institution server. Besides, a network honeypot with server message block (SMB), FTP, HTTP, and ICS was set up in a fake oil company server. The ICS used was above ground storage tanks (AST) and a programmable logic controller (PLC), mostly utilised in the Oil and Gas industry. We recorded honeypot events and determined locations of the potential intruders using source IP addresses. We found that the oil company site's SMB server had the most honeypot events and the highest repeat attacker rate. We also determined the countries that hosted the most attackers. This information can be used to better detect potential attacks and defend against them.*

Keywords: *Threat Analysis, Cybersecurity, Honeypot, OWASP, Dionaea, Conpot*