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*

1. Introduction

The recent growth in worldwide internet users, means a similar growth in web applications and services globally. Developing countries also share in this rapid growth rate as there are people becoming connected to the internet, due to increased availability and lower costs for a connection. In the case of South America, the average internet accessibility rate per person is tied with a positive trend in economic growth measured through gross domestic products (GDP) (Ochoa-Jimenez et al., 2018).

This general trend in developing countries would also indicate that proper cybersecurity measures are put in place, but this is not always the case. Developed countries have had the time and capability to fully develop Critical Information Infrastructure Protection (CIIP) Systems, unlike developing countries. In turn, these countries are becoming a haven for cyberattacks due to the weaker cybersecurity measures in place (Ellefsen and Solms, 2010). Relevant persons in these countries are sometimes unaware of the attacks due to insufficient groundwork conducted on target identification or the general inability to detect cyberattacks.

Significant research has been reported on the design, use and results of Honeypots. There are specialised honeypots for IoT (Internet of Things) devices (Pa et al., 2016) and even ones for detecting ransomware (Moore, 2016). An exhaustive survey of the software available for deploying a honeypot can be found in Nawrocki et al (2016) and the number of options indicate the interest in using such devices. Work on preventing honeypot detection and compromise is contained in Tsikerdekis et al. (2018). Design of honeypots is also an area of interest and patents are also being led such as the one led on a Cognitive Honeypot (Saikawa and Klyuev, 2019).

To properly design and create customised dynamic network security systems, groundwork on attack characteristics and patterns must be conducted. A network honeypot can be used to gather such information. A network honeypot is defined as a security resource whose value lies in being probed, attacked or compromised (Spitzner, 2003). Honeypot systems are traditionally deployed in controlled environments that lure attackers, which in turn, generate valuable information about the network (Zhang et al, 2002).

We present a framework that was used to capture intruder information using three honeypots. We then analyse this data to determine the extent and frequency of attempts, and determine the nature of the attackers. This work will form the basis for policies on protecting important sites such as those deployed by the Government and those Companies that are attractive targets.

Honeypots are classified on the environment that they are implemented within as well as the level of interaction associated with the honeypot. On the basis of implementation a honeypot can either be a Research or Production honeypot, while on the basis of its environment, a honeypot can be a low, medium or high interaction honeypot (Nagpal et al, 2015).

Low Interaction honeypots (LIHs) is defined as a system designed to attract attackers by emulating an operating system or networking features on a host system. The attacker is only allowed access to the services and files as defined by the honeypot software, meaning that there will be no direct interaction with the attacker and the host system (McGrew, 2006). These types of honeypots offer easy installation and maintenance primarily due to the low risk associated with the "sandbox" environment provided to the attacker, however present the least amount of information on the attack.

Medium Interaction honeypots (MIHs) allows for more data collection than LIHs. MIHs does not simulate the network protocol stack by itself, but rather binds to sockets and utilises the Operating System to do this (Fan et al., 2018). MIHs allows for a better illusion of a computing system through the use of the Operating System meaning there will be more potential information that can be logged from the attackers' actions (Mokube and Adams, 2007). MIHs typically have higher risk associated due to operating system being used as part of the honeypot.

High Interaction honeypots (HIHs) is a normal functioning system where there is no restriction to the attacker. This allows for the most amount of data to be extracted from different types of attacks and is typically used to find the full intentions of attackers. HIHs provide the most amount of risk, as they allow the attacker the most amount of control.

Production honeypots are typically utilised by organisations and is part of a protection system for that organisation. They are integrated into a larger system that eliminates threats on a given network (Spitzner, 2003). Production honeypots involve a higher level of risk due to its deployment environment. Research honeypots are designed with the intention to track and monitor behaviour with no scheduled secondary action. They are used purely as a data collection tool to create information on new defensive techniques (Campbell et al., 2015).

A Virtual Private Network (VPN) is an encrypted connection over the internet that can mask the true source of an experienced attacker. However, location information of script-based attackers, victim machines that perpetuate automated attacks and the VPN servers used for attacks can still be useful.

2. Research Objective

The susceptibility of developing countries to cyberattacks compared to developed nations can be attributed to many factors, namely, commonness of software piracy, inadequate awareness of cybersecurity practices and a lack of cybersecurity strategies, laws and regulatory frameworks (Elkhannoubi and Belaissaoui, 2016). The resulting weakness of infrastructure can be improved upon efficiently by evaluating the attacks being currently made to high priority targets within the SID, including critical infrastructure, Governmental sites and educational sites. Information like common origins of attacks and the most frequently targeted server types and systems could help shape the policies and regulations that strengthen a SID's resilience to cyberattacks. For example, if an FTP server is most frequently targeted, an organisation could use the honeypot data to prepare IP blacklists, aid in risk assessments and prioritisation of security plans as well as calibrate firewalls or intrusion detection systems (IDS).

Honeypots are deployed on a network and used to lure attackers and generate data for these attackers. Moreover, one of the main reasons for deploying a honeypot is to get a better insight into attack methodologies used and therefore create more robust security systems (Rase and Deshmukh, 2015). Therefore, this paper is an attempt to provide such an assessment of educational sites and industrial sites by using honeypots. The Cybersecurity Threat Analysis for a SID purpose is to determine the attack surface on Trinidad and Tobago, an energy rich small island developing state. In the future we also plan to assess attacks on sites within the government domain.

3. Deployment of a Honeypot for an Educational Site

In the network setup utilised in this research, an isolated server was used and two real domain names were assigned for use with this server. The domains were real sub-domains of the domains used for educational institutions and commercial organisations of the country being evaluated. Low interaction level research honeypots were used for data collection as the intention of this paper that is to evaluate the types of protocols being targeted.

For the educational site, the OWASP Python Honeypot (OHP) was used to create the different application servers with varying levels of access security (OWASP, 2021). This honeypot utilises

Linux-Containers (LXC) to run multiple isolated Linux systems on a single host system and an overarching MongoDB database on the host system for data storage. This Honeypot deploys four different types of modules with varying security access on each module, resulting in 7 total access points. Traditional servers such as FTP, SSH and HTTP were used with both weak and strong passwords. Additionally, an Industrial Control System (ICS) for a Veeder-Root Guardian Above-ground Storage Tank (AST) was also deployed. Although such a server would normally not use an educational institution domain name we believed that it would still attract attackers.

The honeypot logs both honeypot related events as well as network related events. The honeypot related events are any events recorded on the various types of servers deployed, while the network related events is general network trac to the web server. The fields collected for honeypot events are shown in Listing 1, with redacted IP and country fields. The IP address associated with the event and their ISO 3166-1 A2 two letter country code are logged.

Listing 1 Fields for OWASP Honeypot Events

"_id":{"$oid":"5d932e04b0aa3067c9fa1f34"},
"machine_name":"127.0.1.1",
"ip":"xxx.xxx.xxx.xxx",
"country":"XX",
"date":"2019-10-01 10:44:20",
"module_name":"ftp/strong_password",
"port":21

Figure 1 depicts the collection of different entry points created by the Honeypot and its network architecture. The data used for this honeypot was collected over a 10-day period.

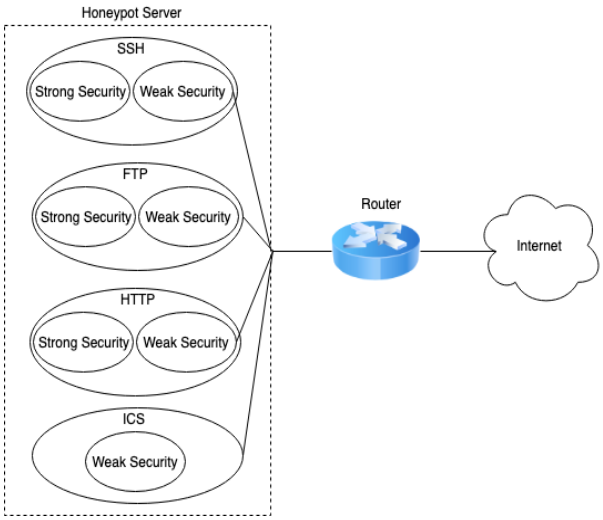

Figure 1 Network Architecture of OWASP Honeypot

Table 1 provides the number of events, unique IP addresses and Repeat Attacker Rates for the educational site sorted by server type and security level over the data collection period. A honeypot event is defined as an attempt to access a certain honeypot server. The repeat attacker rate is the average number of events per unique IP address for each server. This number indicates, on average, how many attempts were made from a particular IP address for a specific server. This repetition rate may indicate the level of automation of the attacks using scripts.

Table 1. OWASP Honeypot Results on Educational site

	Security Level	Events	Unique IPs	Repeat Attacker Rate
FTP	Weak	5912	846	6.99
	Strong	32368	1954	16.56
SSH	Weak	279	29	9.62
	Strong	448	41	10.93
HTTP	Weak	1656	43	11.19
	Strong	262	12	6.09
ICS	Weak	151	8	18.88

Domain Name Used: http: ths.edu.tt

4. Deployment of Honeypots for Industrial Sites

The industrial site represented a fake oil and gas company belonging to the country being evaluated. The Dionaea (Carnivore, 2021) and Conpot honeypots (Conpot, 2021) were used. The former deployed HTTP, FTP and SMB servers and logged their corresponding connection events to a SQLite database. Dionaea is a LIH used for capturing malware aimed at exploiting the vulnerabilities in its exposed services. Once an attacker successfully deploys a payload, the binary is downloaded, and Dionaea computes the file hash to avoid duplicates. We used MetaDefender and VirusTotal, online services that provide file scanning using various anti-virus engines, to scan and classify the obtained binaries. In addition to capturing malware, all connection events are logged including source IP and protocol. For each connection, the p0f (Zalewsk, 2021) passive TCP/IP stack fingerprinting tool is used to attempt to identify the system running on the machine that sent the network trac. For FTP events, any login attempts are also logged.

Since Dionaea does not support any ICS protocols and the purpose of the industrial site was to analyse threats in the Oil and Gas Industry, two instances of Conpot were also deployed. Conpot is another LIH honeypot but specifically provides ICS protocols emulating configurable industry systems. One instance once again, represented a Guardian AST system and the other was a Siemens S7-300 Programmable Logic Controller (PLC). Listing 2 details the fields collected per event by Conpot, with the addition of a country field

determined using the source IP. Conpot events are any network events recorded on the server, for example, TCP connections and system specific events like querying the AST inventory data.

Listing 2 Fields for Conpot Events

```
"id":{"9b7296fa-0197-4d21-bd16-
   3cd5bceced08"},
"src_ip":"xxx.xxx.xxx.xxx",
"src_port":44796,
"data_type":"guardian_ast",
"country":"XX",
"request":null,
"response":null,
"timestamp":"2020-04-30
   05:21:29.092130",
"event_type":"NEW_CONNECTION"
```

The data used from Conpot and Dionaea were collected over 10 and 20 days, respectively. Table 2 presents the results obtained from Dionaea and Conpot for the industrial site, containing the number of events, unique IP addresses and repeat attacker rates.

Table 2. Dionaea and Conpot Results on Industrial site

	Service	Events	Unique IPs	Repeat Attacker Rate
Dionaea	FTP	2976	115	25.88
	HTTP	1850	728	2.54
	SMB	2117954	12007	176.39
Conpot	Guardian AST	27	11	2.45
	S7-S300 IEC104	75	25	3.0

Domain Name Used: http: oil.com.tt

4. Discussion

4.1 Educational Site

The FTP servers had the most attention on this site with 38,280 total events and the second highest repeat attacker rate, fourth across both sites. Figure 2 shows the rate of events for the site against the hours in the day, where most attacks occurred during the period of 8:00AM to 4:00PM UTC.

Figure 3 shows the top 5 country names and their percentage of contribution to the events of OHP. China has the highest number of events with 38.06% and United States of America was recorded as second with 8.55%. There was a large difference between the first and second countries and from there onward, the remainder of countries gently trend downwards with small intervals between them.

Similarly, Table 3 shows the percentage-wise top contributing countries, to events over each of the services for the educational site. It is seen that there are a few countries that constantly fell in the top contributing countries of the four services: United States with four occurrences, followed by China, Netherlands, Iceland and Seychelles all with two occurrences.

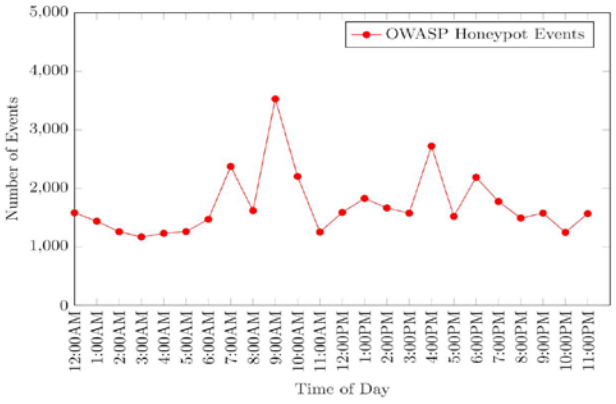

Figure 2 Educational Site OHP Attack rate dependence on time of day

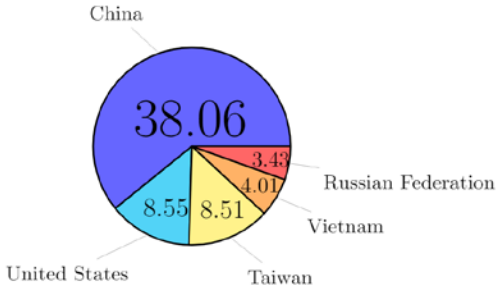

Figure 3. Top 5 Percentages of Total Educational Site OHP Events by Country

Table 3. Percentage of Educational Site Honeypot events by Service and Country

Server Type	Country	Percentage
FTP	China	40.54
	Taiwan	8.96
	United States	8.33
	Vietnam	4.01
	Russia	3.51
HTTP	Iceland	33.52
	United States	8.76
	Netherlands	8.6
	United Kingdom	7.46
	Brazil	6.1
SSH	Iceland	28.61
	United States	21.32
	Seychelles	16.92
	China	5.5
	Ireland	4.68
ICS (AST)	Netherlands	35.76
	Seychelles	35.76
	Spain	13.91
	Germany	5.96
	United States	2.65

4.2 Industrial Site

The results in Table 2 indicate that the industrial site SMB server under Dionaea is targeted the most across both sites with the highest number of events (2,117,954) and the highest repeat attacker rate (176.39), both by a significantly large margin. This repeat rate indicates the use of automated scripts or attacks being perpetuated by victim machines. Table 4 shows that 81.68% of the successful payload downloads were variants of WannaCry ransomware, further supporting the notion that the SMB attacks came from victim machines.

Table 4. Number of Malware Binaries Caught by Dionaea

Malware Family	Events
Wanna Cry	10017 (81.68%)
Small	2231 (18.19%)
Blackshades	11 (0.09%)
Trojan Downloader	5 (0.04%)

Tables 4 and 5 list the results of the scanned malware binaries and the most commonly used credentials of the 2,781 FTP login attempts. The FTP server was the second most targeted and Table 5 shows the most common attempted login credentials. The importance of strong passwords is one of the more well-established and commonly known security practices, but this information serves as a reinforcing example as to why this is the case.

Table 5. Most Commonly used Login Credentials on Industrial Site FTP

	Credential		Events
Username	anonymous		208
	test		184
	admin		184
	ftp		184
	user123		183
Password	anonymous		65
	admin		49
	test		48
	123		48
	admin123		48
Username/ Password Pair	anonymous	anonymous	23
	admin	admin	7
	anonymous	anonymous@	7
	test	test	6
	admin	admin123	6

In addition to the Industrial Control System (ICS) protocols deployed using Conpot on the industrial site, a similar ICS was set up on the previously mentioned OWASP Honeypot (OHP). The OHP ICS had the third highest repeat rate overall at 18.88. As it is an above ground storage tank, mainly used in the Oil and Gas Industry, this shows that attackers have a persistent interest in these devices or that specific automated scripts are being used. The Conpot services, a S7-S300 PLC and an AST, had the least events and were among the lowest repeat rates.

Considering the difference in results compared to the OHP ICS over the same time period and the similarity between the emulated ASTs, this could suggest that the Conpot services used have a higher degree of detect-ability as a honeypot, deterring attackers. Among those Conpot events, 3 from China and Netherlands queried the AST inventory data, while the rest were generally probing connections.

The rate of Dionaea and Conpot events on the industrial site are plotted against the hours of the day in Figures 4 and 5, respectively. This shows that most of the ICS attacks fall within the time frame of 8:00 AM to 4:00 PM UTC, similar to the educational site results whereas SMB, FTP and HTTP attacks were mostly during 8:00PM to 1:00 AM UTC.

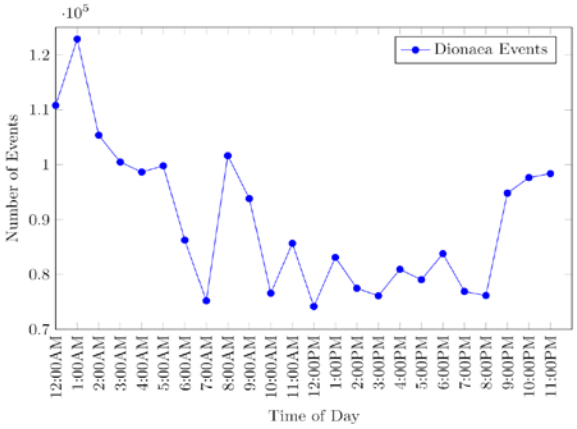

Figure 4. Industrial Site Dionaea Attack rate dependence on time of day

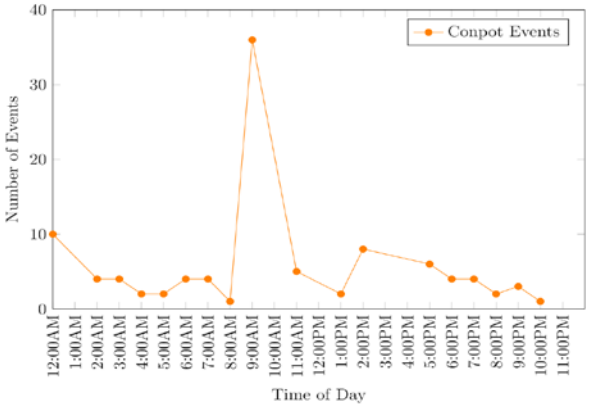

Figure 5. Industrial Site Conpot Attack rate dependence on time of day

Figure 6 shows the top 5 contributing countries to the Dionaea events and the Conpot ICS events. Among the ICS events, again China and United States were the top contributors with 51.96% and 35.29% respectively. However, neither country was present in the top 5

contributors to Dionaea events on the industrial site, where Vietnam at 10.87% closely followed by Russia at 10.16% had the highest number of events. The difference between the top 2 countries as well as the top 2 and second 3 countries were much smaller in Dionaea events when compared to Conpot and the previously discussed OHP. For both honeypots, the remainder of countries gently trend downwards with small intervals between them.

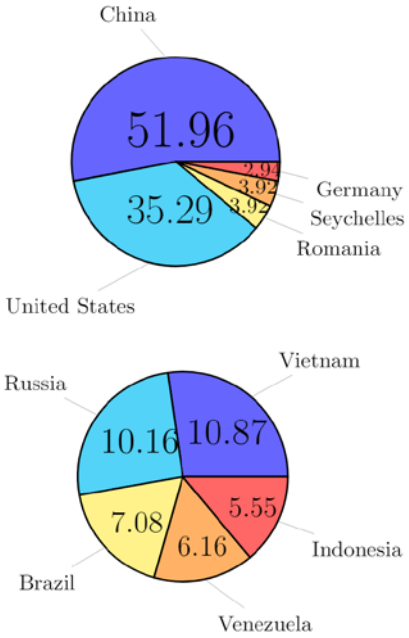

Figure 6. Top 5 Industrial Site ICS Events by Country: Dionaea (top) and Conpot (bottom)

The top countries per server type within the industrial site are shown in Table 6. China was amongst the top contributors for 3 out of 4 server types, followed by United States and Russia with 2 appearances. Seychelles was also a frequent occurrence, appearing in both the Conpot and OHP ICS services. Four out of the top 5 contributors to the industrial site's Dionaea attacks, Vietnam, Russia, Brazil and Indonesia, were also observed in the top 5 of the Japan based study (Saikawa, and Klyuev, 2019), suggesting some independence from victim region among these attacks.

4.3 Comparison of Sites

The similarities between the Conpot top contributors and that of the educational site's OHP, particularly the prevalence of contributions from China and United States, are not seen in Dionaea on the industrial site where those countries are ranked 17th and 18th. Furthermore, Table 7 illustrates the top 20 contributors grouped by region for each site and their server types. Both sites predominantly source from Europe and Asia, with the Educational site having Europe as the most represented region and the Industrial site having Asia.

Table 6. Percentage of Industrial Honeypot events by Service and Country

Server Type	Country	Percentage
FTP	China	31.89
	Japan	31.45
	Taiwan	31.32
	United States	3.33
	Romania	0.34
HTTP	Iceland	31.51
	China	9.89
	Russia	7.57
	Canada	4.11
	Germany	3.62
SMB	Vietnam	11.07
	Russia	10.34
	Brazil	7.2
	Venezuela	6.27
	Indonesia	5.65
ICS (AST & S7-300)	China	51.96
	United States	35.29
	Seychelles	3.92
	France	1.96

Table 7. Countries in Top 20 Contributors grouped by Region per Server Type

Site	Server Type	Region and Number of Countries in Top 20 Contributors				
Educa-ional	FTP	Europe 9	Asia 7	N. America 1	Africa 1	Oceania 1
	HTTP	Asia 9	Europe 8	S. America 2	N. America 1	
	SSH	Europe 7	Asia 4	Africa 2	N. America 1	
	ICS	Europe 4	Africa 1	N. America 1	Asia 1	
Indus-trial	SMB	Asia 9	S. America 4	Europe 3	N. America 2	Oceania 1
	FTP	Asia 9	Europe 5	N. America 4	Africa 2	
	HTTP	Asia 9	Europe 7	N. America 2	S. America 1	Africa 1
	ICS	Europe 2	Asia 1	N. America 1	Africa 1	

A noteworthy exception is South America, the second top region for the industrial site SMB server, the primary source of events and the source of the downloaded malware. This alludes to South America either having a higher presence of script based attackers since the WannaCry attack was first observed or a higher susceptibility to such attacks than other regions.

Table 8 shows the events per day of the common servers between the honeypots deployed on the two sites. For each OHP server type the security module with more events was chosen. The honeypots chosen for the industrial site were able to capture a wider variety of data including malware binaries, FTP login attempts and OS fingerprinting, however the educational site had a higher rate of events across all common services.

Table 8. Events per Day of Educational Site vs. Industrial Site

Server Type	Events/Day		Repeat Attacker Rate	
	Educational	Industrial	Educational	Industrial
FTP	3237	149	16.56	25.88
HTTP	166	93	11.19	2.54
ICS	15 (AST)	3 (AST) 8 (S7-300)	18.88 (AST)	2.45 (AST) 3.0 (S7-300)

The honeypots were released, according to the date their GitHub repositories were created, on July 2018 for OHP, December 2015 for Dionaea and March 2013 for Conpot, respectively. The difference in age and popularity over time resulting in a higher degree of detect-ability is likely a major contributor to the gap in rate of events. It is worth noting that the repeat attacker rates were also lower, with the exception of the FTP servers where the industrial site had a 56.2% higher repeat attack rate despite the aforementioned differences.

5. Conclusions and Future Work

From the honeypot data collected, there are many sources of attacks over FTP, HTTP, SSH, SMB and ICS servers. All geolocation data was evaluated through the use of the attackers IP addresses. However, one must keep in mind that such hackers tend to use VPNs to hide their origin. The total number of honeypot events was 2,155,855 over 20 days on the industrial site and 41,076 honeypot events with 294,623 network events on the educational site over 10 days.

China had the most honeypot events over the educational site (15,633) while Vietnam had the most on the industrial site (234,399). The United States had the most presence across all types of servers as a top-5 contributor in 7 out of 8. Moreover, certain locations were also, popular launching points for these attacks across the different types of servers, such as Seychelles, Netherlands, Iceland, Russia and Romania. There was a high repeat attacker rate for the SMB server (176.39) and 81.68% of malware payloads captured from this server were variants of WannaCry ransomware. Indicating the likely use of automated scripts and perpetuated attacks from victims.

Future work will analyse events over a much longer period and investigate other factors and log file records across a wider variety of sites including commercial and government sites. This can be done by using different types of honeypots, such as MIHs and HIHs. This information will be used to determine a plan for protecting sites and policies that should be put in place to ensure that valuable information is not being extracted from the country. Moreover, SIDs have a reliance on maritime ports as a key part of their national infrastructure. Considerations for other industries like those will be included in the future.

References:

Campbell, R.M., Padayachee, K., and Masombuka, T. (2015), "A survey of honeypot research: Trends and opportunities", *Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, Heathrow Windsor Marriott Hotel, December 14-16, London, UK, pp. 208-212. DOI 10.1109/ICITST.2015.7412090

Carnivore (2021), *Dionaea* (Rep.: Mark Schloesser), Available at: URL http://dionaea.carnivore.it/

Conpot (2021), *CONPOT ICS/SCADA Honeypot*. Available at: URL http://conpot.org/

Elkhannoubi, H., and Belaissaoui, M. (2016), "Assess developing countries' cybersecurity capabilities through a social influence strategy", *Proceedings of the 2016 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, Hammamet, Tunisia, December 18-20, pp. 19-23

Ellefsen, I. and Solms, S.V. (2010), "Critical information infrastructure protection in the developing world", *Proceedings of the Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, ICCIP 2010, Washington, DC, USA, March 15-17, pp, 29-40 (2010). DOI 10.1007/978-3-642-16806-2

Fan, W., Du, Z., Fernandez, D., and Villagra, V.A. (2018), "Enabling an anatomic view to investigate honeypot systems: A survey", *IEEE Systems Journal*, Vol.12, No.4, 3906-3919. DOI 10.1109/jsyst.2017.2762161

Goldberg, I., Kozloski, J.R., Pickover, C.A., Sondhi, N., and Vukovic, M. (2017), *Cognitive Honeypot*, US Patent 9,560,075

McGrew, R. (2006), "Experiences with honeypot systems: Development, deployment, and analysis", *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Kauai, Hawaiivol. January 4-7, pp. 220. DOI 10.1109/HICSS.2006.172

Mokube, I., and Adams, M. (2007), "Honeypots: concepts, approaches, and challenges" *Proceedings of the 45th Annual ACM Southeast Regional Conference (ACM SE07)*, Winston-Salem North Carolina, March pp. 321-326 (2007)

Moore, C. (2016), "Detecting ransomware with honeypot techniques", *Proceedings of the IEEE 2016 Cybersecurity and Cyberforensics Conference (CCC*), Amman, Jordan, August 2-4, pp. 77-81

Nagpal, B., Singh, N., Chauhan, N., and Sharma, P. (2015), "Catch: Comparison and analysis of tools covering honeypots" *Proceedings of the 2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, India, March 19-20, pp. 783-786 (2015). DOI 10.1109/ICACEA.2015.7164809

Nawrocki, M., Waählisch, M., Schmidt, T.C., Keil, C., and Schoönfelder, J. (2016), "A survey on honeypot software and data analysis", *arXiv preprint arXiv*: 1608.06249

Ochoa-Jimenez, D., Moreno-Hurtado, C., and Ochoa-Moreno, W.S. (2018), "Economic growth and internet access in developing countries: The case of South America", *Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, Cáceres, Spain, June 3-16, p.1-4. DOI 10. 23919/CISTI.2018.8399465

OWASP (2021), *Owasp Python Honeypot*, Available at: URL https://www.owasp.org/index.php/OWASP_Python_Honeypot

Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., and Rossow, C. (2016), "Iotpot: A novel honeypot for revealing current iot threats", *Journal of Information Processing*, Vol.24, No.3, pp.522-533

Rase, S.B., and Deshmukh, P. (2015), "Summarisation of honeypot-a evolutionary technology for securing data over network, and comparison with some security techniques", *International Journal of Science and Research*, Vol.4, No.3, March, pp.1440-1445,

Saikawa, K., and Klyuev, V. (2019), "Detection and classification of malicious access using a Dionaea honeypot", *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data*

Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, September 18-21, vol. 2, pp.844-848

Spitzner, L. (2003), *Honeypots: Tracking Hackers*, Addison-Wesley

Tsikerdekis, M., Zeadally, S., Schlesener, A., and Sklavos, N. (2018), "Approaches for preventing honey-pot detection and compromise", *Proceedings of the IEEE 2018 Global Information Infrastructure and Networking Symposium (GIIS)*, Thessaloniki, Greece, October 23-25, pp.1-6

Zalewsk, M. (2021), *p0f v3 (version 3.09b)*, Available at: URL https://lcamtuf.coredump.cx/p0f3/

Zhang, F., Zhou, S., Qin, Z., and Liu, J. (2002), "Honeypot: a supplemented active defense system for network security", *Proceedings of the 8th International Scientific and Practical Conference of Students, Post-graduates and Young Scientists. Modern Technique and Technologies. MTT2002*, (Cat. No.02EX550, Tomsk, Russia, April 8-12, DOI 10.1109/pdcat.2003.1236295

Authors' Biographical Notes:

Reshawn Ramjattan *obtained B.Sc and MSc. Degrees in Computer Science from The University of the West Indies, St. Augustine. During his second year, he interned at First Citizens Internal Audit where he wrote data analysis scripts. Mr. Ramjattan went on to spend some time as a developer at a retail software company before becoming a part time tutor at the Department of Computing and Information Technology. He is currently a member of the TTLAB research group and a Data Science Intern at CIBC First International Caribbean Bank.*

Darren Ramsook *completed his BSc. Electrical & Computer Engineering and MSc. Data Science at The University of the West Indies. He has done work on a large-scale network reliance tool with the Telecommunications Service of Trinidad and Tobago and developed a Hybrid Intrusion Detection System for the Trinidad and Tobago Network Information Center. Mr. Ramsook is currently pursuing his PhD in Electronic & Electrical Engineering at Trinity College Dublin where he is part of the Sigmedia group. His current research area includes video analysis, video restoration using perceptual criteria and developing differentiable perceptual metrics. Darren also is an alumni member of the TTLAB research group.*

Patrick Hosein *attended the Massachusetts Institute of Technology (MIT) where he obtained five degrees including a PhD in Electrical Engineering and Computer Science. He has worked at Bose Corporation, Bell Laboratories, AT&T Laboratories, Ericsson and Huawei. He has published extensively with over 100 refereed journal and conference publications. He holds 40 granted and 42 pending patents in the areas of telecommunications and wireless technologies. Dr. Hosein was nominated for the Ericsson Inventor of the Year award in 2004, was the Huawei US Wireless Research Employee of the year for 2007 and is a 2015 Anthony Sabga Caribbean Laureate for Science and Technology. He is presently the administrative and technical contact for the TT top level domain, CEO of the TTNIC and a Professor of Computer Science at The University of the West Indies. His present areas of research include radio resource management, QoS and pricing for 5G cellular networks.* ■