Faking Smart Industry: A Honeypot-Driven Approach for Exploring Cyber Security Threat Landscape

S. M. Zia Ur Rashid[1], Ashfaqul Haq[2], Sayed Tanimun Hasan[2], Md Hasan Furhad[3], Mohiuddin Ahmed[4], and Abu S. S. M. Barkat Ullah[5(✉)]

[1] Augmedix Inc., San Francisco, USA
[2] International Islamic University Chittagong, Chittagong, Bangladesh
tanimun@ieee.org
[3] Canberra Institute of Technology, Canberra, Australia
hasan.furhad@cit.edu.au
[4] Edith Cowan University, Joondalup, Australia
m.ahmed.au@ieee.org
[5] University of Canberra, Canberra, Australia
Abu.BarkatUllah@canberra.edu.au

Abstract. The digital evolution of Industry 4.0 enabled Operational Technology (OT) infrastructures to operate and remotely maintain cyber-physical systems bridging over IT infrastructures. It has also expanded new attack surfaces and steadily increased the number of malicious cyber incidents for the interconnected smart critical systems. Within Industrial Control System (ICS), Programmable Logic Controller (PLC) plays a crucial function to bridge between cyber and physical environments which made them the victim of sophisticated cyber-attacks that are designed to interrupt and damage their operations. Honeypots have been used as a key tool for aggregating real threat data e.g., malicious activities and payloads, to observe and determine different attack methods and strategies that can easily affect poorly secured cyber-physical systems. In this research, we deployed T-pot honeypot in Amazon Elastic Compute Cloud (AWS EC2) instance across six different regions to determine the current threat landscape as well as how knowledgeable and ingenious threat actors could be in compromising internet-facing Industrial Control System (ICS).

Keywords: ICS security · Cybersecurity · OT security · Honeypot · Cyber-physical security · Threat intelligence

1 Introduction

Industrial Control System (ICS) includes numerous types of control and management devices used by critical industries and smart factories, for instance,

H. Jin et al. (Eds.): CROWNCOM 2021/WiCON 2021, LNICST 427, pp. 307–324, 2022.
https://doi.org/10.1007/978-3-030-98002-3_23

Programmable Logic Controllers (PLC), Supervisory control and data acquisition (SCADA) etc. [1]. These are widely used to operate many critical infrastructures such as energy and smart grids, waste water treatment facilities, food and medicinal, oil and natural gas stations, transportation grids, and telecommunication which are essential to people's daily life. Disruption to these crucial public utilities may cause remarkable dam-ages and losses. The fourth industrial revolution (Industry 4.0) accelerated the integration of several industrial technologies in Information and Communication Technologies (ICT). The incidents of cyberattacks targeting ICS environments are steadily increasing due to the accessibility of interconnected modern ICS equipments and devices over the internet. Some noteworthy examples for rising the cyberattacks on ICS are inadequate security architecture and design, lack of baseline configuration and change management policy, inadequate security audits and standard monitoring procedures [2,3] etc.

In the last decade, cybercriminals had shown their notorious skills to undermine industrial core networks. In 2010, the infamous Stuxnet malware was used against Iran's nuclear installations which first showed that ICS networks are not secure [4]. Even in April 2021, we have seen another speculation of cyberattack at the Natanz uranium enrichment facility in Iran [5]. The network of a gas network operator in southern Germany and an energy network in Australia was injected by malformed commands caused disrupt controls in all flow operators in 2013 [6]. CrashOverride, which in 2015, triggered blackouts in Ukraine and left a large number of people with-out access to electricity for hours [7]. In 2017, Triton or Trisis malware was used to attack a Saudi petrochemical by the Xenotime hacking group, specifically targeting Triconex safety [8]. A recent report showed that critical industries across the world are being targeted by different notorious hacking groups [9]. Most attacks were carried out due to a lack of general protection in the communication protocols, applications, and operating systems used in ICS. While countless new threats are being generated on a daily basis, many of them depend on old security vulnerabilities to function. For too many malware looking to target the same few weaknesses over and over again, after they are found, one of the greatest risks an organization may face is failure to fix certain vulnerabilities. In addition, owing to severe real-time constraints and possibly fatal malfunction effects, these vital cyberphysical devices may sometimes not be upgraded or fixed, rendering it dangerous to conduct some kind of protection testing at all in live production systems. The necessity for security testing endures. To have an efficient threat defense system, we need to understand the current threat landscape and trending attack techniques.

This research contributes by illustrating large-scale threat analysis through deploying honeypots in various locations and it allows us to understand the vulnerabilities those are targeting Industrial Control System devices, collection of real intruders data including malware samples, exploits and post-exploitation activities for future analysis. The research conducted using a honeypot provides advantages over trying to spot intrusion in the real system. For example, a honeypot does not accept any legal traffic by design, so any logged behavior is

likely to be a probe or intrusion attempt. This makes it simple and easier to track and classify a collection of IP addresses used to carry out a network sweep. In comparison, these tell-tale indicators of an intrusion are quickly overlooked in the background when we're gazing at the traffic on our core network.

2 Background and Related Work

Honeypot is a purposely vulnerable machine to look attractive to attackers or auto-mated scanners that can be probed, inspected and eventually exploited by adversaries [10], allows to collect and store information on any attempted exploits. Honey-pots are classified into a low-interaction honeypot and high interaction honeypot. Low-interaction honeypots offer to learn quantitative information about adversaries intentions, tactics, techniques and procedures by emulating the operating system and different services over ports with limited interactions and minimal risk [11]. High-interaction honeypots are integrated with real-time operating system, applications and devices which are more complex to implement but attract sophisticated attackers to interact for a long time [11]. Researchers use both types of honeypots to conduct various kinds of threat landscape research. However, existing researches on ICS honeypots as exhibits in Table 1, were failed to simulate a wide range of services used by smart ICS and also incapable to aggregate vast amount of real data, in-depth threat analysis e.g., malware, exploit, post-exploitation activities. To overcome these shortcomings, we utilizes an open-source honeypot called T-pot [12] developed by Deutsche Telekom (DTAG) that contains a couple of Intrusion Detection System (IDS) sensors and can simulate a wide range of services and protocols. It is simple to set up and easy to investigate incidents using its user-friendly dashboard [13].

Honeypots is a useful technique to expose security vulnerabilities in major systems. It shows the high level of threat posed by attacks on different internet facing devices. It can also help to identify potential security gaps within the IT infrastructure which protection may need to be increased. There are some drawbacks of using a honeypot over attempting to detect interference into the actual system. For example, a honeypot does not accept any legal traffic by design, so any activity or event logged is likely to be a probe or intrusion attempt. That makes it much easier to spot payload patterns that are used to carry out a network sweep, such as common IP addresses (or IP addresses all coming from one country). For comparison, when you are looking at high volumes of legal traffic on your core network, those tell-tale signs of an intrusion are easy to miss in the chaos. The benefit of using honeypot encryption is that the only ones you see could be these malicious addresses, making it much easier to detect the threat. Since honeypots manage very small traffic, they are also light tools. They're not making major hardware demands; you can set up a honeypot with old machines that you don't need anymore.

Table 1. Summary of existing ICS honeypot related research.

Focus	Testbed	Protocols	Findings	Gaps
Honeynet [14]	Snort, Amazon EC2	Modbus, XMPP, DNP3, ICCP, TFTP, SNMP, IEC-104	Discovered SHODAN and non-SHODAN based peer interactions and correlation	Missing result on attackers techniques and payloads
CryPLH [15]	VMware	ISO-TSAP, SNMP HTTP, HTTPS	Effective simulation of Siemens PLC via Linux	Missing detail result and analysis on adversaries payloads, malware signature and post-exploitation activities
Conpot [16]	Splunk, Syslog	Modbus, HTTP, SNMP	Conpot sensor was used in pre-existing air gapped SCADA network	Lack of services simulation on more protocols
Custom Linux Based [17]	VMware	HTTP, HTTPS, SNMP, ISO-TSAP	Effective simulation using Siemens PLC with attacker's actions logging capability in high interaction environment	Testbed prepared with limited port services and in-depth result on attackers interactions are missing
Custom [18]	Snort	HTTP	BeEF tool was used to detect attacker locations accurately	Limited number of services were simulated over limited number of ports
Digital Bond Honeynet [19]	VMware, Snort	Modbus, SNMP, Telnet, FTP, HTTP, VxWorks Debugger	Limited interactions due to be deployed on university network	Limited interactions and attackers data for analysis

3 Methodology

3.1 Overview

In this research, our approach is to implement honeypots in AWS EC2 across multiple AWS regions to lure potential cyber criminals to make interaction with deployed honeypots and collect a huge amount of data for analysis as depicted in Fig. 1. Since low-interaction honeypots are easily identical, modification of default service banners and settings will be helpful to make them more real. The major goals are to monitor malicious intruders actions, analyze their origin and accrue different attack techniques, collecting malware samples and payloads. Furthermore, the obtained data could be shared to open-source community so

that researchers and security engineers can utilize those data to extend their research as well as enrich intrusion detection systems.

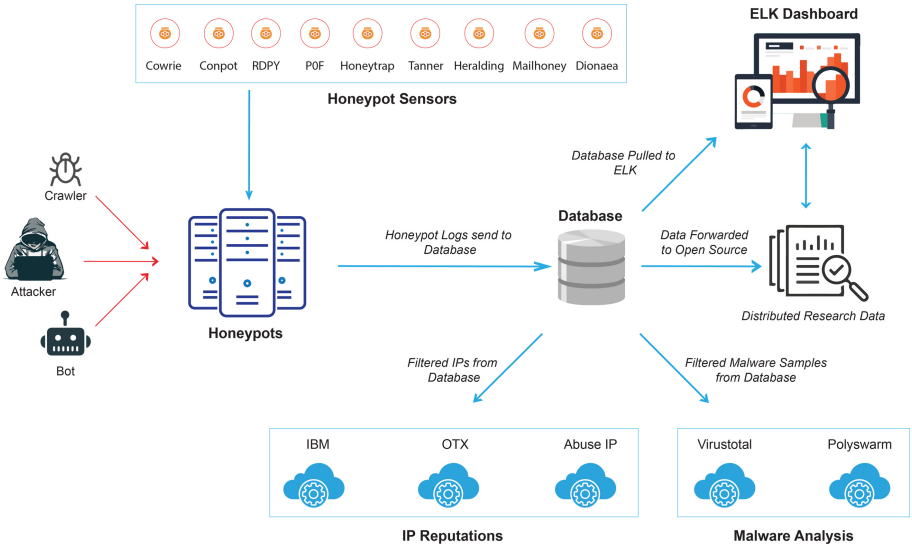


Fig. 1. Overview of experiment workflow.

3.2 T-Pot Installation

To handle a large number of attack processes and accumulate data from different places, Amazon Web Services Elastic Cloud Computing (AWS EC2) instances were chosen to install honeypot across six different regions. Following configuration was used for each instance:

```
Operating System: Debian (Stretch)
Ram: 32 GB, vCPUs: 8, Storage: 500 GB
Virtualization Type: HVM AMI
Instance Size: m5.xlarge
```

After configuring instances, Elastic IP or Public IP was allocated to each instance to avoid changing IP addresses after each reboot as well as make those instances publicly accessible through internet. SSH and Kibana dashboard were accessed over port 64295 and 64296, and security rules for both services were configured to restrict public access. Table 2 shows the information about deployed honeypots in six different regions using Amazon Elastic Compute Cloud (AWS EC2).

Table 2. Information about honeypot implementation in different AWS EC2.

Name	Region	Zone	Elastic IP	Instance ID
honeypot1	S. Africa	sa-east-1a	18.229.221.32	i-0fbe504f309251757
honeypot2	US East	us-east-2a	18.224.232.49	i-0106c86a7021f4ac
honeypot3	Europe	eu-north-1a	13.49.35.25	i-0fe18ac2494217ac5
honeypot4	Japan	ap-northeast-1a	52.194.106.24	i-00aba9778984dd671
honeypot5	Bahrain	me-south-1c	15.185.124.89	i-0be2b29a4a670f4e6
honeypot6	Australia	ap-southeast-2a	3.24.201.18	i-08be99ad2000ada56

4 Result Analysis

Our deployed honeypots were run from March 01, 2020 to April 22, 2020 and after deploying them on AWS EC2, they started getting the attention of attackers and scanners within a very short time. Table 3 exhibits the comparison of alerts received by different sensors based on different honeypot servers.

Table 3. Events captured by different sensors across different honeypot servers.

Sensors	Africa	USA	Europe	Japan	Bahrain	Australia
Dionaea	10711011	3218223	6361103	19281901	20771502	18222375
Cowrie	3273499	673290	3834526	1937548	2393980	1872987
Heralding	1072527	327941	2636491	1059014	395374	275885
Honeytrap	2122578	803156	1626080	933148	1120573	1018931
Rdpy	142722	12533	152024	619043	67578	28648
Adbhoney	7524	2811	13747	2190	135	944
Mailoney	4692	2455	12897	10636	6438	2601
Tanner	5170	1192	10533	7191	4083	2219
Conpot	1270	1086	872	800	876	1248
Total events	17340993	5042687	14648273	23851471	24760512	21425838

Dionaea: C and Python based low-interaction honeypot sensor which logging capabilities offer compatibility with log.json, hpfeeds, Fail2Ban and log.sqlite. The highest amount of log captured by this sensor is 18222375 in Australia region.

Cowrie: Cowrie is a medium SSH honeypot interaction that provides a Debian 5.0-based fake file system, enabling user to include and remove files as their wish. This program often stores in a safe and quarantined region all the downloaded and uploaded data, so if appropriate, we may conduct later re-view. This sensor recorded highest number of log which is 3273499 in Africa region and lowest amount of log in USA region.

Heralding: In Table 3 we got 1072527 logs from honeypot Africa on the honeypot service named Heralding. This honeypot sensor is nothing more but simply gathers credentials by emulating following protocols: ssh, ftp, telnet, http, https, imap, imaps, pop3, pop3s, smtp, vnc, socket5 and postgresql5. This sensor recorded 1072527 amount logs in Africa region which is the highest among other regions.

Honeytrap: Honeytrap is an extensible and open-source framework for honeypots to be run, tracked and maintained. In Africa region, there are 2122578 number of logs captured by this sensor.

Remote Desktop Protocol (RDPY): This python-based honeypot sensor was de-signed to function as vulnerable Microsoft RDP service (client and server side). In this service, the lowest and the highest number of logs are 12533 and 142722 respectively.

Mailhoney: Mailhoney is a Simple Mail Transfer Protocol (SMTP) Honeypot. There are various modules or types that provide custom modes.

Tanner: A remote data review and classification service to analyze and compose the response of HTTP queries, then served by Super Next Generation Advanced Reactive Honeypot (SNARE). When offering responses to SNARE, TANNER utilizes several program vulnerability style emulation approaches.

Conpot: Conpot is a low interactive honeypot engineered to be easy to install, change and extend. It encompasses with a set of standard industrial control protocols, capable of emulating complex infrastructures to persuade a competitor that he has just discovered a massive industrial complex.

Table 4 shows the connections received from different type of users and crawlers which are automatically categorized by honeypot sensor based on IP reputation.

Table 4. Interactions received from various sources.

Type	Africa	Australia	USA	Japan	Bahrain	Europe	Total
Known attacker	6026579	2564464	807187	689	2745911	4365988	16510818
Mass scanner	4909	28	1191	49	942	4140	11259
Bad reputation	1661122	14340	474263	10	3911	402237	2555883
Bot, crawler	32330	15	175	2	2957	1380	36859
Compromised	1054	–	9	–	11	95	1169

4.1 Attacks Origin Breakdown

In Table 5, we have presented the connections received by different ICS devices where IPMI device received the highest number of interactions and Siemens S7-200 PLC received the lowest number of interactions from attackers.

Intelligent Platform Management Interface (IPMI) is used to handle hardware over port 623 on a network. It is mainly used to track data such as temperatures or power status of devices in the network for industrial control

systems. By booting, restarting, or switching them off, IPMI will monitor devices as well. Documentation of device action and data are also logged using IPMI. The number of IPMI connections received by geo-location are shown in Table 6.

Table 5. Interactions received by different ICS devices.

ICS devices	Africa	Australia	Bahrain	Europe	USA	Japan	Total
IPMI	441	364	269	232	362	318	1986
Guardian AST	379	382	201	227	317	220	1726
Siemens S7-200	246	228	129	116	85	125	929
Smart meter	204	274	277	297	322	137	1511

Table 6. IPMI connections received by geo-location.

Country	Africa	Australia	Bahrain	Europe	USA	Japan
United States	139	95	–	–	44	12
China	67	13	73	69	92	80
Brazil	95	135	–	40	1	152
UK	5	2	63	96	87	–
France	–	4	2	–	–	16
Hong Kong	94	75	26	4	–	–
Russia	41	–	86	23	125	58
Seychelles	–	40	19	–	13	–

Guardian AST is a gas tank monitoring system that was simulated through port 10001. Table 7 shows the interactions received by geo-location of Guardian AST. The most targeted gas tanks were the ones in the Australia (382), followed by the ones in Africa (379).

Table 7. Guardian AST interactions received by geo-location.

Country	Africa	Australia	Bahrain	Europe	USA	Japan
United States	286	103	12	23	–	–
China	–	32	–	13	–	43
UK	–	9	122	97	8	112
France	18	23	52	–	21	9
Seychelles	8	148	11	–	9	–
Russia	60	–	1	22	277	56
Hong Kong	–	–	–	57	2	–
Moldova	7	67	3	15	–	–

Conpot simulated Programable Logic Controller (PLC) through the S7 Communication protocol over tcp port 102. In Table 8 and 9 shows the interaction received by geo-location of Simens S7-200 and Smart Meter where S7-200 received the highest number of attacks in Africa based honeypot and Smart Meter received the highest number of interactions in USA based honeypot.

Table 8. Simens S7-200 interactions received by geo-location.

Country	Africa	Australia	Bahrain	Europe	USA	Japan
United States	60	–	11	–	–	11
China	85	–	–	23	43	24
United Kingdom	–	71	48	3	–	–
France	6	30	54	–	2	10
Seychelles	–	21	3	–	–	7
Russia	27	3	–	10	13	69
Hong Kong	54	15	8	51	–	3
Netherlands	14	9	–	9	27	1
Germany	–	79	5	20	–	–

Table 9. Originating countries for Smart Meter interactions.

Country	Africa	Australia	Bahrain	Europe	USA	Japan
United States	–	6	54	44	284	24
China	–	–	90	–	–	5
UK	195	177	77	83	2	32
France	6	–	35	4	–	50
Seychelles	2	78	–	140	36	26
Germany	1	13	21	26	–	–

4.2 Attacks Scenario

Different username and password combination were used by malicious attackers to carry out brute force authentication attack that was logged by honeypot sensors. These usernames and passwords were scanned against the largest dictionary wordlist rockyou.txt to find out the percentage of unique usernames and passwords received through all six honeypot servers as depicted in Fig. 2 and 3.

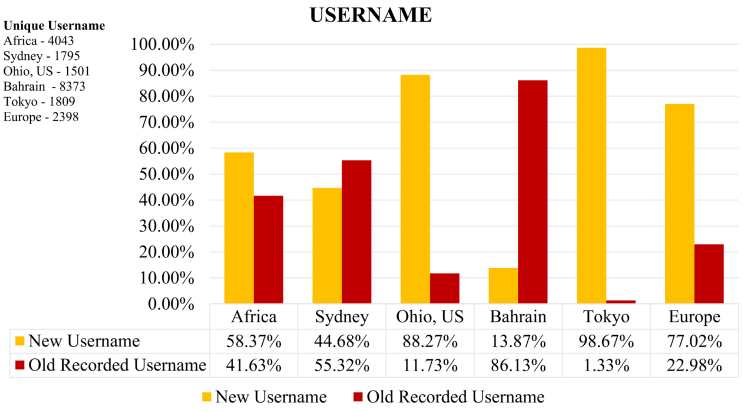


Fig. 2. Rate of unique and old usernames received.

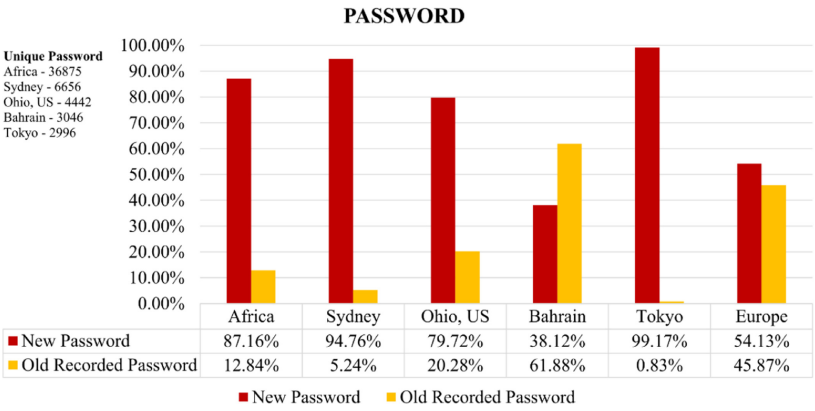


Fig. 3. Rate of unique and old password received.

Tokyo based honeypot recorded highest percentage of new username and password combination whether Bahrain based honeypot observed highest rate of previously used username and password combination. These commonly used weak username and password should be avoided for ICS devices and their corresponding services.

Table 10 illustrates the numbers of different types of authentication events captured across different region-based honeypots.

Table 10. Different types of authentication events recorded in all honeypots.

Event name	Africa	Europe	USA	Australia	Japan	Bahrain
Login attempt	20217	16771	16844	17380	7552	13659
Root failed authentication	319	388	397	366	208	483
Trying authentication password	1044	1003	439	408	438	879
Authenticated	2076	1747	1833	1826	793	1242
Remote error	19751	16200	15088	17158	6793	15232
Direct-TCP connection request	190	2912	44	36	76	14
Connection lost	25784	20668	18621	18262	15773	15663

Post-exploitation, as the term implies, literally involves the levels of action after the perpetrator has breached the mechanism of a target. The importance of the compromised device is calculated by the value of the real knowledge contained in it and how it may be exploited for harmful reasons by an intruder. Through this fact, the notion of post-exploitation has only emerged as to how you might utilize the data of the victim's corrupted device. In reality, this stage is about gathering confidential information, logging it, and getting an understanding of configuration configurations, network interfaces, and other channels of communication.

After honeypot systems were exploited, attackers executed different commands and conducted lateral movement, as seen in Table 11 and Table 12.

Table 11. Different types of post-exploitation activities.

Action type	Africa	Australia	USA	Japan	Bahrain	Europe
Pivot attacks	535	415	490	458	1010	646
CPU info	1671	1271	1507	1655	3493	2055
Crontab info	554	422	502	557	1162	681
Clean history	0	0	1	12	6	3
Operating system info	1129	1270	1009	1678	3467	2047
File execute	1130	850	1008	1127	2324	1364
Botnet	24	31	23	21	42	21
Change password	270	210	278	216	1717	434
Delete files	76	8	48	647	611	71
Shells	72	21	82	164	553	84

Table 12. Sample of commands executed after post-exploitation.

Command Type	Command input
Cleanup bash history	cat /dev/null >~/.bash_history && history -c && exit
CPU info	lscpu lscpu — grep Model cat /proc/cpuinfo — grep model — grep name — wc -l
System Info	sudo lshw -short hwinfo -short lsscsi
Remove files	rm -rf /var/tmp/.var03522123 rm -rf /var/tmp/dota*
Lateral Movement	CMD: cd ~ && rm -rf .ssh && mkdir .ssh && echo "ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli 2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7+vD0EpZ3Tz /+0kX34uAx1RV/75GVOmNx+9EuWOnvNoaJe0QXxziIg9eLBHpgLMuak b5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmPecjd ySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGPK5w6hYp5 zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQTTWYYjIIu5Pm Uux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw==mdrfckr">>.ss h/authorized_keys && chmod -R go= ~/.ssh && cd ~

Attackers used different types of known vulnerabilities to exploit our honeypot services. Figure 4 shows the number of various CVE used to exploit different services running within honeypots. CVE-2006-2369, CVE-2002-0013 and CVE-2002-2012 were mostly used to exploit our honeypot services. This indicates that known vulnerabilities and outdated services are lucrative endpoint for attackers to exploit and get into the internal networks.

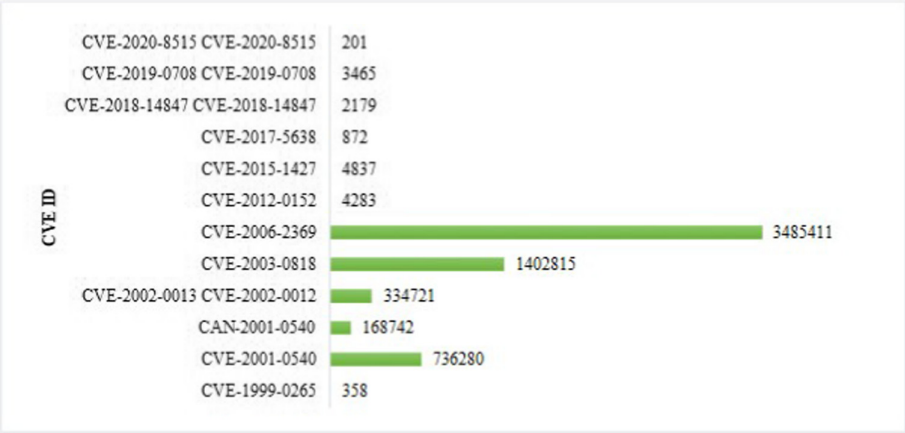


Fig. 4. CVE used to exploit honeypot services.

4.3 Malware Analysis

The malware samples received from all six honeypots were listed by unique hashes and uploaded to the VirusTotal website to find their categories. The VirusTotal scan provided results with 60% ransomware and 40% trojan. In Table 13, some sample malware hashes and corresponding malware type is provided.

Table 13. Types of malware with signature.

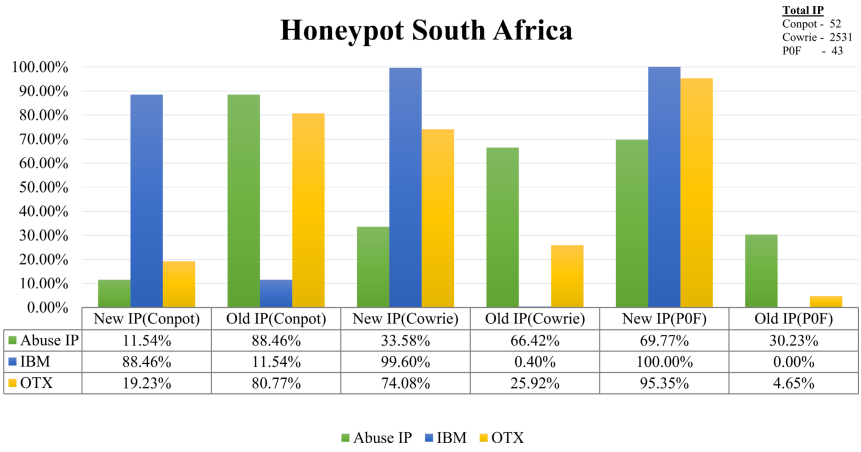
Malware types	Malware signature
Ransomware	414a3594e4a822cfb97a4326e185f620
Trojan	33d373e264dc7fdb0bcdbd8e075a6319
Trojan	759c8ee1f7042c118573a85407fec743
Trojan	414a3594e4a822cfb97a4326e185f620
Trojan	8c17c326a6be24f9fa845fea48106c3a
Ransomware	46e7d73f5bce2770af1e8626eb918af8
Trojan	6009b7eeced6e2ab0fb6df51887c2308
Trojan	ce223b231f2862124386c585e9b95ca1
Ransomware	ae12bb54af31227017feffd9598a6f5e
Ransomware	996c2b2ca30180129c69352a3a3515e4

4.4 IP Reputation

The reputation of the IP address is dependent on another IP address, such as whether it is registered with a data center, storage company, or a cellular or residential network. If their credibility is bad or if several IPs inside the subnet often participate in suspicious activity, certain services totally block whole neighborhoods of IP addresses. From the honeypot logs, all IPs were extracted

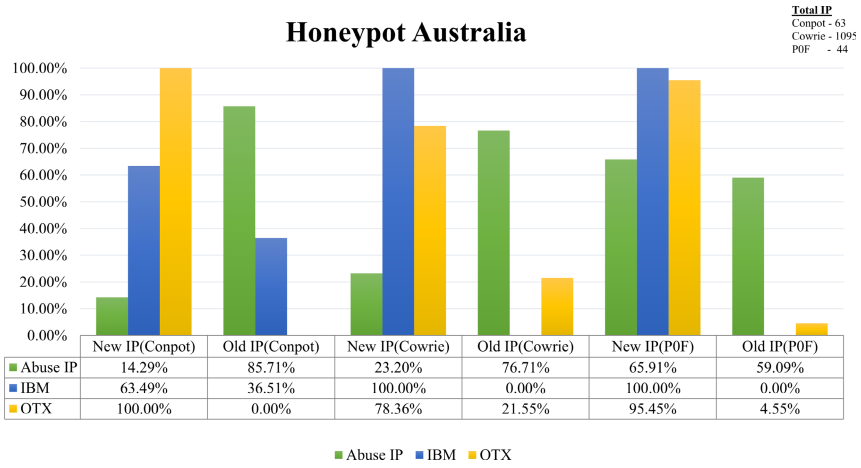
and duplicated IP records were removed. The unique IPs from all six honeypot servers were scanned against AbuseIP, IBM X-Force and AlienVault OTX to find their IP reputation. In this part of experiment all the unique IPs were analysed using these services with a specific range of score. Newly recorded source IPs have less or mere bad reputation, whether old IPs are reported multiple times as attackers or scanners. A sample bash script to check IP threat score from AlienVault OTX is given below:

Figure 5, 6, 7, 8, 9 and 10 illustrates IP reputation received from different sensor across the six honeypots. The data reveals that the largest percentage of newly recorded malicious IPs were received by P0F sensor. Later, all malicious IPs were submitted to AbuseIP database based on their attacks or intention types such as brute force attacks, exploitation attempts etc.



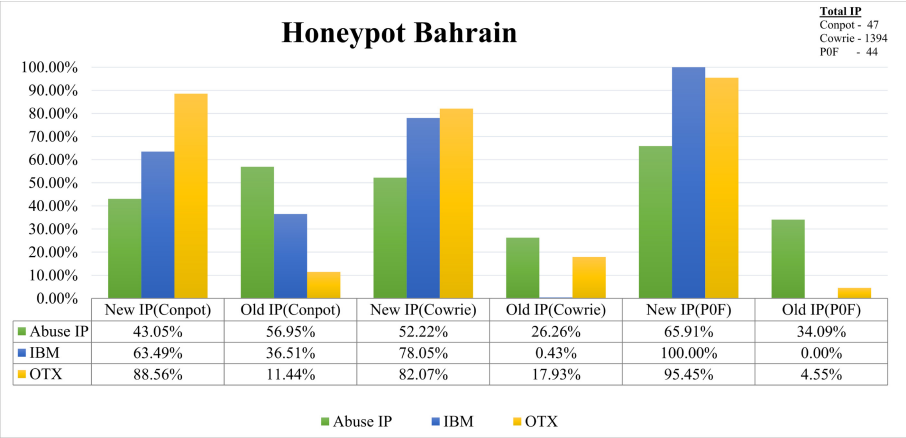
	New IP(Conpot)	Old IP(Conpot)	New IP(Cowrie)	Old IP(Cowrie)	New IP(P0F)	Old IP(P0F)
Abuse IP	11.54%	88.46%	33.58%	66.42%	69.77%	30.23%
IBM	88.46%	11.54%	99.60%	0.40%	100.00%	0.00%
OTX	19.23%	80.77%	74.08%	25.92%	95.35%	4.65%

Fig. 5. Comparison of IP reputation (Africa Honeypot).



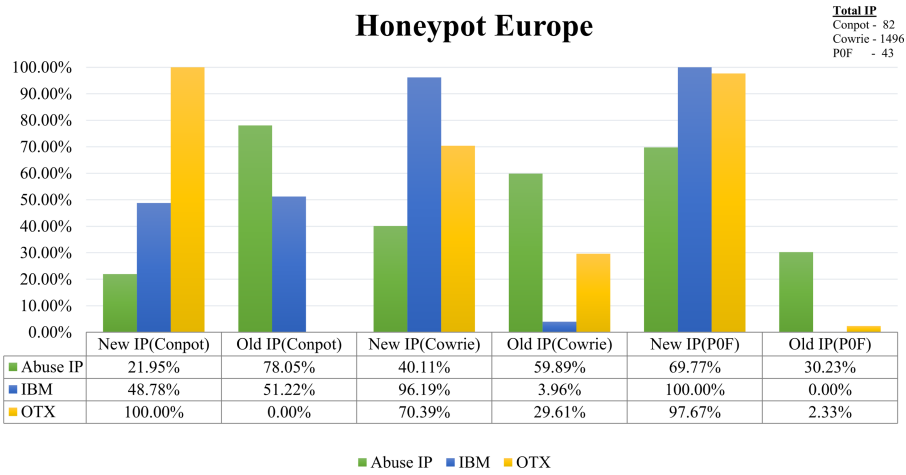
	New IP(Conpot)	Old IP(Conpot)	New IP(Cowrie)	Old IP(Cowrie)	New IP(P0F)	Old IP(P0F)
Abuse IP	14.29%	85.71%	23.20%	76.71%	65.91%	59.09%
IBM	63.49%	36.51%	100.00%	0.00%	100.00%	0.00%
OTX	100.00%	0.00%	78.36%	21.55%	95.45%	4.55%

Fig. 6. Comparison of IP reputation (Australia Honeypot).



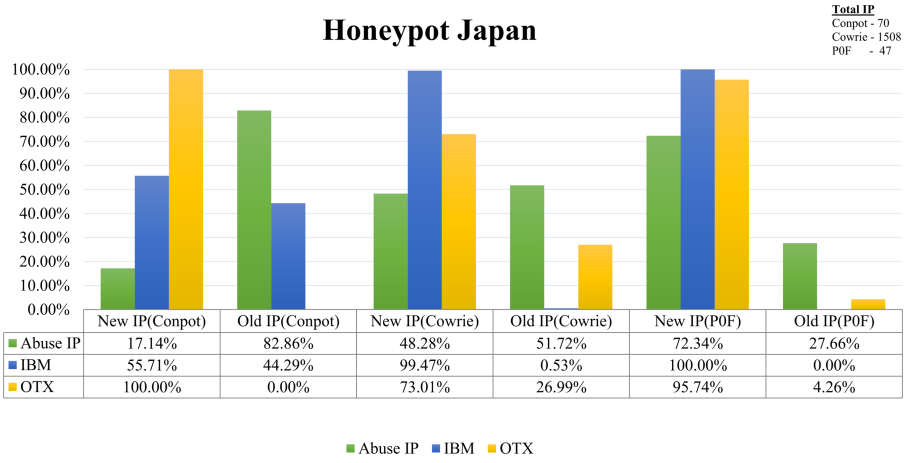
	New IP(Conpot)	Old IP(Conpot)	New IP(Cowrie)	Old IP(Cowrie)	New IP(P0F)	Old IP(P0F)
Abuse IP	43.05%	56.95%	52.22%	26.26%	65.91%	34.09%
IBM	63.49%	36.51%	78.05%	0.43%	100.00%	0.00%
OTX	88.56%	11.44%	82.07%	17.93%	95.45%	4.55%

Fig. 7. Comparison of IP reputation (Bahrain Honeypot).



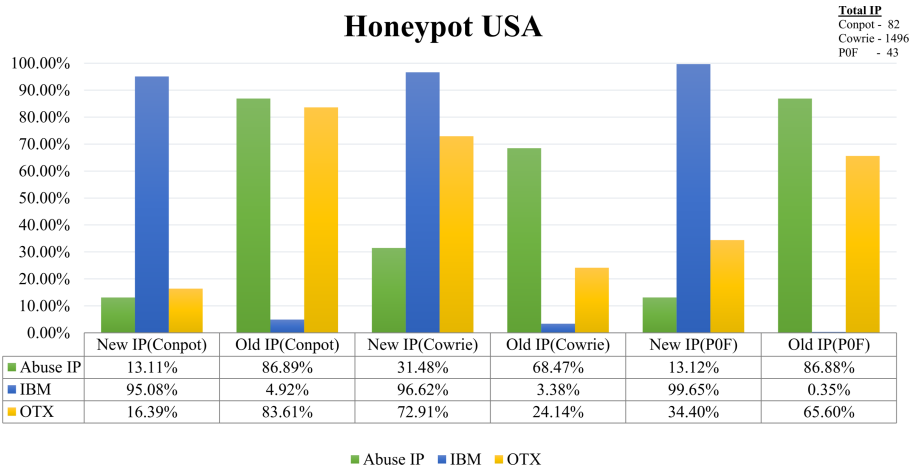
	New IP(Conpot)	Old IP(Conpot)	New IP(Cowrie)	Old IP(Cowrie)	New IP(P0F)	Old IP(P0F)
Abuse IP	21.95%	78.05%	40.11%	59.89%	69.77%	30.23%
IBM	48.78%	51.22%	96.19%	3.96%	100.00%	0.00%
OTX	100.00%	0.00%	70.39%	29.61%	97.67%	2.33%

Fig. 8. Comparison of IP reputation (Europe Honeypot).



	New IP(Conpot)	Old IP(Conpot)	New IP(Cowrie)	Old IP(Cowrie)	New IP(P0F)	Old IP(P0F)
Abuse IP	17.14%	82.86%	48.28%	51.72%	72.34%	27.66%
IBM	55.71%	44.29%	99.47%	0.53%	100.00%	0.00%
OTX	100.00%	0.00%	73.01%	26.99%	95.74%	4.26%

Fig. 9. Comparison of IP reputation (Japan Honeypot).



	New IP(Conpot)	Old IP(Conpot)	New IP(Cowrie)	Old IP(Cowrie)	New IP(P0F)	Old IP(P0F)
Abuse IP	13.11%	86.89%	31.48%	68.47%	13.12%	86.88%
IBM	95.08%	4.92%	96.62%	3.38%	99.65%	0.35%
OTX	16.39%	83.61%	72.91%	24.14%	34.40%	65.60%

Fig. 10. Comparison of IP reputation (USA Honeypot).

5 Conclusion

Honeypot is an intentionally vulnerable computer system that plays a crucial role in moving away attacker's attention from the production systems. It enables us to better understand the attacker's motive, methods and strategies by collecting and logging attacker's information through mimicking the environment as a real system. Intruder's information received through honeypots could be used to develop machine learning-based intrusion detection. The more attackers lured to the honeypot systems, and the more real information could be obtained. As the research progressed, more and more curious peers are drawn to our system.

Threat actors also connected and exploited our honeypot systems, thinking of them as a real machine. The findings clearly indicate that current attacks in OT infrastructures follow similar attack trends for common IT environments. It is understood that each attacker follows his own "strategy" in order to be able to complete the attack. However, certain tasks of a general nature that they can carry out may be recognized as their goal. Specifically, the most common attack vectors against critical infrastructures include brute force authentication, remote code execution and buffer overflow attack on exposed devices through known vulnerabilities, malware attacks in the networks after post-exploitation. Our findings from this experiment should serve as cautionary examples for smart industries, particularly those that run internet-facing ICS, to ensure that adequate security measures are in place on their systems.

References

1. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: NIST special publicayion 800–82, revision 2: Guide to Industrial Control Systems (ICS) Security (2014). https://doi.org/10.6028/NIST.SP.800-82r2
2. Weiss, J.: Protecting Industrial Control Systems from Electronic Threats. Momentum Press (2010). ISBN: 978-1-60650-197-9
3. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security - a survey. IEEE Internet Things J. **4**(6), 1802–1831 (2017)
4. Hemsley, K.E., Fisher, E., et al.: History of industrial control system cyber incidents, Technical report, Idaho National Lab. (INL), Idaho Falls, ID (United States) (2018)
5. Corera, G.: Iran nuclear attack: mystery surrounds nuclear sabotage at natanz. In: BBC News (2021). https://www.bbc.com/news/world-middle-east-56722181.. Accessed 29 Sept 2021
6. Masood, R.: Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives. Cybersecurity and Privacy Research Institute the George Washington University (2016)
7. D. U. Case, Analysis of the cyber attack on the ukrainian power grid, Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388 (2016)
8. Di Pinto, A., Dragoni, Y., Carcano, A.: Triton: the first ICS cyber attack on safety instrument systems. Proc. Black Hat USA **2018**, 1–26 (2018)
9. Slowik, J.: Evolution of ICS attacks and the prospects for future disruptive events, Threat Intelligence Centre Dragos Inc (2019)
10. Provos, N.: Honeyd-a virtual honeypot daemon. In: 10th DFN-CERT Workshop, vol. 2, p. 4. Hamburg, Germany (2003)
11. Mokube, I., Adams, M.: Honeypots: concepts, approaches, and challenges. In: Proceedings of the 45th Annual Southeast Regional Conference, pp. 321–326 (2007)
12. T-pot - The All In One Honeypot Platform. https://github.com/dtag-dev-sec/tpotce. Accessed 29 Sept 2021
13. Rashid, S.Z.U., Uddin, M.J., Islam, A.: Know your enemy: analysing cyber-threats against industrial control systems using honeypot. In: 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), pp. 151–154. IEEE (2020)

14. Serbanescu, A.V., Obermeier, S., Yu, D.-Y.: Ics threat analysis using a large-scale honeynet. In: 3rd International Symposium for ICS and SCADA Cyber Security Research 2015 (ICS-CSR 2015), vol. 3, pp. 20–30 (2015)
15. Buza, D.I., Juhász, F., Miru, G., Félegyházi, M., Holczer, T.: Cryplh: protecting smart energy systems from targeted attacks with a plc honeypot. In: International Workshop on Smart Grid Security, pp. 181–192. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10329-7_12
16. Scott, C., Carbone, R.: Designing and Implementing a Honeypot for a Scada Network, vol. 39. SANS Institute Reading Room (2014)
17. Buza,D., Juhasz, F., Miru, G.: Design and implementation of critical infrastructure protection system. In: Budapest University of Technology and Economics, Department of Networked Systems and Services, pp. 1–58 (2013)
18. Wilhoit, K.: The Scada that Didn't Cry Wolf. Trend Micro Inc., White Paper (2013)
19. Wade, S.M.: SCADA Honeynets: the attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats (2011)