1. Introduction

The first honeypot studies were released by Clifford Stoll in 1990 in his book The Cuckoo's Egg. Since then, the demand for honeypot technology has only increased. Efforts to monitor attackers have been continued at the Canadian Honeynet chapter, which was founded at the University of New Brunswick, NB, Canada in April in 2008.

In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally, honeypots essentially turn the tables for Hackers and Computer Security Experts. They consist of a computer, data, network, or a site that appears to be part of a network but is isolated. These systems seem to contain information or a resource that would be of value to attackers.

The benefits of having a honeypot include:

- The ability to observe attackers in action and learn about their behavior
- Gather intelligence on attack vectors, malware, and exploits. Then use that intel to train your IT staff
- Create profiles of attackers that are trying to gain access to your systems
- Improve your security posture
- Waste attackers' time and resources
- Reduced false positive rate of detection systems
- Cost Effective

Our primary objectives are to gain insight into the security threats, vulnerabilities, and behavior of the attackers, investigate tactics and practices of the hacker community, and share learned lessons with the IT community and the appropriate forums in academia and Canadian law enforcement. In pursuit of these goals the CIC is using cutting edge technology to collect a dataset for Honeynet which includes honeypots on the inside and outside of our network.

These reports are generated based on the weekly traffic collected in our network. For more information or to request the weekly captured data, please contact us at <EMAIL-ADDRESS>.

2. Technical Setup

In the CIC-T_POT project, we have defined a separated network with these services:

- ADB(Android Debug Bridge over TCP/IP)(ADBHoney)
- -HTTPS(CitrixHoneypot)
- -SNMP-ASF-RMCP-IPMI-RMCP(Conpot)
- -SSH-Telnet(Cowrie)

- -DICOM(Digital Imaging and Communications in Medicine)(Dicompot)
- -FTP-TFTP-RPC-SAMBA-SQL-MySQL(Dionaea)
- -ElasticSearch(ElasticPot)
- -SSH(Endlessh)
- -SSH(Glutton)
- -POP-IMAP-IMAPS-POP3s-SOCKs5-PostgreSQL-VNC(Heralding)
- -HTTP(HellPot)
- -SAP(HoneySAP)
- -IPP(IPPHoney)
- -SMTP(Mailoney)
- -HL7-HFIR(Medpot)
- -RDP(RDPY)
- -RedisRedisHopyPot)
- -HTTP(SNARE)
- -HTTP(TANNER)

Inside the network there are faux real users. Each user has real behaviors and surfs the Internet based on the above protocols. The web server is accessible to the public and anyone can see the website. Inside the network, we put Untangle firewall at the edge of the network and NAT different services for public users. In the firewall, some ports such as 20, 21, 22, 53, 80, 143, 443 are opened intentionally to capture and absorb attackers' behaviors. Also, there are some weak policies for PCs such as setting common passwords. The data the PC's capture is mirrored through TAPs and is captured and monitored by TCPDump and Security Onion.

Furthermore, we use WordPress 4.9.4 and MySQL as databases to publish content on the website. We have also formed a kind of honeypot inside of the contact form. So, when the bots want to produce spams, we can grab these spams through "Contact Form 7 Honeypot" (Figure 1).

Figure1: Contact Form 7 Honeypot

_____

CIC-Honeynet uses T-POT tool outside the firewall which is equipped with several tool s. T-Pot is based on well-established honeypot daemons which include IDS and other tools for attack submission.

T-Pot is the all in one, optionally distributed, multiarch (amd64, arm64) honeypot plattform, supporting 20+ honeypots and countless visualization options using the Elastic Stack, animated live attack maps and lots of security tools to further improve the deception experience.

T-Pot is based on the Debian 11 (Bullseye) Netinstaller and utilizes docker and docker-compose to reach its goal of running as many tools as possible simultaneously and thus utilizing the host's hardware to its maximum.

The idea behind T-Pot is to create a system, which defines the entire TCP network range as well as some important UDP services as a honeypot . It forwards all incoming attack traffic to the honeypot daemons best suited to respond and process it. T-Pot includes docker versions of the following honeypots:

- adbhoney,
- ciscoasa,
- citrixhoneypot,
- conpot,
- cowrie,
- ddospot,
- dicompot,
- dionaea,
- elasticpot,
- endlessh,
- glutton,
- heralding,
- hellpot,
- honeypots,
- honeytrap,
- ipphoney,
- log4pot,
- mailoney,
- medpot,
- redishoneypot,
- sentrypeer,
- snare,
- tanner

Figure 2 demonstrates the network structure of the CIC - Honeynet and associated security tools. There are two TAPs for capturing, network activities. Outside the firewall, there is T-POT which captures the users' activities through external-TAP. Behind the **Untangle** firewall in the internal network Security

Onion has been used to analyze the captured data through internal-TAP. It is a Linux distro for intrusion detection, network security monitoring, and log mana gement. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and other security tool s.

In the internal network three PCs are running the CIC-Benign behavior generator (an in house developed agent), which generates activity such as internet surfing, FTP uploading and downloading, and Emailing. Also, four servers include Webserver with WordPress, and MySQL, Email Server (Postfix), File Server (Openmediavault) and SSH Server have been installed for different common services. We will change our firewall structure to test different brands every month.
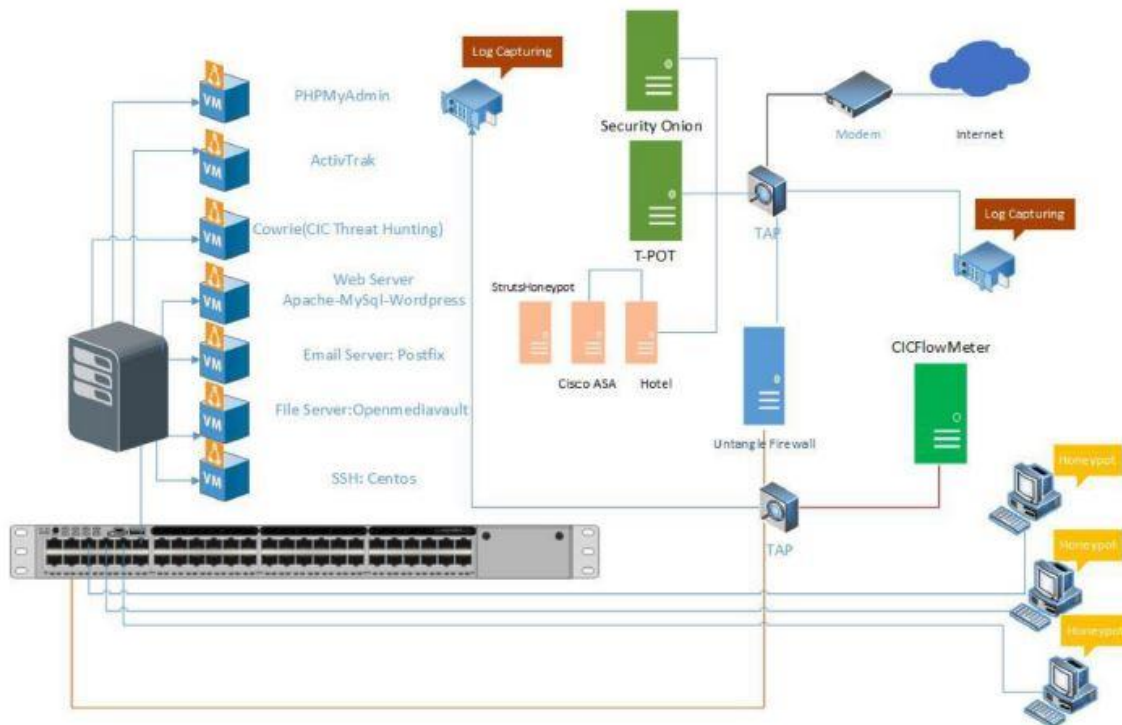

Figure2: Network Diagram

We use T-POT tools as it is demonstrated in figure 2 .These tools are used for specific attacks :

- **Cowrie** : mimic the SSH command inside the firewall and captures the user commands. Some easy password such as 1234, 123... are entered in cowrie database to make it vulnerable to attackers.

- **Adbhoney** : The Android Debug Bridge (ADB) is a protocol designed to keep track of both emulated

and real phones/TVs/DVRs connected to a given host.

- **Ciscoasa** : A low interaction honeypot for the Cisco ASA component capable of detecting CVE-2018-0101, a DoS and remote code execution vulnerability.

- **Citrixhoneypot** : Detect and log CVE-2019-19781 scan and exploitation attempts.

- **Conpot** : Conpot is a low interactive server side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend. By providing a range of common industrial control protocols .

- **DDoSPot** : DDoSPot is a honeypot "platform" for tracking and monitoring UDP-based Distributed Denial of Service (DDoS) attacks.

- **Dicompot** : Dicompot is a Digital Imaging and Communications in Medicine (DICOM) Honeypot.

- **Dionaea** : Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls.

- **ElasticPot** : ElasticPot is an Elasticsearch Honeypot. This is a honeypot simulating a vulnerable Elasticsearch server opened to the Internet. It uses ideas from various other honeypots, like [ADBHoneypot](#) (for output plugin support), [Citrix Honeypot](#) (for general structure), [Elastichoney](#).

- **Endlessh** : Endlessh is an SSH tarpit [that *very* slowly sends an endless, random SSH banner](#).

- **Glutton** : Glutton provide SSH and a TCP proxy. SSH proxy works as a MITM between attacker and server to log everything in plain text.

- **Heralding** : Heralding simple honeypot that collects credentials,

- **HellPot** : HellPot is an endless honeypot based on [Heffalump](#) that sends unruly HTTP bots to hell.

- **Honeypots** : 25 low-high level honeypots in a single PyPI package for monitoring network traffic, bots activities, and username \ password credentials.

- **Honeytrap** : Honeytrap is a network security tool written to observe attacks against TCP or UDP services.

- **IPPHoney** : This is a honeypot simulating a printer that supports the Internet Printing Protocol and is exposed to the Internet.

- **Log4Pot** : A honeypot for the Log4Shell vulnerability (CVE-2021-44228).

- **Mailoney** : Mailoney is a SMTP Honeypot.

- **Medpot** : Medpot Is a honeypot that tries to emulate HL7 / FHIR honeypot.It is a highly interactive honeypot system that supports the Redis protocol. Developed in Golang language.

- **RedisHoneyPot** : It is a highly interactive honeypot system that supports the Redis protocol. Developed in Golang language.

- **SentryPeer** : SentryPeer is a fraud detection tool. It lets bad actors try to make phone calls and saves the IP address they came from and number they tried to call.

- **Snare** : Snare, a web application honeypot sensor, is the successor of Glastopf. SNARE has feature parity with Glastopf and allows to convert existing web pages into attack surfaces.

- **Tanner** : Tanner is Snares "brain". Every event is send from SNARE to TANNER, gets evaluated and TANNER decides how SNARE should respond to the client.

... alongside the following tools ...

- Cockpit for a lightweight and secure WebManagement and WebTerminal.
- Cyberchef a web app for encryption, encoding, compression and data analysis.
- Elastic Stack to beautifully visualize all the events captured by T-Pot.
- Elasticvue a web front end for browsing and interacting with an Elastic Search cluster.
- Fatt a pyshark based script for extracting network metadata and fingerprints from pcap files and live network traffic.
- Geoip-Attack-Map a beautifully animated attack map optimized for T-Pot.
- P0f is a tool for purely passive traffic fingerprinting.
- Spiderfoot an open source intelligence automation tool.
- Suricata a Network Security Monitoring engine.

... to give you the best out-of-the-box experience possible and an easy-to-use multi-honeypot appliance.

3. T-Pot Report

In this section, we give an overview of the of the attacks on T-Pot.

T-Pot Attacks Overview

_____

We analyzed the IP addresses that made login attempts using the T-POT. The top ten Honeypots that we received login attempts from are listed in Table 1,Figure 1,2.

Table 1: Honeypots Attacks

Honeypots	Attacks(Dec**16th-Dec31th**)	Attacks(Dec 1**th-15th**)
Heralding	369,386	391,672
Cowrie	201,997	218,735
Ciscoasa	149,776	146,349
RedisHoneypot	89,885	94,784
Dionaea	12,375	10,786
Tanner	8,993	7,573
Sentrypper	4,011	3,784
Honeytrap	3,774	4,957
Adbhoney	3,239	3,479
ElasticPot	2,723	2,894
Mailoney	1826	1948
Conpot	616	739
Dicompot	212	249
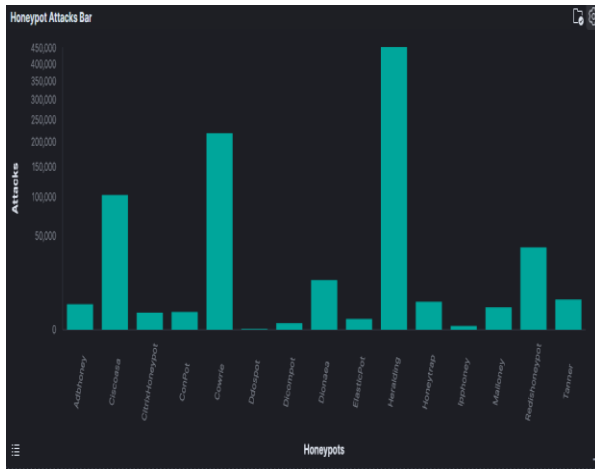
Figure 1 : Honeypots Attacks Bar
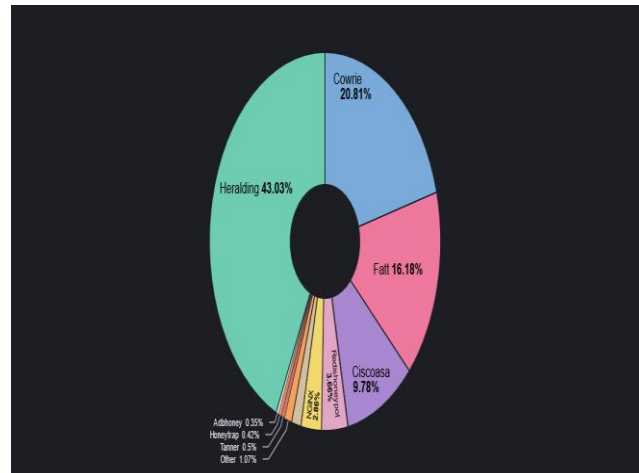
Figure 2: Honeypots Attacks Pie chart

In Table2, top 10 of source IP addresses and the number of attacks are showcased.

Table 2: Attacker Source IP-Top 10

Source IP	Count
185.170.144.131	92,242
185.170.144.129	71,298

185.170.144.130	57,969
185.196.8.45	45,416
185.73.125.23	40,721
87.251.07.229	29,696
94.232.43.201	20,500
185.73.124.20	13,337
79.124.56.106	12,111
185.73.124.159	10,356

In Table3, Figure3, top 10 of country and the number of attacks are showcased.

Table 3: Attacks by country

Country	Count
Estonia	3,209,434
United States	732,789
Russia	589,356
Poland	493,272
Bulgaria	409,434
China	216,012
Australia	197,696
Canada	179,734
Netherlands	94,469
Germany	78,588
Other	448,248
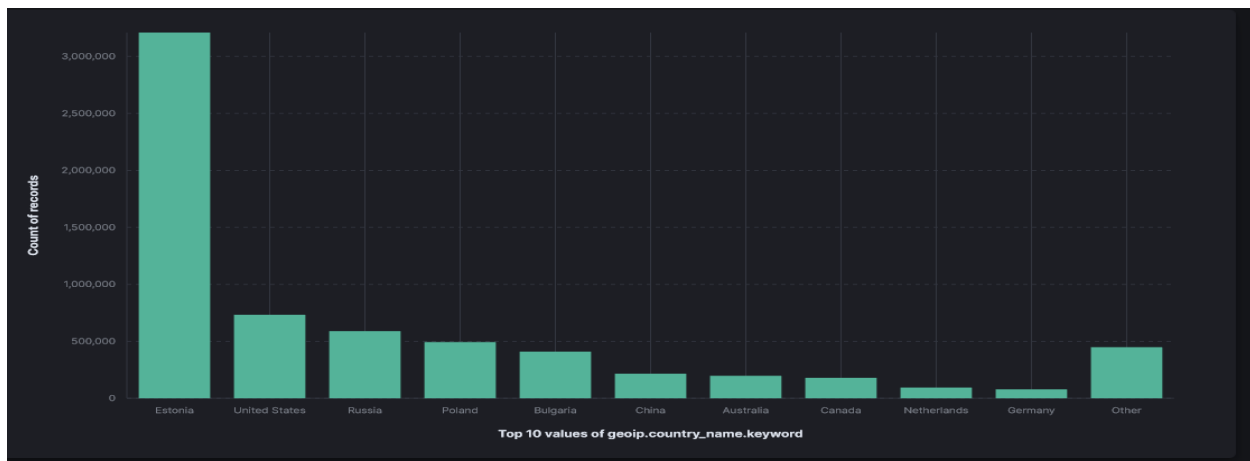
Figure 3: Attacks by country Bar

Table 4 and Figure 4 show 99% attackers use Linux 2.2x-3x.

Table 4: Attacks by OS Distribution

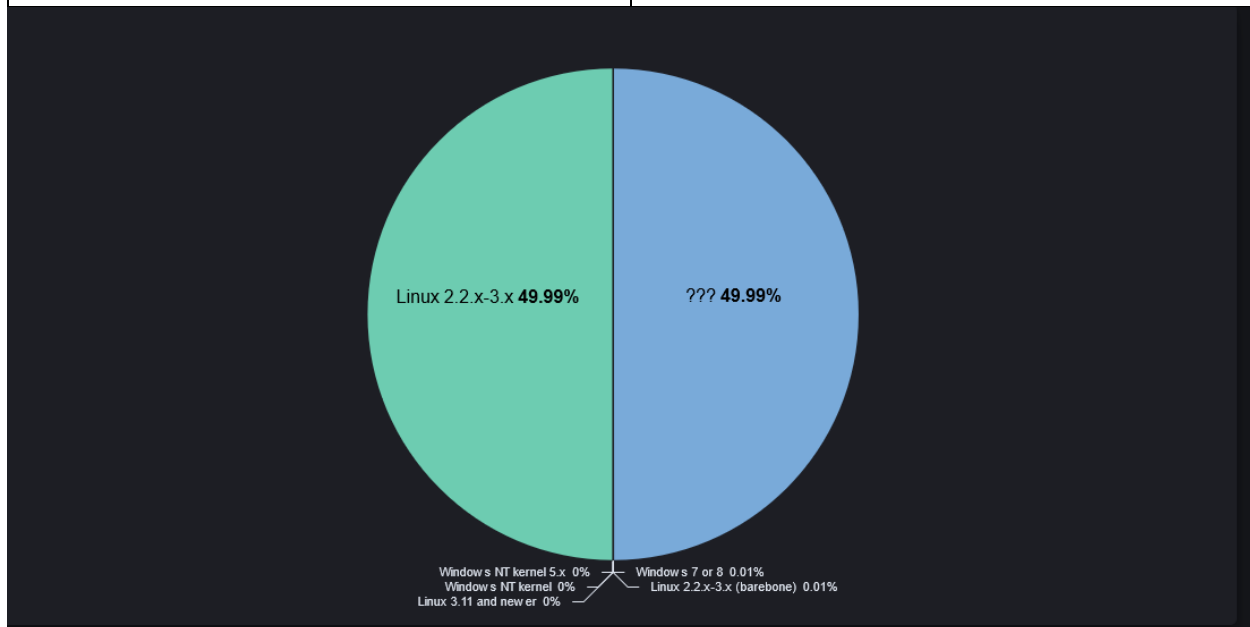| OS Distribution	Count
Linux 2.2.x-3.x	777,288
???	777,178
Windows 7 or 8	129
Linux 3.11 and newer	45
Linux 2.2.x-3.x (barebone)	78
Windows NT kernel 5.x	3
Windows NT kernel	21

Figure 4: POf OS Distribution

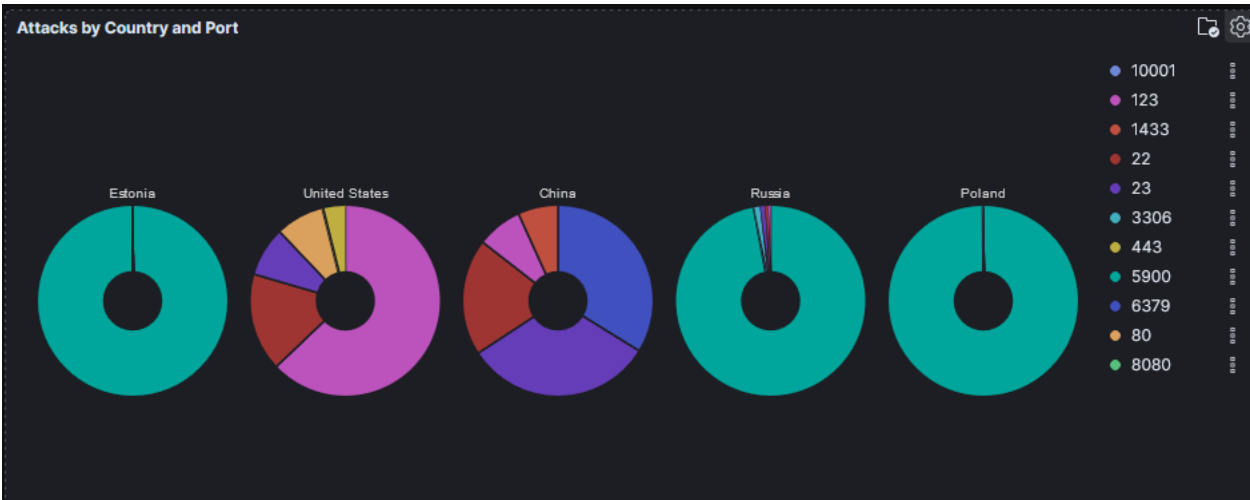In figure5, top 5 of countries are demonstrated by related ports. For example, the attacks from Russia have been 99% through port 5900.

Figure 5 : Attacks by country and port
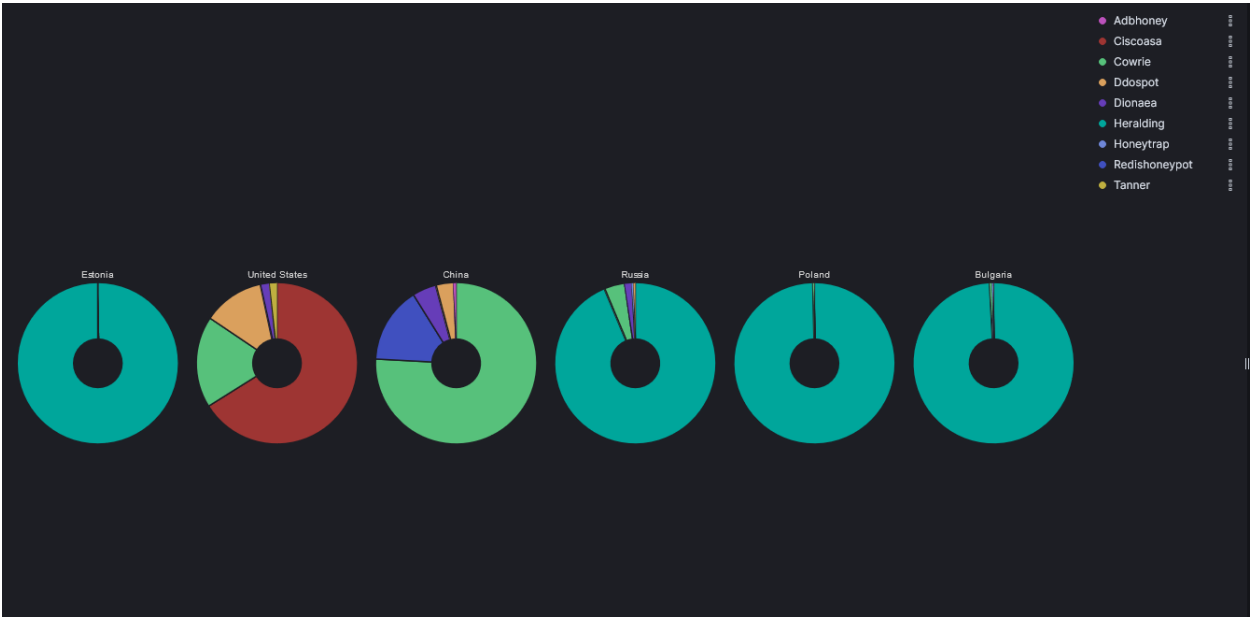
Figure 6 : Honeypots Attacks by country

The most frequently used usernames and passwords for brute force attacks, are listed in table 5,6 and Figure 7,8:

Table 5: Common usernames used by attackers

User name	Count
root	8,180
support	2,596
sa	2,278

postgres	1,584
admin	1,102
ubnt	447
user	273
pi	246
(empty)	233
Admin	171
Other	5,443
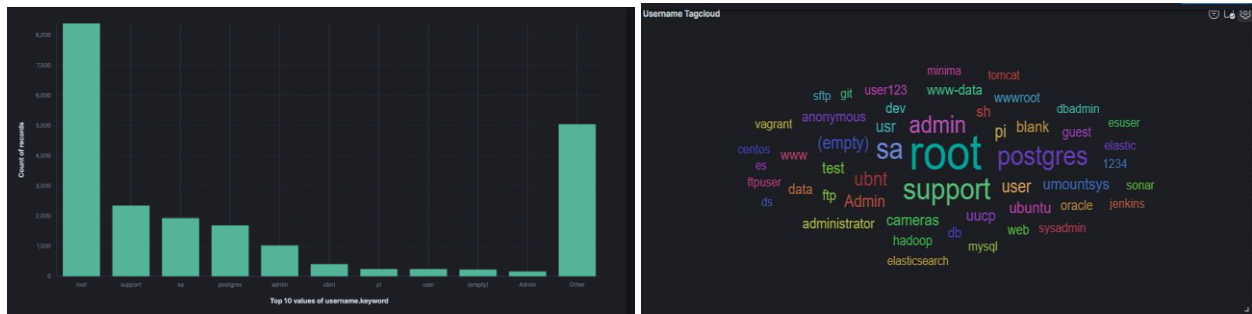
Figure 7: Common usernames used by attackers

Table 6: Common passwords used by attackers

Password	Count
support	2,604
(empty)	1,447
admin	1,220
123456	1,040
password	910
12345678	639
123	324
root	301
1234	276
12345	273
Other	37,624

Figure 8: Common passwords used by attackers

CVE ID	Count
CVE-2006-2369	487,501
CVE-2020-11899	441
CVE-2002-0013 CVE-2002-0012	373
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	328
CVE-2019-11500 CVE-2019-11500	84
CVE-2003-0825	22
CVE-2019-9621 CVE-2021-2109 CVE-2019-9621	14
CVE-2019-9670 CVE-2019-9670	14

Figure 9: Number of attacks for each CVE

The location of attackers based on the IPs is presented in Figure 10.

Figure 10: The approximate locations of the attacker's IP addresses.

Based on T-POT, 86% of attacks are from known attackers, while only 0.06% are from addresses with a bad reputation (figure11).
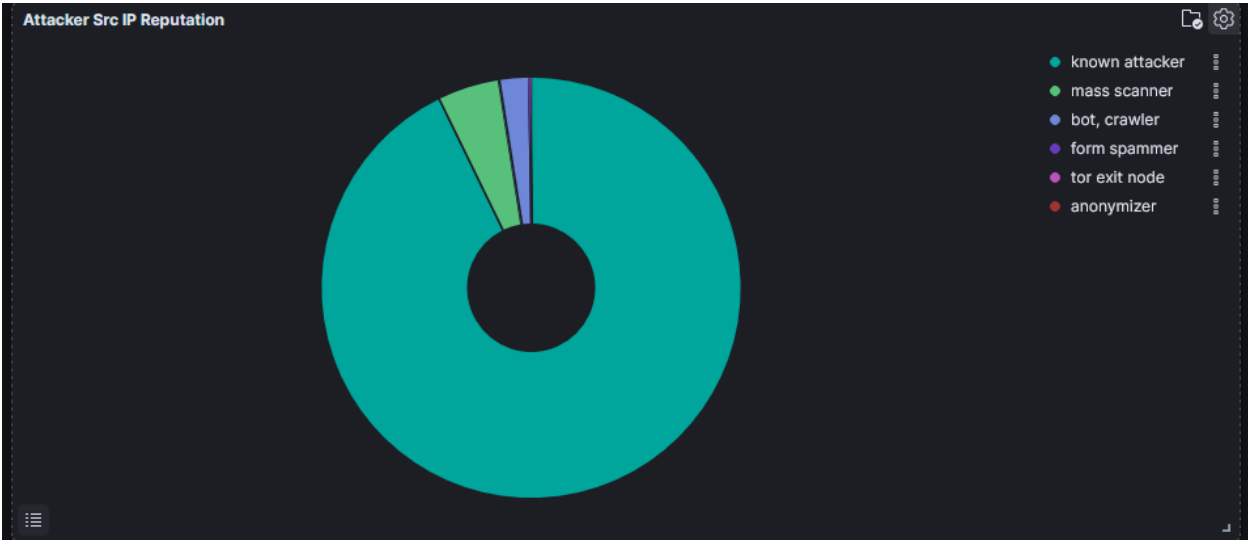
Figure 11: External Honeypot source IP Reputation

ID	Description	Count
2100560	GPL POLICY VNC server response	1,053,806
2002923	ET EXPLOIT VNC Server Not Requiring Authentication (case 2)	487,489
2002920	ET POLICY VNC Authentication Failure	486,955
2210045	SURICATA STREAM Packet with invalid ack	89,826
2210029	SURICATA STREAM ESTABLISHED invalid ack	89,823
2210065	SURICATA STREAM ESTABLISHED ack for ZWP data	89,823
2002911	ET SCAN Potential VNC Scan 5900-5920	13,742
2001978	ET POLICY SSH session in progress on Expected Port	12,098
2002752	ET POLICY Reserved Internal IP Traffic	10,997
2210020	SURICATA STREAM ESTABLISHED packet out of window	5,954

Figure 12: Suricata Alert Signature - Top 10

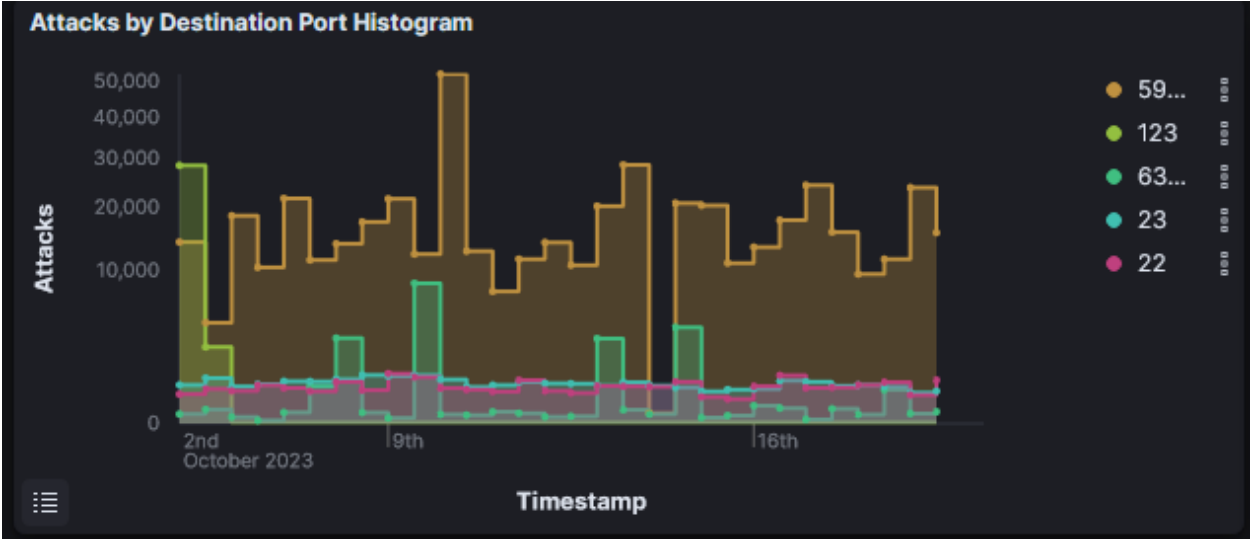Figure 13: Suricata Alert Attacker AS/N- Top 10
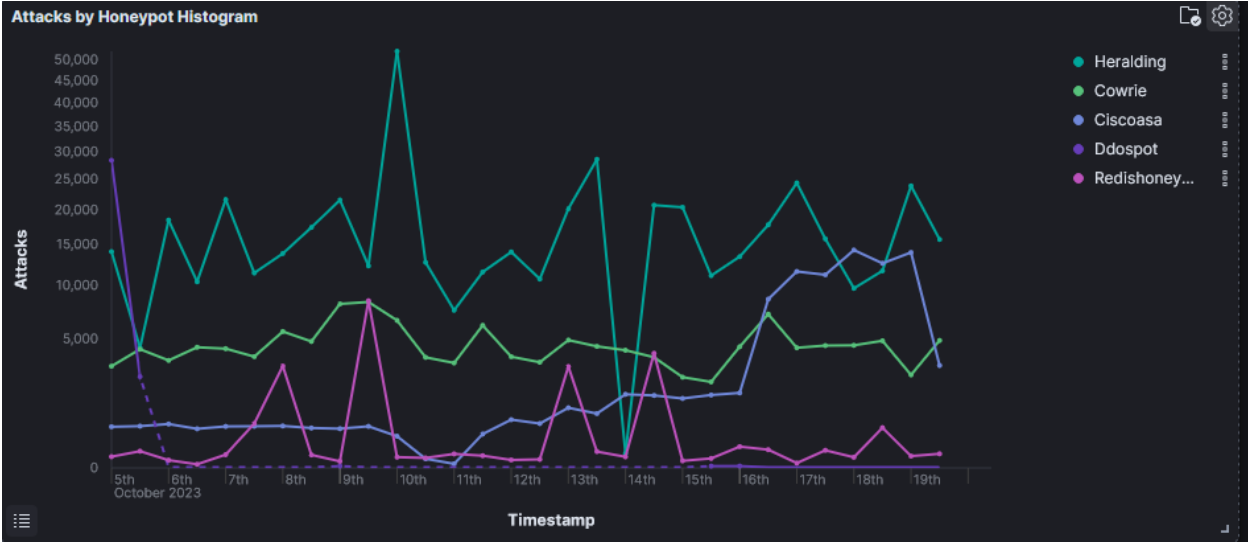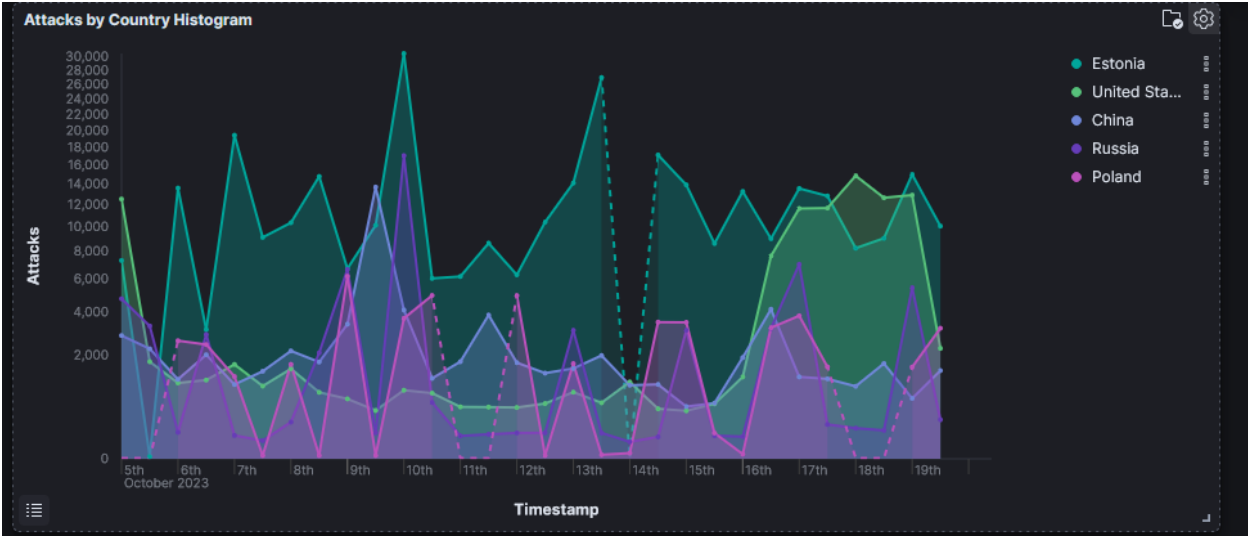
Figure 14: Attacks by Destination Port Histogram

Figure 15: Attacks by Honeypot Histogram

Figure 15: Attacks by Country Histogram