



Captured from Jan 16st to 31th, 2024

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)

Honeynet Monthly Report **Canadian Institute for Cybersecurity (CIC)**



- -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).

The image shows a standard Contact Form 7 interface. It consists of four input fields: 'Your Name (required)', 'Your Email (required)', 'Subject', and 'Your Message'. Below these fields is a green 'Send' button. The form is designed to capture spam submissions from bots.

Figure1: Contact Form 7 Honeypot

Honeynet Monthly Report

Canadian Institute for Cybersecurity (CIC)



CIC-Honeynet uses [T-POT](#) tool outside the firewall which is equipped with several tools. 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 platform, 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](#),
- [endlesssh](#),
- [glutton](#),
- [heralding](#),
- [hellpot](#),
- [honeypots](#),
- [honeytrap](#),
- [ipphoney](#),
- [log4pot](#),
- [mailoney](#),
- [medpot](#),
- [redishoneypot](#),
- [sentrypeer](#),
- [snare](#),
- [tanner](#)

Honeynet Monthly Report

Canadian Institute for Cybersecurity (CIC)



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 management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and other security tools.

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.

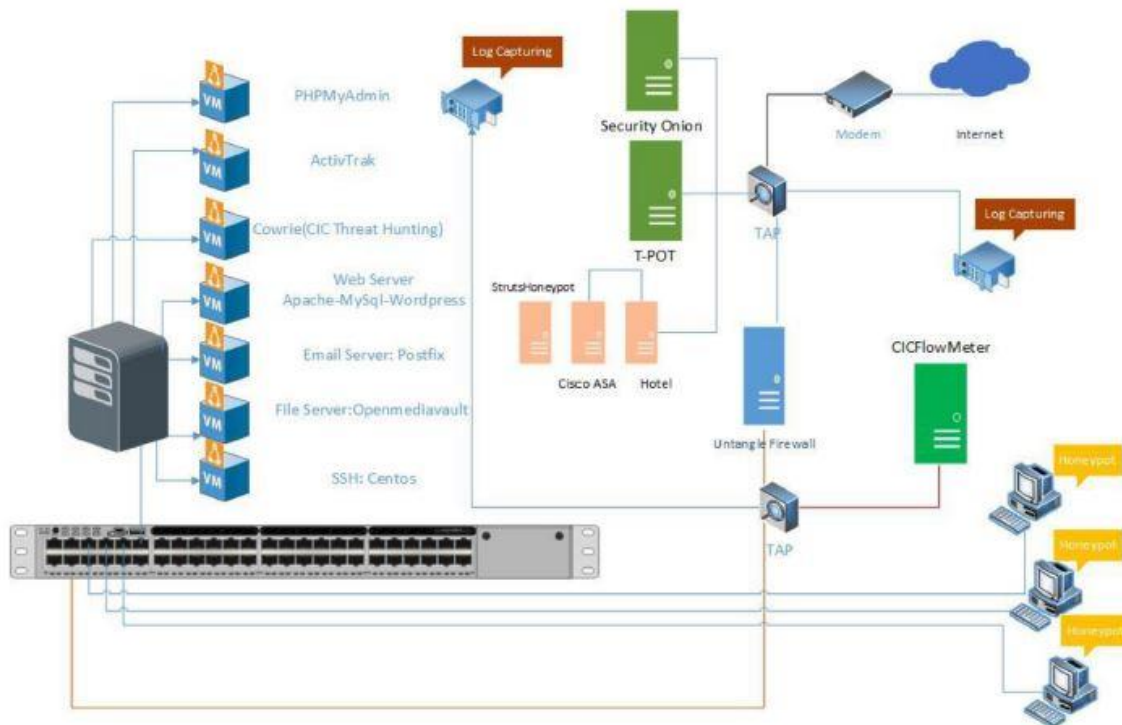


Figure2: Network Diagram

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** : Heraldng 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 sent 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

Honeynet Monthly Report

Canadian Institute for Cybersecurity (CIC)



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(Jan 15th-31th)	Attacks(Jan 1th-15th)
Heralding	39,899	37,9984
Cowrie	220,667	215,727
Ciscoasa	161,771	159,188
RedisHoneypot	95,882	92,776
Dionaea	14,667	11,885
Sentrypper	12,209	8,901
Honeytrap	9,774	7,977
Tanner	8,779	7,854
ElasticPot	5,662	3,100
Adbhoney	4,446	2,250
Mailoney	2,899	1,733
Conpot	1,022	804
Dicompot	568	201

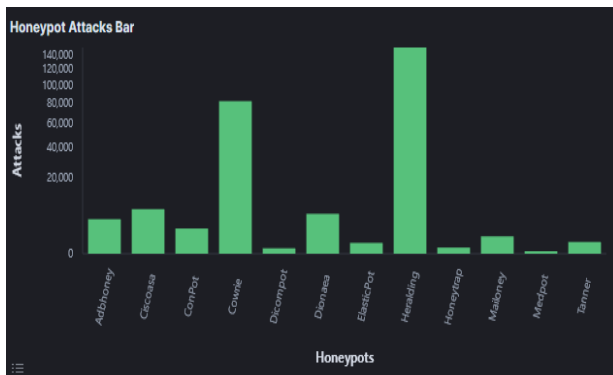


Figure 1 : Honeypots Attacks Bar

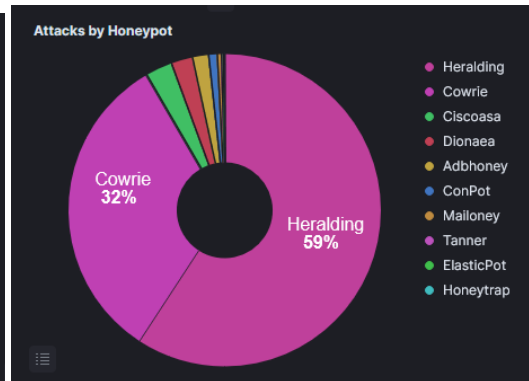


Figure 2: Honeypots Attacks Pie chart

In Table 2, top 10 of source IP addresses and the number of attacks are showcased.

Table 2: Attacker Source IP-Top 10

Source IP	Count
185.11.61.122	112,112
79.124.58.138	98,443
79.124.56.106	88,559
87.251.67.229	77,334
185.73.124.20	56,834
185.73.125.94	49,332

Honeynet Monthly Report
Canadian Institute for Cybersecurity (CIC)



210.113.102.171	38,126
94.232.43.201	28,566
193.105.134.95	21,336
195.3.147.52	19,443

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

Table 3: Attacks by country

Country	Count
China	3,012,996
Bulgaria	2,376,129
Russia	1,312,778
United states	1,112,772
Netherlands	989,448
Germany	554,774
Switzerland	414,992
Kyrgyzstan	350,449
South Korea	104,228
Brazil	98,445
Other	88,334

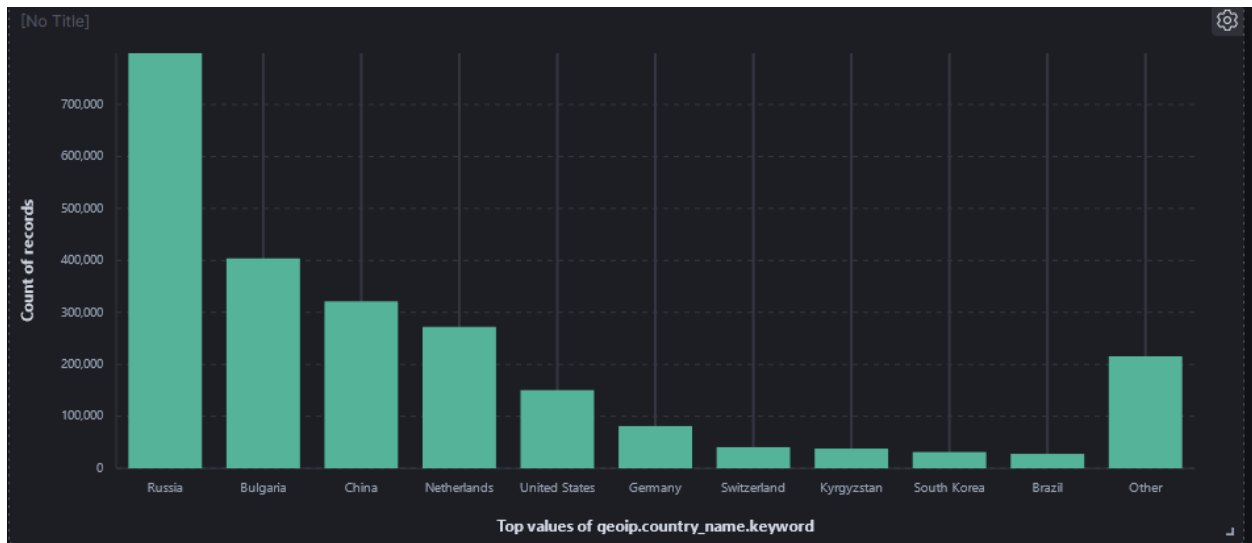


Figure 3: Attacks by country Bar



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	790,213
???	712,805
Linux 3.11 and newer	471
Linux 2.2.x-3.x (barebone)	82
Windows NT kernel	11
Windows NT kernel 5.x	4
Windows 7 or 8	3



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.

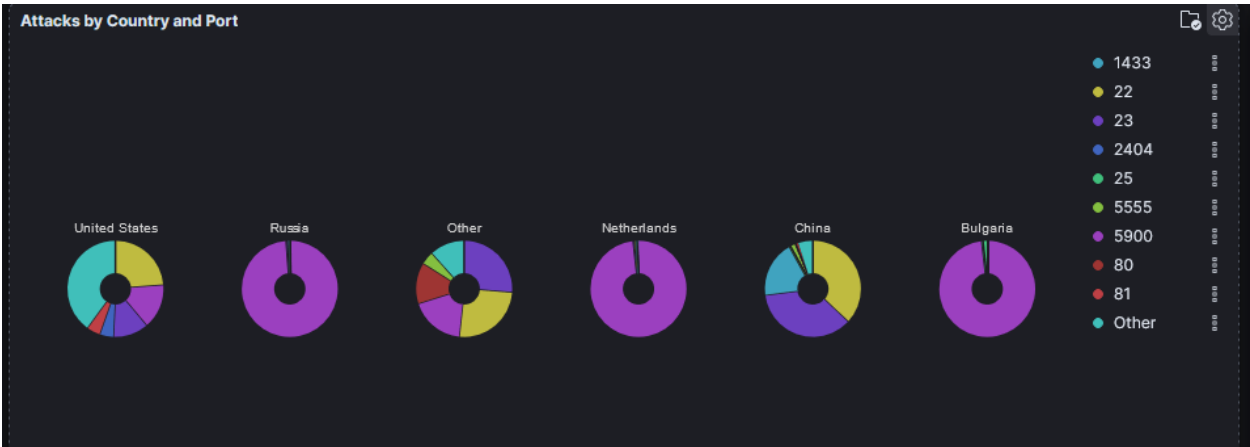


Figure 5 : Attacks by country and port



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	9,080
Other	2,417
Sa	1,515
admin	799
postgres	293
ubnt	213



Suricata CVE - Top 10

CVE ID	Count
CVE-2006-2369	150,065
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	393
CVE-2002-0013 CVE-2002-0012	274
CVE-2019-11500 CVE-2019-11500	68
CVE-2021-44228 CVE-2021-44228	12
CVE-2006-3602 CVE-2006-4458 CVE-2006-4542	11
CVE-2021-24563 CVE-2021-24563 CVE-2021-24563	6
CVE-2009-2765	5
CVE-2010-0569	2

Figure 9: Number of attacks for each CVE

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

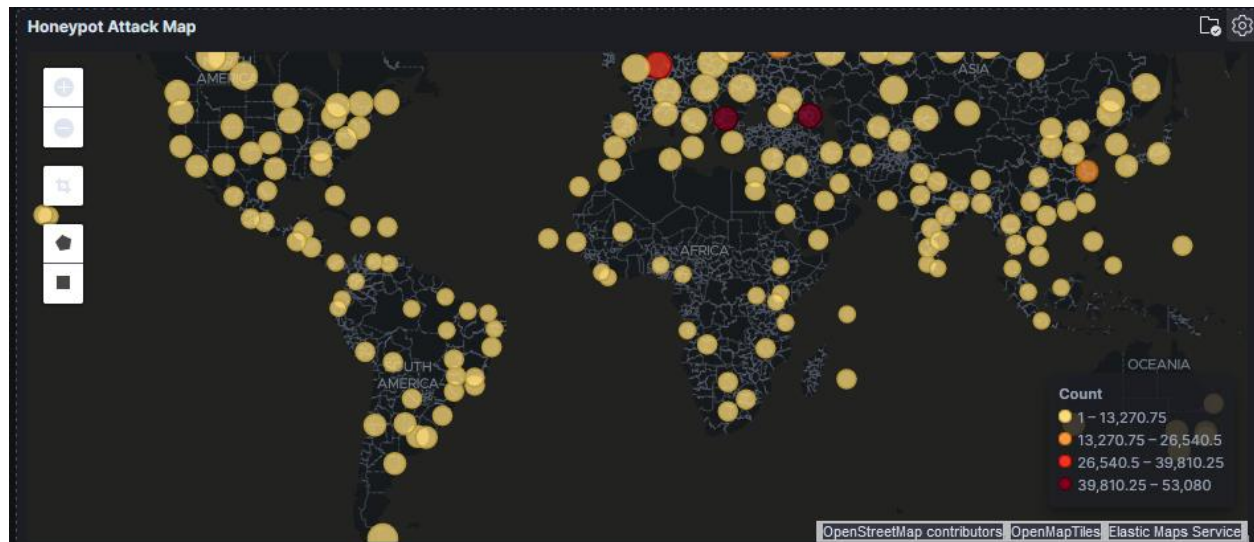


Figure 10: The approximate locations of the attacker's IP addresses.

Based on T-POT, 86% of attacks are from known attackers, while only 0.06% are from addresses with a bad reputation (figure11).

Honeynet Monthly Report Canadian Institute for Cybersecurity (CIC)

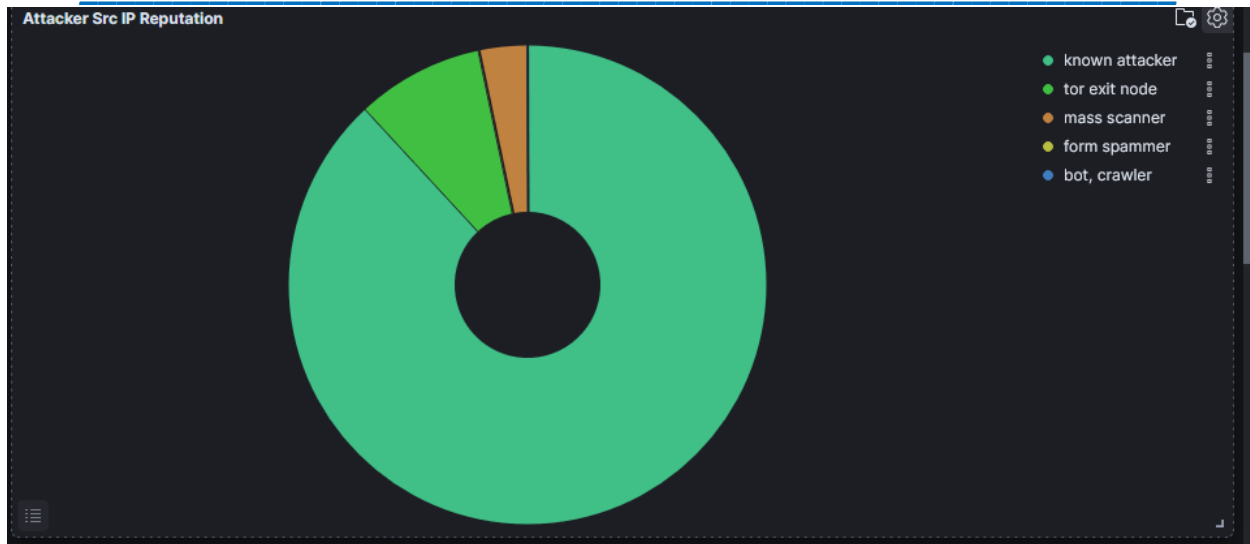


Figure 11: External Honeypot source IP Reputation

ID	Description	Count
2100560	GPL POLICY VNC server response	424,697
2002923	ET EXPLOIT VNC Server Not Requiring Authentication (case 2)	150,062
2002920	ET POLICY VNC Authentication Failure	149,975
2210045	SURICATA STREAM Packet with invalid ack	93,181
2210029	SURICATA STREAM ESTABLISHED invalid ack	93,179
2210020	SURICATA STREAM ESTABLISHED packet out of window	19,994
2002752	ET POLICY Reserved Internal IP Traffic	9,461
2001978	ET POLICY SSH session in progress on Expected Port	6,882
2010935	ET SCAN Suspicious inbound to MSSQL port 1433	2,956

Figure 12: Suricata Alert Signature - Top 10

Honeynet Monthly Report

Canadian Institute for Cybersecurity (CIC)



Attacker AS/N - Top 10

AS	ASN	Count
199539	Vertex Ltd.	53,042
50360	Tamatiya EOOD	40,601
59753	Vault Dweller LTD	26,452
4134	No.31,Jin-rong Street	21,238
20803	Alexander Valerevich Mokhon...	15,614
4766	Korea Telecom	9,991
42237	Icme Limited	6,042
41390	RN Data SIA	5,932
10225	Nettlinx Limited	3,296

Figure 13: Suricata Alert Attacker AS/N- Top 10

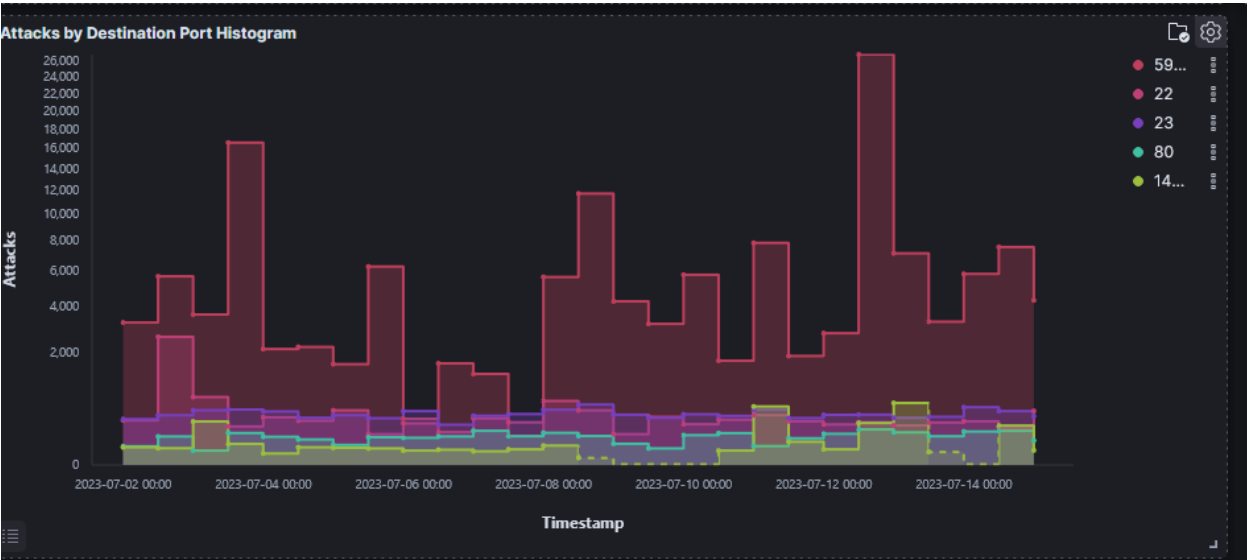


Figure 14: Attacks by Destination Port Histogram

Honeynet Monthly Report Canadian Institute for Cybersecurity (CIC)

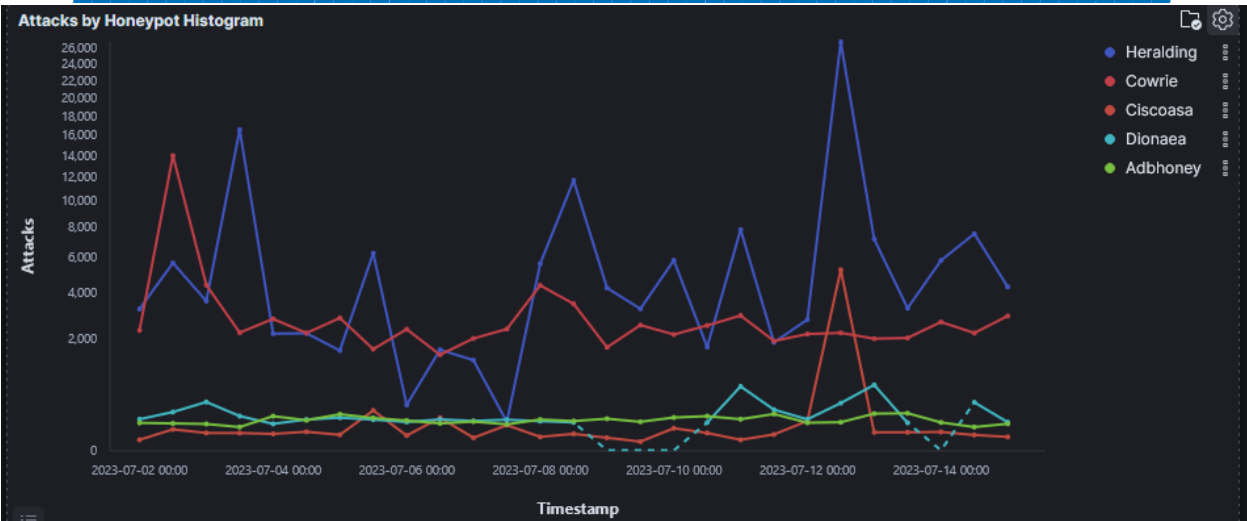


Figure 15: Attacks by Honeypot Histogram

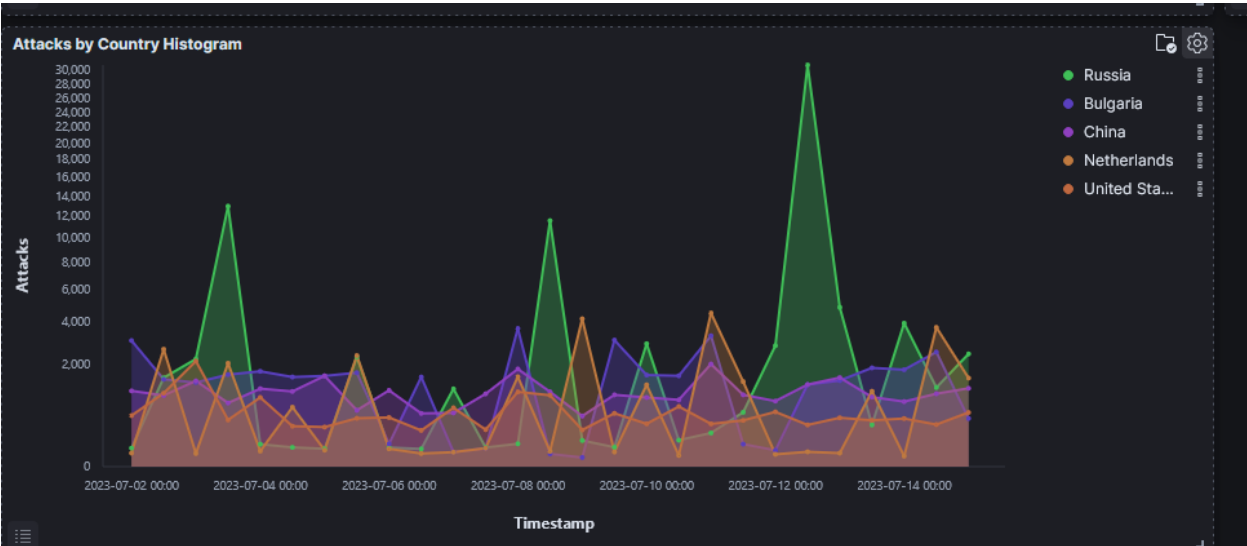


Figure 15: Attacks by Country Histogram