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

*Captured from 2023-03-01 to 2023-03-31*

## 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.

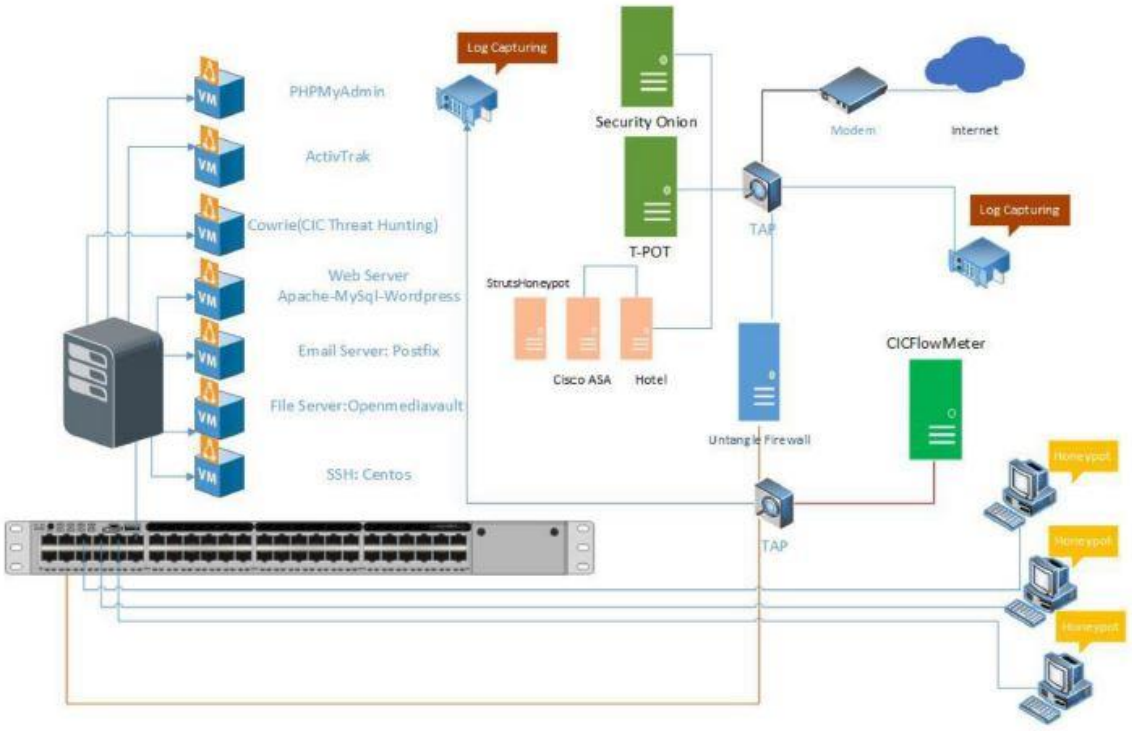



Figure2: Network Diagram

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(March2023) | Attacks(Feb2023) |
|---|---|---|
| Heralding | 466,851 | 1,003,758 |
| Cowrie | 331,651 | 478,634 |
| Dionaea | 38,677 | 47,727 |
| Tanner | 20,766 | 855 |
| Ciscoasa | 20,218 | 2,278 |
| Adbhoney | 11,044 | 19,631 |
| ElasticPot | 7,594 | 777 |
| Mailoney | 3,370 | 4,346 |
| Conpot | 3,118 | 2,683 |
| Honeytrap | 1,211 | 1,384 |
| Dicompot | 153 | 101 |
| Honeysap | 82 | 34 |
| Medpot | 12 | 9 |

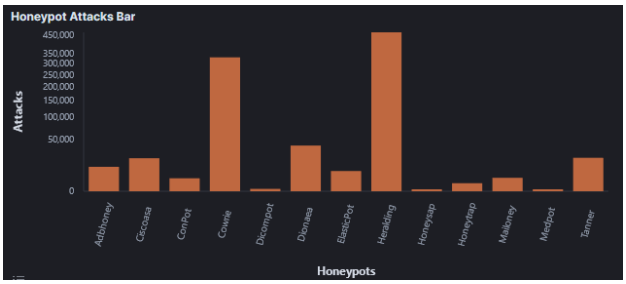



Figure 1 : Honeypots Attacks Bar

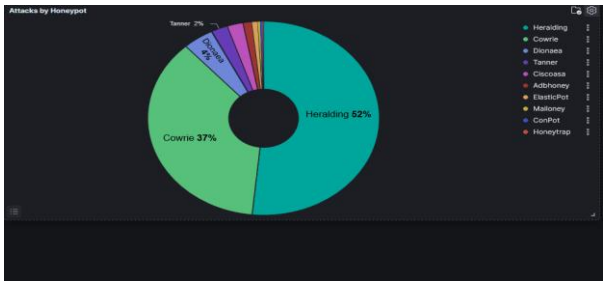



Figure 2: Honeypots Attacks Pie chart

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 |
|---|---|
| 80.66.66.48 | 100,651 |
| 185.11.61.190 | 93,298 |
| 185.73.125.94 | 53,448 |
| 79.124.56.106 | 41,693 |
| 52.70.250.122 | 40,902 |
| 80.66.76.51 | 33,732 |
| 87.251.67.229 | 22,814 |
| 78.128.114.2 | 17,948 |

| | |
|---|---|
| 91.35.136.93 | 16,422 |
| 185.73.124.20 | 15,829 |

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

Table 3: Attacks by country

| Country | Count |
|---|---|
| Russia | 2,871,530 |
| United States | 1,505,847 |
| China | 1,092,434 |
| Netherlands | 996,931 |
| Bulgaria | 649,859 |
| Germany | 180,874 |
| Sweden | 132,680 |
| Romania | 70,147 |
| Ireland | 55,539 |
| Turkey | 41,865 |
| Other | 421,954 |

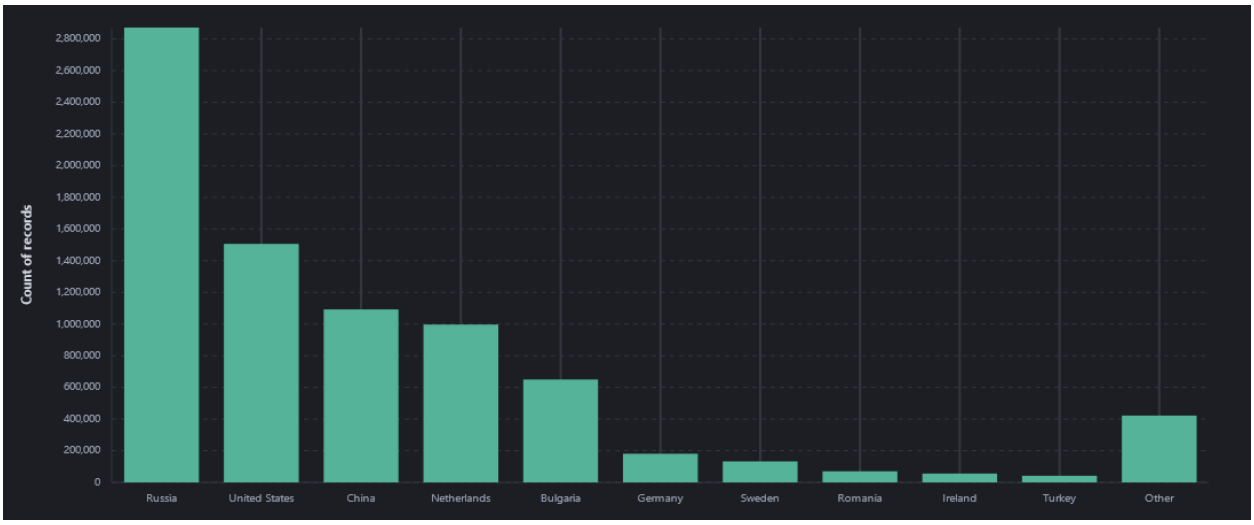



Figure 3: Attacks by country Bar

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

Table 4: Attacks by OS Distribution

| OS Distribution | Count |
|---|---|
| ??? | 965,701 |
| Linux 2.2.x-3.x | 963,738 |
| Windows 7 or 8 | 1,934 |
| Linux 3.11 and newer | 779 |
| Linux 2.2.x-3.x (barebone) | 111 |
| Windows NT kernel | 30 |
| Windows NT kernel 5.x | 3 |
| Linux 3.1-3.10 | 0 |

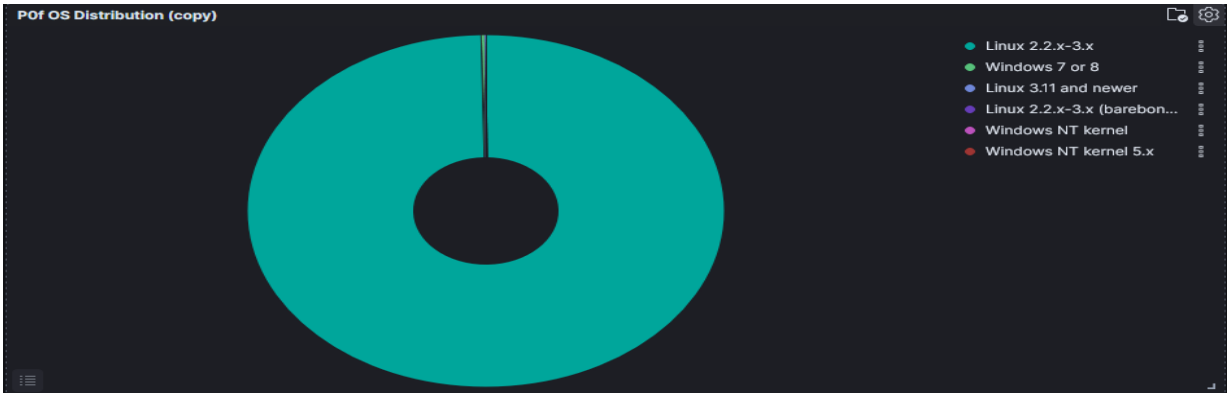



Figure 4: POf OS Distribution

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

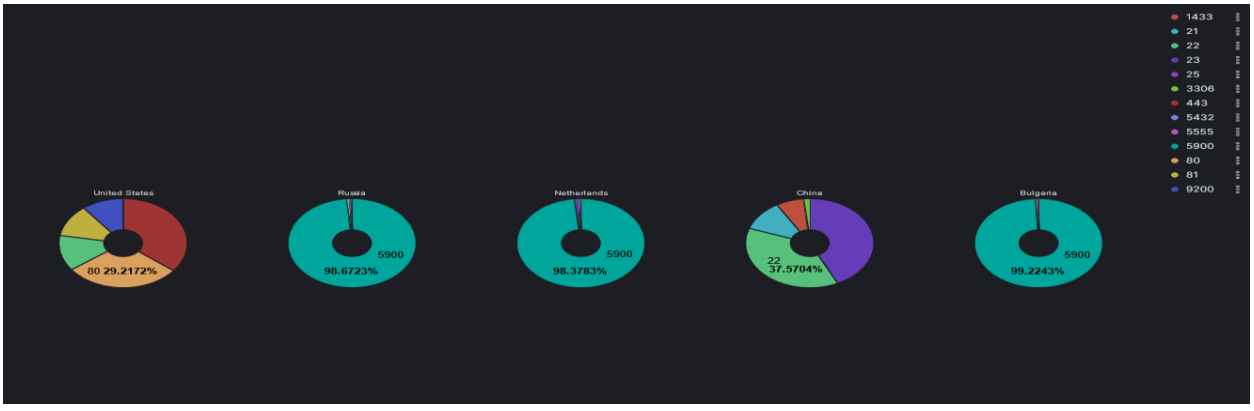


Figure 5 : Attacks by country and port

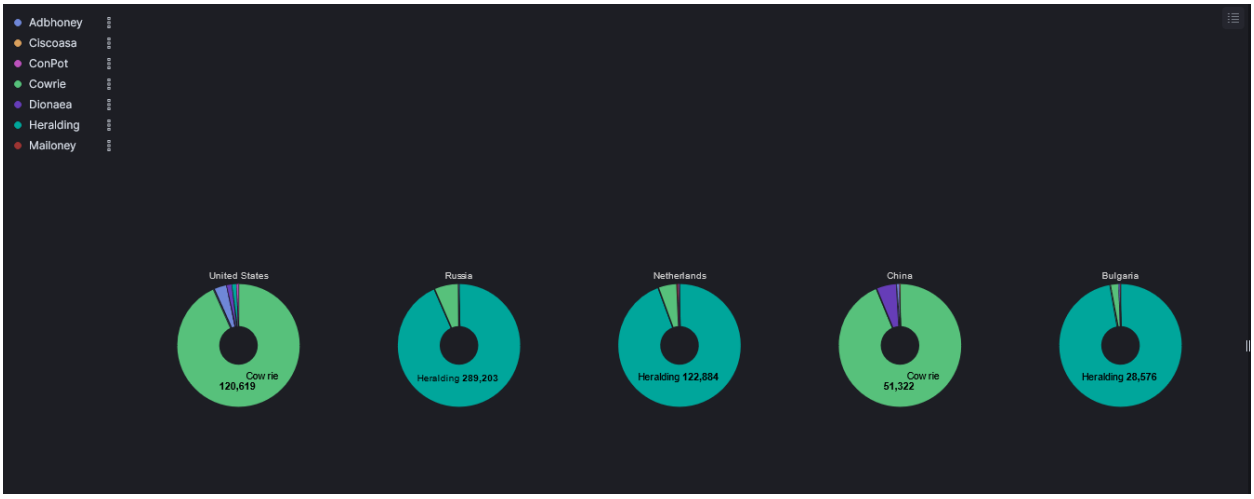
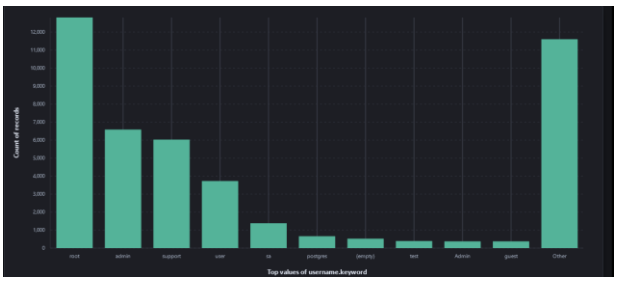



Figure 6 : Honeypots Attacks by country

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 | 12,815 |
| admin | 6,588 |
| support | 6,030 |
| user | 3,729 |
| sa | 1,383 |
| postgres | 661 |
| (empty) | 525 |
| test | 394 |
| Admin | 376 |
| guest | 376 |
| Other | 11,608 |



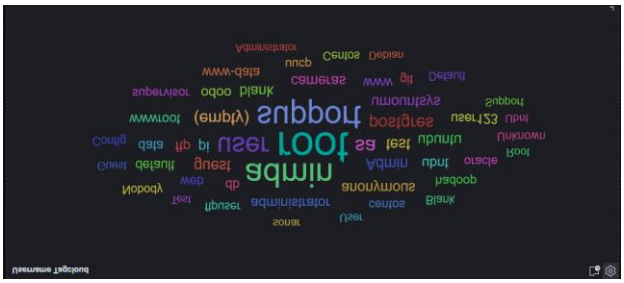
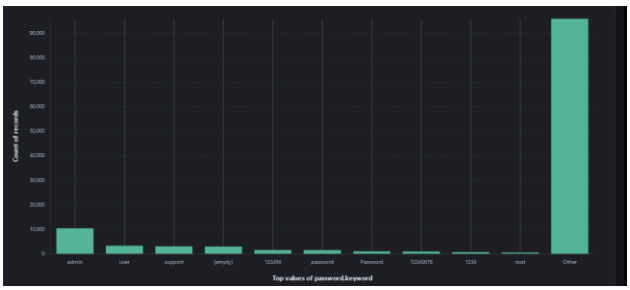


Figure 7: Common usernames used by attackers

Table 6: Common passwords used by attackers

| Password | Count |
|---|---|
| admin | 10,408 |
| user | 3,298 |
| support | 3,050 |
| (empty) | 2,962 |
| 123456 | 1,533 |
| password | 1,506 |
| Password | 996 |
| 12345678 | 945 |
| 1234 | 681 |
| root | 519 |
| Other | 95,904 |



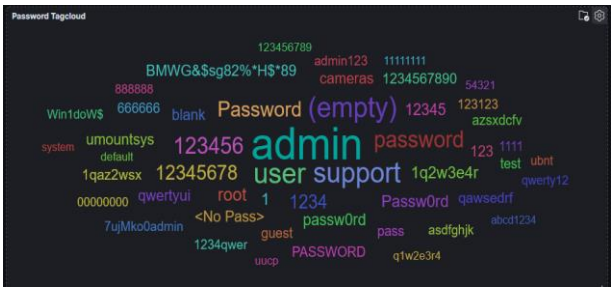



Figure 8: Common passwords used by attackers

**Suricata CVE - Top 10**

| CVE ID | Count |
|---|---|
| CVE-2006-2369 | 465,646 |
| CVE-2021-44228 CVE-2021-44228 | 973 |
| CVE-2006-3602 CVE-2006-4458 CVE-2006-4542 | 703 |
| CVE-2002-0013 CVE-2002-0012 CVE-1999-0517 | 588 |
| CVE-2002-0013 CVE-2002-0012 | 587 |
| CVE-2002-0953 | 495 |
| CVE-2018-11776 | 453 |
| CVE-2019-11500 CVE-2019-11500 | 94 |
| CVE-2013-2251 | 90 |

Figure 9: Number of attacks for each CVE

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

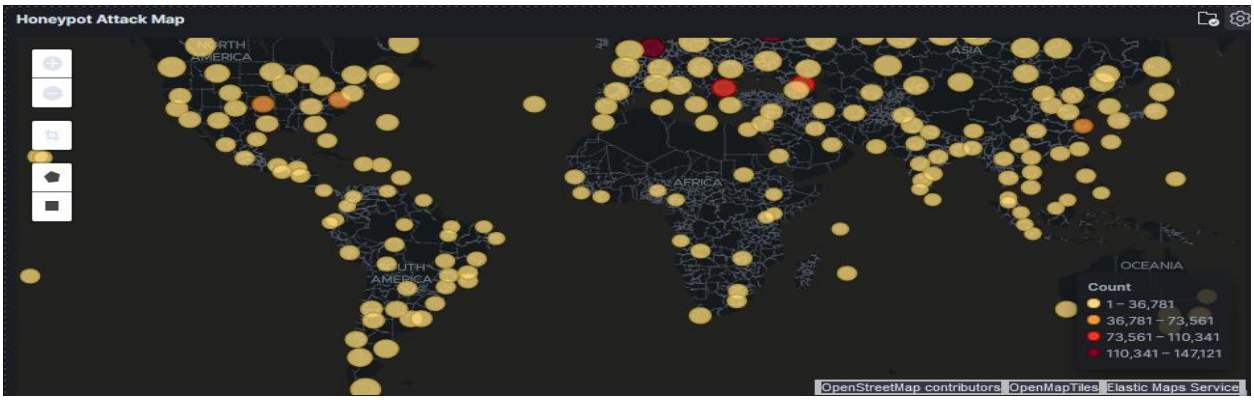



Figure 10: The approximate locations of the attacker's IP addresses.

Based on T-POT, 85% of attacks are from known attackers, while only 0.06% are from addresses with a bad reputation (figure11).

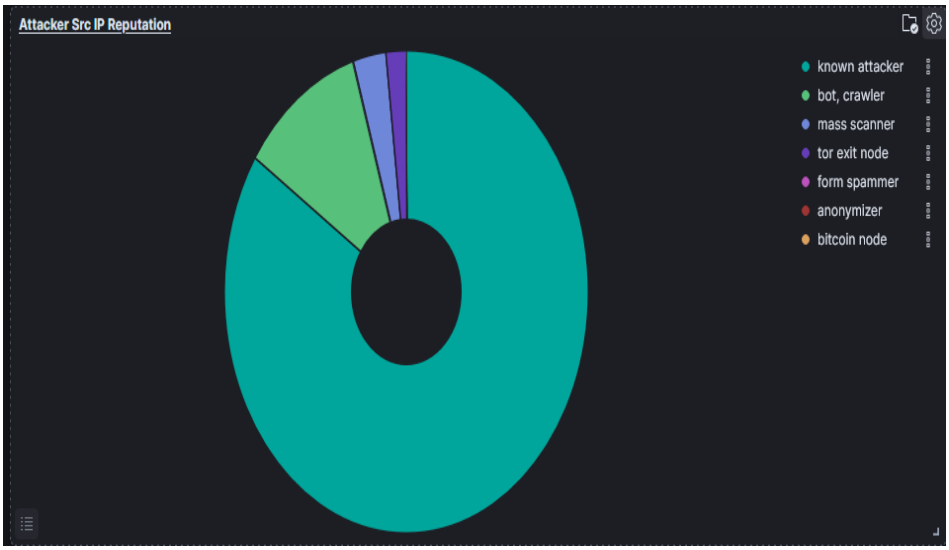



Figure 11: External Honeypot source IP Reputation

**Suricata Alert Signature - Top 10**

| ID | Description | Count |
|---|---|---|
| 2100560 | GPL POLICY VNC server response | 1,407,172 |
| 2002923 | ET EXPLOIT VNC Server Not Requiring Authentication (case 2) | 465,981 |
| 2002920 | ET POLICY VNC Authentication Failure | 465,719 |
| 2002752 | ET POLICY Reserved Internal IP Traffic | 25,406 |
| 2001978 | ET POLICY SSH session in progress on Expected Port | 24,694 |
| 2002911 | ET SCAN Potential VNC Scan 5900-5920 | 11,292 |
| 2010935 | ET SCAN Suspicious inbound to MSSQL port 1433 | 5,034 |
| 2260002 | SURICATA Applayer Detect protocol only one direction | 4,606 |
| 2101122 | GPL WEB_SERVER /etc/passwd | 3,599 |
| 2402000 | ET DROP Dshield Block Listed Source group 1 | 3,556 |

Figure 12: Suricata Alert Signature - Top 10

**Attacker AS/N - Top 10**

| AS | ASN | Count |
|---|---|---|
| 20803 | Alexander Valerevich Mokhon... | 157,368 |
| 59753 | Vault Dweller LTD | 98,606 |
| 199539 | Vertex Ltd. | 93,298 |
| 4134 | No.31,Jin-rong Street | 69,554 |
| 50360 | Tamatiya EOOD | 66,300 |
| 14618 | Amazon.com, Inc. | 41,466 |
| 197328 | Istanbuldc Veri Merkezi Ltd Sti | 22,226 |
| 42237 | Icme Limited | 11,696 |
| 41390 | RN Data SIA | 11,330 |
| 14061 | DigitalOcean, LLC | 10,699 |

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

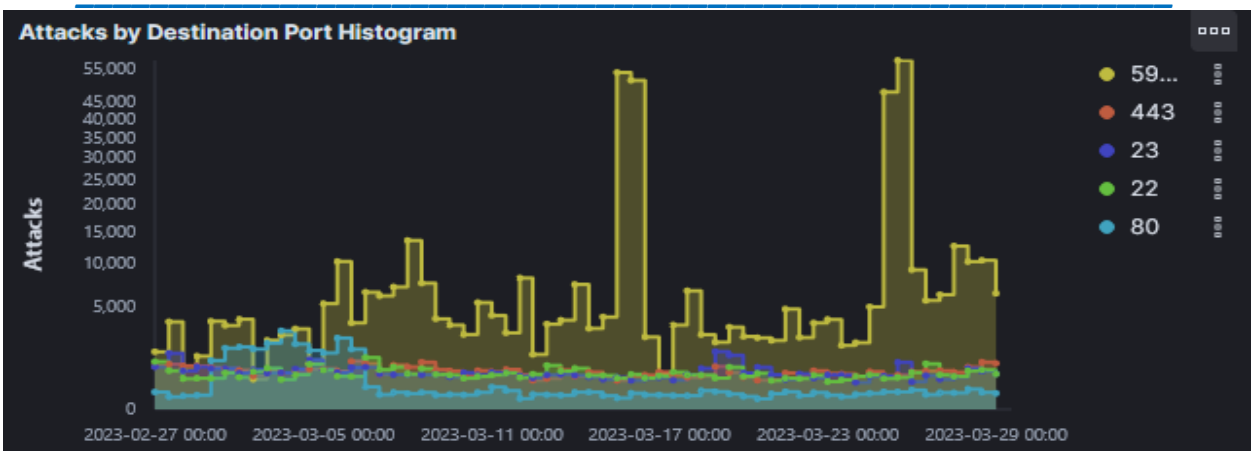



Figure 14: Attacks by Destination Port Histogram

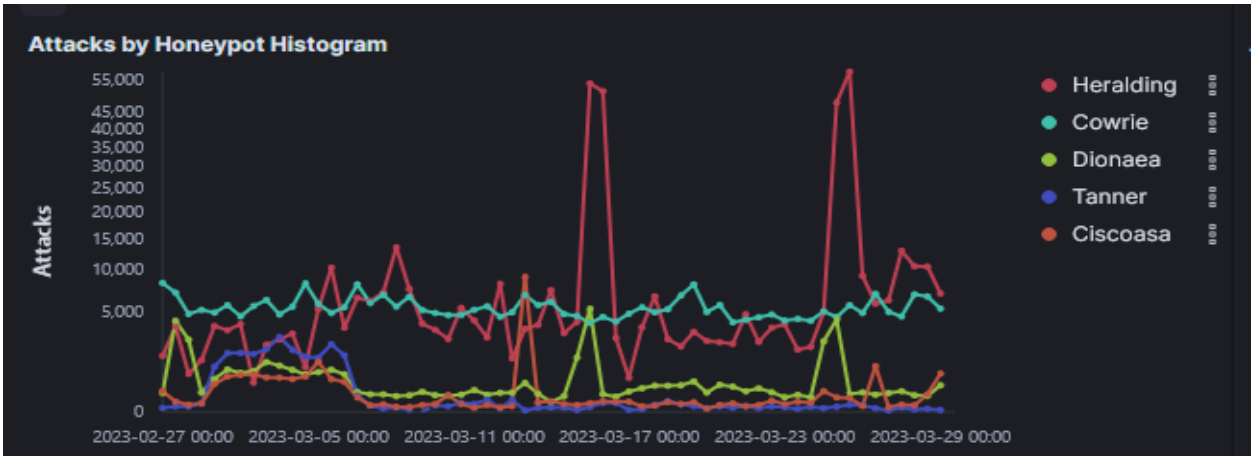



Figure 15: Attacks by Honeypot Histogram


Figure 15: Attacks by Country Histogram