

Modern Honey Network

**Pauline Finlay**

**B00107945**

***Department of Informatics***

***School of Informatics & Engineering***

***Technological University Dublin, Blanchardstown***

***Dublin 15.***

**Word Limit for Assignment: 3000 Actual Word Count: 2926**

**BSc (Hons) in Computing in Digital Forensics & Cyber Security**

**DFCS H4015 Network Security Analytics**

**14th December 2020**

**Plagiarism Declaration**

I hereby certify that this material, which I am submitting for assessment for the course title of BSc. (Hons) In Computing in Digital Forensics and Cyber Security is my own work and that I have:

* Clearly referenced/listed all sources as appropriate
* Given the sources of all pictures, data etc. that are not my own
* Any work of any other student(s) either past or present is clearly referenced
* Not submitted for assessment work previously submitted for any other course, degree or qualification
* Not incorporated any text acquired from external agencies other than extracts from attributed sources (including online facilities)
* Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
* My work may be electronically checked for plagiarism, including, but not exclusively, by the use of plagiarism detection software and stored for future comparison
* Any false claim for this work will be penalised in accordance with the College’s regulations

**Signature:** Pauline Finlay **Date:** 14/12/2020

**Abstract**

This paper is a report on the data analysis of a Modern Honey Network deployment. The results contained a significant number of attacks originating from Irish sources, here those attacks are compares and contrasted in relation to the overall global attack data.

Table of Contents

[1 Introduction 8](#_Toc58748035)

[1.1 System Setup 8](#_Toc58748036)

[1.2 Sensors 10](#_Toc58748037)

[1.2.1 Amun 10](#_Toc58748038)

[1.2.2 Conpot 10](#_Toc58748039)

[1.2.3 Cowrie 10](#_Toc58748040)

[1.2.4 Dianoea 10](#_Toc58748041)

[1.2.5 Elastic Honey 10](#_Toc58748042)

[1.2.6 P0f 10](#_Toc58748043)

[1.2.7 Shockpot 10](#_Toc58748044)

[1.2.8 Snort 10](#_Toc58748045)

[1.2.9 Wordpot 10](#_Toc58748046)

[1.3 Overview 11](#_Toc58748047)

[2 Methodology 12](#_Toc58748048)

[3 Findings 13](#_Toc58748049)

[3.1 Top Attack Countries 13](#_Toc58748050)

[3.2 Top Attack Cities 14](#_Toc58748051)

[3.3 Top Honeypots 16](#_Toc58748052)

[3.4 Attack IP Addresses 18](#_Toc58748053)

[3.4.1 Top Attack IP 18](#_Toc58748054)

[3.4.2 Top Irish IP 21](#_Toc58748055)

[3.4.3 Dublin 24](#_Toc58748056)

[3.4.4 Maynooth 27](#_Toc58748057)

[3.4.5 Other Locations 27](#_Toc58748058)

[3.4.6 Portmagee 28](#_Toc58748059)

[3.4.7 Galway 28](#_Toc58748060)

[3.4.8 Enniscorthy 29](#_Toc58748061)

[3.4.9 Tullamore 29](#_Toc58748062)

[3.5 Malware 30](#_Toc58748063)

[3.5.1 Top md5 values 30](#_Toc58748064)

[3.5.2 Irish Values 31](#_Toc58748065)

[3.6 Attack Signatures 32](#_Toc58748066)

[3.6.1 Top Signatures 32](#_Toc58748067)

[3.6.2 Top Signatures Excluding Irish Values 33](#_Toc58748068)

[3.6.3 Top Irish Signatures 33](#_Toc58748069)

[3.7 Top Attack Ports 34](#_Toc58748070)

[3.8 Top Commands 36](#_Toc58748071)

[3.9 Highest Daily Record 38](#_Toc58748072)

[3.10 Top SSH Username/Password 40](#_Toc58748073)

[3.11 Top p0f OS 42](#_Toc58748074)

[3.12 Top URLs 43](#_Toc58748075)

[4 Conclusion 44](#_Toc58748076)

[5 References 45](#_Toc58748077)

[6 Appendix 46](#_Toc58748078)

[6.1 Presentation Link 46](#_Toc58748079)

**Table of Tables**

[Table 1: MHN Server Configuration 8](#_Toc58748080)

[Table 2: Honey Pot Servers Configuration 9](#_Toc58748081)

**Table of Figures**

[Figure 1: Attack Timeline 8](#_Toc58748082)

[Figure 2: Overview of Deployment showing live attacks 11](#_Toc58748083)

[Figure 3: Top Attack Countries 12](#_Toc58748084)

[Figure 4: Panama enters Top 10 Countries when Ireland excluded 13](#_Toc58748085)

[Figure 5: Splunk Global Attack Map 13](#_Toc58748086)

[Figure 6: Top 10 Cities including Irish results 14](#_Toc58748087)

[Figure 7: Top 10 Cities excluding Irish Locations 14](#_Toc58748088)

[Figure 8: Locations of Attacks in Ireland 15](#_Toc58748089)

[Figure 9: Top Honeypots by Type 16](#_Toc58748090)

[Figure 10: Top Honeypots Excluding Ireland 16](#_Toc58748091)

[Figure 11: Top Irish Honeypots 17](#_Toc58748092)

[Figure 12: Top Attack IP’s 18](#_Toc58748093)

[Figure 13: 51.89.192.84 report from https://whatismyipaddress.com/ 18](#_Toc58748094)

[Figure 14:51.89.192.84 on https://www.shodan.io/ 19](#_Toc58748095)

[Figure 15: 51.89.192.84 report on https://www.abuseipdb.com/ 19](#_Toc58748096)

[Figure 16: Sample of Abuse Reports from https://www.abuseipdb.com/ 20](#_Toc58748097)

[Figure 17: Macroom IP Addresses 21](#_Toc58748098)

[Figure 18: Ballingeary IP Addresses 21](#_Toc58748099)

[Figure 19: IP 5.188.86.167identified using https://whatismyipaddress.com 22](#_Toc58748100)

[Figure 20: IP 5.188.86.167 identified using https://www.abuseipdb.com 22](#_Toc58748101)

[Figure 21: IP Abuse Report 5.188.86.167using https://www.abuseipdb.com 23](#_Toc58748102)

[Figure 22: Dublin IP Addresses 24](#_Toc58748103)

[Figure 23: Top 10 md5 Values 30](#_Toc58748104)

[Figure 24: Malware Attacks 31](#_Toc58748105)

[Figure 25: Top Attack Signatures 32](#_Toc58748106)

[Figure 26: Top Signatures Excluding Ireland 33](#_Toc58748107)

[Figure 27: Top Irish Signatures 33](#_Toc58748108)

[Figure 28: Top Attack Ports 34](#_Toc58748109)

[Figure 29: Irish Attack Ports 34](#_Toc58748110)

[Figure 30: Top Commands 36](#_Toc58748111)

[Figure 31: Top Irish Commands 37](#_Toc58748112)

[Figure 32: Highest Daily Attack Locations 38](#_Toc58748113)

[Figure 33: Top Countries 10.11.20 excluding Irish Data 38](#_Toc58748114)

[Figure 34: Top Cities 10.11.20 39](#_Toc58748115)

[Figure 35: Top Cities 10.11.20 excluding Irish Data 39](#_Toc58748116)

[Figure 36: Top SSH Usernames 40](#_Toc58748117)

[Figure 37: Top SSH Passwords 40](#_Toc58748118)

[Figure 38: Irish Attack Usernames 41](#_Toc58748119)

[Figure 39: Irish Attack Passwords 41](#_Toc58748120)

[Figure 40: Top p0f OS 42](#_Toc58748121)

[Figure 41: Top Irish p0f OS 42](#_Toc58748122)

[Figure 42: Top 10 URL's 43](#_Toc58748123)

# Introduction

The Honeypot deployment ran from the 10th October 2020 until the 12th November 2020. During this period, a total of 5,847,124 attacks were observed and the log files corresponding to these attacks analysed using Splunk Enterprise 8.1.1 [1].

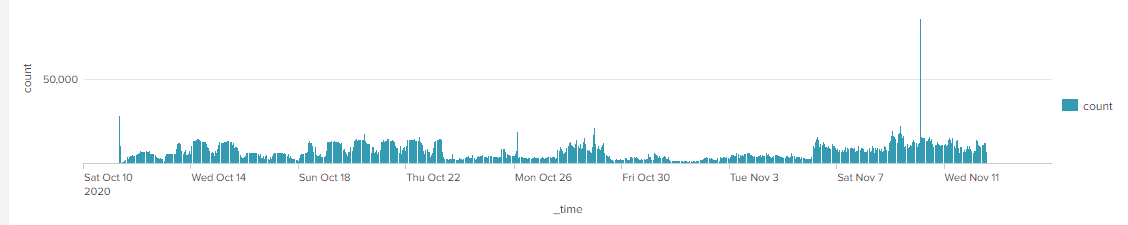


Figure 1: Attack Timeline

## System Setup

Using Digital Ocean droplets, the MHN Server ran on an Ubuntu 18.04 Server with 4GB Ram, 2CPU’s and an 80Gb SSD Disk and hosted in Amsterdam.

4 identical Ubuntu 18.04 Servers with 1GB Ram, 1 CPU with a 25Gb SSD were used for the Honeypot Sensors and located in London, New York, Amsterdam, and San Francisco to expand the geographical spread [2], [3], [4], [5].

Table 1: MHN Server Configuration

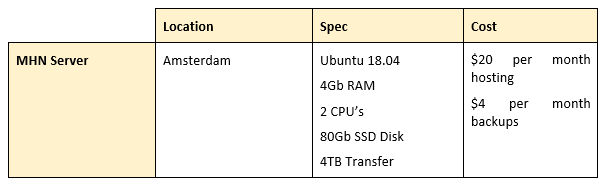
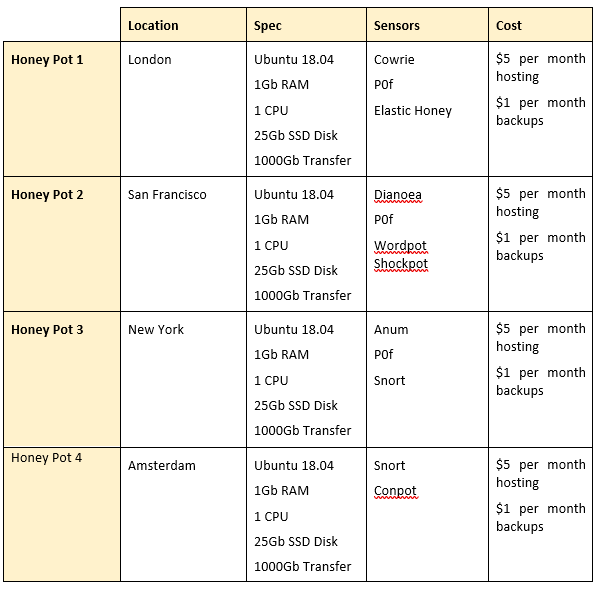


Table 2: Honey Pot Servers Configuration



## Sensors

In total I chose 9 different sensors, and these were deployed in various combinations over the 4 honey pot servers as outlined in Table 2. The sensors chosen were:

### Amun

This is a low interaction honeypot emulating several services and listening on other ports for incoming connections [6]. It records attacker and honeypot IP addresses & ports.

### Conpot

This is a low interaction honeypot which mirrors industrial environments. The goal is to collect intelligence about the motives and methods of attackers targeting Industrial Control Systems.

### Cowrie

This is a medium interaction SSH & Telnet honeypot which is used to log brute force attacks and the shell interaction the attacker performs [7].

### Dianoea

This is a low interaction honeypot which exposes the following services MSSQL, SIP, HTTP, FTP, TFTP. It is designed to trap malware and ultimately gain a copy of same.

### Elastic Honey

Elastichoney is a simple elasticsearch honeypot designed to catch attackers exploiting RCE vulnerabilities in elasticsearch [8].

### P0f

A passive fingerprinting tool used to identify the OS behind a TCP connection.

### Shockpot

A webapp honeypot exposing the CVE-2014-6271 vulnerability.

### Snort

This is an IDS/IPS used to detect attacks on a network. The full signature detail is recorded, Signature and packets.

### Wordpot

This is a WordPress emulator honeypot. It detects probes for plugins, themes and other common files used to fingerprint a wordpress installation.

## Overview

Once the deployment was up and running the MHN server was accessible on 167.172.38.233:3000. Here an overview world map was available indicating live attacks. MHN also provides attack statistics and graphs, the deployment scripts to add additional sensors to honeypots and a summary of the sensors already running.

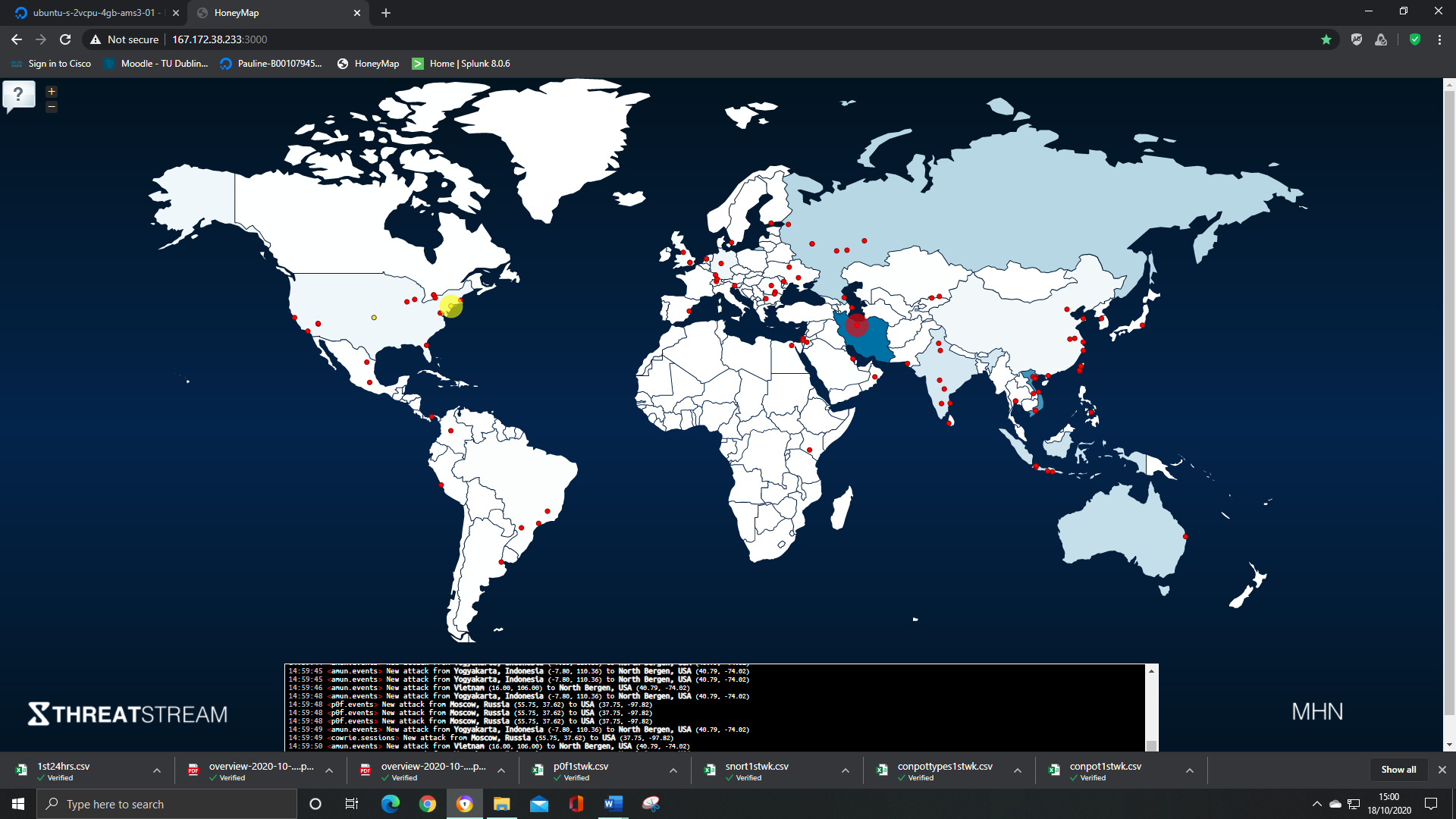


Figure 2: Overview of Deployment showing live attacks

# Methodology

At the end of the deployment 5,847,124 attacks were recorded. Ireland ranked 6th in the Top Attack Countries at 9.47% with 383,506 attacks which was surprising. Due to this fact and the significant volume of data, I decided to compare the Irish attacks to attacks originating in the rest of the world.

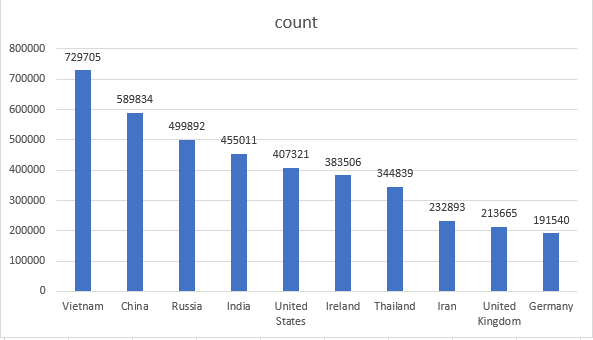


Figure 3: Top Attack Countries

These attacks were analysed under the following criteria:

* Attack Countries
* Attack Cities
* Top Honeypots
* IP Addresses
* Malware
* Attack Signatures
* Attack Ports
* Commands
* Daily Spike
* Username/Password
* Top P0f OS
* Top URL’s

# Findings

## Top Attack Countries

The top attack country was Vietnam with 729,705 attacks, followed by China with 589,834 and Russia on 499,892. The figures for China and Russia were not surprising but to see Vietnam at No. 1 was. Looking into the rise in cyber-attacks from Vietnam a DARKReading article from 2019 states that the ‘*country's rapid economic growth and other factors are driving an increase in cybercrime and cyber espionage activity’* [9].When you exclude the Irish results from the data, Panama now appears at No. 10 in the Top 10 Countries at 3.902% with 148,800 results.

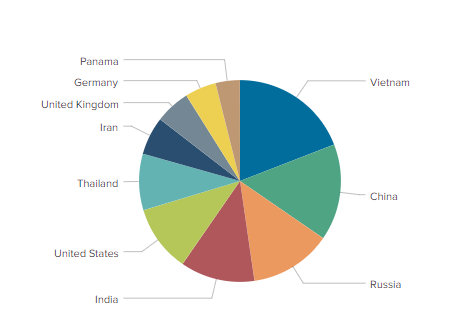


Figure 4: Panama enters Top 10 Countries when Ireland excluded

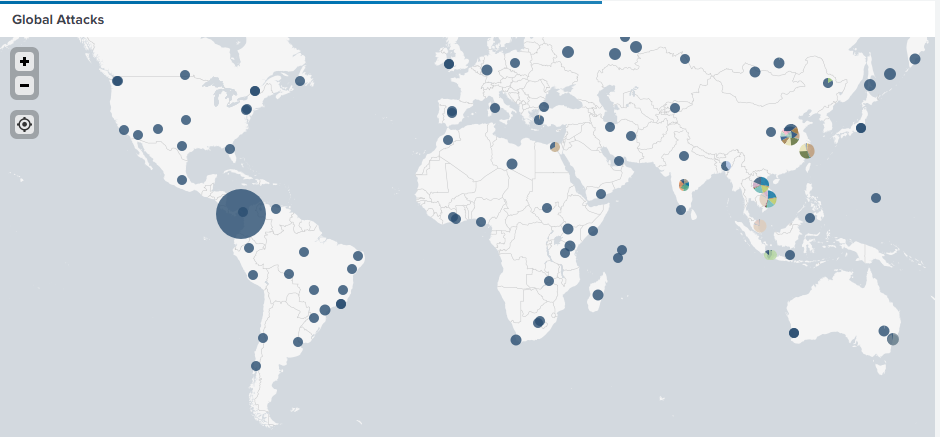


Figure 5: Splunk Global Attack Map

## Top Attack Cities

In the overall data two Irish Cities appear in the Top 10 Attack Cities, Macroom at No. 1 with 259,411, 23.217% and Ballingeary at No. 4 with 114,456, 10.244% of attacks. Eliminating Irish locations from the results, Hanoi now becomes the No. 1 location with 187,705, 22.813% of attacks. Cairo enters the list at No. 9 with 40,158, 4.881% and St. Petersburg at No. 10 with 39,169, 4.76% of attacks.

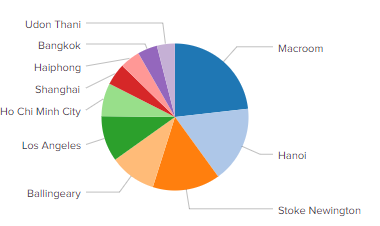


Figure 6: Top 10 Cities including Irish results

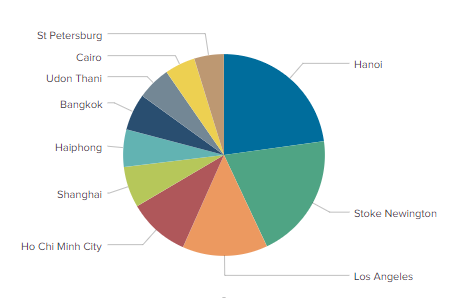


Figure 7: Top 10 Cities excluding Irish Locations

Looking at the statistics for Irish attack locations, in addition to Macroom and Ballingeary, there were 7 other locations identified –

* Dublin 9,568
* Maynooth 26
* Portmagee 6
* Tullamore 6
* Enniscorthy 4
* Galway 4
* Unidentified 25

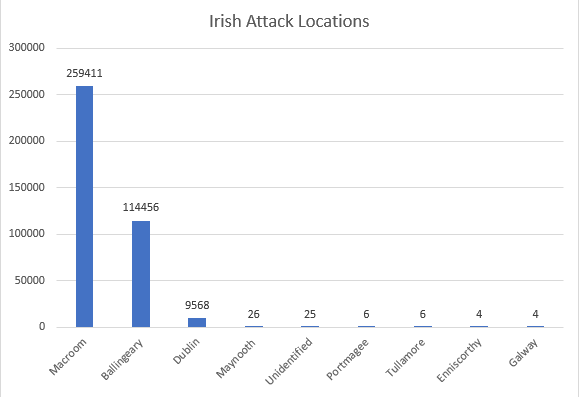


Figure 8: Locations of Attacks in Ireland

The high numbers of attacks originating in Macroom and Ballingeary were very surprising knowing the geography of Ireland and the size of these 2 areas. The 2016 census recorded the population of Macroom at 3,765 people and Ballingeary at 235. Dublin was 3rd highest with 9,568 attacks. The remaining locations were Maynooth with 26 attacks, Portmagee and Tullamore with 6, Enniscorthy and Galway with 4 and 25 attacks from unidentified locations, which upon further research were identified as originating in Dublin also.

## Top Honeypots

In the overall data the top honeypot type is Amun with 2,874,964 or 49.18%, 2nd is p0f events with 1,786,796 at 30.56% and 3rd is Cowrie with719,809 or 12.31%. Looking at the Irish data Cowrie is the largest with 374,023 or 97.527%. Excluding the Irish attack data Cowrie changes to 4th in the overall attacks moving Dionaea up to 3rd which has 364,374 and 6.67% of attacks. Cowrie now stands on 6.332% of the overall attack data.

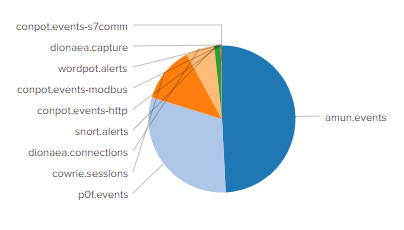


Figure 9: Top Honeypots by Type

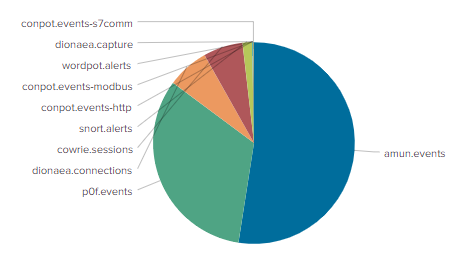


Figure 10: Top Honeypots Excluding Ireland

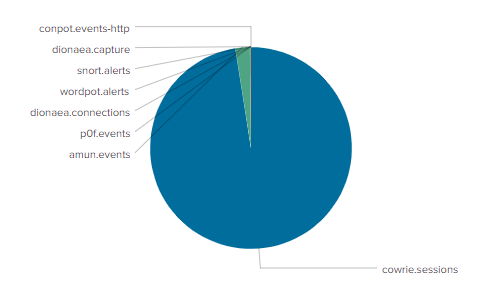


Figure 11: Top Irish Honeypots

## Attack IP Addresses

### Top Attack IP

No Irish IP address appear in the Top 10 Attack IP’s. The top IP address is 51.89.192.84 and accounts for 166,209, 2.84% of attacks.

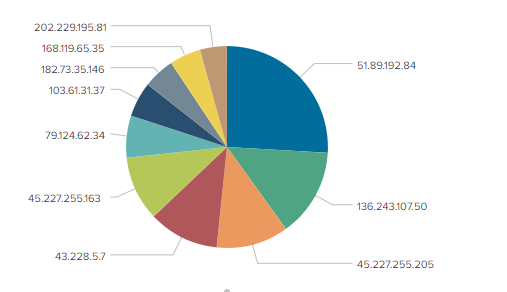


Figure 12: Top Attack IP’s

Investigating this address on <https://whatismyipaddress.com/> and <https://www.shodan.io/> we see that it originates in London, UK. Checking the address on <https://www.abuseipdb.com/> we see that it has been reported 14 times.

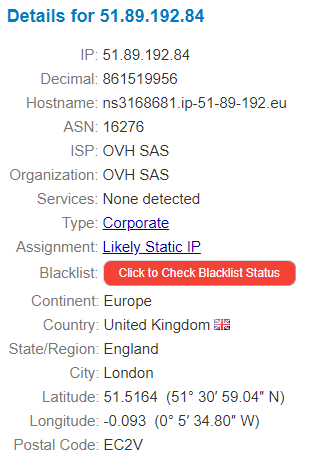


Figure 13: 51.89.192.84 report from <https://whatismyipaddress.com/>

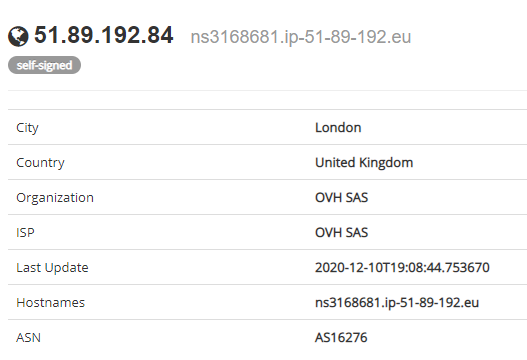


Figure 14:51.89.192.84 on https://www.shodan.io/

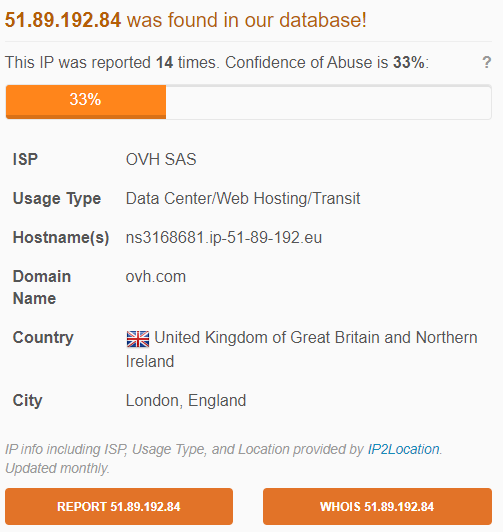


Figure 15: 51.89.192.84 report on <https://www.abuseipdb.com/>

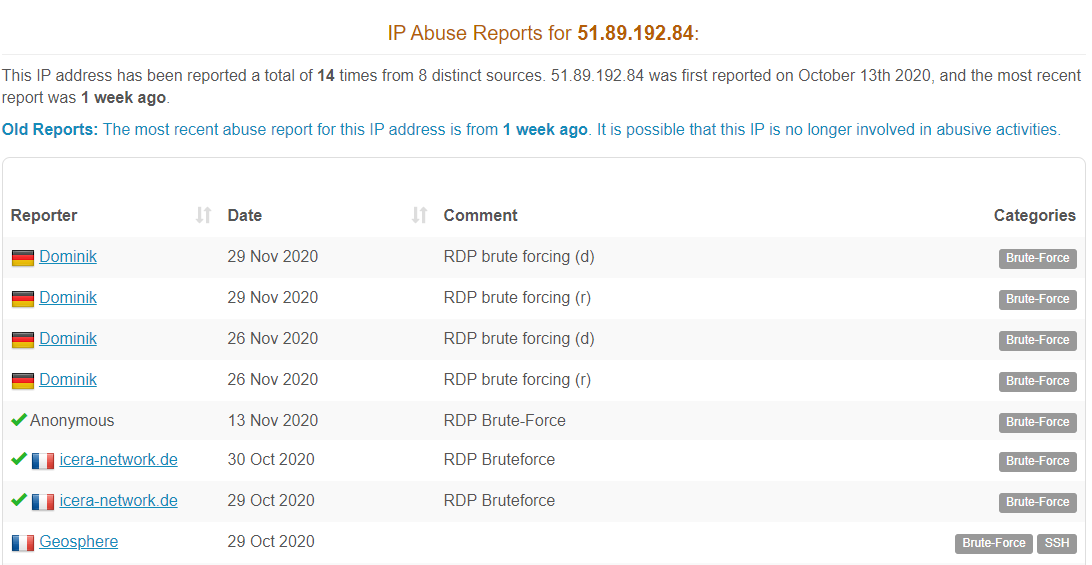


Figure 16: Sample of Abuse Reports from <https://www.abuseipdb.com/>

### Top Irish IP

A total of 68 unique IP addresses were identified in the Irish attack data. The top IP address was 5.188.86.167 accounting for 24,544 attacks and originated in Macroom. This is 14.76% compared to the top IP address.

Using Splunk to drill into the originating IP addresses of the attacks we can see that the Macroom and Ballingeary IP addresses are all very similar and account for 20 of the Irish IP addresses.

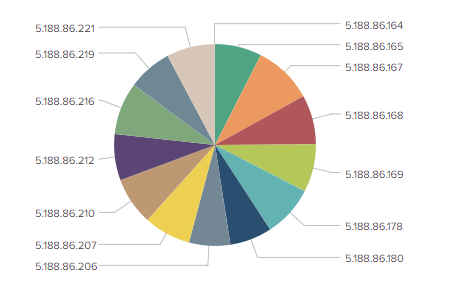


Figure 17: Macroom IP Addresses

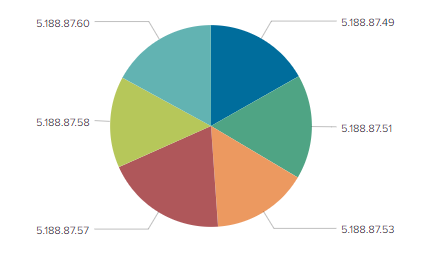


Figure 18: Ballingeary IP Addresses

Investigating 5.188.86.167 and the other Macroom and Ballingeary IP’s with <https://whatismyipaddress.com/> the addresses belong to Global Layer B.V., who are a large-scale IP services provider from the Netherlands, and the Country identifies as Ireland. Checking the same addresses with <https://www.abuseipdb.com/> the Country is identified as the Netherlands.

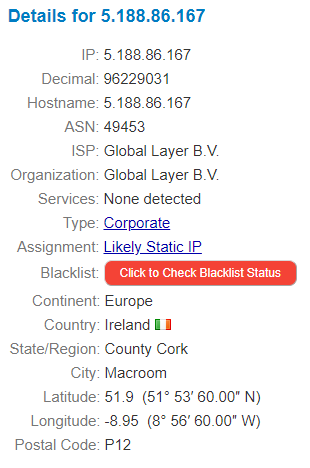


Figure 19: IP 5.188.86.167identified using <https://whatismyipaddress.com>

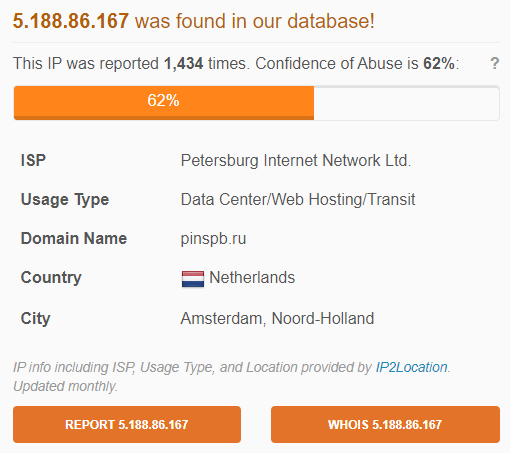


Figure 20: IP 5.188.86.167 identified using <https://www.abuseipdb.com>

5.188.86.167 has 1,434 reports recorded against it on <https://www.abuseipdb.com>.

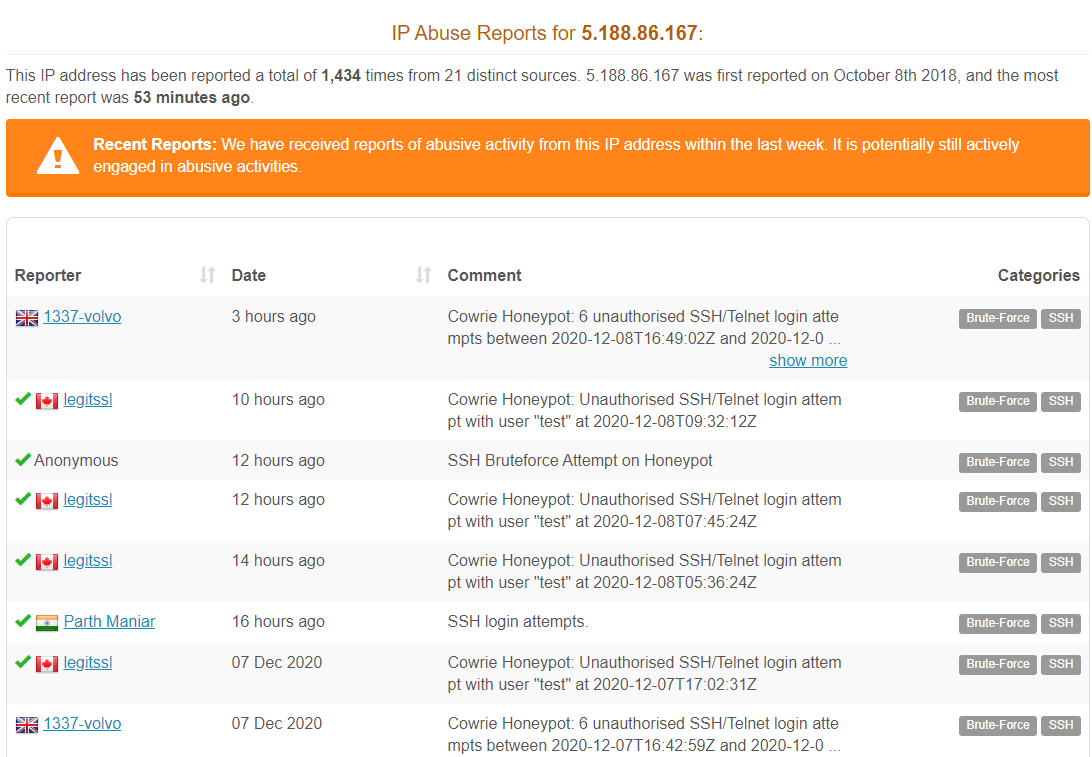


Figure 21: IP Abuse Report 5.188.86.167using <https://www.abuseipdb.com>

The discrepancy between the host country is accounted for by the fact that Global Layer B.V. host their servers in Ireland.

### Dublin

There were 39 unique IP addresses which account for 9,568 attacks accredited to Dublin. These IP’s are listed Fig. 17 below.

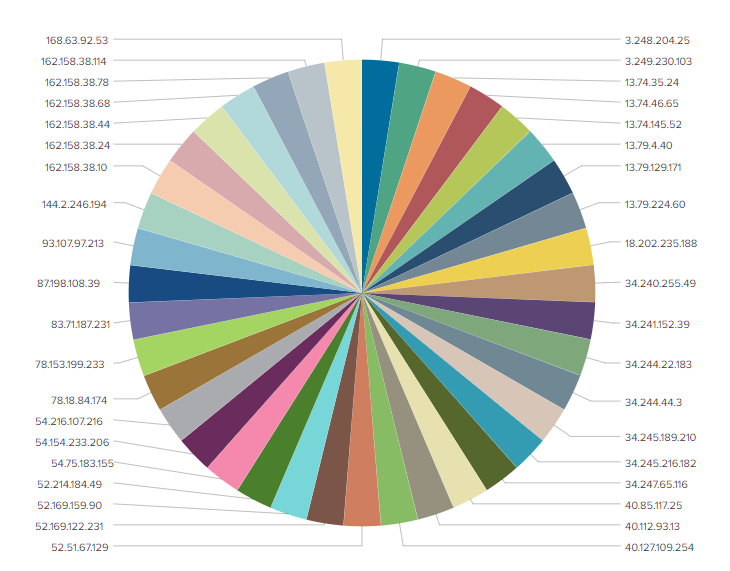


Figure 22: Dublin IP Addresses

Investigating these IP addresses using <https://whatismyipaddress.com> 15 IP addresses were identified as Amazon AWS, 12 MS Azure and 6 Cloudflare who all provide cloud services to users and so were not investigated further. The remaining 6 IP addresses were investigated using <https://whatismyipaddress.com> and <https://www.abuseipdb.com>.

* **78.153.199.233**

ISP: Blacknight Internet Solutions Ltd.

City: Dublin

Attacks: 8

Reports: 0

* **83.71.187.231**

ISP: Eir Broadband

City: Dublin

Attacks: 4

Reports: 130

* **144.2.246.194**

ISP: Leeson Telecom Holdings Ltd

City: Dublin

Attacks: 20

Reports: 25

* **87.198.108.39**

ISP: Magnet Networks Ltd

City: Dublin

Attacks: 1

Reports: 1

* **78.18.84.174**

ISP: Sky

City: Dublin

Attacks: 7

Reports: 5

* **93.107.97.213**

ISP: Vodafone Ireland

City: Dublin

Attacks: 24

Reports: 62

### Maynooth

* **86.45.5.178**

ISP: Eir Broadband

City: Maynooth

Attacks: 26

Reports: 112

As of the 6th December this IP had not been reported in the last week and was possibly no longer involved in abusive activities.

### Other Locations

The remaining IP addresses were also investigated

* **185.24.233.48**

ISP: ServeByte Ltd

City: Tallaght

Attacks: 20

Report: 1,935 times

* **217.78.1.59**

ISP: Digiweb Ltd

City: Dublin

Attacks: 2

Report: 542 times

* **185.24.235.140**

ISP: ServeByte Ltd

City: Tallaght

Attacks: 3

Report: 167 times

### Portmagee

* **91.223.87.66**

ISP: Invertec Ltd

City: Listowel/Cahersiveen

Attacks: 6

Report: 154 times

### Galway

* **89.101.141.136**

ISP: Virgin Media Ireland Ltd

City: Dublin

Attacks: 4

Report: 150 times

### Enniscorthy

* **86.41.117.52**

ISP: Eir Broadband

City: Enniscorthy

Attacks: 4

Report: 1 time

### Tullamore

* **213.233.155.139**

ISP: Vodafone Ireland Ltd

City: Ballyhaunis

Attacks: 4

Report: 6 times

* **213.233.155.159**

ISP: Vodafone Ireland Ltd

City: Granard

Attacks: 2

Report: 1 time

## Malware

### Top md5 values

The top md5 value recorded was:

**ae12bb54af31227017feffd9598a6f5e**

This was identified by 64/70engines on <https://www.virustotal.com/>. The file type a Win32 DLL and a WannaCry, WannaCrypt variant ransomware. It targets Intel 386 or later processors and compatible processors.

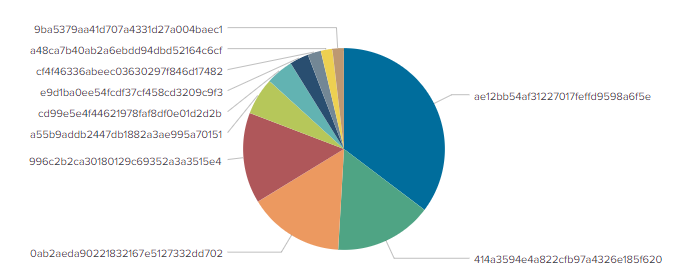


Figure 23: Top 10 md5 Values

### Irish Values

There were 3 malware attacks originating in Ireland with 2 distinct md5 values none of which appeared in the global Top 10 Values. Investigating each of these on virus total revealed the following results.

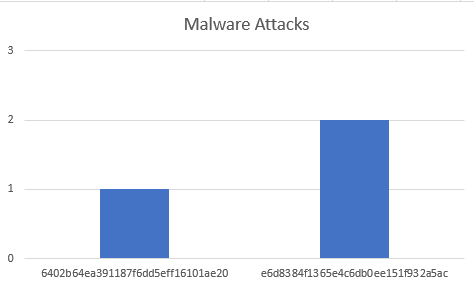


Figure 24: Malware Attacks

**e6d8384f1365e4c6db0ee151f932a5ac**

This was identified by 60/69 engines on <https://www.virustotal.com/>. The file type a Win32 DLL and a WannaCry, WannaCrypt variant ransomware. It targets Intel 386 or later processors and compatible processors.

**6402b64ea391187f6dd5eff16101ae20**

This was identified by 60/69 engines on <https://www.virustotal.com/>. The file type a Win32 DLL and a WannaCry, WannaCrypt variant ransomware. It targets Intel 386 or later processors and compatible processors.

This Irish malware attacks were in keeping with top attack values sharing a similar signature and executing in a similar fashion.

## Attack Signatures

### Top Signatures

In the overall attack statistics, the top signature is ‘Connection to Honeypot’ accounting for 3,253,258 attacks. Observing the Irish data, the top signature is ‘SSH session on cowrie honeypot’ and amounts to 373,891 attacks and 97.49% of the overall Irish signatures. When the Irish data is excluded from the totals is does not affect the overall ranking of signatures but does account for 64.6% of the total for ‘SSH session on cowrie honeypot’. The 2nd highest value in the Irish data is ‘Connection to Honeypot’ at 8,855 but only amounts to .2% in the overall data. The remaining Irish values are negligible in terms of the overall data.

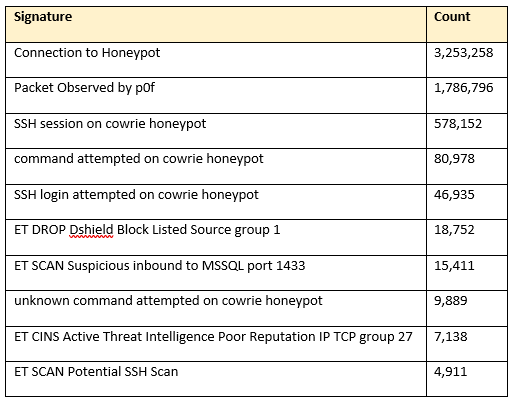


Figure 25: Top Attack Signatures

### Top Signatures Excluding Irish Values

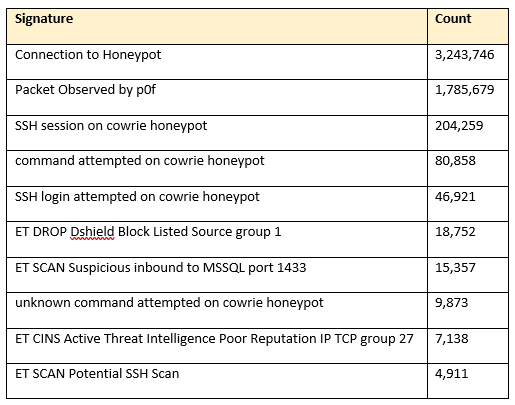


Figure 26: Top Signatures Excluding Ireland

### Top Irish Signatures

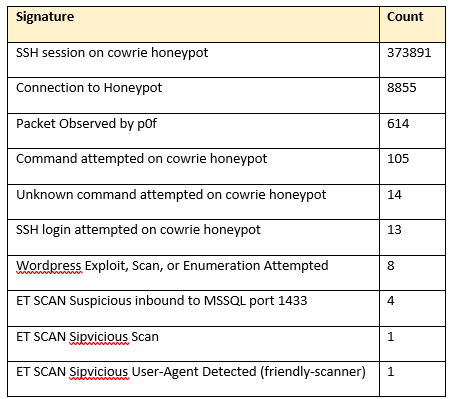


Figure 27: Top Irish Signatures

## Top Attack Ports

Overall, there was 100+ port numbers recorded in the attacks. The top port was Port 445 with 2,745,265 attacks which is the default port for SMB over IP. It is susceptible to trojan attacks through file sharing. The 2nd highest port was Port 22 the default SSH port with 1,448,507 attacks. Port 3389 was 3rd with 716,537 attacks the default port used for Remote Desktop Protocol (RDP) allowing the user to connect remotely to another computer over a network connection.

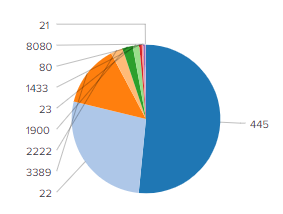


Figure 28: Top Attack Ports

In the Irish attacks there were 19 ports recorded with the Top 10 Ports represented as follows:

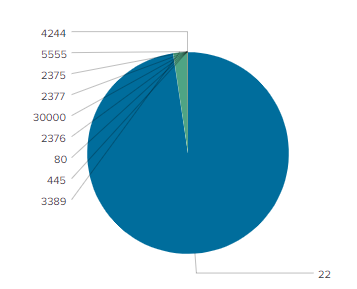


Figure 29: Irish Attack Ports

Port 22 with 374,488 attacks and 3389 with 8,828 attacks had the highest values and were the only ones which could significantly impact the overall results. With the Irish data excluded the order is not impacted but it does account for 25% of the attacks on Port 22 and 1.2% of the attacks on Port 3389.

## Top Commands

In the overall statistics the top command entered was ***echo -e\*** with a count 9,255 or 19.685% and the 2nd highest command was ***uname -a*** with a count of 5,024 or 10.686%.

* ***echo -e\*** This command is used for writing formatted text to the terminal window and can include shell variables, filenames, and directories. You can also redirect echo to create text files and log files
* ***uname -a*** This command provides users with important system information such as OS kernel name, [hostname](https://linuxhandbook.com/debian-change-hostname/), kernel release, details about the last time the kernel was compiled, Machine architecture, the processor architecture, the operating system’s architecture, and operating system in a single output string.

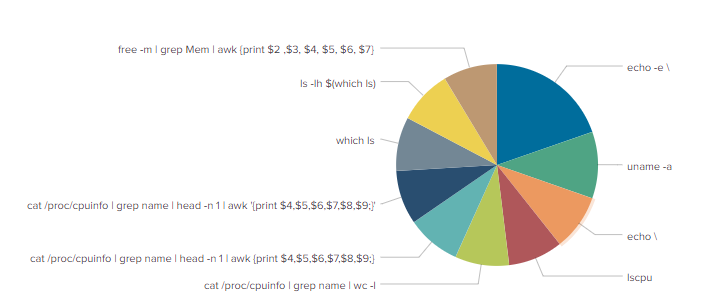


Figure 30: Top Commands

There was a total of 17 unique commands executed in the Irish attacks and each one of them was executed 7 times. The commands entered were:

|  |
| --- |
| * cat /proc/cpuinfo | grep model | grep name | wc -l |
| * cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}' |
| * cat /proc/cpuinfo | grep name | head -n 1 | awk {print $4,$5,$6,$7,$8,$9;} |
| * cat /proc/cpuinfo | grep name | wc -l |
| * cd ~ && rm -rf .ssh && mkdir .ssh && echo \ |
| * crontab -l |
| * echo \ |
| * free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}' |
| * free -m | grep Mem | awk {print $2 ,$3, $4, $5, $6, $7} |
| * ls -lh $(which ls) |
| * lscpu | grep Model |
| * top |
| * uname |
| * uname -a |
| * uname -m |
| * w |
| * which ls |

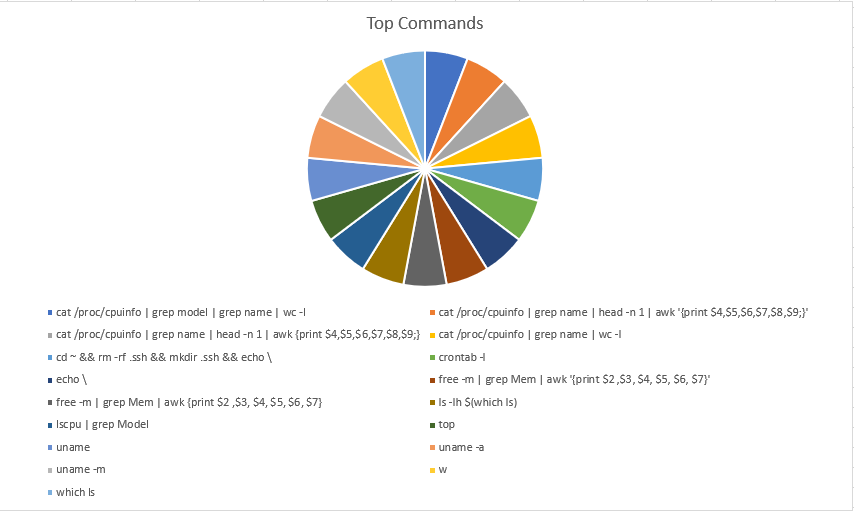


Figure 31: Top Irish Commands

None of the commands from the Irish data were recorded in significant numbers to impact the overall data.

## Highest Daily Record

The highest number of events recorded on a single day was 382,938 on the 10th November. Looking into the breakdown of events on that day to see what percentage of them originated in Ireland was interesting in that 9.725%, 30,190 events were recorded which was in keeping the overall for the entire period of 9.47%

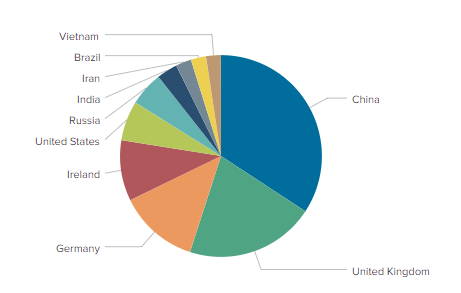


Figure 32: Highest Daily Attack Locations

When the Irish data is excluded for the day France enters the ‘Top Attack Countries’ at No. 10 with 6,990 attacks or 1.98% of the overall total.

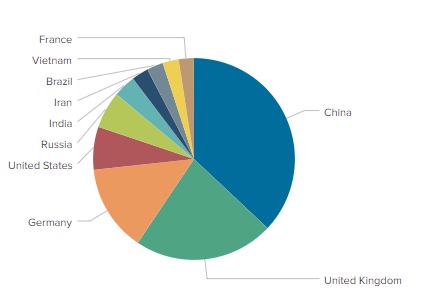


Figure 33: Top Countries 10.11.20 excluding Irish Data

Macroom and Ballingeary appeared in the ‘Top 10 Cities’ at No. 2 and No. 3

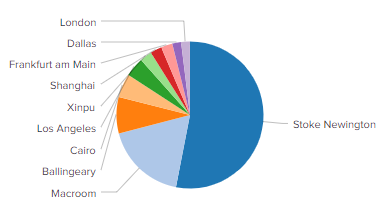


Figure 34: Top Cities 10.11.20

When the Irish data is excluded from the search Amsterdam enters the Top Cities at No. 9 with 2,062 attacks or 2.298%, and Jakarta at no. 10 with 1,808 attacks or 2.015%.

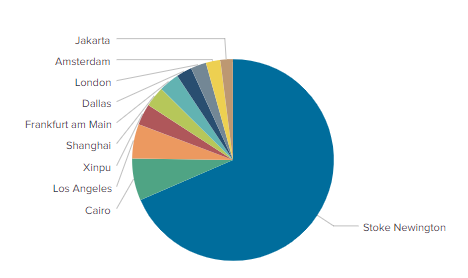


Figure 35: Top Cities 10.11.20 excluding Irish Data

## Top SSH Username/Password

The top usernames used in SSH attacks were ***admin*** with 8,612, followed by ***service*** with 7,218 and ***nproc*** with 4,079.

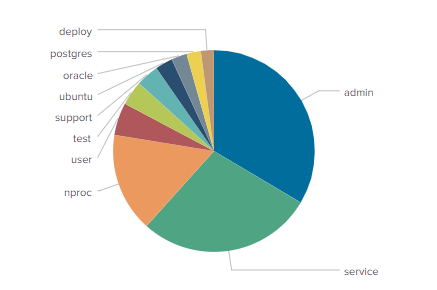


Figure 36: Top SSH Usernames

The top 10 ssh passwords were ***nproc*** with 4,079, followed by ***123456*** with 2,375 and ***123*** with 1,599.

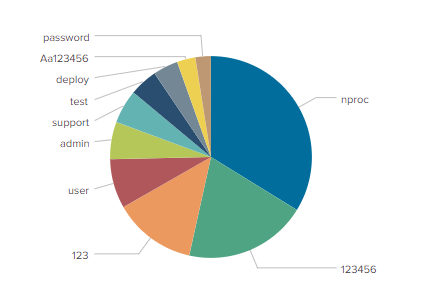


Figure 37: Top SSH Passwords

Analysing the top values used in the Irish attacks revealed 3 distinct usernames ***pi*** with 6, ***nproc*** with 5 and ***support*** with 2.

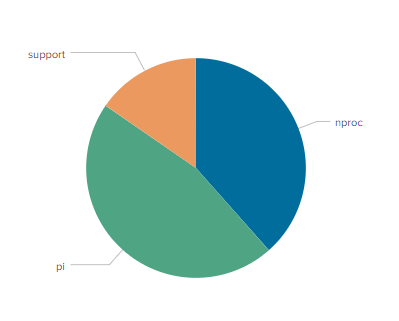


Figure 38: Irish Attack Usernames

There were 4 distinct passwords ***nproc*** with 5, ***raspberry*** with 3, ***raspberryraspberry993311*** with 3 and ***12345678*** with 2.

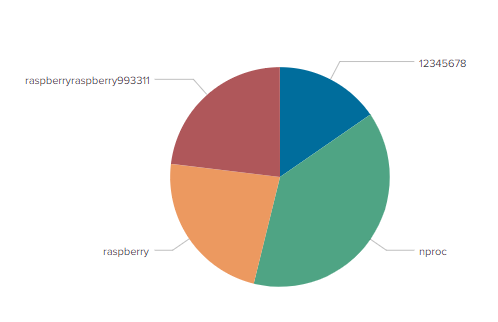


Figure 39: Irish Attack Passwords

The Irish figures were not significant in relation to the overall data.

## Top p0f OS

In the overall data ‘Windows 7 or 8’ was identified as the top p0f OS with a count of 209,554 and ‘Linux 3.11 and newer’ 2nd with 151,215.

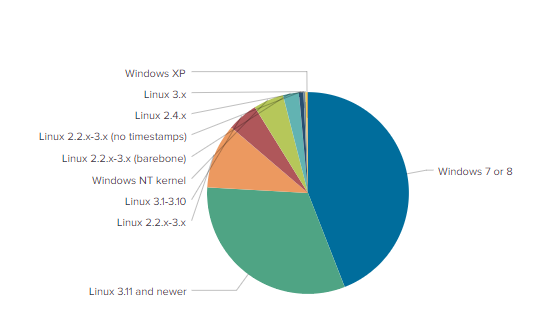


Figure 40: Top p0f OS

The p0f operating systems in the Irish originating attacks were identified as follows:

Linux 3.11 and newer 79

Linux 2.2.x-3.x 45

Windows 7 or 8 32

Linux 2.2.x-3.x (barebone) 2

Windows NT kernel 1

|  |
| --- |
|  |

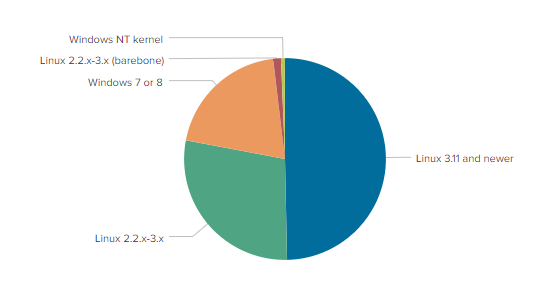


Figure 41: Top Irish p0f OS

The Irish figures do not significantly impact the overall results.

## Top URLs

There were 47 distinct URL’s detected but none were recorded in the attacks originating in Ireland. The top 10 URL’s were as follows:

|  |
| --- |
| http://193.228.91.109/Otpzl/7rtya.x86 |
| http://104.168.195.213/Thorbins.sh |
| http://119.147.213.57/bot.pl |
| http://45.145.185.25/wash.sh |
| http://193.228.91.123/pwnInfect.sh |
| http://45.153.203.197/nigga.x86 |
| http://45.153.203.197/nigga.sh4 |
| http://45.153.203.197/nigga.mips |
| http://45.153.203.197/nigga.m68k |
| http://45.153.203.197/nigga.arm7 |

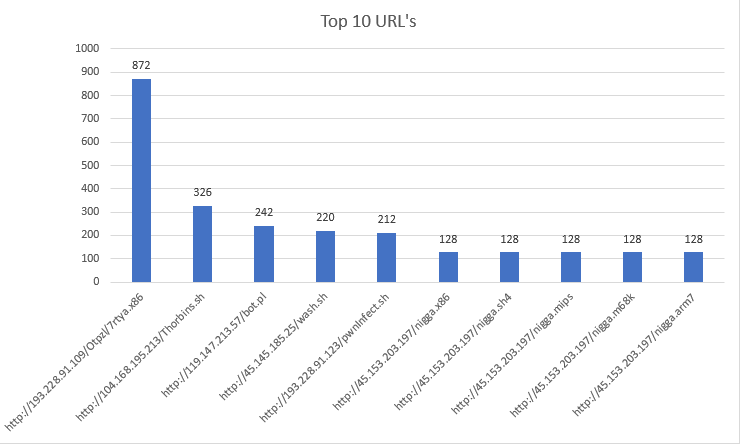


Figure 42: Top 10 URL's

The 1st item on the list <http://193.228.91.109/Otpzl/7rtya.x86> was identified on <https://www.virustotal.com/> by 14/80 engines as malicious and was responsible for 872 attacks, the 2nd [http://104.168.195.213/Thorbins.sh was identified by 5/80](http://104.168.195.213/Thorbins.sh%20was%20identified%20by%205/80) engines as malicious and responsible for 326 attacks while the 3rd <http://119.147.213.57/bot.pl> was identified by 12/82 engines and responsible for 242 attacks.

# Conclusion

The attacks originating in Ireland are significant, but their impact is targeted to specific areas rather than spread evenly.

The greatest number of Irish attacks are Cowrie honeypot-based accounting for 97.527% in Ireland and 5.641% of the global Cowrie figures. Cowrie logs brute force attacks and the shell interaction the attacker performs. Ireland’s top attack signature is ‘SSH session on cowrie honeypot’ and represents 97.49% of the overall Irish signatures and 64.6% of the global figure. The most attacked port in the Irish data is Port 22 which accounts for 97.657% of Irish data and 25% of the global figures for the port and as the default SSH port is in keeping with the rest of the attack date for Ireland.

The attacks originating in Macroom & Ballingeary make up 97.487% of the Irish attacks and account for 33.461% of the overall global attacks with Macroom No. 1 in the Top Attack Cities. The company responsible for these IP addresses are a Dutch Cloud service provider launched in 2011 because of bad experiences with previous service providers. Slowness and unstable connectivity motivated the business set-up to provide large-scale IP services and capacity services worldwide. They host servers in Cork which identifies their origin as Irish. Tracking the culprits behind the attacks launched from these addresses would require access to the company records so does not reflect the true location of the attackers.

# References

[1]"Modern Honey Network | Splunkbase", *Splunkbase.splunk.com*, 2020. [Online]. Available: https://splunkbase.splunk.com/app/2707/. [Accessed 18 October 2020].

[2]"Build Your Own Honeypot Network In Under An Hour", *JerryGamblin.com*, 2020. [Online]. Available: https://jerrygamblin.com/2017/05/29/build-your-own-honeypot-network-in-under-an-hour/. [Accessed 18 October 2020].

[3]"Honeypot Networks", *IT & Security Stuffs!!!*, 2020. [Online]. Available: https://itandsecuritystuffs.wordpress.com/2015/02/03/honeypot-networks/. [Accessed 18 October 2020].

[4]J. Stevenson, R. Sterio, J. Stevenson and J. Stevenson, "What's a Honeypot, and how to set one up in under an hour - Hacking Insider", *Hacking Insider*, 2020. [Online]. Available: http://www.hackinginsider.com/2016/03/whats-a-honeypot-and-how-to-set-one-up-in-under-an-hour/. [Accessed 18 October 2020].

[5]2020. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-create-your-first-digitalocean-droplet-virtual-server. [Accessed 18 October 2020].

[6]Lane, Mark, “Honeypots”. 2020. Moodle - TU Dublin Blanchardstown Campus: Log in to the site. [ONLINE] Available at: https://vle-bn.tudublin.ie/pluginfile.php/235706/mod\_resource/content/0/Honeypots.pdf. [Accessed 18 October 2020].

[7] Cowrie - CommunityHoneyNetwork. 2020. Cowrie - CommunityHoneyNetwork. [ONLINE]Available at: https://communityhoneynetwork.readthedocs.io/en/stable/cowrie/. [Accessed 02 December 2020].

[8] GitHub. 2020. GitHub - jordan-wright/elastichoney: A Simple Elasticsearch Honeypot. [ONLINE] Available at: https://github.com/jordan-wright/elastichoney. [Accessed 02 December 2020].

[9]Dark Reading. 2020. Vietnam Rises as Cyberthreat. [ONLINE] Available at: https://www.darkreading.com/attacks-breaches/vietnam-rises-as-cyberthreat-/d/d-id/1334890. [Accessed 10 December 2020].

# Appendix

## Presentation Link

<https://www.youtube.com/watch?v=kJW-2czquVw>