

**Modern Honey Network:   
An Investigation into MHN, Deployment &   
Analysis of Collected Data**

**James Finglas**

**B00094138**

Department of Informatics

School of Informatics and Engineering

Technological University Dublin

Submitted to Technological University Dublin in Partial Fulfilment of the requirements for the degree of:

Bachelor of Science (Honors) in Computing

Course: Network Security Analytics

Lecturer: Mark Lane

Submission Date: /12/2019

Word count (Introduction to Conclusions): 3148

# Project Submission/Declaration Form

Submitted by: James Finglas

Course Coordinator: Stephen O'Shaughnessy

Module Name: Network Security Analytics

Course Code: H4015

Lecturer: Mark Lane

Submission Date: /12/2019

I declare that the work contained in this report which I now submit on the program of study leading to the award of Degree of Honors B.Sc. in Computer Science in Technological University for Dublin is my own work and has not been taken from the work of others. Any sources which have been referenced or analyzed have been cited using the Harvard/IEEE standard within the body of this report. It is entirely my own work except where otherwise stated and has not been submitted for assessment for an academic purpose at this or any other academic institution other than in partial fulfilments of the requirements stated above.

I have read and understood the Technology University Dublin’s policy regarding plagiarism.

X

James Finglas

# Abstract

This report herein documents the research undertaken into Modern Honey Network (MHN) by James Finglas (B00094138), and the deployment research, data collection and analysis gained while using the network.   
  
The report does not include any information pertaining to the installation or setup. Nor does the report delve into the inner functioning of each individual Honeypot sensor as this would be out of the scope of the assignment brief.  
  
The research into the Management, deployment and logging of MHN is restricted to the types of honeypots available within MHN, good combinations of honeypots and goals behind my deployment choices. This section also includes my research into geo-location deployment vectors in order to discern patterns of attacks.

While There is a wealth of General analytical data available to be mined from MHN logs, due to the assignment word constraint limit of 3000 words, I have elected to focus on Threat intelligence related data, Malware threat actors and URL Threat actors/vectors. Data collection is documented as much as is possible within the document and all data shall be provided via disc’s or PDF’s or additional pertinent info within appendix’s along with the document. Data analysis is also documented from which the conclusions is derived. Physical malware analysis has been deemed beyond scope.

Contents

[Project Submission/Declaration Form 2](#_Toc23979101)

[Abstract 3](#_Toc23979102)

[Table of figures: 5](#_Toc23979103)

[1.0 Introduction 6](#_Toc23979104)

[2.0 Summary 6](#_Toc23979105)

[2.1 Methodology 6](#_Toc23979106)

[2.2 Research Goals 6](#_Toc23979107)

[2.3 What is MHN? 6](#_Toc23979108)

[2.3.1 Ubuntu – Conpot 6](#_Toc23979109)

[2.3.2 Ubuntu/Raspberry Pi – Drupot 7](#_Toc23979110)

[2.3.3 ubuntu/Raspberry Pi – Magenpot 7](#_Toc23979111)

[2.3.4 Ubuntu – Wordpot 7](#_Toc23979112)

[2.3.5 Ubuntu – Shockpot 7](#_Toc23979113)

[2.3.6 Ubuntu - p0f 7](#_Toc23979114)

[2.3.7 Ubuntu – Suricata 7](#_Toc23979115)

[2.3.8 Ubuntu – Glastopf 7](#_Toc23979116)

[2.3.9 Ubuntu – Elastichoney 7](#_Toc23979117)

[2.3.10 Ubuntu – Amun 7](#_Toc23979118)

[2.3.11 Ubuntu – Snort 7](#_Toc23979119)

[2.3.12 Ubuntu/Raspberry Pi – Dionaea 8](#_Toc23979120)

[2.3.13 Ubuntu Shockpot Sinkhole 8](#_Toc23979121)

[3.0 Practical Deployment of MHN 9](#_Toc23979122)

[4.0 Primary Research Outcomes 12](#_Toc23979123)

[4.1 General data Analytics 12](#_Toc23979124)

[4.2 Dionaea Analytics 15](#_Toc23979125)

[4.3 p0f Analytics 27](#_Toc23979126)

[4.4 Cowrie Analytics 29](#_Toc23979127)

[4.5 Snort Analytics 30](#_Toc23979128)

[5.0 Conclusions 35](#_Toc23979129)

[6.0 Glossary 36](#_Toc23979130)

[7.0 References 38](#_Toc23979131)

# Table of figures:

[Figure 1 Total Data collected. 6](#_Toc24921387)

[Figure 2 Data center options available from Digital-Ocean. 9](#_Toc24921388)

[Figure 3The Talos Cyber Attack Map [14]. 9](#_Toc24921389)

[Figure 4 CYBER THREAT MAP (Check Point SOFTWARE TECNOLOGIES LTD.) as viewed at the time and date of being accessed [14]. 10](#_Toc24921390)

[Figure 5 My Server details. 11](#_Toc24921391)

[Figure 6 Total Events for MHN.LOG, MHN.LOG.1, MHN.LOG.2, & MHN.LOG.3. 12](#_Toc24921392)

[Figure 7 Top Attackers by country. 13](#_Toc24921393)

[Figure 8 Top honeypots by type. 14](#_Toc24921394)

[Figure 9 Top 10 Hashes for MHN.LOG/MHN.Log.1. 15](#_Toc24921395)

[Figure 10 Top 10 Hashes for MHN.LOG.2/MHN.LOG.3 15](#_Toc24921396)

[Figure 11 Top URL’s for MHN.LOG. 17](#_Toc24921397)

[Figure 12 Top URL’s for MHN.LOG.1. 17](#_Toc24921398)

[Figure 13 Top URL’s for MHN.LOG.2 17](#_Toc24921399)

[Figure 14 Top URL’s for MHN.LOG.3 18](#_Toc24921400)

[Figure 15 Here we see our clean response for the subdomain and the higher domain indicated below it. 18](#_Toc24921401)

[Figure 16 Here we see the parent domain recognized as a Chinese botnet attack vector. 19](#_Toc24921402)

[Figure 17 ESET Detection of http://49.79.224.66:2642/360nb.exe. 19](#_Toc24921403)

[Figure 18 Another Chinese attack vector revealed. 20](#_Toc24921404)

[Figure 19 http://211.75.223.67:6272/ndcn Detected by Spamhaus. 20](#_Toc24921405)

[Figure 20 Another Chinese attack vector revealed. 21](#_Toc24921406)

[Figure 21 http://188.122.148.4:9695/vybd Detected by two engines. 21](#_Toc24921407)

[Figure 22 http://188.122.148.4:9695/vybd Swedish origin revealed 21](#_Toc24921408)

[Figure 23 http://112.27.156.182:22290/360dr.exe detected by 4 engines. 22](#_Toc24921409)

[Figure 24 Chinese origins revealed. 22](#_Toc24921410)

[Figure 25 http://5.56.134.38:6771/mryisgl detection. 23](#_Toc24921411)

[Figure 26 http://5.56.134.38:6771/mryisgl very curious origin & routing information. 24](#_Toc24921412)

[Figure 27 Top Dionaea attackers by IP/Country/Count. 25](#_Toc24921413)

[Figure 28 Top Dionaea port detections by count. 26](#_Toc24921414)

[Figure 29 Top p0f attackers by IP/Country. 27](#_Toc24921415)

[Figure 30 30 Top p0f ports by destination/count. 28](#_Toc24921416)

[Figure 31 Top 10 Signature hits for MHN.LOG & MHN.LOG.1. 30](#_Toc24921417)

[Figure 32 Top 10 Signature hits for MHN.LOG.2 & MHN.LOG.3. 31](#_Toc24921418)

[Figure 33 General timeline of events, for all events with peak uptake at Oct 21st for MHN.LOG. 32](#_Toc24921419)

[Figure 34 p0f timeline of events, with peak uptake at Oct 21st for MHN.LOG. 32](#_Toc24921420)

[Figure 35 Snort timeline of events, with peak uptake at Oct 19th for MHN.LOG. 32](#_Toc24921421)

[Figure 36 Here we see heavy activity detected by snort on ports 1433 & 3306, both associated with MySQL coinciding with the release of the new CVE. 33](#_Toc24921422)

[Figure 37 Here we see heavy activity detected by p0f on ports 1433, both associated with MySQL coinciding with the release of the new CVE. 33](#_Toc24921423)

# Introduction

The Modern-Honeypot-Network (MHN) is a deployment platform written in Python. It is aimed at rapid deployment of Honeypot sensors data collection and analysis. The deployment can be integrated with Splunk, or Elk/Kabana. A Splunk app called MHN-Splunk is available for direct Splunk Analysis.

# Summary

Here I summarize how I deployed MHN, what MHN and what each sensor does at its most basic level. Following on from that I documented samples of data analysis results, before drawing up some conclusions regarding the platform and what I gleamed from the data analysis.

## 2.1 Methodology

MHN was deployed on several servers on the Digital-Ocean-platform. I planned to attempt to make a custom version of the MHN-Splunk app for data mining/analysis of my data once I felt I had collected enough data (1TB collected over a 21-day period).

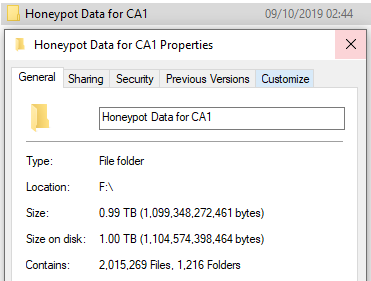


Figure 1 Total Data collected.

Finally, having mined the data and produced analytical reports I also considered conducting some research look-ups via virus-total or threat-intelligence websites. Data & logs were collected on a windows pc in my home and analyzed via Splunk. I chose to focus on threat-intelligence, malware and URL related data.

## 2.2 Research Goals

The goal of this assignment is to research MHN and understand what each of the honeypot sensors are capable of. We must then design a honeypot or series of honey pots and deploy MHN. We must then analyze the data collected.

## 2.3 What is MHN?

Modern Honey Network (MHN) is a modular platform designed for rapid deployment of honeypot sensors which acts as a central server collection point for data relating to these sensors.

### 2.3.1 Ubuntu – Conpot

Conpot is a honey designed to emulated industrial systems and architecture [1].

### 2.3.2 Ubuntu/Raspberry Pi – Drupot

Drupot is a distribution of the Drupal honeypot project, designed to intercept, monitor and deter spam-bots [2].

### 2.3.3 ubuntu/Raspberry Pi – Magenpot

Magenpot Is another distribution of Drupal honeypot [3].

### 2.3.4 Ubuntu – Wordpot

Wordpot is a WordPress honeypot which aim to detect bots scanning for WordPress themes and plugins.

[4].

### 2.3.5 Ubuntu – Shockpot

Shockpot is a web-based honey pot which attempts to detect attack agents attempting to deploy remote bash scripts. It is specifically focused on the remote vulnerability CVE-2014-6271 [5]. This vulnerability was incorrectly patched and CVE-2014-7169 was later deployed [6] [7].

### 2.3.6 Ubuntu - p0f

‘p0f’ is a passive fingerprint scanner which aims to document TCP/IP related information, such as operating system & uptime pertaining to attack agents [8].

### 2.3.7 Ubuntu – Suricata

Suricata acts as real time intrusion detection system or inline intrusion prevention system. It can also serve as a network security monitoring system (NSM) and has the capability to process PCAP files offline [9].

### 2.3.8 Ubuntu – Glastopf

Glastopf is an interesting Honeypot which aims to emulate types of web-vulnerabilities without simulating the actual vulnerability. This is a Honeypot popular with people who use to attract attacks relating to Dork or Google Dork searches. [10].

### 2.3.9 Ubuntu – Elastichoney

Elastichoney is a honey pot designed to detect attack agents attempting to exploit web-based RCE vulnerabilities [11].

### 2.3.10 Ubuntu – Amun

Amun is a low interaction honeypot which emulates vulnerabilities and attempts to capture malware attack actors. Amun allows for personalization to suit the users needs through the scripting of XML files and Python scripts to deploy custom vulnerability emulations [12].

### 2.3.11 Ubuntu – Snort

Snort is a real time intrusion-prevention-system. It is capable of logging and analyzing incoming packets for research purposes. [13].

### 2.3.12 Ubuntu/Raspberry Pi – Dionaea

Dionaea is a malware trap honeypot based in python. Like Amun, is a malleable and attempts to emulate vulnerabilities to attract malware and capture copies of the malware attack agents for analysis and research purposes [14].

### 2.3.13 Ubuntu Shockpot Sinkhole

The Shockpot Sinkhole is an extension of the Shockpot honeynet which adds Sinkhole abilities.

# 3.0 Practical Deployment of MHN

Pertaining to geo-location deployment there is a limitation in that Digital Ocean as a hosting provider is very restricted in its data center deployment options.

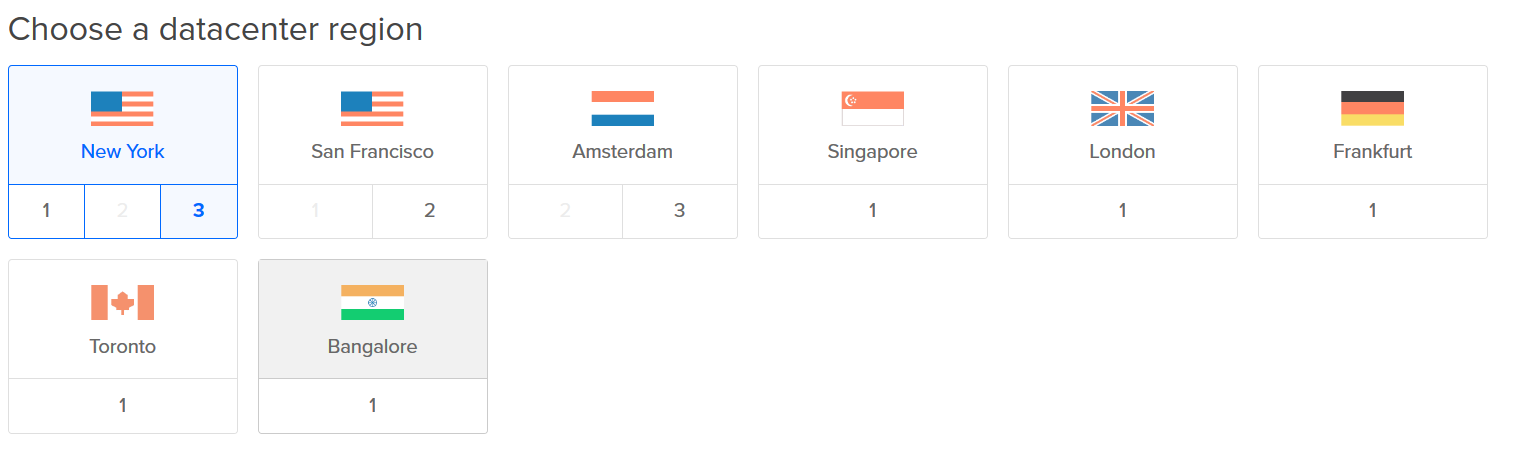


Figure 2 Data center options available from Digital-Ocean.

I spent some time examining the Talos threat map. This is an interesting perspective coming from one of the worlds leading networking/threat-intelligence providers and focuses uniquely on attack origin rather than destination.

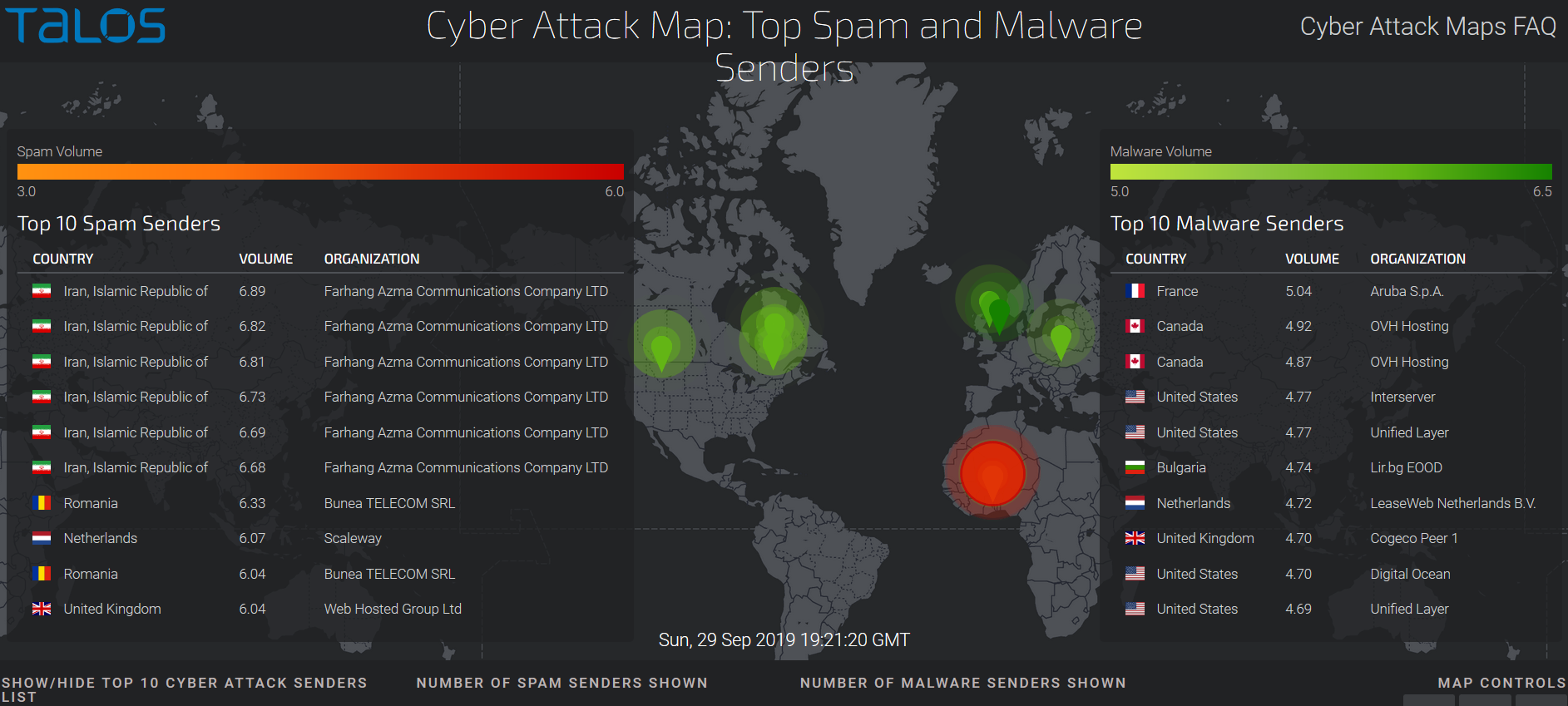


Figure 3The Talos Cyber Attack Map [14].

As we see above, this highlights 3 of the countries available in data center selection options as the being in the top 10 malware originators and 2 as being in the top 10 origin countries for spam.

Lastly, I spent some time observing the Check Point (Software Technologies LTD) CYBER THREAT MAP. This map highlights the reverse perspective and focuses on the destination attacks, as well as attack vector type and the type or target being attacked.

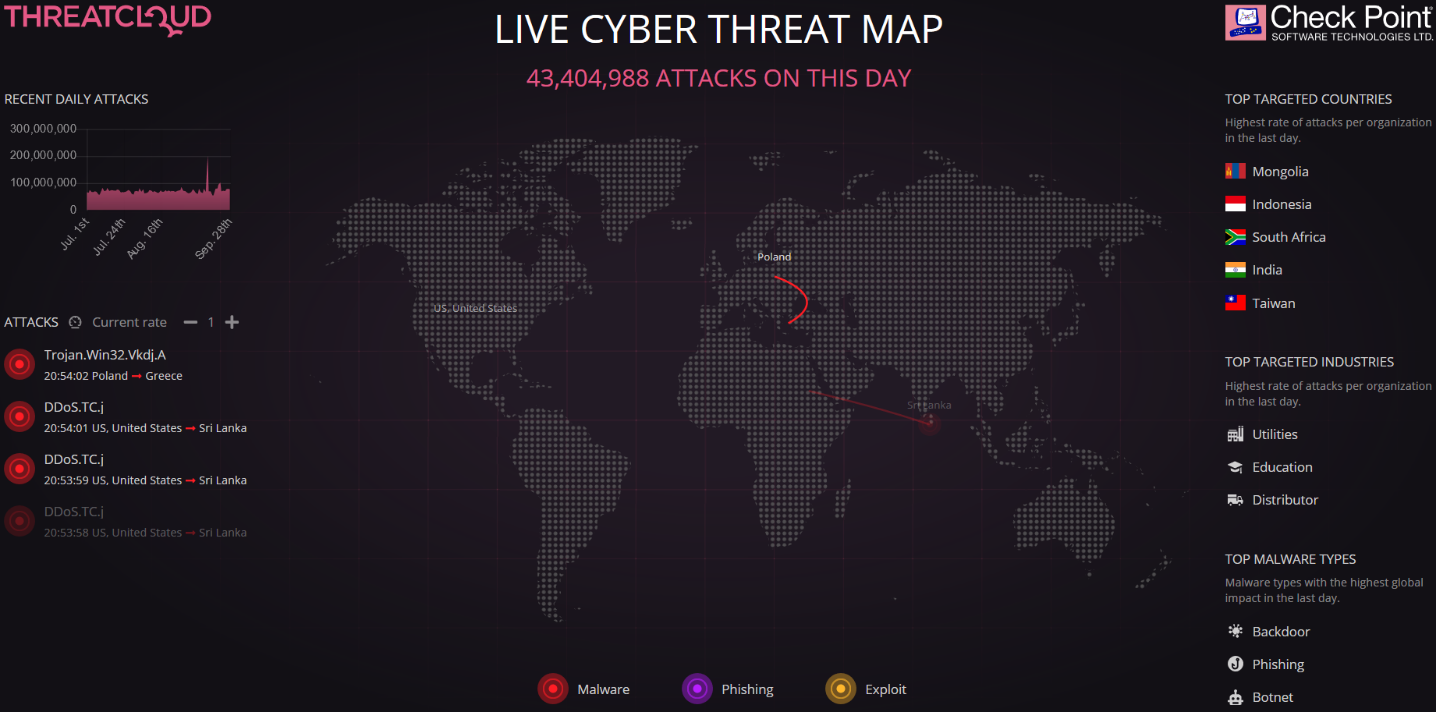


Figure 4 CYBER THREAT MAP (Check Point SOFTWARE TECNOLOGIES LTD.) as viewed at the time and date of being accessed [14].

Combining these 3 data points I deployed my droplets in the following locations: The US and the UK and India. I created 3 Honeypots. My honey pots will deploy Conpot to emulate utility-based servers with a naming convention designed to emulate financial based servers. My honeypot combination was:

* Conpot: to emulate an industrial/utilities-based server
* Cowrie: To capture SSH based data.
* Shockpot: To determine if the CVE related to Shockpot is active.
* Dionaea: because malware is the principal type of attack.
* Elastichoney: to attempt to detect web-based deployment attack agents.
* Snort: as a detection and protection measure.
* Glastopf to compliment Elastichoney.
* Pof: as my passive sniffer.

The details of my servers were as follows:

* MHN-Management-UK(London)-68.183.183.39.38
* Accounts-Receiving-US(New-York)-209.97.154.182
* Account-Payable-India(Bangalore)-139.59.34.232.
* Accounts-Forwarding-UK(London)-159.65.95.114.

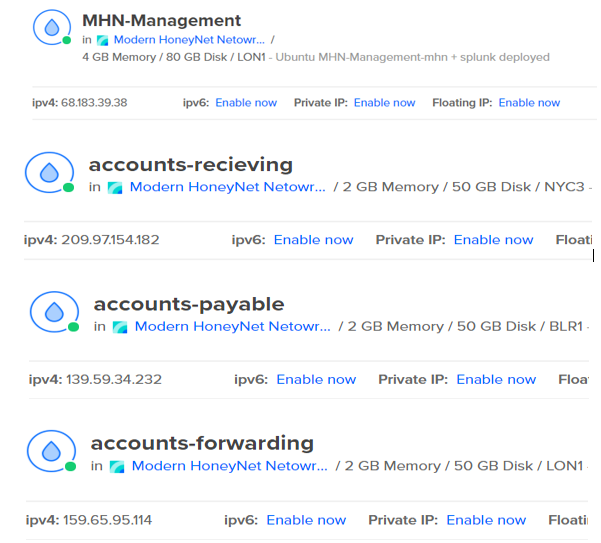


Figure 5 My Server details.

# 4.0 Primary Research Outcomes

Due to the nature of MHN, regular maintenance is required. Should the mongo database go down on the MHN management server it needs to be restarted. This changes file permissions and a new MHN log file is created. For this reason, I ended up with a total of 4 MHN log files to analyze. For this reason, the main MHN.LOG is the primary largest file and the second MHN.LOG.1/2/3 files are snippets of later time zones.

I ran my servers for a total of 21 days and generated a total of 3.45GB of log files and 1TB of binary scrapings and bistreams, although direct analysis of this files is considered beyond the scope of this assignment. Having attempted to mine my log files with the MHN-Splunk app I found the app limiting as it was designed for continuous hourly logging and not indexing a file over an extended period.

For this reason, I developed my own version of the MHN-Splunk app designed to index large files over an extended period. My App produced two pdf reports totaling almost 1200 pages of analytical data which of course far exceeds the scope of this assignment (both will be included with my submission) so what follows is the abridged version of the data I mined from these log files, focusing on threat Intelligence, malware and URL related data:

## 4.1 General data Analytics

Total events documented: 14, 551,624

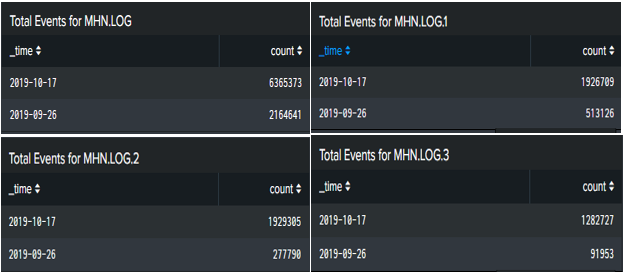


Figure 6 Total Events for MHN.LOG, MHN.LOG.1, MHN.LOG.2, & MHN.LOG.3.

Top Attackers by country:

1. United States
2. China
3. South Korea
4. Vietnam
5. Ireland

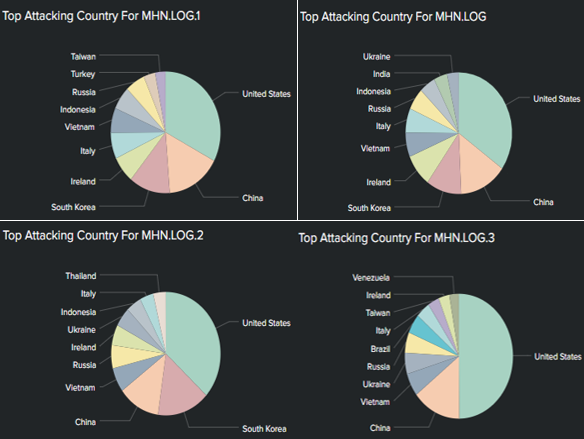


Figure 7 Top Attackers by country.

Top Honeypots by type:

1. Dionaea
2. p0f
3. Snort
4. Cowrie
5. Elastichoney

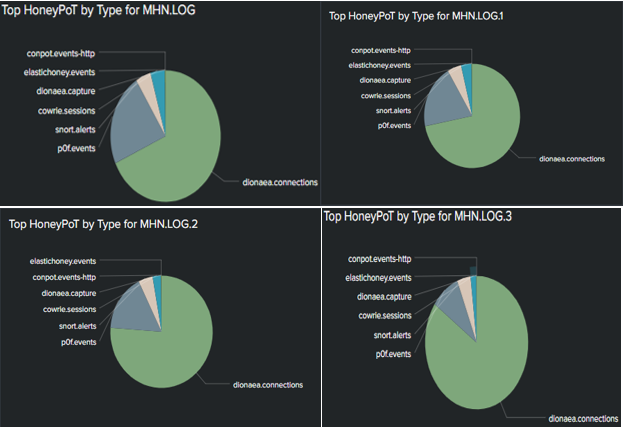


Figure 8 Top honeypots by type.

## 4.2 Dionaea Analytics

Top ten MD5’s for each file:

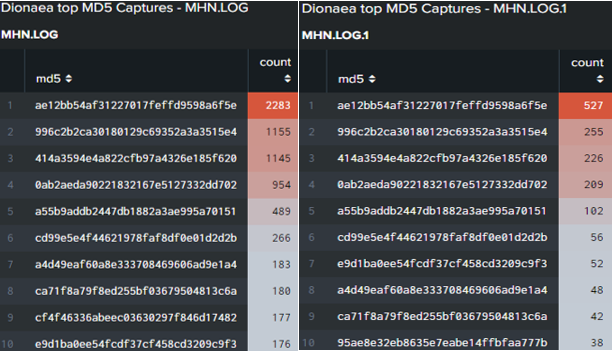


Figure 9 Top 10 Hashes for MHN.LOG/MHN.Log.1.

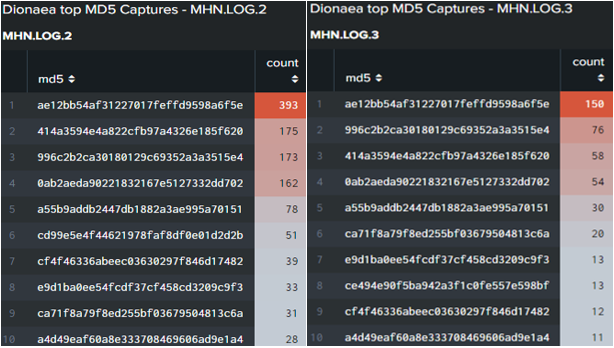


Figure 10 Top 10 Hashes for MHN.LOG.2/MHN.LOG.3

There are 12 non repeating MD5’s in the top results across all 4 files. These were investigated in detail. The results are as follow:

1. ae12bb54af31227017feffd9598a6f5e: 63 engine detections. This is a variant of WannaCry ransom-ware [17].
2. 996c2b2ca30180129c69352a3a3515e4: 62 engine detections. This is a variant of WannaCry ransom-ware [18].
3. 414a3594e4a822cfb97a4326e185f620: 63 engine detections. This is a variant of WannaCry ransom-ware [19].
4. 0ab2aeda90221832167e5127332dd702: 61 engine detections. This is a variant of WannaCry ransom-ware [20].
5. a55b9addb2447db1882a3ae995a70151: 62 Engine detections. This is a variant of WannaCry ransom-ware [21].
6. cd99e5e4f44621978faf8df0e01d2d2b: 65 engine detections. This is a variant of WannaCry ransom-ware [22].
7. ca71f8a79f8ed255bf03679504813c6a: 52 engine detections. This is a back-door worm CVE [23].
8. cf4f46336abeec03630297f846d17482: 62 engine detections. This is a variant of WannaCry ransom-ware [24].
9. e9d1ba0ee54fcdf37cf458cd3209c9f3: 64 engine detections. This is a variant of WannaCry ransom-ware [25].
10. a4d49eaf60a8e333708469606ad9e1a4: 61 engine detections. This is a variant of WannaCry ransom-ware [26].
11. 95ae8e32eb8635e7eabe14ffbfaa777b: 64 engine detections. This is a variant of WannaCry ransom-ware [27].
12. ce494e90f5ba942a3f1c0fe557e598bf: 61 engine detections. This is a variant of WannaCry ransom-ware [28].

As we can see, by far and away the greatest Threat actor detected is ransom-ware. We see regular active attempts to infect systems are ongoing 24 hours a day all over the world.

Top Dionaea URL captures:

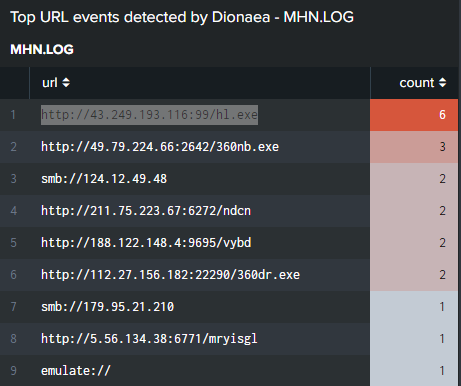


Figure 11 Top URL’s for MHN.LOG.

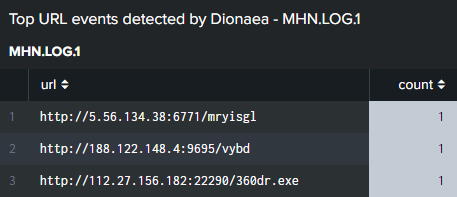


Figure 12 Top URL’s for MHN.LOG.1.

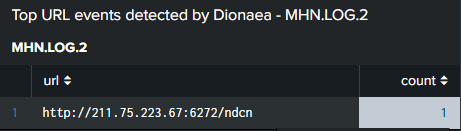


Figure 13 Top URL’s for MHN.LOG.2

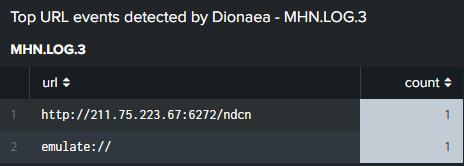


Figure 14 Top URL’s for MHN.LOG.3

We can see that the URL’s to be investigated via virus-total repeat across all 4 files. First, we have http://43.249.193.116:99/hl.exe. The process hl.exe relates to an old video game produced by the valve company. This suggests this file is likely an altered binary file. Our initial lookup tells us the URL appears to be clean with 0 detections, however if strip the URL to just it’s IP and investigate, we discover it is a known botnet attack vector as seen below.

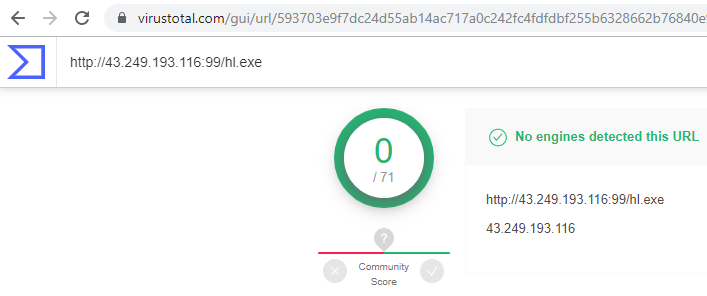


Figure 15 Here we see our clean response for the subdomain and the higher domain indicated below it.

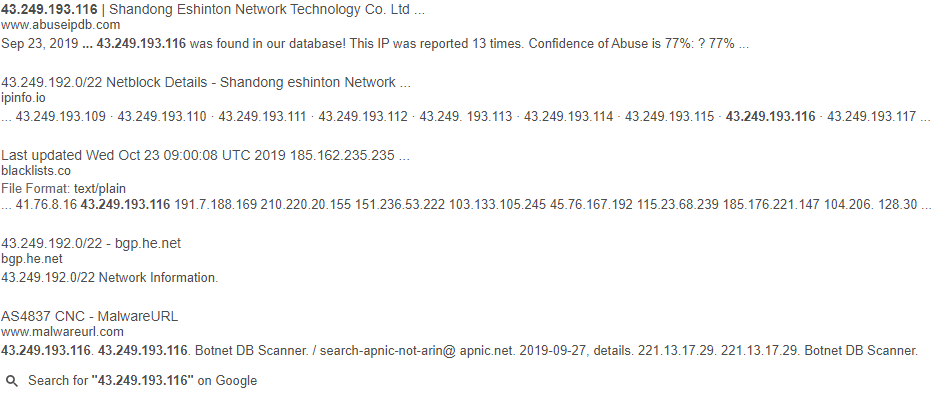


Figure 16 Here we see the parent domain recognized as a Chinese botnet attack vector.

Next, we have http://49.79.224.66:2642/360nb.exe. This file is immediately recognized as malware by 1 detection engine, ESET and is another Chinese attack agent.

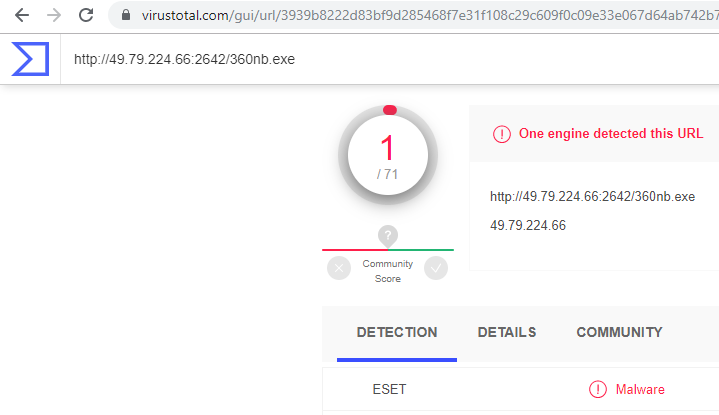


Figure 17 ESET Detection of http://49.79.224.66:2642/360nb.exe.

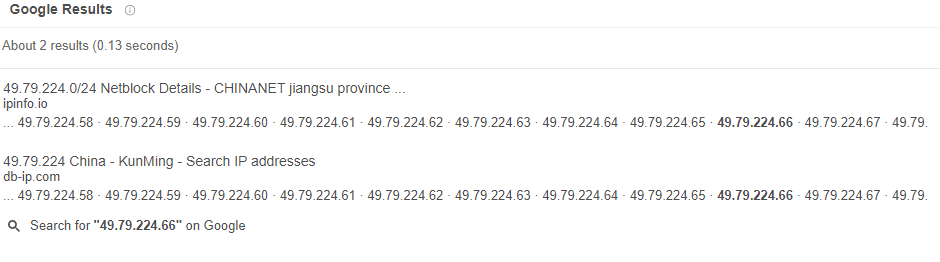


Figure 18 Another Chinese attack vector revealed.

The third URL, smb://124.12.49.48, is not detected as a threat so we move onto number 4, http://211.75.223.67:6272/ndcn. This URL is immediately detected by 1 engine, Spamhaus and the parent domain is a Taiwanese attack vector.

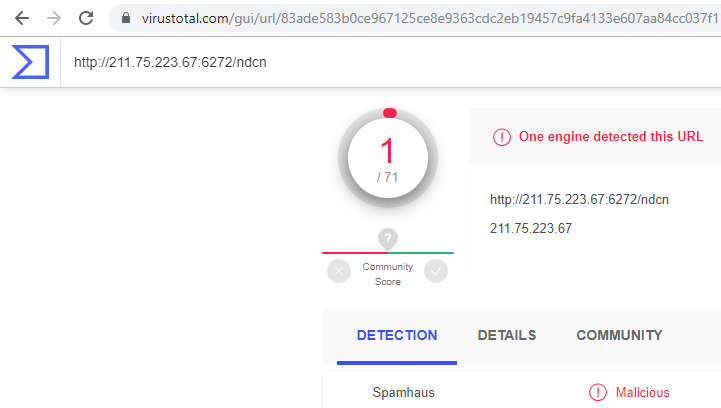


Figure 19 http://211.75.223.67:6272/ndcn Detected by Spamhaus.

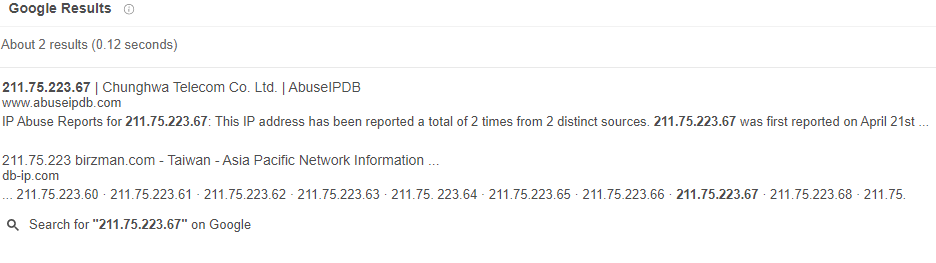


Figure 20 Another Chinese attack vector revealed.

The fifth URL, http://188.122.148.4:9695/vybd is detected by two engines; Spamhaus & Forcepoint ThreatSeeker and is revealed to be a Swedish attack vector.

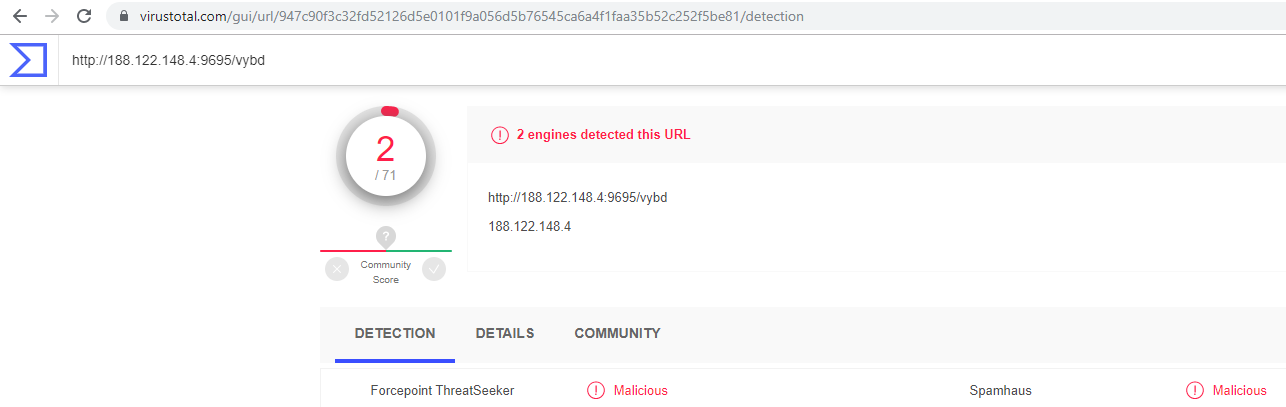


Figure 21 http://188.122.148.4:9695/vybd Detected by two engines.

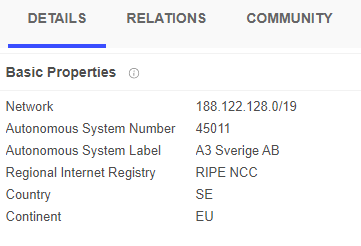


Figure 22 http://188.122.148.4:9695/vybd Swedish origin revealed

The sixth URL,  http://112.27.156.182:22290/360dr.exe is detected by 4 engines; Bit Defender, CRDF, Dr.Web, Sophos AV and is revealed to be yet another Chinese Attack vector.

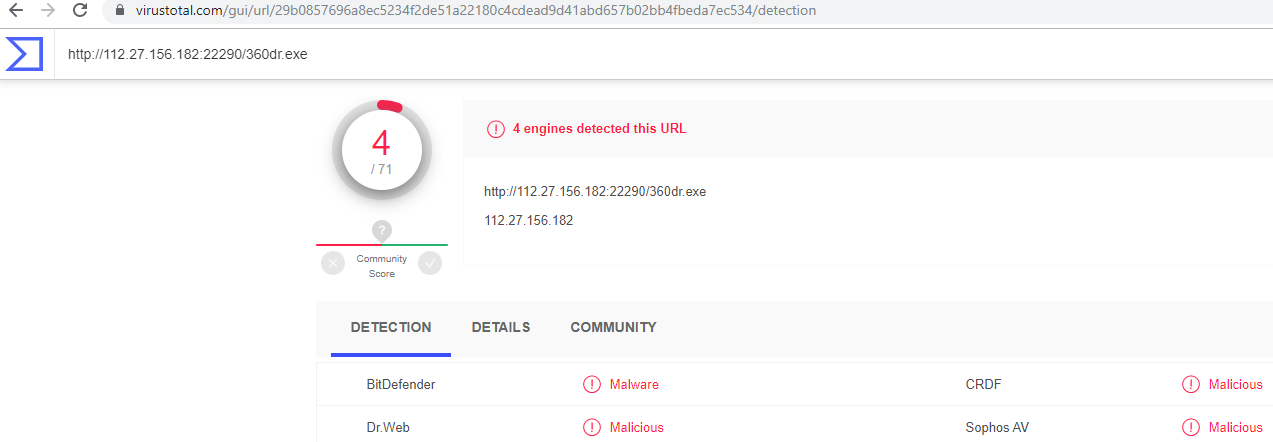


Figure 23 http://112.27.156.182:22290/360dr.exe detected by 4 engines.

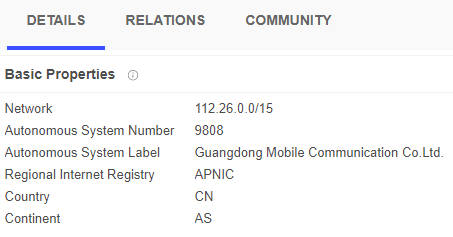


Figure 24 Chinese origins revealed.

The 7th URL, smb://179.95.21.210 reveals no detections or details so I moved onto the 8th URL, http://5.56.134.38:6771/mryisgl. This one proved interesting. The URL was detected by one engine, Spamhaus. However, the origin showed as Great Britain yet registered to a Persian company and routed through both an Iranian and a Chinese internet node. This leads me to suspect it is either a Chinese or Iranian attack agent being routed through a VPN tunnel vector.

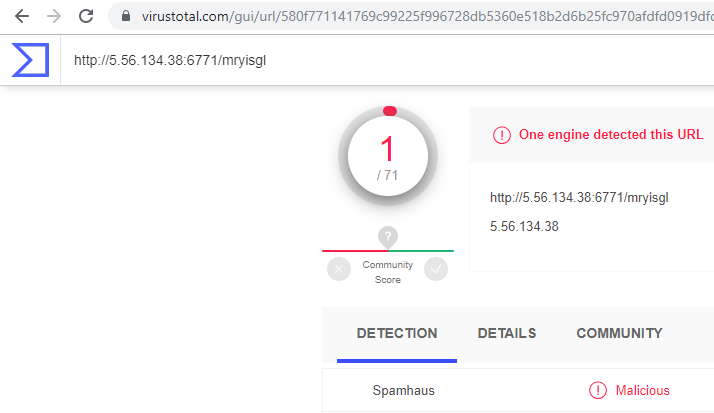


Figure 25 http://5.56.134.38:6771/mryisgl detection.

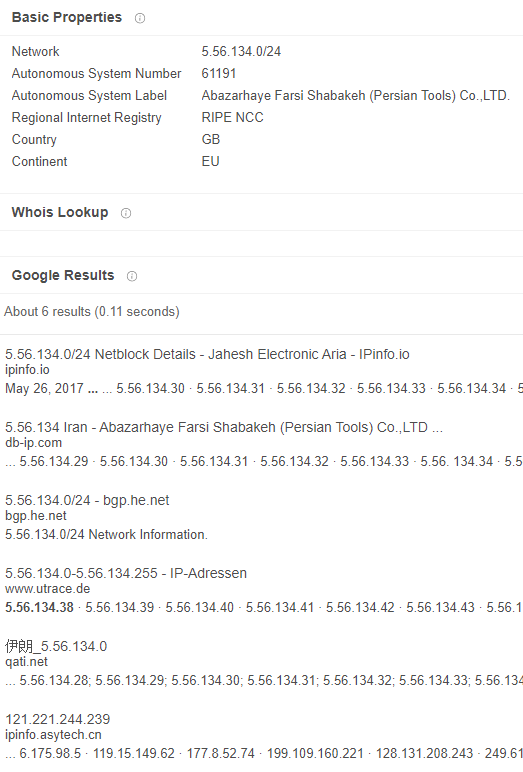


Figure 26 http://5.56.134.38:6771/mryisgl very curious origin & routing information.

The final URL emulate:// revealed no information. This is likely an attempt to execute a script or shell commend via a web port.

Top Dionaea attackers by IP/Country/Count:

1. 157.245.130.209-United States-3,566,221
2. 211.44.226.158-South Korea-113,207
3. 112.175.124.2-South Korea-109,036
4. 89.248.174.201-Seychelles-107,133
5. 161.9.133.141-Turkey-91,887

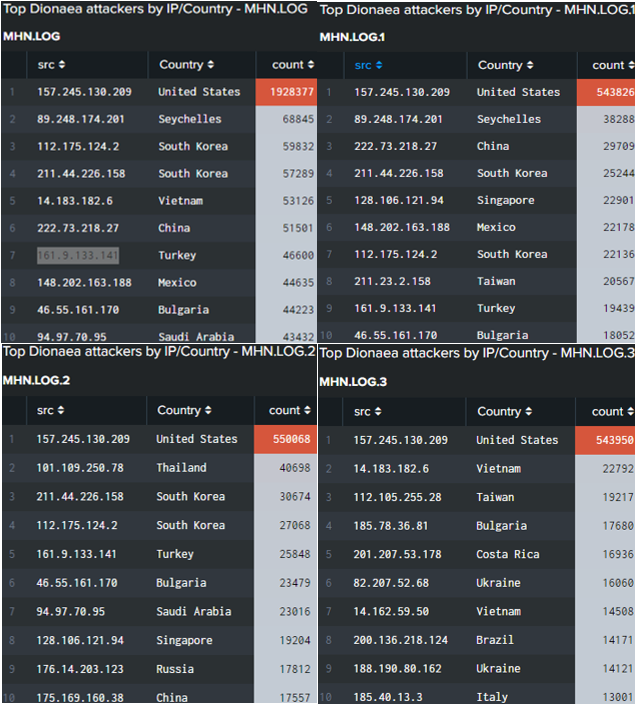


Figure 27 Top Dionaea attackers by IP/Country/Count.

We can clearly see that the United States was clearly the greatest attack vector for events during my network’s uptime.

Top Dionaea port detections by count:

1. 1433-5,696,735.
2. 445-276,195.
3. 465-59,190.
4. 25-55,365.
5. 995-54,408.

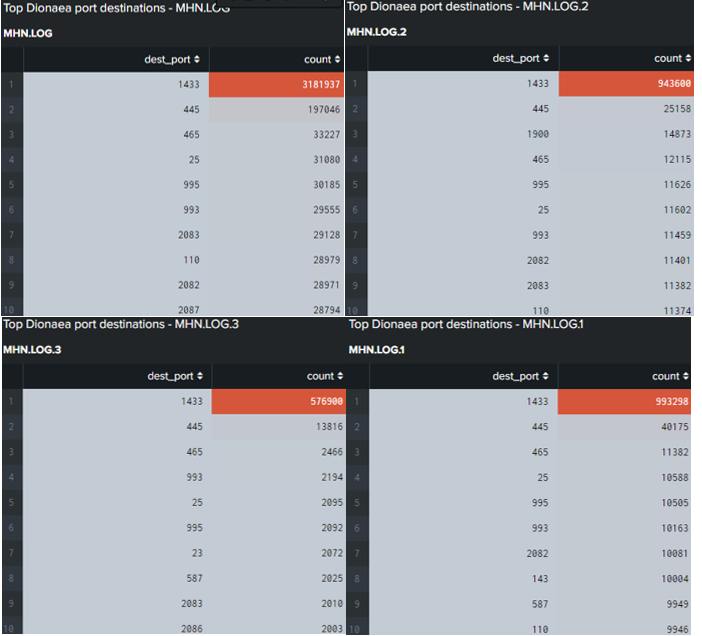


Figure 28 Top Dionaea port detections by count.

We can see that port 1433 is by far and away the most active port. This is a port generally used by SQL databases and this activity alone with other ports was investigated further later in the document.

## 4.3 p0f Analytics

Top p0f attackers by IP/Country:

1. 112.175.124.2-South Korea:111,118.
2. 211.44.226.158-South Korea:97,469.
3. 112.175.127.179-South Korea:61,172.
4. 112.175.127.189-South Korea:47,864.
5. 112.175.126.18-South Korea:47.734.

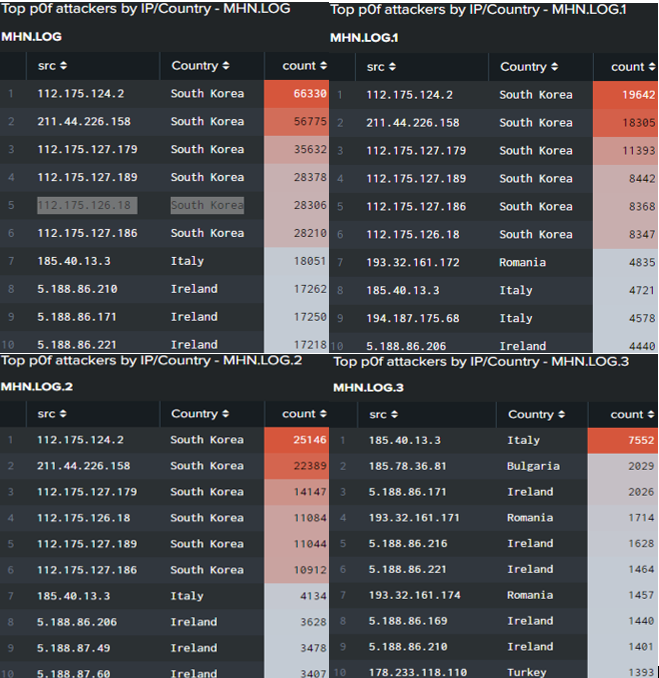


Figure 29 Top p0f attackers by IP/Country.

Top p0f ports by destination/count:

1. 22:1,062,938.
2. 1433:432,935.
3. 80:250,513.
4. 443:248,165.
5. 445:165,241.

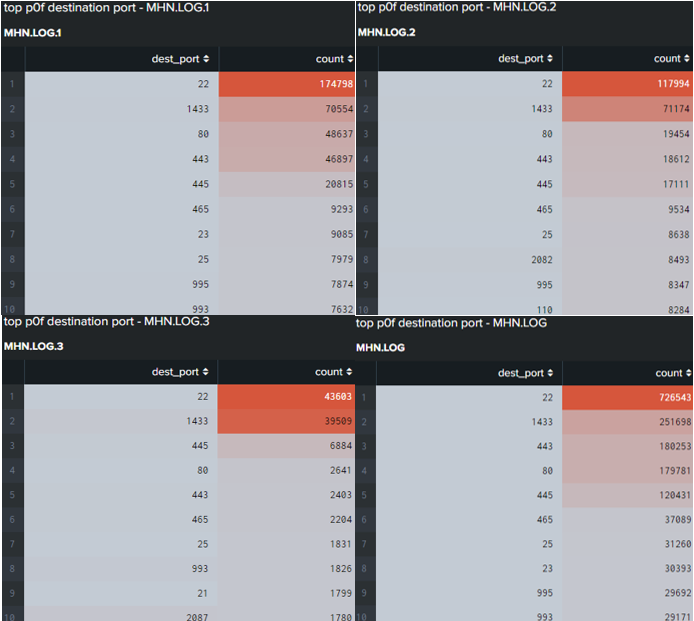


Figure 30 30 Top p0f ports by destination/count.

## 4.4 Cowrie Analytics

Cowrie naturally generated a significant amount of analytic data, however I found most of it to be very basic; such as top username and password attempts, which were as expected. Also, SSH scanning is a standard function of botnets so I expected to see consistent activity on port 22 and I did indeed see this.

However, Cowrie did generate some URL data and this I documented the data recovered from virus-total and other sources.

Top URLs documented:

1. http://46.246.63.60/bin.sh: While this URL does not return a virus total match, it is found on a known abuse IP address list [29].
2. http://0x099as0xd.duckdns.org/zatoempire.sh: 9 engine detection hits. While no information regarding attack agent type is available, the use of DNS suggested a DNS hijacking attempt [30].
3. ftp://anonymous:anonymous@0x099as0xd.duckdns.org/zatoempire1.sh: This URL Did not reveal any data, however yet again the use of DNS suggest it was an attempt to upload a script to hijack my machines DNS.
4. http://milnetscan.duckdns.org/sensi.sh: 11 engine detections. This appears to be a malicious attempt to hijack DNS [31].
5. http://91.209.70.174/Corona.sh: 11 engine detections. This is a known botnet attack originating out of Russia [32].
6. http://milnetbrasil.duckdns.org:8088/sensi.sh: 6 engine detections. Yet another likely attempt at DNS hijacking [33].
7. ftp://anonymous:anonymous@milnetscan.duckdns.org/sensi1.sh: While not detection engines detected this URL as malicious, the file sensi.sh is part of a known multi-part RCE exploit [34].
8. ftp://anonymous:anonymous@milnetbrasil.duckdns.org/sensi1.sh: While not detection engines detected this URL as malicious, the file sensi.sh is part of a known multi-part RCE exploit [34].

## 4.5 Snort Analytics

Snort produces a great wealth of analytics including interesting IP, port information and severity; however, the most interesting data pertains to signature threat-intelligence.

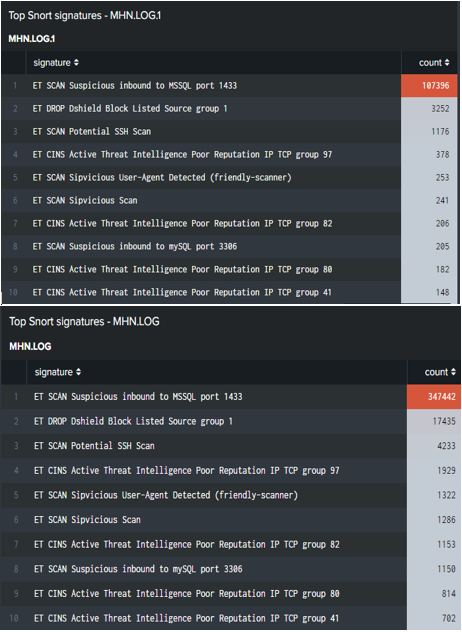


Figure 31 Top 10 Signature hits for MHN.LOG & MHN.LOG.1.

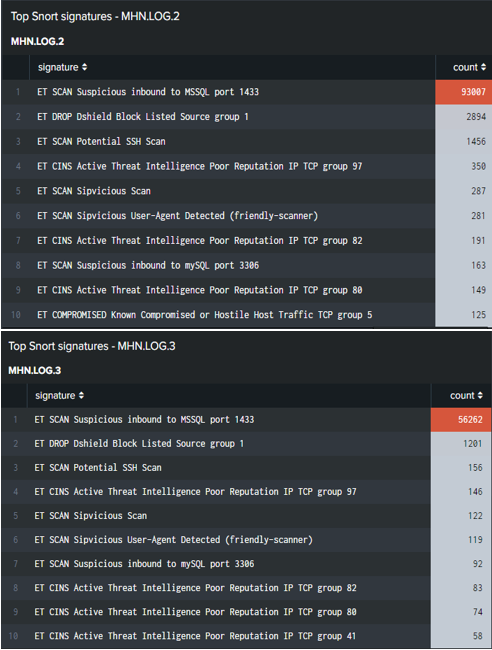


Figure 32 Top 10 Signature hits for MHN.LOG.2 & MHN.LOG.3.

There are 10 non repeating signatures across all 4 files and these I investigated further and documented my results:

1. ET SCAN Suspicious inbound to MSSQL port 1433: This is a denial of service attempt via syn-food typically launched against MSSQL which could be mitigated via syn limiting [35]. This is likely connected to a recently discovered MySQL CVE discovered mid-October which explains the uptake in attacks per hour as this CVE was being hunted [36].

The activity surrounding these events coincides with a pattern we can clearly see in our analytics where event activity significantly increases around Oct--21st and can clearly be seen in the general events and specific sensor data relating to activity, and port destinations, the earliest documentation of the CVE I could find being Oct18th.[37].

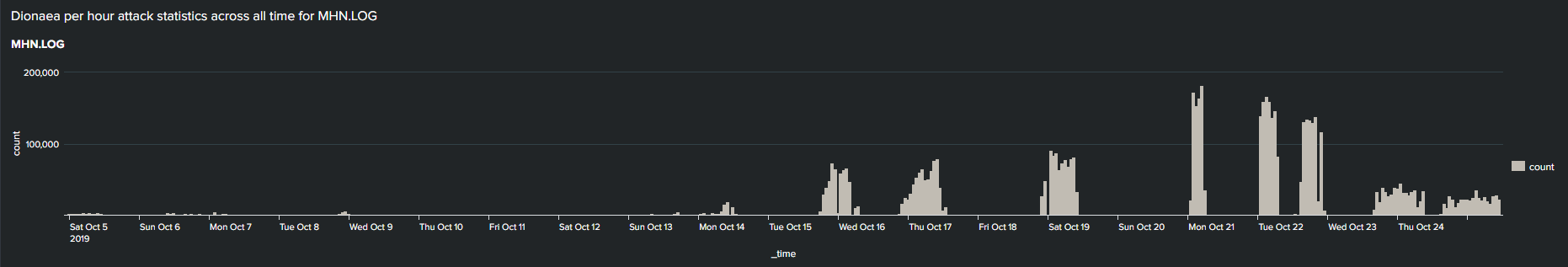


Figure 33 General timeline of events, for all events with peak uptake at Oct 21st for MHN.LOG.

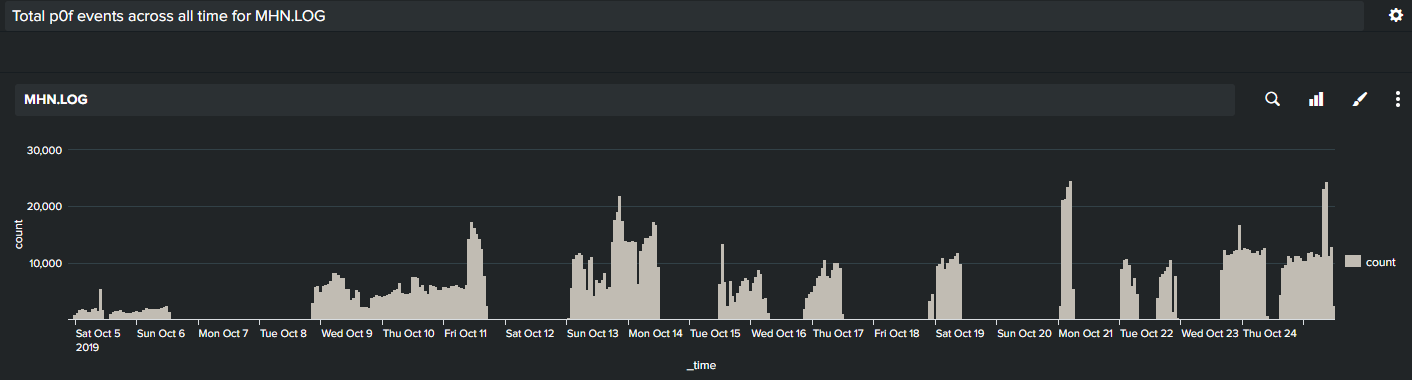


Figure 34 p0f timeline of events, with peak uptake at Oct 21st for MHN.LOG.

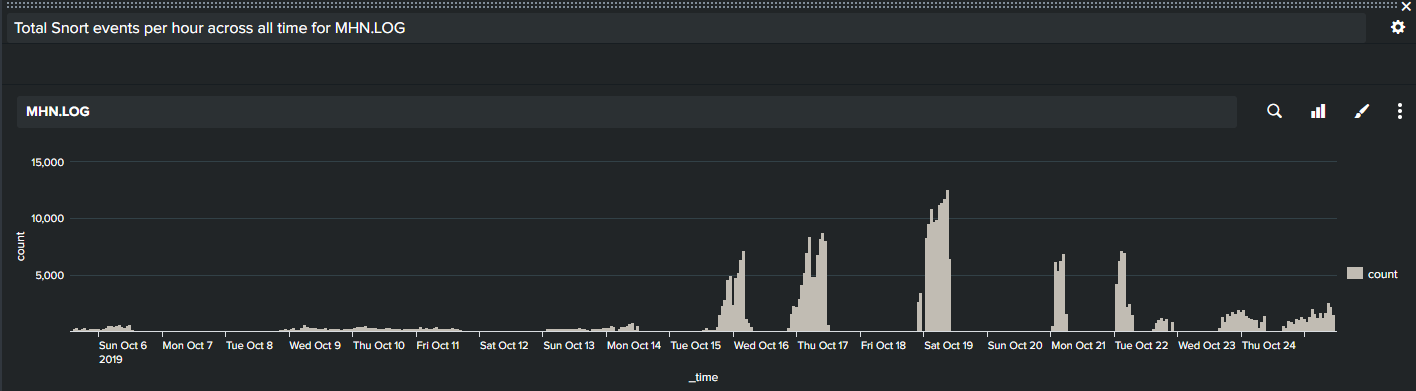


Figure 35 Snort timeline of events, with peak uptake at Oct 19th for MHN.LOG.

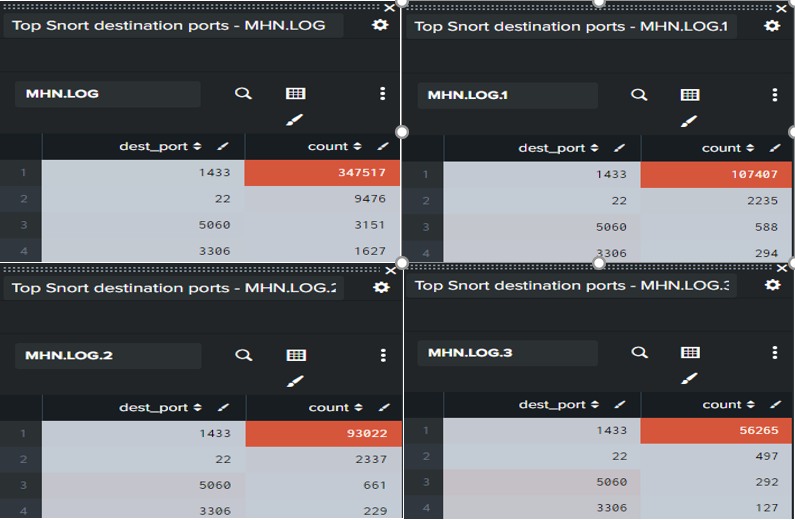


Figure 36 Here we see heavy activity detected by snort on ports 1433 & 3306, both associated with MySQL coinciding with the release of the new CVE.

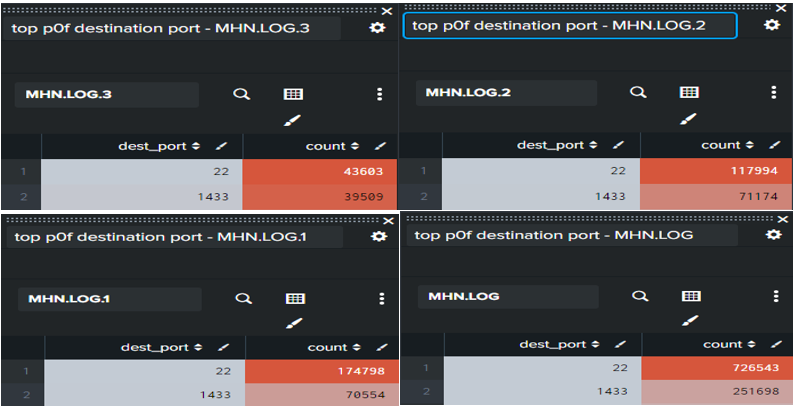


Figure 37 Here we see heavy activity detected by p0f on ports 1433, both associated with MySQL coinciding with the release of the new CVE.

1. ET DROP Dshield Block Listed Source group 1: This is a dropped IP connection due to an IP being listed on a list of bad IPs’ [38].
2. ET SCAN Potential SSH Scan: This is obviously an attempt to scan for active SSH ports. [39]
3. ET CINS Active Threat Intelligence Poor Reputation IP TCP group 97: This is a report of dropped IP connections due to poor reputation [39].
4. ET SCAN Sipvicious User-Agent Detected (friendly-scanner): This is a report related to attempts to scan for VOIP devices [40].
5. ET SCAN Sipvicious Scan: This is a report related to attempts to scan for VOIP devices[40].
6. ET CINS Active Threat Intelligence Poor Reputation IP TCP group 82: This is a report of dropped IP connections due to poor reputation [39].
7. ET SCAN Suspicious inbound to MySQL port 3306: This report relates to several attack vectors such as Simple LFI, LDI using NULL byte, Full SYN scan, Full Connect90 port scan, SQL injection (UNION SELECT) & Netcat reverse shell. Due to the possibility of reverse shell and the known new MySQL CVE previously mentioned, this is a critical threat. [41]
8. ET CINS Active Threat Intelligence Poor Reputation IP TCP group 80: This is a report of dropped IP connections due to poor reputation [39].
9. ET CINS Active Threat Intelligence Poor Reputation IP TCP group 41: This is a report of dropped IP connections due to poor reputation [39].

# 5.0 Conclusions

It is interesting to note that much of the intelligence I mined regarding attacks from virus-total & other sources were initially gathered using MHN. Naturally the platform produces much more data than could be documented in a short assignment. As a threat intelligence tool, it is simple, despite its few maintenance issues, quick to deploy, effective, lost cost and it produces quantifiable results that serve to easily pain an intelligence profile that could be very useful is designing physical network topologies to be my robust, and logical security profiles to resist common threat actors and vectors.

The variety of sensors make documenting the various types of actors common today relatively simple, however integration with mining tools could be modernized and made more inclusive regarding many sensors currently missing from the MHN-Splunk App.

In terms of analytics the log files produced by MHN are very simple to mine And Its integration with Splunk, which is itself a powerfully data mining tool is fantastic. I found the process of developing an App to mine my data to be thoroughly enjoyable and rewarding and the data sets produced were amazingly rich in detail.

As expected, malware is the principal threat with many variants of the WannaCry ransom-ware virus still very active. CVE attacks are of great concern too with direct port attempts web-based exploitation being quite commonplace. The lack of fuzzing and port scanning in general was surprising however, on reflection; it seems malicious user may prefer to spend resources on simply attempting attack rather than scanning services first if for example botnets are being used for the sake of efficiency.

So, what was the single most important thing I learned from my time investigating MHN? Well, I would have to conclude that it teaches us rapidly that complacency is costly and the results of lack of vigilance can be devastating to a device, user, Soc or downstream client. Wanna-cry is everywhere, botnets are everywhere and every second of every day somebody is watching, waiting scanning and attempting to pounce. Constant vigilance, monitoring auditing and update maintenance must be upkept to protect ourselves, devices and clients from the vast ever present threats on the open unfiltered world wide web.

# 6.0 Glossary

Python: A programming language.

Flask: A Docker style container application within the Python programming language framework.

SSH: Secure Shell, used to securely remote log into servers.

MHN: Modern Honeypot Network.

PCAP: Packet Capture.  
  
Dork: This a term used in a modern context to describe a person who, while they may or may not be competent, have accidently left a back door or vulnerability open in a computer system that is relatively easy to find. Google has an Entire database of such sites, entities and vulnerabilities called ‘Exploit Database: Google Hacking Database’. Commonly known as ‘Google Dorks’.

RCE: Remote code execution.

SPLUNK: Splunk is a SIEM.

SIEM: ‘Security Information and Event Management’ tool. Use to capture, gather visualize analyze and research machine-based data in the age of the ‘IOT’.

IOT: Internet of things: the collection of all digital devices connected to the internet with generate data.

ELK: The Elastic Stack (ELK) is an open source SIEM.

ELSA: ELSA is another open source SIEM.

ubuntu-desktop: The default desktop environment for the Ubuntu Linux distribution.

Talos: The Cisco based data collect and analytical security department within the Cisco networking company.

Mongo: a database management system used by MHN.

Bistream: an abbreviation of Bit-Stream used is computing terminology to describe a continuous stream of binary data sent over a communications pathway.

ESET: An anti-Virus Detection engine.

Spamhaus: An anti-Virus Detection engine.

Forcepoint ThreatSeeker: An anti-Virus Detection engine.

Bit Defender: An anti-Virus Detection engine.

CRDF: An anti-Virus Detection engine.

Dr.Web: An anti-Virus Detection engine.

Sophos AV: An anti-Virus Detection engine.

SQL: Structure Query Language, a language used by database systems such MySQL and Apache.

# 7.0 References

1. Lukas 'glaslos' Rist, Project Lead (et al), ‘About’, [ONLINE] Available at: <http://Conpot.org> [Accessed Sept. 27, 2019].
2. Geerlingguy (Jeff Geerling, https://www.drupal.org/u/geerlingguy), ‘Honeypot’, [ONLINE] Available at: <https://www.drupal.org/project/honeypot> [Accessed Sept. 27, 2019].
3. TrevorLeake (Trevor Leake, <https://github.com/TrevorLeake>), ‘Magenpot -README.md’, [ONLINE] Available at: <https://github.com/TrevorLeake/magenpot> [Accessed Sept. 27. 2019].
4. Gbrindisi (Gianluca Brindisi, <https://github.com/gbrindisi>), ‘Wordpot – README.md’, [ONLINE] Available at: https://github.com/gbrindisi [Accessed Sept. 27, 2019].
5. Common Vulnerabilities and Exposures, ‘CVE-2014-6271’, [ONLINE] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271> [Accessed Sept. 28, 2019].
6. Common Vulnerabilities and Exposures, ‘CVE-2014-7169’, [ONLINE] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169> [Accessed Sept. 28, 2019].
7. threatstream ( threatstream, <https://github.com/threatstream>), ‘Shockpot -README.md’, [ONLINE] Available at: <https://github.com/threatstream/shockpot> [Accessed Sept. 28, 2019]
8. majek (et all) ‘p0f – docs - README’ [ONLINE] Available at: <https://github.com/p0f/p0f/blob/master/docs/README> [Accessed Sept. 28, 2019].
9. Brady Sullivan, ‘Suricata Sensor’ [ONLINE] Available at: <https://github.com/threatstream/mhn/wiki/Suricata-Sensor> [Accessed Sept. 28, 2019].
10. mushorg ( MushMush, <https://github.com/mushorg>), ‘glastopf – README’ [ONLINE] Available at: <https://github.com/mushorg/glastopf> [Accessed Sept. 28, 2019].
11. Jordan-wright (Jordan Wright), ‘elastichoney -README.md’ [ONLINE] Available at: <https://github.com/jordan-wright/elastichoney> [Accessed Sept. 28, 2019].
12. Zeroq/amun, ‘README.MD’, [ONLINE] Available at: <https://github.com/zeroq/amun> [Accessed Sept. 28, 2019].
13. Cisco, ‘Get Started’, [ONLINE] Available at: <https://www.snort.org/#get-started> [Accessed Sept. 28, 2019].
14. Diontools/Dionaea, ‘README.MD’, [ONLINE] <https://github.com/DinoTools/dionaea> [Accessed Sept. 28, 2019].
15. Cisco, ‘Cisco Attack Map’, [ONLINE] Available at: <https://talosintelligence.com/fullpage_maps/pulse> [Accessed Sept. 29, 2019].
16. SOFTWARE TECHNOLOGIES LTD, ‘LIVE CYBER THREAT MAP’, [ONLINE] <https://threatmap.checkpoint.com/> [Accessed Sept. 29, 2019].
17. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/c05e2dab77349cd639aa837e7e121710b8a0718d8fc93fb4cc6458ae90e5c597/details> [Accessed Oct. 3, 2019].
18. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/df6d5b29a97647bca44e2306069f7675ef992f591c8c761af99bbdc17cfa7692/details> [Accessed Oct. 3, 2019].
19. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/6c8f85db6604cf701c5fbe62c872e21625a51f7edb407f813eb67918722d33b7/details> [Accessed Oct. 3, 2019].
20. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/64bb708b31b4b043018457c1098465ea83da7d6408c7029b2f68c333fc25891c/details> [Accessed Oct. 3, 2019].
21. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/cf5ddb5dedea0104a3fc464c822e6181a9dd9fa6e27e713c54af0eafb7c5faf0/details> [Accessed Oct. 3, 2019].
22. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/9348ff35903052b6874508e0fa116dacc4dca5b0a60710a6084c3ac5f01ae85f/details> [Accessed Oct. 3, 2019].
23. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/397e054981e16af9cc59d62897d9cf037470289df8844f1b6121d5e2fb6afbf0/details> [Accessed Oct. 3, 2019].
24. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/f54fbfcb038af9a12d446f0150b97fef7a71ca02eec07c517f0ed00fdbea8185/details> [Accessed Oct. 3, 2019].
25. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/7d8644271eb48be35e35f1d4c06649ba6878b4672f3d57bdea1f2ff9074bc434/details> [Accessed Oct. 3, 2019].
26. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/e2b54741be34be2c0d2bdebb78f32d3f79a885397b3a46f87f62e896f1a42371/details> [Accessed Oct. 3, 2019].
27. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/fb648bfb485f910e065cc18778364a56be32044d1ac4729449f3cc28221b12e8/details> [Accessed Oct. 3, 2019].
28. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/file/9ce656f2fdeef73ccf15b8589b150d2a5e3d22b03c1947d7e2f65e69e4909488/details> [Accessed Oct. 3, 2019].
29. Urlhaus, ‘URLhaus Plain-Text URL List’, [ONLINe] Available at: <https://urlhaus.abuse.ch/downloads/text/> [Accessed Nov. 3, 2019].
30. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/url/f4bfd008178d3770781a81c5b024eebbb9fb59ebe3682b6258d6aead4ba2c7dc/details> [Accessed Oct. 3, 2019].
31. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/url/b4c48fd2c1f4ae4480ce571d9fe9b95a3b35d2ff8e867d4c523e90cec52a7769/details> [Accessed Oct. 3, 2019].
32. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/ip-address/91.209.70.174/details> [Accessed Oct. 3, 2019].
33. Virus-Total, ‘DETAILS’ [ONLINE] Available at: <https://www.virustotal.com/gui/url/8d793e857d90ddc46b73830b3c1bfc80dc1336133157d5b0d90daced37713019/details> [Accessed Oct. 3, 2019].
34. Simple Computer Security, ‘Remote Code Exploit’, [ONLINE] Available at: <https://simplecomputersecurity.blogspot.com/2018/04/remote-code-exploit.html> [Accessed Nov. 3, 2019].
35. CVE, ‘CVE-2019-2910’, [ONLINE] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2910> [Accessed Nov. 3, 2019].
36. Tenable, ‘MySQL 5.6.x < 5.6.46 Multiple Vulnerabilities (Oct 2019 CPU)’ [ONLINE] Available at: <https://www.tenable.com/plugins/nessus/130025> [Accessed Nev 3, 2019].
37. Mike, ‘Chasing Snort ET Drop Shield IP addresses’, [ONLINE] Available at: <https://networktidbits.wordpress.com/2015/01/21/chasing-snort-et-drop-shield-ip-addresses/> [Accessed Nov. 3, 2019].
38. Oinkmaster, ‘snort-2.9.0-enhanced open’, [ONLINE] Available at: <https://rules.emergingthreats.net/changelogs/snort-2.9.0-enhanced.open.2019-01-24T23:49:35.txt> [Accessed Nov. 3, 2019].
39. Aldeid, ‘Suricata-vs-snort/Test-cases/Denial-of-service’, [ONLINE] Available at: <https://www.aldeid.com/wiki/Suricata-vs-snort/Test-cases/Denial-of-service> [Accessed Nov. 3, 2019].
40. Matt Martin, ‘SIPVicious – The Not So “friendly-scanner”’, [ONLINE] Available at: <https://www.nurango.ca/blog/sipvicious-the-not-so-friendly-scanner> [Accessed Nov. 3,2019].
41. Aldeid, ‘Suricata-vs-snort/Test-cases/Test-rules’, [Online] Available at: <https://www.aldeid.com/wiki/Suricata-vs-snort/Test-cases/Test-rules> [Accessed nov. 3, 2019].