Purpose

The purpose of assignment two in Part 2: Interacting with Application Programming Interfaces is to analyze data of threat intelligence that are organized information about potential or current attacks against organizations. The primary purpose of threat intelligence is to help organizations in protecting themselves from types of attacks that are facing risks of common and severe external threats, such as zero-day threats, advanced persistent threats, etc. A threat intelligence platform is a tool to proactively increase awareness about threats that are facing organizations. After all, intelligence is information that provides organizations with decision-making support and with strategic advantage.

Requirements

- Windows-based operating system — current version 10
- RStudio version 1.1.423
- R statistical computing programming language version 3.4.3

Objectives

- Describes data that are provided by Application Programming Interface (API)
- Write code or utilize other codes to interact with API
- Describes how API can extract useful data
- Perform some exploratory data analysis using R and Python programming language on data that are provided through API
- Come up with interesting questions to be answered about API

Consideration

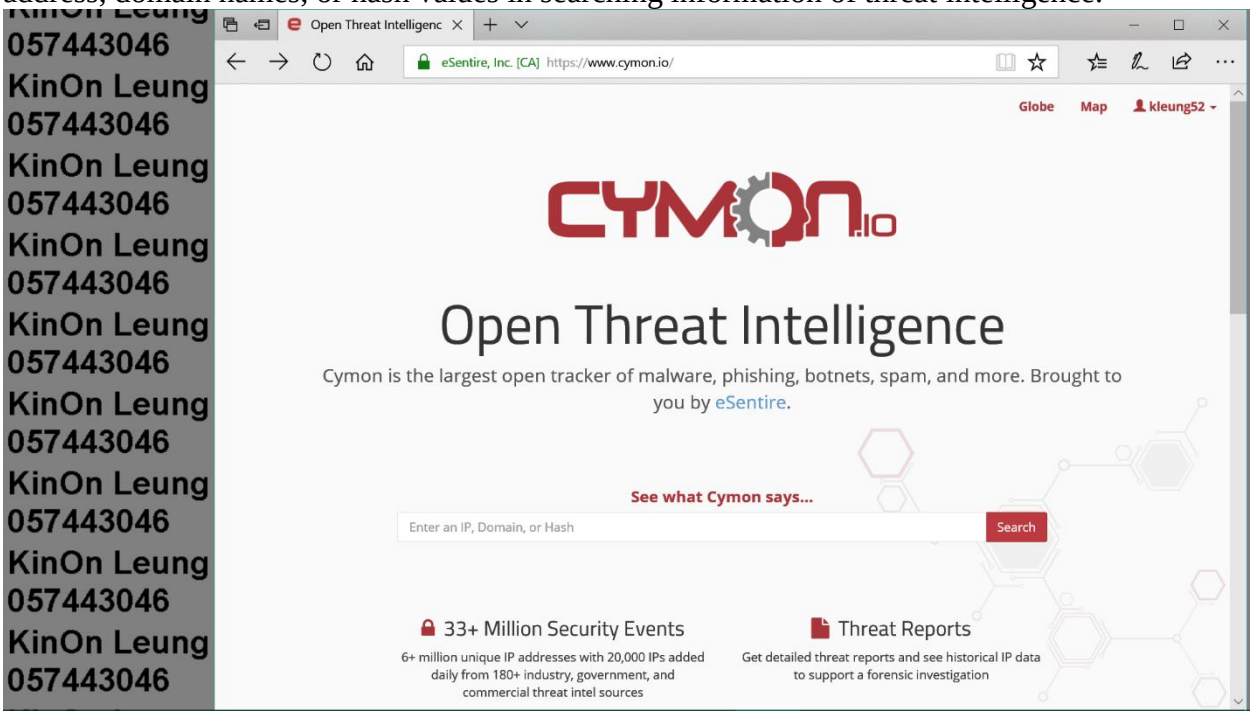
When considering best tools for threat intelligence, some questions to ask are:

- What is it that you are trying to detect? For example, are you trying to detect malicious Internet Protocol (IP) involving with Distributed Denial-of-Service, malicious IP involving email spams and phishing, or malicious IP involving malware?
- What criteria to consider the best for threat intelligence? Accuracy? Timeliness?
- What is the point of using threat intelligence? For example, are you trying to harden security on Security Information and Event Management or to undertake forensics?
- What is an acceptable level of false positive from threat intelligence?

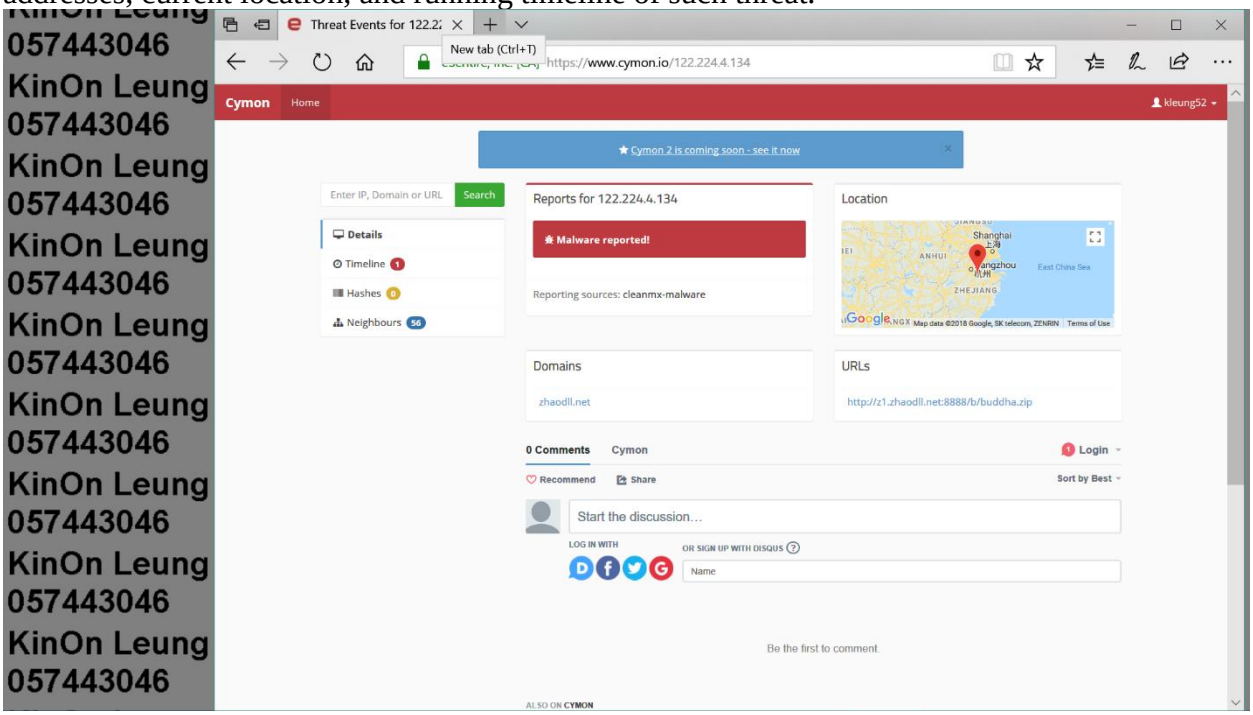
Cymon Threat Intelligence

Cymon through its Application Programming Interface (API) is a tracker and aggregator of security reports. Developed by eSentire, Cymon API investigates into events about malware, botnets, phishing, spams, and other malicious activities. With recent Cymon API version 2, the focus of this new version is to create a platform for collecting and distributing Indicators of Compromise feeds. Furthermore, Cymon API is synchronous, so that a search request is issued via GET and POST method using Hypertext Transfer Protocol (HTTP) call. Result of which is computed and returned. Any requests being made to Cymon API need to include HTTP Basic Authentication header using authentication token. Even if modern web browsers support basic authentication, Cymon API is secured enough for communication over the Internet as it occurs over Secure Socket Layer/Hypertext Transfer Protocol Secure.

Below image is how Cymon Application Programming Interface (API) looks like on a web browser at https://www.cymon.io/ that has a text bar for users to input Internet Protocol (IP) address, domain names, or hash values in searching information of threat intelligence.

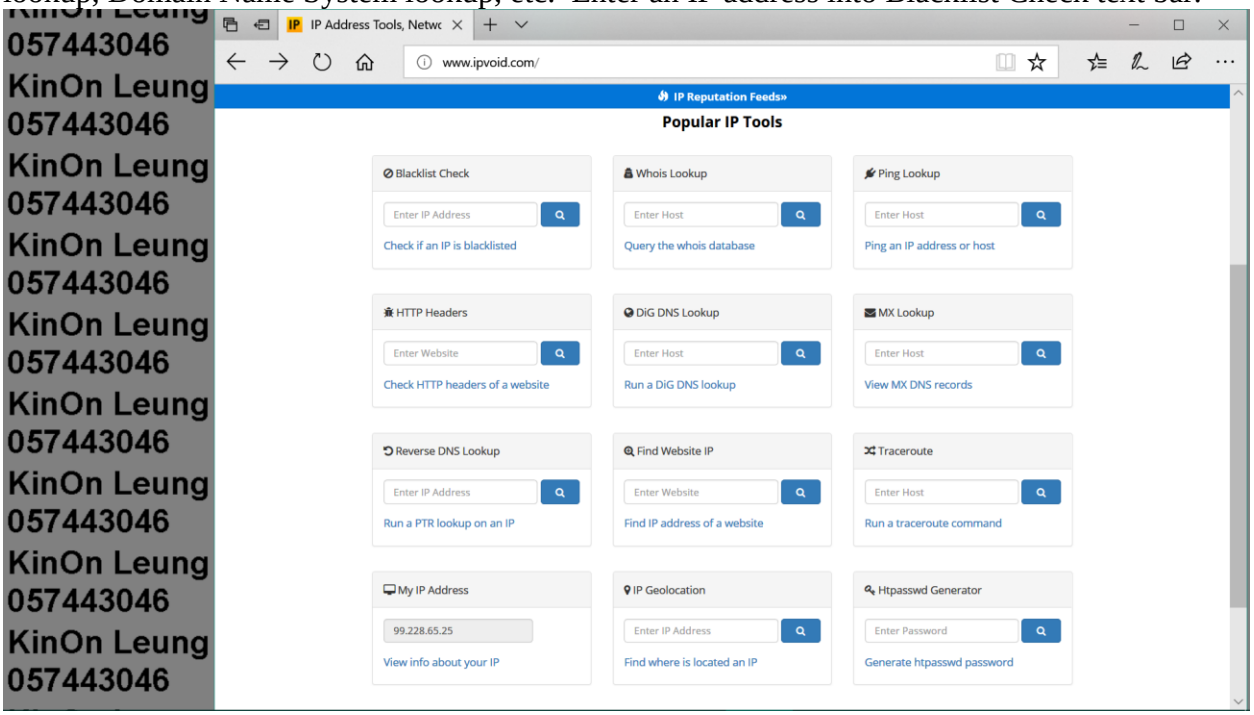


If a threat is found whether for IP address, domain name, or hash value, such threat would be shown in a report in below image; otherwise, Cymon API returns Domain Not Found message. Cymon, as shown by below image, shows related domain names and Universal Resource Locator addresses, current location, and running timeline of such threat.

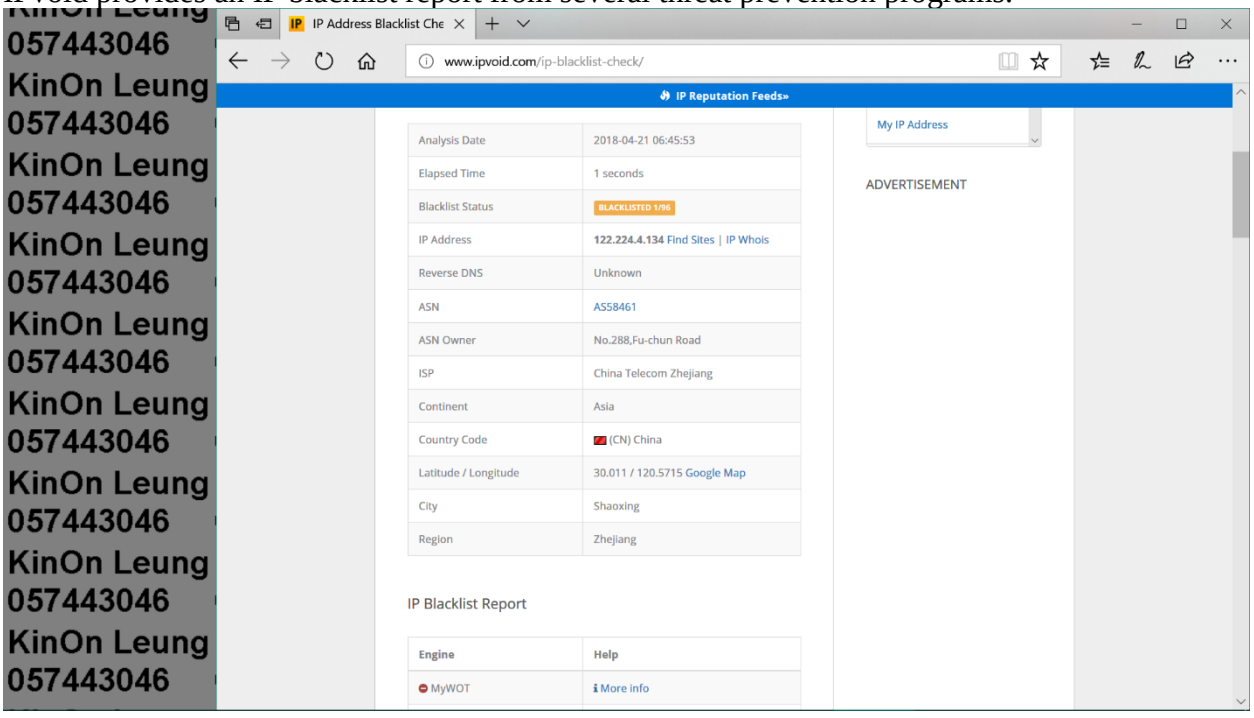


IPvoid Threat Intelligence

Below image shows Application Programming Interface of IPvoid at http://www.ipvoid.com/ that offers a range of Internet Protocol (IP) address tools, such as IP blacklist check, whois lookup, Domain Name System lookup, etc. Enter an IP address into Blacklist Check text bar.

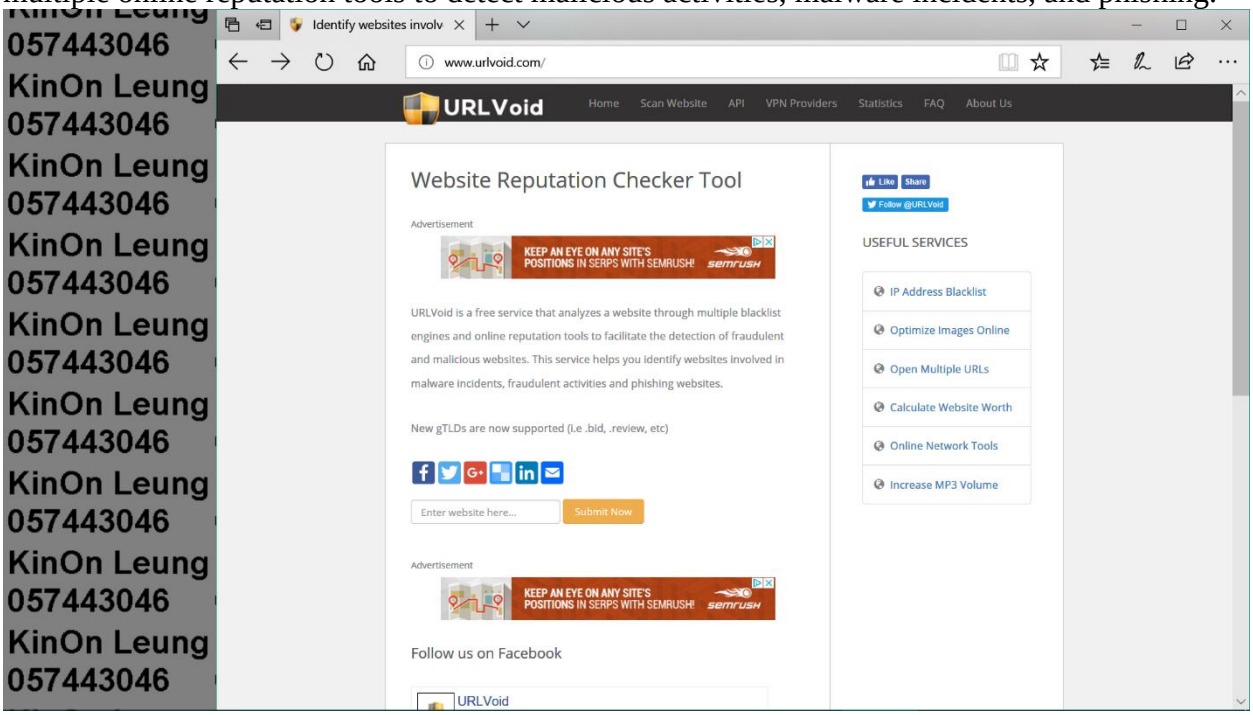


If a threat is found, IPvoid lists IP address information, such as blacklist status, Autonomous System Number (ASN), ASN owner, Internet Service Provider, longitude and latitude, etc. Also, IPvoid provides an IP blacklist report from several threat prevention programs.

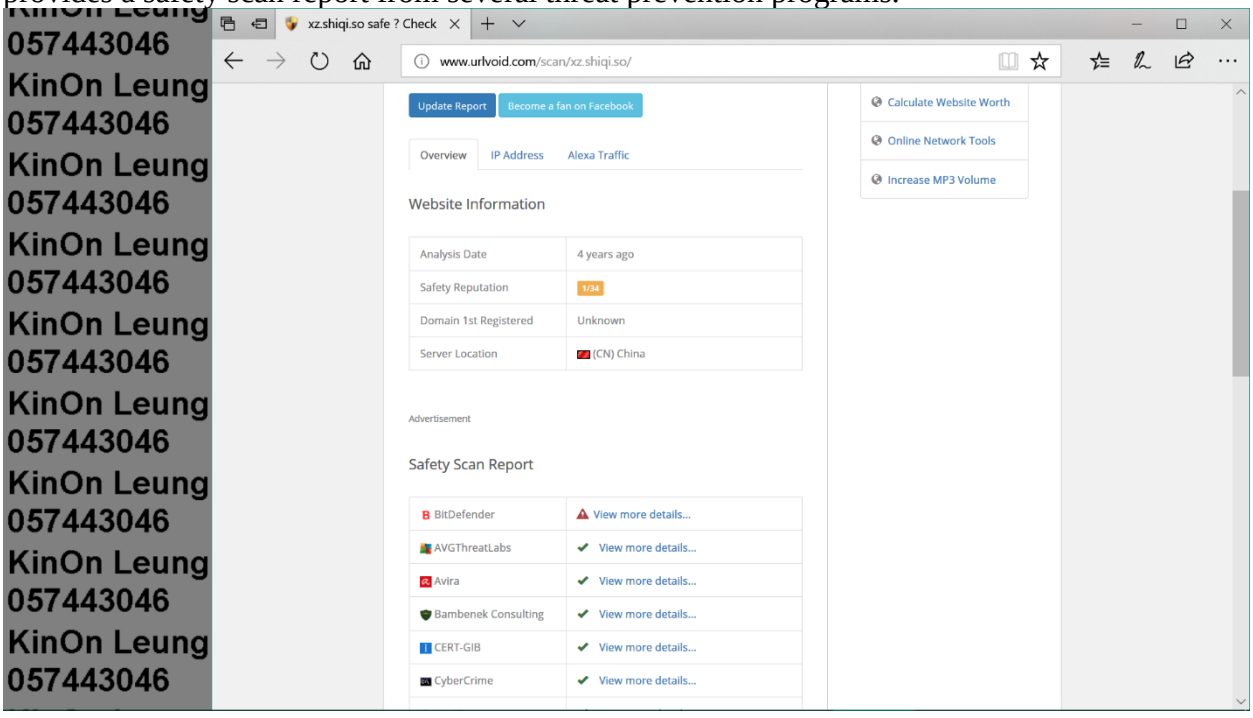


URLvoid Threat Intelligence

Below image shows Application Programming Interface of URLvoid at http://www.urlvoid.com/ to offer analysis of domain names or website addresses through multiple blacklist engines and multiple online reputation tools to detect malicious activities, malware incidents, and phishing.

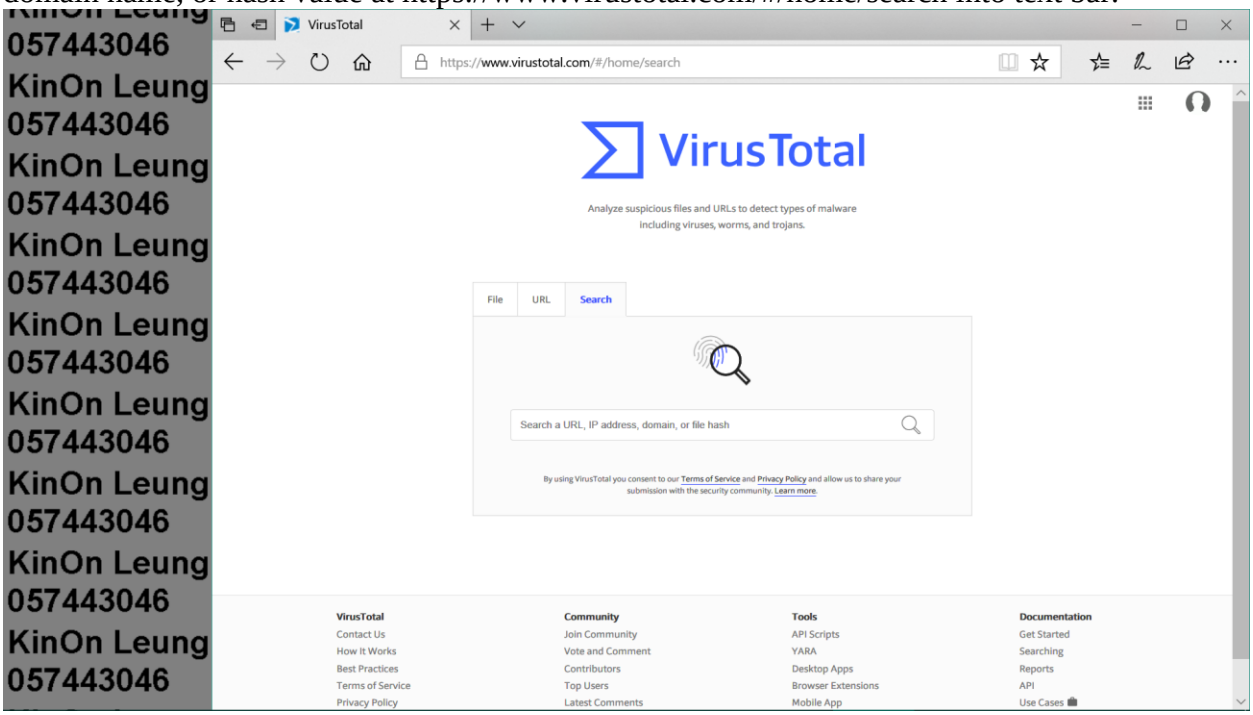


If a threat is found, URLvoid lists website and Internet Protocol address information, such as Autonomous System Number (ASN), ASN owner, longitude and latitude, etc. Also, URLvoid provides a safety scan report from several threat prevention programs.

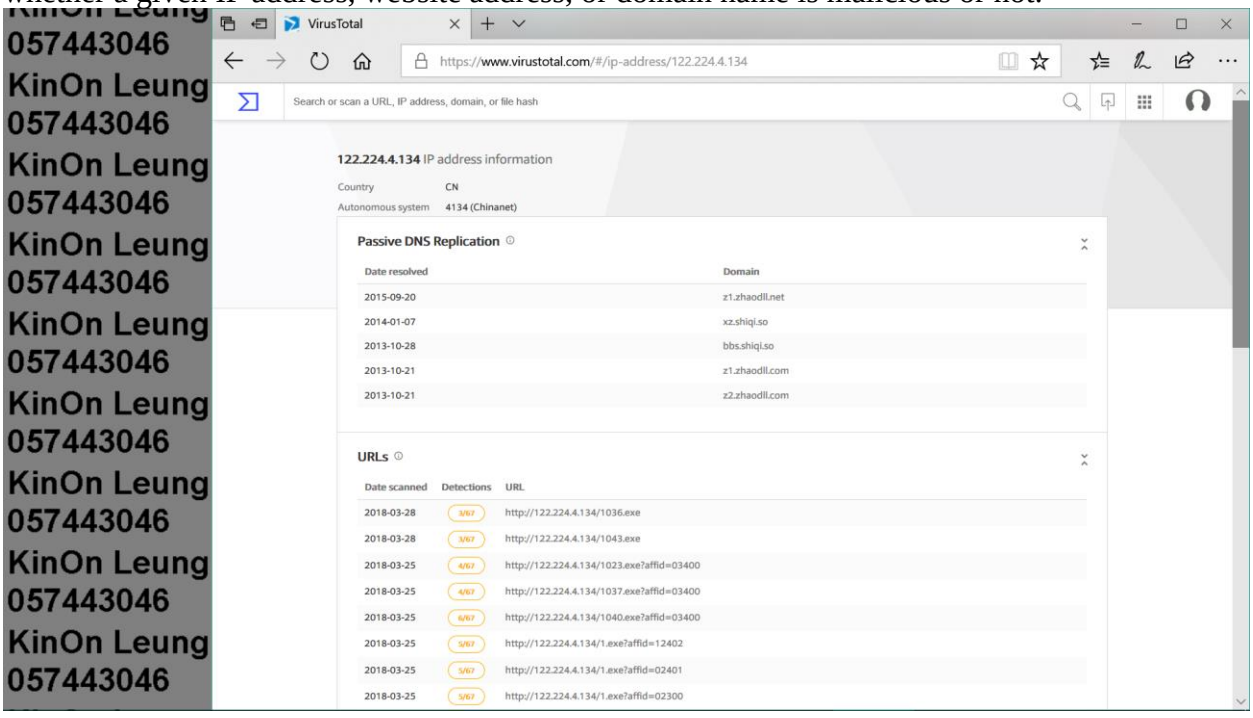


VirusTotal Threat Intelligence

Below image shows Application Programming Interface of VirusTotal to be able to detect threat activities by entering Universal Resource Locator (URL) address, Internet Protocol (IP) address, domain name, or hash value at https://www.virustotal.com/#/home/search into text bar.



If a threat is found, VirusTotal gives a list of related domain names, URLs, download files, and files being referred. Also, VirusTotal gives a list of threat prevention programs indicating whether a given IP address, website address, or domain name is malicious or not.



Harbinger Threat Intelligence

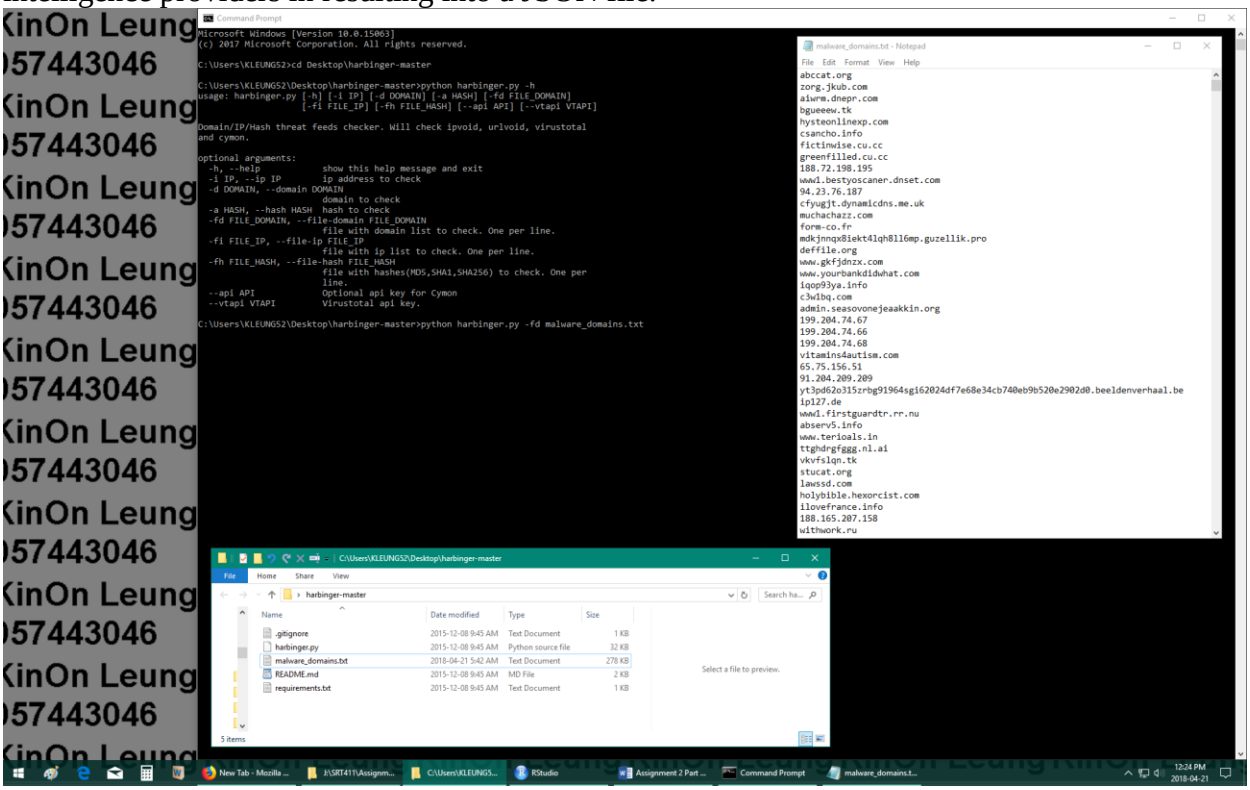
Harbinger itself is a Python programming script to allow query of multiple online threat aggregators through a single host operating system interface. Running Harbinger Python programming script checks for domain names, Internet Protocol (IP) addresses, or hash values from each of the previous four threat intelligence providers, which are http://ipvoid.com, http://urlvoid.com, https://cymon.io and https://virustotal.com. Such feeds check from each of the previous threat intelligence providers is to determine on malware incidents, fraud activities, blacklist domains/hosts, IP blocked addresses, website malicious status, or Universal Resource Locator (URL) potential threats. If threats are detected in those domain names, IP addresses, or hash values, result is saved into a JavaScript Object Notation (JSON) file for further analysis into statistical computing programming language, like R. Before running Harbinger Python programming script, Harbinger requires few installed Python code packages through pip in the Command Prompt. Of course, make sure Python programming language is installed beforehand that can be accessed in the Command Prompt.

> pip install <Python code package>

Run the above command to install Python code packages of requests, cymon, and beautifulsoup4 into the Command Prompt.

> python harbinger.py <options>

Below image shows running the above command to parse a domain file through those four threat intelligence providers in resulting into a JSON file.



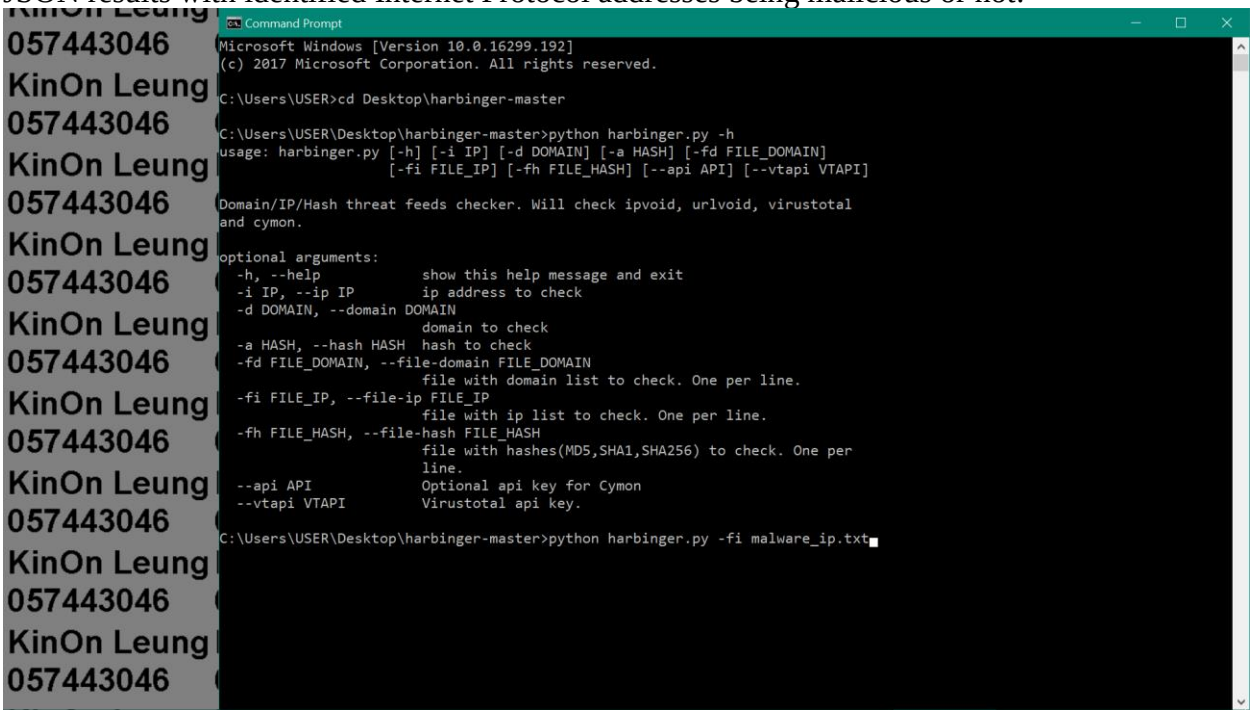
Full code of the Harbinger Threat Intelligence in Python programming language can be found by visiting the following URL repository on GitHub:

https://github.com/exp0se/harbinger
OR
https://github.com/kleung52/SRT411-Assignment-Two

From GitHub repository at https://github.com/kleung52/SRT411-Assignment-Two, there are several JavaScript Object Notation, JSON, (.json) files as well as several Comma-Separated Value, CSV, (.cvs) files are being provided. JSON files are converted into CSV files for ease of readability into R statistical computing programming language and into Microsoft Excel Spreadsheet. Since those JSON and CSV files dataset can get quite large, only Internet Protocol (IP) addresses are being investigated for malicious incidents, malware existence, and fraudulent activities by passing into those four threat intelligence providers through Application Programming Interface, which are http://ipvoid.com, http://urlvoid.com, https://cymon.io and https://virustotal.com. Even investigating on just malicious IP addresses and malware IP addresses, there are already over 500 identified IP addresses that may appear suspicious, as determined by Harbinger Threat Intelligence. An even larger dataset of IP addresses can be inspected by Harbinger Threat Intelligence, but there is really no point because exploratory analysis is what matter the most. For executing Harbinger threat intelligence in Command Prompt, the following command is executed.

> python harbinger.py -fi malware_ip.txt

Below image shows the above command in execution. After running the above command, a JSON results with identified Internet Protocol addresses being malicious or not.



Below image shows originally there are this many columns from Harbinger Threat Intelligence but not all columns have values though.

```
colnames(csvMalIP)
```

```
##  [1] "ï..ip"
##  [2] "vt_last10_dns_resolutions"
##  [3] "vt_url"
##  [4] "vt_asn"
##  [5] "ipvoid_location"
##  [6] "ipvoid_asn_owner"
##  [7] "cymon_url"
##  [8] "cymon_record_created"
##  [9] "vt_count_samples_malicious_communicated_with"
## [10] "ipvoid_url"
## [11] "ipvoid_reverse_dns"
## [12] "vt_count_malicious_urls_hosted_by"
## [13] "vt_count_samples_undetected_communicated_with"
## [14] "cymon_last_updated"
## [15] "ipvoid_asn"
## [16] "vt_count_samples_malicious_embed_this_address"
## [17] "vt_count_samples_undetected_downloaded_from"
## [18] "vt_location"
## [19] "ipvoid_last_time_analysed"
## [20] "vt_count_samples_undetected_embed_this_address"
## [21] "cymon_blacklists____001"
## [22] "cymon_blacklists____002"
## [23] "cymon_blacklists____003"
## [24] "cymon_blacklists____004"
## [25] "cymon_blacklists____005"
## [26] "cymon_blacklists____006"
## [27] "cymon_blacklists____007"
## [28] "cymon_blacklists____008"
## [29] "cymon_blacklists____009"
## [30] "cymon_blacklists____010"
## [31] "cymon_blacklists____011"
## [32] "cymon_blacklists____012"
## [33] "cymon_blacklists____013"
## [34] "cymon_blacklists____014"
## [35] "cymon_blacklists"
## [36] "ipvoid_blacklists"
## [37] "vt_count_samples_malicious_downloaded_from"
## [38] "vt_asn_owner"
```

Below image shows dataset of Harbinger Threat Intelligence after being filtered to be left with eighteen columns in having values only.

```
colnames(MalIP)
```

```
##  [1] "ï..ip"                  "cymon_url"
##  [3] "cymon_record_created"   "cymon_last_updated"
##  [5] "cymon_blacklists____001" "cymon_blacklists____002"
##  [7] "cymon_blacklists____003" "cymon_blacklists____004"
##  [9] "cymon_blacklists____005" "cymon_blacklists____006"
## [11] "cymon_blacklists____007" "cymon_blacklists____008"
## [13] "cymon_blacklists____009" "cymon_blacklists____010"
## [15] "cymon_blacklists____011" "cymon_blacklists____012"
## [17] "cymon_blacklists____013" "cymon_blacklists____014"
```

In the next three pages, summary function and describe function are used to explain dataset of malicious Internet Protocol addresses.

```
MalIP <- csvMalIP[,colSums(is.na(csvMalIP)) < nrow(csvMalIP)]

summary(MalIP)
```

```
##           ï..ip                              cymon_url
##  103.30.42.71 :  1   https://cymon.io/93.78.123.111 : 57
##  103.31.186.13:  1   https://cymon.io/93.104.215.155: 43
##  106.187.94.91:  1                                   : 25
##  107.170.120.5:  1   https://cymon.io/223.26.55.97   : 21
##  108.59.12.115:  1   https://cymon.io/178.74.199.7   : 19
##  108.61.43.150:  1   https://cymon.io/5.149.248.85   : 19
##  (Other)      :544   (Other)                         :366
##           cymon_record_created            cymon_last_updated
##  2015-08-01T05:33:21Z: 57       2015-08-01T05:33:21Z: 57
##  2015-01-24T23:36:04Z: 43       2017-10-16T19:12:53Z: 43
##                      : 25                              : 25
##  2016-08-22T07:16:53Z: 21       2017-12-20T20:14:58Z: 21
##  2015-04-30T01:45:15Z: 19       2015-04-30T01:45:19Z: 19
##  2015-06-24T02:12:04Z: 19       2017-12-20T20:14:52Z: 19
##  (Other)             :366       (Other)             :366
##         cymon_blacklists____001      cymon_blacklists____002
##  ibm x-force exchange: 60                        :134
##  pbl.spamhaus.org    : 60        urlquery.net    : 80
##  virustotal.com      : 55        zen.spamhaus.org : 60
##                      : 47        malwr.com       : 43
##  c-sirt.org          : 43        tor.ahbl.org    : 36
##  ipbl.mailhosts.org  : 39        spam.spamrats.com: 25
##  (Other)             :246        (Other)         :172
##           cymon_blacklists____003     cymon_blacklists____004
##                         :232                        :328
##  b.barracudacentral.org:124        tor.ahbl.org    : 57
##  urlquery.net          : 45        all.s5h.net     : 43
##  zen.spamhaus.org      : 26        zen.spamhaus.org: 35
##  virustotal.com        : 19        urlquery.net    : 19
##  dnsbl-1.uceprotect.net: 17        esentire.com    : 17
##  (Other)               : 87        (Other)         : 51
##     cymon_blacklists____005           cymon_blacklists____006
##                  :364                             :384
##  dnsbl.ahbl.org  : 57        urlquery.net          : 57
##  tor.ahbl.org    : 46        dnsbl.ahbl.org        : 43
##  sbl.spamhaus.org: 30        zen.spamhaus.org      : 19
##  xbl.spamhaus.org: 18        b.barracudacentral.org: 17
##  zen.spamhaus.org: 14        bl.spamcannibal.org   : 15
##  (Other)         : 21        (Other)               : 15
##          cymon_blacklists____007           cymon_blacklists____008
##                         :460                              :478
##  openphish.com          : 43        cbl.abuseat.org       :  1
##  cbl.abuseat.org        : 20        sbl.spamhaus.org      :  7
##  senderbase.org         : 11        urlquery.net          :  4
##  spam.dnsbl.sorbs.net   :  5        v6.fullbogons.cymru.com: 17
##  alienvault reputation:  4          virustotal.com        : 43
##  (Other)                :  7
##          cymon_blacklists____009          cymon_blacklists____010
##                         :479                             :496
##  alienvault reputation: 17        b.barracudacentral.org:  5
##  db.wpbl.info           :  5      google safebrowsing   :  4
##  senderbase.org         :  4      hphosts-phishing      : 43
##  urlquery.net           : 43      spam.dnsbl.sorbs.net  :  2
##  zen.spamhaus.org       :  2
##
##           cymon_blacklists____011          cymon_blacklists____012
##                         :496                             :501
##  b.barracudacentral.org:  2        alienvault reputation:  2
##  hphosts-phishing      :  4        cleanmx-malware       : 43
##  phishtank             : 43        phishtank             :  4
##  virustotal.com        :  5
##
##
##      cymon_blacklists____013     cymon_blacklists____014
##                  :503                        :546
##  cleanmx-malware :  4        cleanmx-phishing:  4
##  cleanmx-phishing: 43
##
##
##
##
```

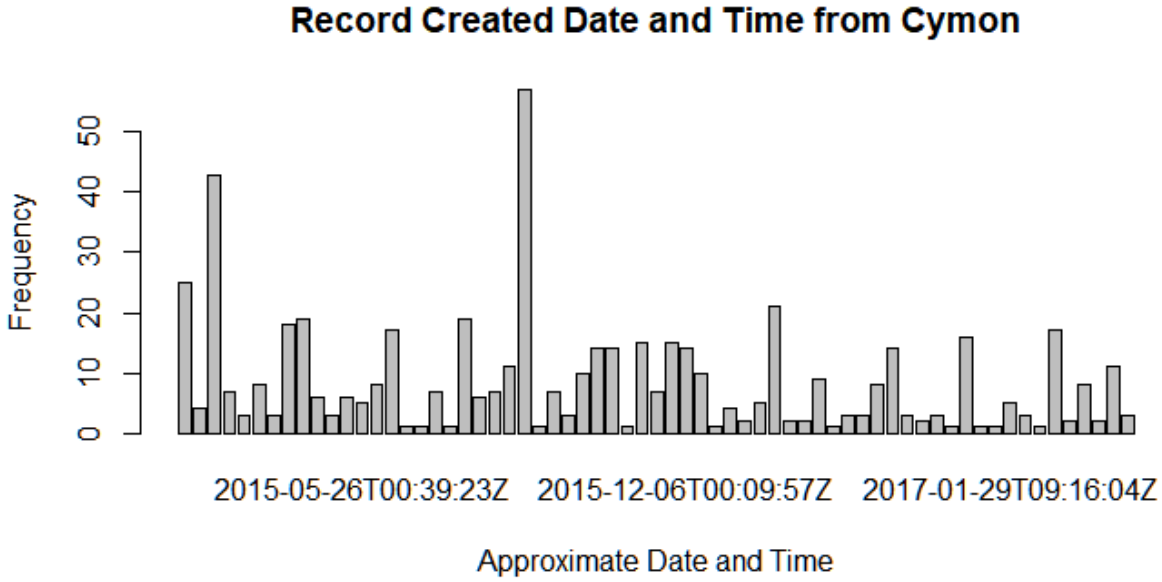
```
describe(MalIP)
```

```
## MalIP
##
##  18  Variables      550  Observations
## ---------------------------------------------------------------------------
## ï..ip
##        n  missing distinct
##      550        0      550
##
## lowest : 103.30.42.71   103.31.186.13  106.187.94.91  107.170.120.5  108.59.12.115
## highest: 95.168.187.204 95.211.158.225 95.215.0.153   95.65.117.173  98.130.136.152
## ---------------------------------------------------------------------------
## cymon_url
##        n  missing distinct
##      550        0       69
##
## lowest :                                https://cymon.io/109.236.82.48  https://cymon.io/109.236.82.61  https:
//cymon.io/109.236.85.57  https://cymon.io/109.236.88.105
## highest: https://cymon.io/93.104.215.155 https://cymon.io/93.114.252.53  https://cymon.io/93.78.123.111  https:
//cymon.io/95.211.158.225 https://cymon.io/95.215.0.153
## ---------------------------------------------------------------------------
## cymon_record_created
##        n  missing distinct
##      550        0       65
##
## lowest :                     2015-01-24T23:15:37Z 2015-01-24T23:36:04Z 2015-02-17T06:52:58Z 2015-02-24T06:31:1
1Z
## highest: 2017-05-13T17:53:39Z 2017-05-23T17:52:58Z 2017-08-17T08:28:58Z 2017-09-17T01:15:25Z 2017-11-28T04:52:0
0Z
## ---------------------------------------------------------------------------
## cymon_last_updated
##        n  missing distinct
##      550        0       66
##
## lowest :                     2015-02-17T08:21:34Z 2015-02-24T06:31:14Z 2015-03-14T03:20:04Z 2015-04-10T00:22:2
6Z
## highest: 2017-10-12T06:24:31Z 2017-10-16T19:12:53Z 2017-11-29T03:27:40Z 2017-12-20T20:14:52Z 2017-12-20T20:14:5
8Z
## ---------------------------------------------------------------------------
## cymon_blacklists____001
##        n  missing distinct
##      550        0       22
##
## lowest :                         alienvault reputation   all.s5h.net             b.barracudacentral.org  bl.ema
ilbasura.org
## highest: ptr                     quttera.com             reputationauthority.org urlquery.net            virust
otal.com
## ---------------------------------------------------------------------------
## cymon_blacklists____002
##        n  missing distinct
##      550        0       21
##
## lowest :                       alienvault reputation bl.spamcannibal.org   ciarmy.com            dnsbl.httpbl.o
rg
## highest: ubl.unsubscore.com    urlquery.net          virustotal.com        web.dnsbl.sorbs.net   zen.spamhaus.o
rg
## ---------------------------------------------------------------------------
## cymon_blacklists____003
##        n  missing distinct
##      550        0       17
##
## lowest :                        b.barracudacentral.org bl.spamcop.net         dnsbl-1.uceprotect.net dnsbl.ahbl
.org
## highest: tor.ahbl.org           ubl.unsubscore.com     urlquery.net           virustotal.com         zen.spamha
us.org
## ---------------------------------------------------------------------------
## cymon_blacklists____004
##        n  missing distinct
##      550        0       13
##
## (328, 0.596), all.s5h.net (43, 0.078), dnsbl-2.uceprotect.net (1, 0.002),
## dnsbl.ahbl.org (8, 0.015), dyna.spamrats.com (5, 0.009), esentire.com (17,
## 0.031), sbl.spamhaus.org (17, 0.031), spam.dnsbl.sorbs.net (15, 0.027),
## tor.ahbl.org (57, 0.104), ubl.unsubscore.com (2, 0.004), urlquery.net (19,
## 0.035), xbl.spamhaus.org (3, 0.005), zen.spamhaus.org (35, 0.064)
## ---------------------------------------------------------------------------
```

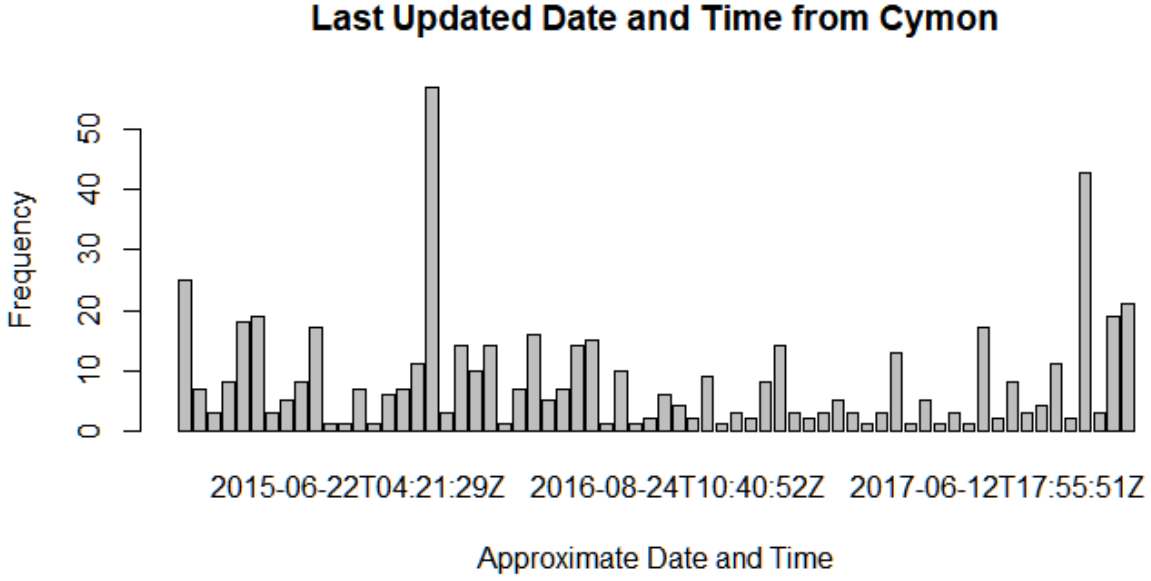
```
## ------------------------------------------------------------------------
## cymon_blacklists____005
##        n  missing distinct
##      550        0       15
##
## lowest :                        alienvault reputation  b.barracudacentral.org dnsbl.ahbl.org        dnsbl.sorb
s.net
## highest: tor.ahbl.org           urlquery.net           virustotal.com         xbl.spamhaus.org       zen.spamha
us.org
## ------------------------------------------------------------------------
## cymon_blacklists____006
##        n  missing distinct
##      550        0       10
##
## (384, 0.698), b.barracudacentral.org (17, 0.031), bl.spamcannibal.org (15,
## 0.027), dnsbl.ahbl.org (43, 0.078), dnsbl.sorbs.net (2, 0.004),
## sbl.spamhaus.org (1, 0.002), senderbase.org (3, 0.005), urlquery.net (57,
## 0.104), virustotal.com (9, 0.016), zen.spamhaus.org (19, 0.035)
## ------------------------------------------------------------------------
## cymon_blacklists____007
##        n  missing distinct
##      550        0        9
##
## (460, 0.836), alienvault reputation (4, 0.007), cbl.abuseat.org (20,
## 0.036), dnsbl.httpbl.org (2, 0.004), openphish.com (43, 0.078),
## senderbase.org (11, 0.020), spam.dnsbl.sorbs.net (5, 0.009), urlquery.net
## (4, 0.007), zen.spamhaus.org (1, 0.002)
## ------------------------------------------------------------------------
## cymon_blacklists____008
##        n  missing distinct
##      550        0        6
##
## (478, 0.869), cbl.abuseat.org (1, 0.002), sbl.spamhaus.org (7, 0.013),
## urlquery.net (4, 0.007), v6.fullbogons.cymru.com (17, 0.031),
## virustotal.com (43, 0.078)
## ------------------------------------------------------------------------
## cymon_blacklists____009
##        n  missing distinct
##      550        0        6
##
## (479, 0.871), alienvault reputation (17, 0.031), db.wpbl.info (5, 0.009),
## senderbase.org (4, 0.007), urlquery.net (43, 0.078), zen.spamhaus.org (2,
## 0.004)
## ------------------------------------------------------------------------
## cymon_blacklists____010
##        n  missing distinct
##      550        0        5
##
## (496, 0.902), b.barracudacentral.org (5, 0.009), google safebrowsing (4,
## 0.007), hphosts-phishing (43, 0.078), spam.dnsbl.sorbs.net (2, 0.004)
## ------------------------------------------------------------------------
## cymon_blacklists____011
##        n  missing distinct
##      550        0        5
##
## (496, 0.902), b.barracudacentral.org (2, 0.004), hphosts-phishing (4,
## 0.007), phishtank (43, 0.078), virustotal.com (5, 0.009)
## ------------------------------------------------------------------------
## cymon_blacklists____012
##        n  missing distinct
##      550        0        4
##
## Value                          alienvault reputation
## Frequency                    501                     2
## Proportion                 0.911                 0.004
##
## Value            cleanmx-malware             phishtank
## Frequency                     43                     4
## Proportion                 0.078                 0.007
## ------------------------------------------------------------------------
## cymon_blacklists____013
##        n  missing distinct
##      550        0        3
##
## Value                       cleanmx-malware cleanmx-phishing
## Frequency                              503               4              43
## Proportion                           0.915           0.007           0.078
## ------------------------------------------------------------------------
## cymon_blacklists____014
##        n  missing distinct
##      550        0        2
##
## Value                      cleanmx-phishing
## Frequency                              546               4
## Proportion                           0.993           0.007
## ------------------------------------------------------------------------
```

From the previous three pages, summary function and describe function seems to have a lot of information; however, there is something to be said about that information. In total, 550 observations or rows are made by Harbinger Threat Intelligence for each distinctive Internet Protocol (IP) address. The top five IP addresses that Cymon Threat Intelligence are kept referring to for malicious activities are 93.78.123.111, 93.104.215.155, 223.26.55.97, 178.74.199.7, and 5.148.248.85.

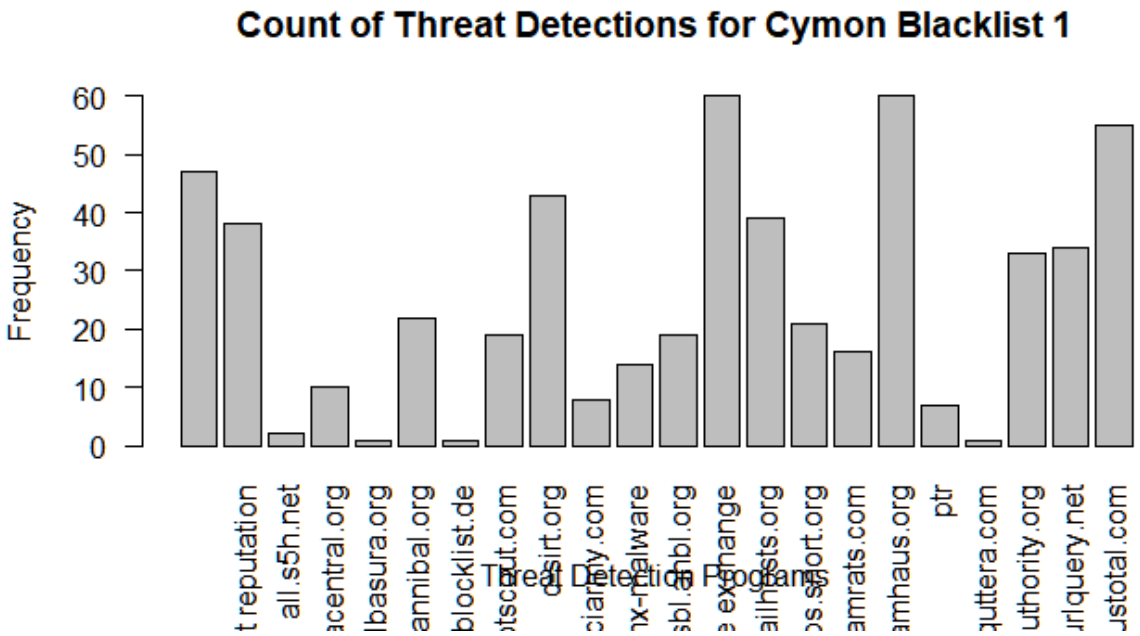
Records that are created for those malicious Internet Protocol (IP) addresses as determined by Cymon Threat Intelligence span across two years. A lot of records for malicious IP addresses are created by Cymon in the second half of the year 2015.



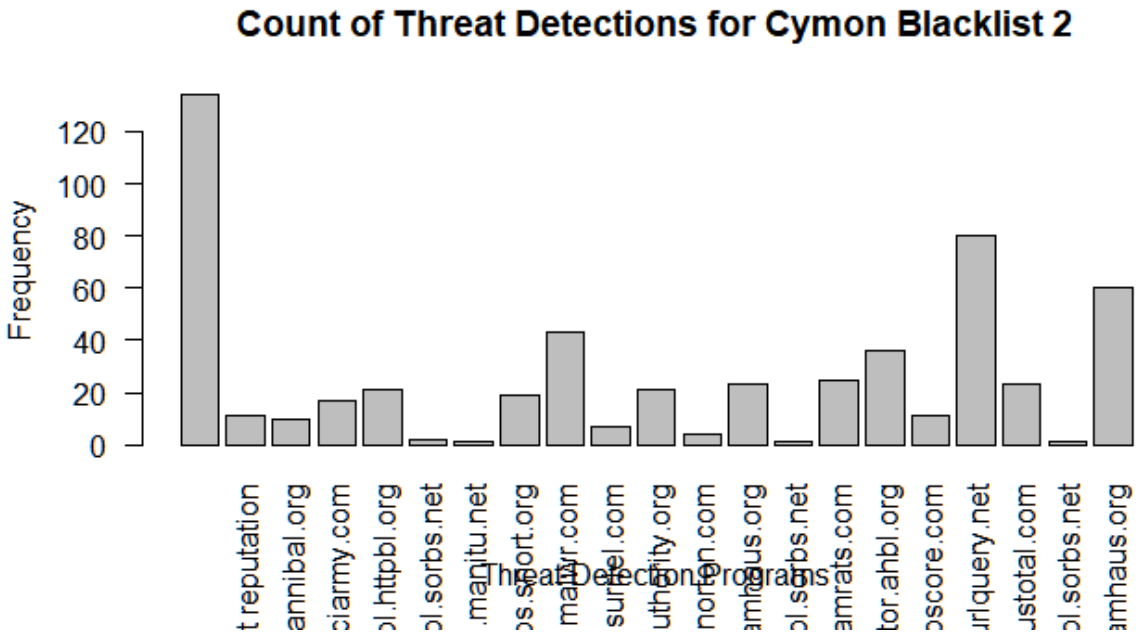
Records that are last updated for those malicious Internet Protocol (IP) addresses as determined by Cymon Threat Intelligence span across two years. A lot of records for malicious IP addresses are updated by Cymon near the end of the year 2015 and near the end of the year 2017.



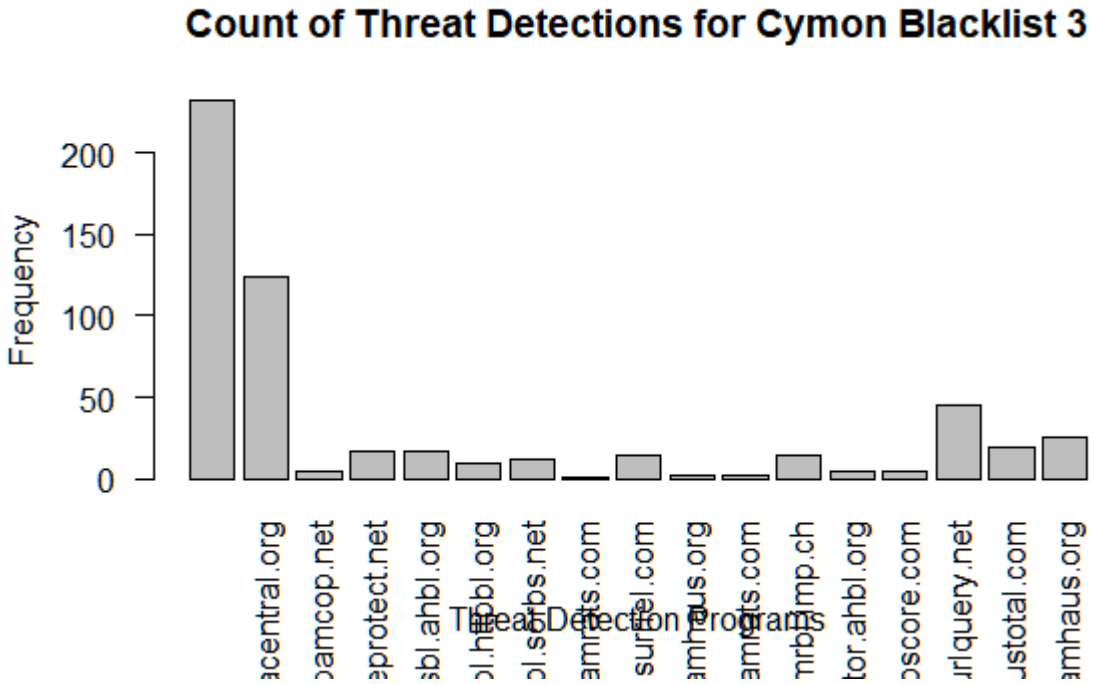
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 1. Having no name means no threats are detected from those IP addresses.



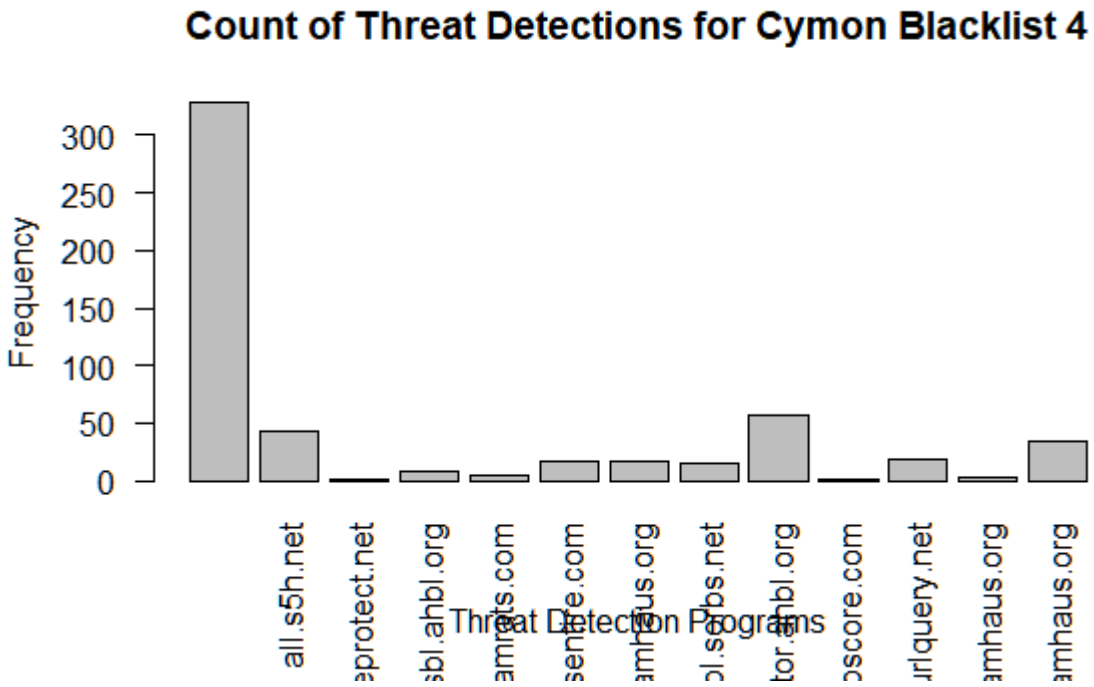
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 1. Having no name means no threats are detected from those IP addresses.



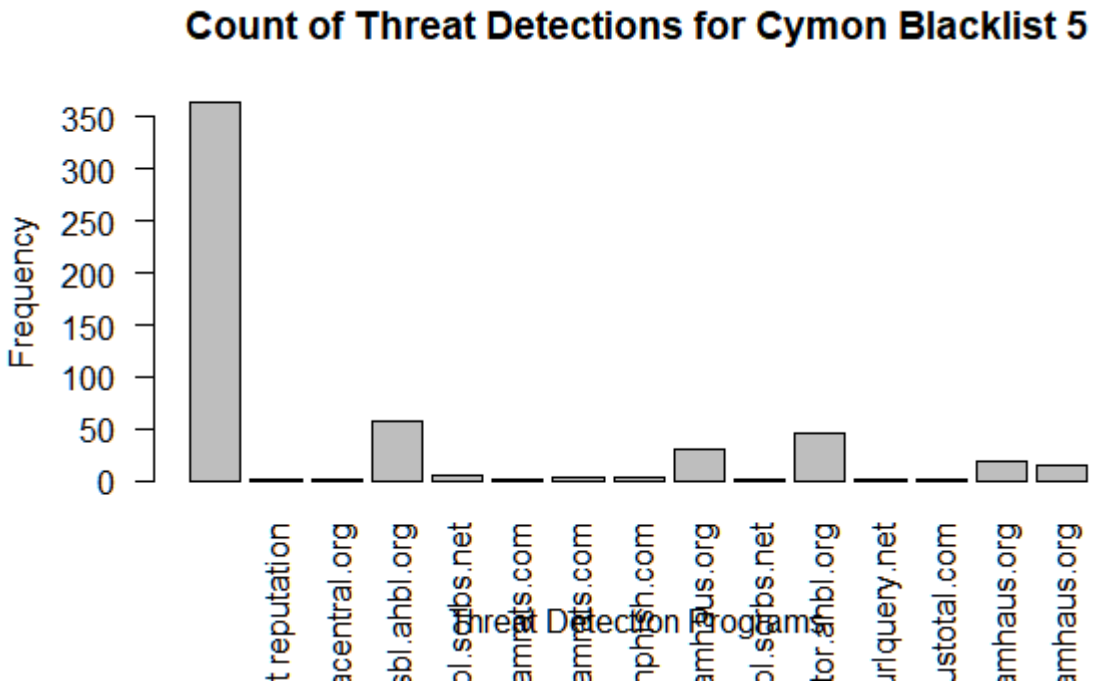
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 3. Having no name means no threats are detected from those IP addresses.



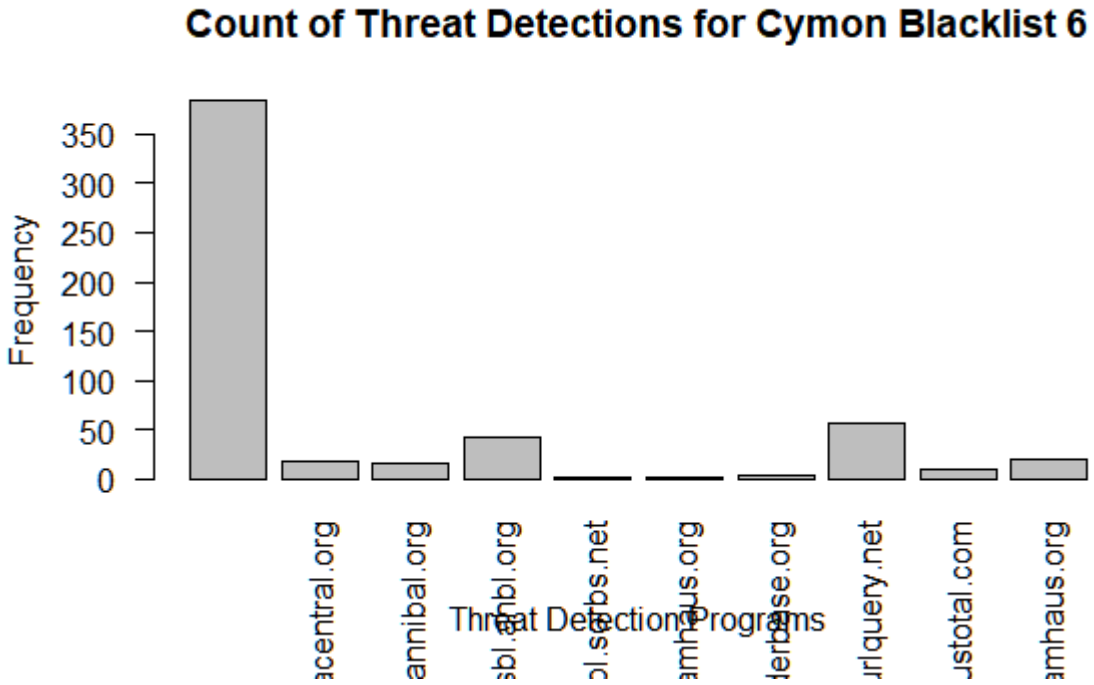
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 4. Having no name means no threats are detected from those IP addresses.



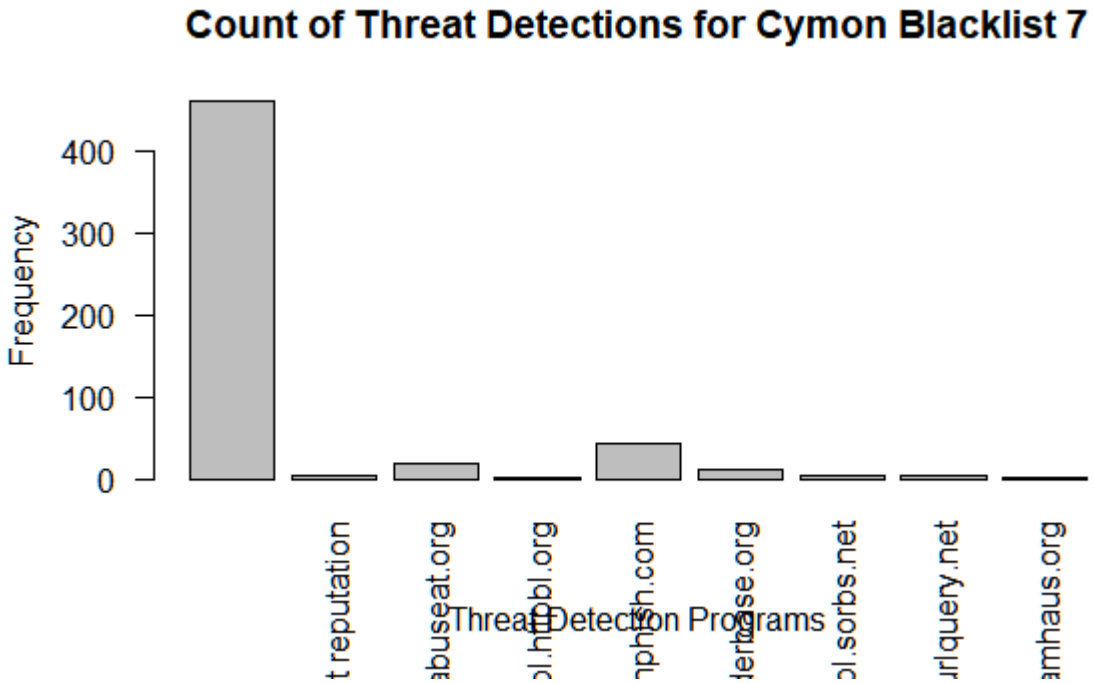
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 5. Having no name means no threats are detected from those IP addresses.



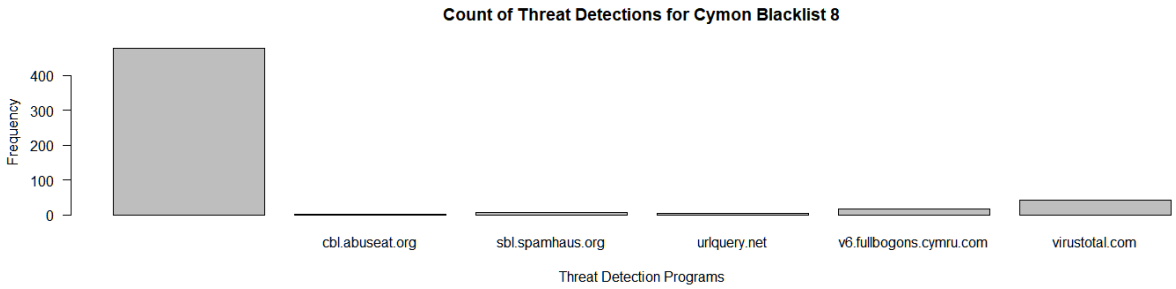
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 6. Having no name means no threats are detected from those IP addresses.



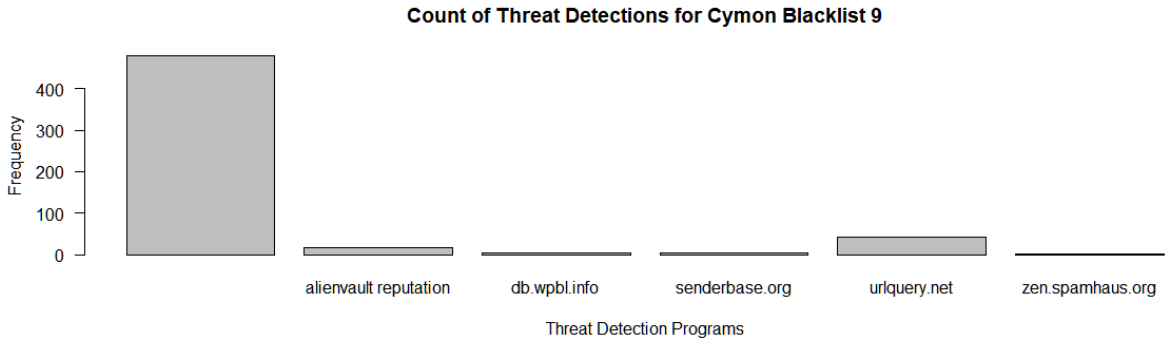
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 7. Having no name means no threats are detected from those IP addresses.



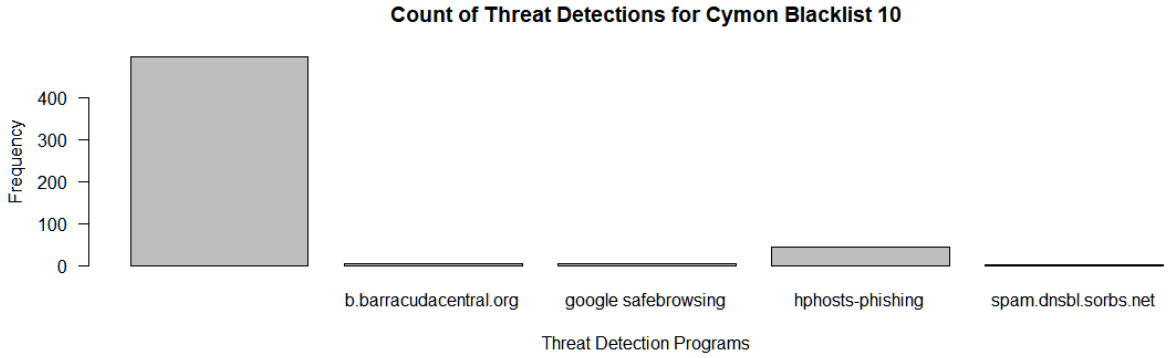
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 8. Having no name means no threats are detected from those IP addresses.



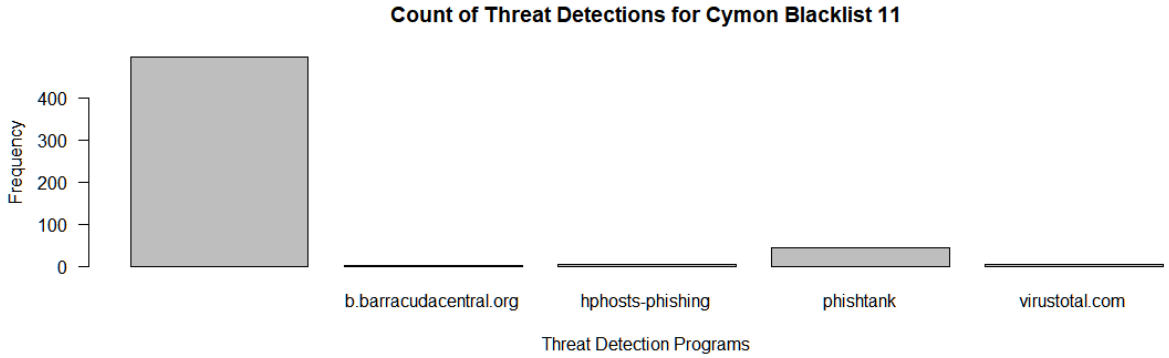
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 9. Having no name means no threats are detected from those IP addresses.



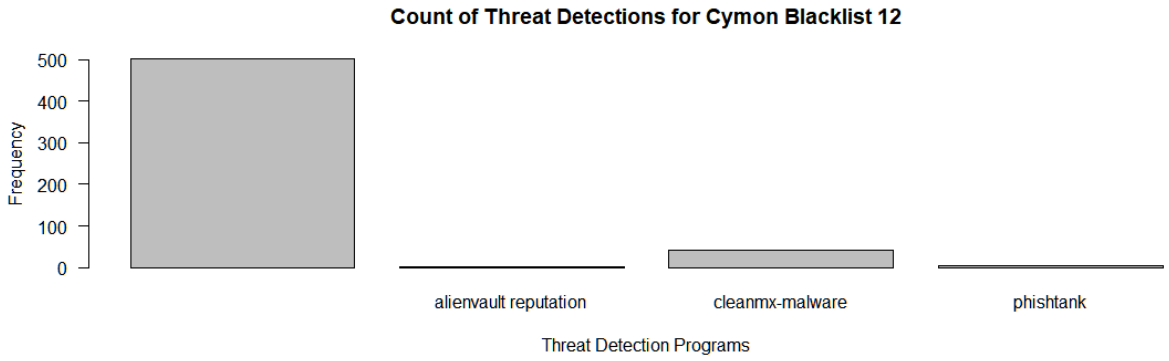
Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 10. Having no name means no threats are detected from those IP addresses.



Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 11. Having no name means no threats are detected from those IP addresses.



Below image shows frequency count of malicious Internet Protocol addresses that are detected by threat prevention programs, as determined by Cymon Threat Intelligence in blacklist 4. Having no name means no threats are detected from those IP addresses 12.



For blacklist 13 and black 14 as determined by Cymon Threat Intelligence, blacklist 13 has between cleanmx-malware and cleanmx-phishing threat prevention programs and blacklist 14 has cleanmx-phishing threat prevention program to detect malicious Internet Protocol addresses.

Below table is a list of threat prevention programs that appear in all blacklists to have detected malicious Internet Protocol addresses as determined by Cymon Threat Intelligence.

virustotal.com	tor.ahbl.org
ibm x-force exchange	ix.dnsbl.manitu.net
urlquery.net	ubl.unsubscore.com
noptr.spamrats.com	psbl.surriel.com
alienvault reputation	dnsbl.httpbl.org
reputationauthority.org	dnsbl.sorbs.net
bl.spamcannibal.org	spam.dnsbl.sorbs.net
b.barracudacentral.org	zen.spamhaus.org
ciarmy.com	web.dnsbl.sorbs.net
labs.snort.org	spamrbl.imp.ch
cleanmx-malware	dyna.spamrats.com
c-sirt.org	dnsbl-1.uceprotect.net
ipbl.mailhosts.org	bl.spamcop.net
ptr	esentire.com
blocklist.de	xbl.spamhaus.org
all.s5h.net	dnsbl-2.uceprotect.net
botscout.com	openphish.com
quttera.com	senderbase.org
dnsbl.ahbl.org	cbl.abuseat.org
pbl.spamhaus.org	google safebrowsing
bl.emailbasura.org	hphosts-phishing
spam.spamrats.com	phishtank
sbl.spamhaus.org	v6.fullbogons.cymru.com
safeweb.norton.com	db.wpbl.info
malwr.com	cleanmx-phishing

To see full code of all plots and charts in R and Python programming language of this assignment two Part 2: Interacting with Application Programming Interfaces, visit the following URL repository on GitHub:

https://github.com/kleung52/SRT411-Assignment-Two