# MAIN DATASOURCES

Monday, February 22, 2016

3:21 PM

#### **MALWARE BlackList**

#### BY IP:

'https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist'#abuse.ch ZeuS

'http://www.malwaredomainlist.com/hostslist/ip.txt'

'http://www.malwaredomainlist.com/mdlcsv.php' #complete database in csv form http://cybercrime-tracker.net/fuckerz.php#pullonlyIP

### **Parsing:**

'http://cybercrime-tracker.net/all.php'

#### **MALWARE Black List**

### BY DOMAIN:

'http://mirror1.malwaredomains.com/files/domains.txt'

'http://secure.mayhemiclabs.com/malhosts/malhosts.txt'

## **SSL\_Black List:**

## **Parsing:**

'https://sslbl.abuse.ch/downloads/ssl\_extended.csv'#

# Timestamp of Listing (UTC) | Referencing Sample (MD5) | Destination IP

## **Phishing Black List:**

## By\_Domain:

'http://dns-bh.sagadc.org/20160219.txt'# domains

'http://mirror1.malwaredomains.com/files/domains.txt' #domains

#### **DNS Black List:**

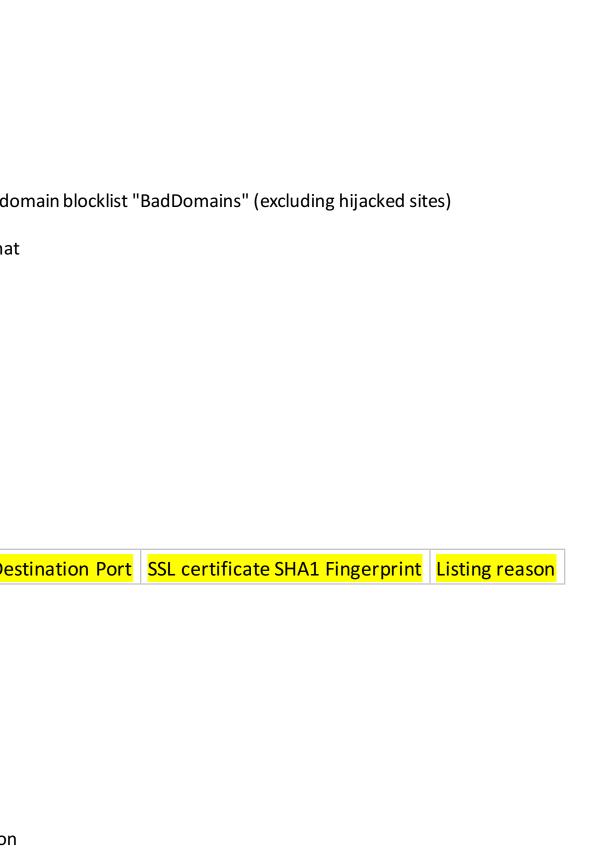
By IP:

'http://www.openbl.org/lists/base\_all.txt']# DNS Black List

## Parsing:

http://www.dnsbl.manitu.net/partners.php?language=en #good parsing information

Snam Plack List



#### Spaill black List.

## By\_IP:

'http://reputation-email.com/reputation/rep\_worst.htm' #just take IPS 'http://www.unsubscore.com/blacklist.txt'

#### Parse:

'http://mirror1.malwaredomains.com/files/domains.txt' #search 'spamhause.org' 'http://dnsbl.inps.de/analyse.cgi?lang=en&action=show\_changes' #Timestamp/ip 'http://antispam.imp.ch/spamlist' # schema to be laid out:ip-address unixtime 'http://spamvertised.abusebutler.com/stats.php'

## **Dynamic DNS Resolution:**

## **By\_Domain:**

'http://dns-bh.sagadc.org/dynamic\_dns.txt'#Dynamic DNS Black List

#### **TOR IP RESOLUTION:**

## **BY\_URL:**

'https://check.torproject.org/exit-addresses'

'http://torstatus.rueckgr.at/router\_detail.php?'

'https://globe.torproject.org/'

in the text file and parse host name/domain name attached to it. This will require parsing script s/domains hostname