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 # pull only IP

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	D

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 informatio

Spam Black List:

domain blocklist "BadDomains" (excluding hijacked sites)

nat

estination Port	SSL certificate SHA1 Fingerprint	Listing reason

on

Spam 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