Completed:

http://s3.amazonaws.com/alexa-static/top-1m.csv.zip

http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-ips.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-ips.txt

all blocklist.de lists

http://rules.emergingthreats.net/open/suricata/rules/compromised-ips.txt

http://danger.rulez.sk/projects/bruteforceblocker/blist.php

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

http://www.dshield.org/ipsascii.html?limit=5000

http://mirror1.malwaredomains.com/files/domains.txt -need to chunk it up by types...

http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt

http://sky.geocities.jp/ro_hp_add/ro_hp_add_hosts.txt

https://reputation.alienvault.com/reputation.genericp

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

http://www.autoshun.org/files/shunlist.csv - done

http://atlas-public.ec2.arbor.net/public/ssh_attackers

http://www.t-arend.de/linux/badguys.txt

http://www.infiltrated.net/blacklisted

http://www.ciarmy.com/list/ci-badguys.txt

https://www.openbl.org/lists/base.txt

http://www.blocklist.de/lists/ssh.txt

http://vmx.yourcmc.ru/BAD_HOSTS.IP4

http://www.geopsy.org/blacklist.html

http://mirror3.malwaredomains.com/files/bulk_registrars.zip http://osint.bambenekconsulting.com/feeds/cl-domlist.txt

http://osint.bambenekconsulting.com/feeds/cl-iplist.txt

https://www.dan.me.uk/torlist/

http://www.dragonresearchgroup.org/insight/http-report.txt

https://isc.sans.edu/block.txt

http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

https://feodotracker.abuse.ch/blocklist.php?download=domainblocklist

https://feodotracker.abuse.ch/blocklist.php?download=ipblocklist

http://malc0de.com/bl/IP_Blacklist.txt

http://malc0de.com/bl/BOOT

http://www.malwaredomainlist.com/updatescsv.php

http://mirror2.malwaredomains.com/files/dynamic_dns.txt

http://www.mirc.com/servers.ini

http://www.nothink.org/blacklist/blacklist_malware_irc.txt

http://www.nothink.org/blacklist/blacklist_malware_dns.txt

https://www.packetmail.net/iprep.txt

http://www.ciarmy.com/list/ci-badguys.txt

http://labs.snort.org/feeds/ip-filter.blf

https://palevotracker.abuse.ch/blocklists.php?download=ipblocklist

http://security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-infected-domains-latest.txt

http://www.spamhaus.org/drop/drop.txt

http://www.spamhaus.org/drop/edrop.txt

https://spyeyetracker.abuse.ch/blocklist.php?download=domainblocklist

https://spyeyetracker.abuse.ch/blocklist.php?download=ipblocklist

http://www.stopforumspam.com/downloads/toxic_ip_cidr.txt

http://rules.emergingthreats.net/open-nogpl/snort-2.8.4/rules/compromised-ips.txt

http://rules.emergingthreats.net/open/snort-2.8.4/rules/compromised-ips.txt

http://www.infiltrated.net/vabl.txt

http://vxvault.siri-urz.net/URL_List.php

https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist

http://data.phishtank.com/data/84d0a4be461da82208dfabe2cbb97e29294289ea580693135e0c6364181885a5/online-valid.json.gz

http://mirror3.malwaredomains.com/files/url_shorteners.zip

http://www.stopforumspam.com/downloads/listed_ip_1_all.zip

http://torstatus.blutmagie.de/ip_list_exit.php/Tor_ip_list_EXIT.csv

http://support.clean-mx.de/clean-mx/xmlviruses.php

http://www.malwareblacklist.com/mbl.xml

http://support.clean-mx.de/clean-mx/xmlphishing?response=alive&format=csv&fields=url,ip,domain&domain=

Issues:

http://rules.emergingthreats.net/open/suricata/rules/botcc.rules
http://rules.emergingthreats.net/open/suricata/rules/tor.rules
http://rules.emergingthreats.net/open/suricata/rules/compromised.rules
http://rules.emergingthreats.net/blockrules/emerging-tor.rules

--all 3 have multiple ips per line, what do

http://urlquery.net/index.php
http://www.spamcop.net/w3m?action=inprogress
http://urlquery.net/index.php
http://vxvault.siri-urz.net/ViriList.php
http://www.malwareblacklist.com/showMDL.php
http://www.mtc.sri.com/live_data/attackers/
https://palevotracker.abuse.ch/
http://www.malwaregroup.com/ipaddresses
http://www.autoshun.org/files/shunlist.html - duplicate of the .csv
->http://stats.denyhosts.net/stats.html
http://www.malwaredomainlist.com/mdl.php?colsearch=All&quantity=All&search=
https://www.projecthoneypot.org/list_of_ips.php
->http://stats.denyhosts.net/stats.html

--all the data in the above is in html tables, the html source isn't split up by line so the per line regex paradigm of CIF doesn't really work here. Need to ask bambenek what to do in these cases.

http://atlas.arbor.net/summary/domainlist

-the domains are not split up by line, how do we get at them?

http://lists.clean-mx.com/pipermail/phishwatch/$today.txt.gz
http://lists.clean-mx.com/pipermail/viruswatch/$today.txt.gz
https://isc.sans.edu/api/topips/records/1000/$today
https://isc.sans.edu/api/sources/attacks/10000/$today

http://lists.clean-mx.com/pipermail/phishwatch/$today.txt.gz

https://isc.sans.edu/api/topips/records/1000/$today

-Can't do today in the config, need to have a feed that only shows current day

http://files.dontneedcoffee.com/track/AnglerEK/domains.txt
http://files.dontneedcoffee.com/track/AnglerMiu/domains.txt
http://files.dontneedcoffee.com/track/AnglerRU8080/domains.txt
http://files.dontneedcoffee.com/track/BrowLockCyber/domains.txt
http://files.dontneedcoffee.com/track/FakeCodecRotator/domains.txt
http://files.dontneedcoffee.com/track/Goon/domains.txt
http://files.dontneedcoffee.com/track/Grandsoft/domains.txt
http://files.dontneedcoffee.com/track/Magnitude/domains.txt
http://files.dontneedcoffee.com/track/Neutrino/domains.txt
http://files.dontneedcoffee.com/track/NuclearPack/domains.txt
http://files.dontneedcoffee.com/track/Sakura_KovtZaccess/domains.txt
http://files.dontneedcoffee.com/track/Styx/domains.txt
http://files.dontneedcoffee.com/track/StyxKein/domains.txt
http://files.dontneedcoffee.com/track/whitehole/domains.txt

- cloud not found

http://rules.emergingthreats.net/blockrules/rbn-malvertisers-ips.txt
http://arakis.pl/en/index.html
http://www3.malekal.com/malwares/
http://jsunpack.jeek.org/dec/go?list=1
http://rss.uribl.com/nic/NAUNET_REG_RIPN.xml
http://abusix.org/service/spamfeeds
http://www.senderbase.org/home/detail_virus_source
intel.martincyber.com/ip/
http://rules.emergingthreats.net/open/snort-2.9.0/rules/rbn-ips.txt
http://dnsbl.abuse.ch/webabusetracker.php
http://www.brawg.com/hosts.deny
http://support.clean-mx.de/clean-mx/xmlviruses?response=alive&format=csv&fields=url,ip,domain&domain=
http://dynastop.tanaya.net/DynaStop.BleedingThreats.conf
http://www3.malekal.com/exploit.txt
http://downloads.prometheus-group.com/delayed/rules/modsec/domain-blacklist.txt
http://www.stopforumspam.com/downloads/bannedips.csv

-404

rsync://psbl-mirror.surriel.com/psbl/psbl.txt
-requires something to use rsync

http://openntpproject.org/ntp-worst-cymru.txt

- nothing here, just says “Please use www.openNTPproject.org instead”

http://minotauranalysis.com/malwarelist.aspx
http://malwareint.com/
-nothing here (under construction)

http://callbackdomains.wordpress.com
- the ips are in blog posts

http://atlas.arbor.net/summary/fastflux?out=xml
-Doesn’t go to an xml

http://honeytarg.cert.br/honeypots/ - nothing to parse here
http://exposure.iseclab.org/ - seems to be nothing to parse here
http://www.spamcop.net/ - found a feed listed below but it would make for a very difficult parse
http://honeytarg.cert.br/spampots/ - nothing to parse here
http://zeltser.com/combating-malicious-software/malicious-ip-blocklists.html - list of other sites
http://contagiodump.blogspot.com/2010/11/links-and-resources-for-malware-samples.html - list of sites
http://dshield.org/diary.html?storyid=12373 - doesnt seem to be a feed
http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report - report is a pdf
http://www.malware.com.br/cgi/submit?action=list
- this is discontinued

http://proxy.org/proxies_sorted2.shtml
-how to parse? info is not in any sort of standard per-line format, in html lists…

http://www.kids-clinic.jp/uni/ipaddress/new_log
- nothing shows up

robert.kolatzek.org/possible_botnet_ips.txt
- blog, nothing found

TO LOOK AT(from other sites)
http://www.spamcop.net/w3m?action=hoshame - found in spamcop site(html table though)
http://www.dshield.org/hpbinfo.html - requires an hpb account(api key)
http://hosts-file.net/rss.asp - this is an rss feed
http://malc0de.com/rss/ - instead of the html table
http://www.malware.com.br/lists.shtml - registration required
http://www.projecthoneypot.org/list_of_ips.php?rss=1 - rss feed for project honeypot bad ips
http://www.shadowserver.org/wiki/pmwiki.php?n=Services/Reports - requires account

http://www.threatstop.com/
http://urlblacklist.com/ - this aint free
https://atlas.arbor.net/ - what from here
http://www.team-cymru.org/Services/Bogons/bogon-dd.html - what is this
http://www.malwaredomainlist.com/hostslist/mdl.xml - rss feed
http://blog.urlvoid.com/247/new-list-of-dangerous-websites-to-avoid/ -blog
http://secuboxlabs.fr/ - html table
http://www.malwareurl.com/ - registration required
http://www.malwaregroup.com/ -html(api doesnt seems to be under construction atm)