Botnet Detection Using Internet Alerts

Vojtěch Krmíček, GEANT3 JRA4 T4 Internal Deliverable

March 25, 2011

Abstract

The goal of this report is to examine freely available Internet alerts for the purpose of botnet detection. We provide a brief overview of free Internet alerts, then we select two of them for the purpose of botnet detection. In the following, we develop methods for automatic conversion and filtering of these Internet alerts lists and generate lists of botnet control centers suitable for automatic processing.

1 Introduction

The botnets are still more frequent and spread all over the world in these days and represent one of the biggest Internet threats. They are rapidly developing due to the huge amount of money, coming from the botnet business [9] and their detection and countermeasures against them are more difficult. Therefore the botnet research is and will be the important task for nowadays Internet security researchers.

There exists a number of both free and commercial online alerting systems, providing lists of infected computers, spam machines, phising sites, botnets, etc. In our work, we will focus on the freely accessible online alerting systems. Although they are operated mainly on volunteer basis or funded by various research projects, we can use them for botnet security research with an advantage.

These systems are based on various types of sources. The honeypots and sensors scattered throughout the Internet that report back about attacks that have targeted them from various IP addresses is one of the main sources. Also the monitors of current spam campaigns, spreading of the current malware and worms through the Internet, large infections notified by Internet providers and other similar methods are used to obtain alerts data.

There is a lot of opportunities how and where to use them. If we have a list of malicious sites, infected computers, phising domains, botnet centers, etc., we can apply various ways to protect our network against these possible threats, independently on the scope of the network. Both a network administrator of small company network and an international Internet provider can use these alerts to protect their networks, block malicious traffic and keep the ordinary users and provided services safe.

The access to these free Internet alerts could be completely free, but there are also particular sources, which provides their lists only on limited basis (besides the business providers). We can see, e.g. the sources providing lists of

Source Name	List Type	Availability	WWW
DNS-BH	malware domains	free	www.malwaredomains.com
PhishTank	phishing sites	free	www.phishtank.com
Google Safe	malware/phising sites	responsible AS	safebrowsingalerts. googlelabs.com
Cyclops	route hijacks	free	cyclops.cs.ucla.edu
BGPmon	route hijacks	free	bgpmon.net
SORBS	DNS blacklisting	free	www.sorbs.net
Spamhaus	DNS blacklisting	free	www.spamhaus.org
SpamCop	DNS blacklisting	free	www.spamcop.net
Abuse.ch	C&C servers	free	www.abuse.ch
Shadowserver	C&C servers	responsible AS	www.shadowserver.org
Team Cymru	C&C servers	data exchange	www.team-cymru.org

Table 1: Overview of the free Internet alerts.

malicious IP addresses to particular ASN (autonomous system network) operators only, or other sources requesting the deployment of their own probes in the administrated networks to be able to expand their alert data.

In this report, we provide an overview of free Internet alerts services (Section 2), then we choose particular Internet alert services most suitable for botnet detection and describe them in detail (Section 3). Following Section 4 brings the methods for the conversion and filtering of Internet alert lists into the unified list of threat sources. The possible implementation of a NfSen detection plugin using list of threat sources is discussed in Section 5.

2 Overview of the Free Internet Alerts

This section provides the overview of freely available Internet alerts, alive in these days. The goal of this overview is not to provide a complete list of all existing Internet alert sources, but to bring an overview of the main Internet alert types and their provided functionality. We have divided this list to following categories: malware domains/phising sites, route hijacks, DNS blacklisting and botnets. The complete overview of presented sources is presented in Table 1.

2.1 Malware Domains and Phising Sites

The goal of Internet alert lists containing malware domains and phising sites is to provide network administrators information about malicious content, which is being hosted on their networks or outside in the Internet. These lists are usually loaded loaded onto an internal network DNS server. When a computer from local network requests an URL or a file from one of the listed domains or phising sites, instead of loading original page a warning is displayed and the user is thus protected against the malware.

- **DNS-BH – Malware Domain Blocklist** [5] – The DNS-BH project creates and maintains a listing of domains that are known to be used

to propagate malware and spyware. The project provides the Bind and Windows zone files, which can be loaded to the client systems and consequently prevent the access to the malicious sites, thus preventing many spyware installs and reporting.

- **PhishTank** [10] – PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

- **Google Safe** [6] – Google Safe provides information about malware and phishing sites inside an administered network. The alerts provided by this site are based on administered ASN and, in general, will only be sent to system contacts registered in RIPE Whois database for the ASN in question.

2.2 IP Hijacking

IP hijacking [17] (sometimes referred to as BGP hijacking, prefix hijacking or route hijacking) is the illegitimate take over of groups of IP addresses by corrupting Internet routing tables. IP hijacking can occur on purpose or by accident in one of several ways:

- An AS announces that it originates a prefix that it does not actually originate.

- An AS announces a more specific prefix than what may be announced by the true originating AS.

- An AS announces that it can route traffic to the hijacked AS through a shorter route than is already available, regardless of whether or not the route actually exists.

IP hijacking is sometimes used by malicious users to obtain IP addresses for use with spamming or a distributed denial-of-service (DDoS) attack.

- **Cyclops** [4] – Cyclops is a system that provides ISPs a view of how their connectivity is perceived from hundreds of vantage points across the network, enabling a comparison between their observed connectivity and their intended connectivity. Anomalies detected by Cyclops include prefix hijacks, unexpected peerings/depeerings, sudden routing shifts, bogon prefixes, bogus ASNs and route leakages among others. Registered users can configure what type of alerts they would like to receive.

- **BGPmon** [2] – BGPmon provides similar functionality like Cyclops systems. It monitors network prefixes and alerts network administrators in case of a suspicious path change. BGPmon classifies these changes in types and provides various types of reporting and configurations.

2.3 DNS Blacklisting

DNS blacklisting (DNSBL, DNS-based blackhole list, or blacklist) [16] is a way of publishing IP addresses through the Internet Domain Name Service (DNS) either as a zone file that can be used by DNS server software, or as a live DNS zone that can be queried in real-time. DNSBLs are most often used to publish the addresses of computers or networks linked to spamming and they are usually used for rejecting or flagging messages which have been sent from a site listed on one or more such lists.

DNSBL is a software mechanism, rather than a specific list or policy. There are dozens of DNSBLs in existence, which use a wide array of criteria for listing and delisting of addresses. These may include listing the addresses of zombie computers or other machines being used to send spam, listing the addresses of ISPs who willingly host spammers, or listing addresses which have sent spam to a honeypot system.

There is more than twenty freely available DNS blacklist on the Internet, therefore we will mention only a few examples in the following list. Comparison of public DNS blacklists can be found in [15]:

- **SORBS** [12] – SORBS (Spam and Open Relay Blocking System) is a list of e-mail servers suspected of sending or relaying spam. It is augmented with complementary lists that include various other classes of hosts. SORBS adds IP ranges that belong to dialup modem pools, dynamically allocated wireless, and DSL connections as well as DHCP LAN ranges by using reverse DNS records, WHOIS records, and also submissions from the ISPs.

- **Spamhaus** [14] – Spamhaus maintains a number of real time spam-blocking databases, including the Spamhaus Block List, the Exploits Block List, the Policy Block List and the Domain Block List. Spamhaus DNSBLs are widely used by the Internet email service providers, corporations, universities, governments and military networks.

- **SpamCop** [3] – SpamCop is a free spam reporting service, allowing recipients of unsolicited bulk email (UBE) and unsolicited commercial email (UCE) to report offenders to the senders' ISPs, and sometimes their web hosts. SpamCop uses these reports to compile a DNSBL of computers sending spam, and websites referenced in the spam are used to create the Spam URI Realtime Blocklists.

2.4 Botnet Control Centers

Besides the Internet alerts providing information about malware domains, route hijacks and spam sources, there are also available services providing monitoring and information about botnet control centers. These services allow network administrators to find potentially infected computers (bots/drones) in their network communicating with the botnet control centers (C&C) or the C&C itself and block the malicious traffic.

- **Abuse.ch** [1] – Abuse.ch website provides several types of botnet C&C lists, regularly updated and divided into the various projects. There is

AMaDa project gathering information about various types of botnets, Palevo Tracker providing lists of computers infected by Palevo worm, SpyEye tracker monitoring C&C servers of the SpyEye botnet and also Zeus tracker providing lists of Zeus C&C.

- **Shadowserver** [11] – Shadowserver tracks and reports on malware, botnet activity and electronic fraud. It aims to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers and the spread of malware. Beside the other activities, Shadowserver publish a lists of malicious IP addresses and C&C servers in requested ASNs. The reports provided by the Shadowserver includes, e.g., detected botnet C&C servers, systems infected by the botnets (drones), scans, click fraud, proxies, etc.

- **Team Cymru** [13] – Team Cymru provides targeted reports specific to ASNs. These reports include botnet C&C servers, phishing sites and malware sites. But this source is not freely available - information provided by Team Cymru is based on a data exchange agreement where Team Cymru provides the daily report data in exchange for data from the data exchange partner (NREN). This might be Darknet, BGP, flow, passive DNS or other data.

3 Selected Internet Alerts

3.1 Abuse.ch – Project AMaDa

The first source chosen for the automatic processing of free Internet alerts is the malware database AMaDa. By using sandboxing and signatures AMaDa is providing a list of C&C servers of various botnets. The list can be used to prevent infected clients connecting to the botnet C&C centers.

C&C servers of the following botnets are included in the blocklists: *Artro Asprox, Avalanche, Backdoor.Tofsee, BlackEnergy1, BlackEnergy2, Bredolab, Carberp, DDoS.Optima, DDoS.Yenibot, DMSpammer, DNSTrojan, Dropper.Harnig, Dropper.Lukicsel, Dropper.Witkinat, Fake-AV, Fraudload, Gbot, Hiloti, Mebroot, Oficla, Rootkit.Sirefef, Rustock, SpyEye, TDL3/TDSS, Unknown.BankingTrojan, Win32.Scar, Worm.Ramnit, Worm.Palevo.*

AMaDa provides three types of blocklists, all these blocklists are freely available from their web page:

- AMaDa Combined C&C Blocklist (Domains+IPs),
- AMaDa C&C Domain Blocklist,
- AMaDa C&C IP Blocklist.

We use the AMaDa combined C&C blocklist because it contains the most of C&C servers. The example of the blocklist content is following:

```
94.75.199.163 # Rootkit.Sirefef
95.211.130.132 # Backdoor.Tofsee
95.211.98.168 # DMSpammer
95.211.98.186 # DMSpammer
96.9.139.213 # DMSpammer
96.9.157.39 # Artro
```

```
aaaadminmont.com # Unknown.BankingTrojan
aabalhtabvf.com # Mebroot
aabeejyafds.com # Mebroot
aaboyriafds.com # Mebroot
aahydrogen.com # Dropper.Harnig
aasmartmoney.com # TDL3/TDSS
abaronaweb.net # BlackEnergy1
aboutflipware.in # Artro
abtdiagnostic.com # Dropper.Harnig
acdldagafds.com # Mebroot
acidsource.com # SpyEye
```

3.2 Abuse.ch – ZeuS Tracker

Beside the above described project AMaDa, Abuse.ch provides also the service called *ZeuS Tracker*. This service provides a blocklist of IP addresses and domains, which are ZeuS botnet C&C servers. Using this list, we are able to block communication with ZeuS botnet C&C servers and prevent therefore connecting ordinary hosts to these botnet servers.

The service provides various types of blocklist, e.g., ZeuS domain blocklist, ZeuS IP blocklist, ZeuS combined blocklist and also various blocklist preformated for uploading to particular firewalls, proxies etc. We use the ZeuS combined blocklist containing both IP addresses and domains of the botnet servers. The example of the blocklist content is following:

```
216\.59\.18\.191
216\.59\.18\.89
216\.59\.18\.92
217\.115\.136\.149
.28843622.biz
.2myagust.com
.33166bannon.cz.cc
.360safeupdate02.gicp.net
.3apa3a.tomsk.tw
46\.161\.21\.10
46\.166\.128\.28
46\.29\.249\.195
46\.29\.252\.96
46\.29\.254\.217
46\.29\.254\.218
46\.29\.254\.221
46\.29\.254\.225
46\.29\.254\.39
46\.4\.154\.109
.486794ytrjdhgfj.vp-service.in
.4ertenok.tk
```

3.3 Shadowserver

Shadowserver has been chosen as the second source for the automatic processing. It provides various types of the blacklisting, including following types of reports: detected botnet C&C servers, infected systems (drones), DDoS attacks (source and victim), scans, click fraud, compromised hosts, proxies, spam relays and others. For our purpose, we have selected these three types of reports:

- **Command and control report** provides a list of C&C servers located in the responsible AS network. While reports focus on the IRC C&C's, there are also HTTP, P2P, and hybrid servers that are being used. Many times a C&C may have leaf nodes to extend out its reliability. These leaf nodes are listed for each C&C to provide more information about single botnet.

- **Drone report** provides a list of all infected machines (drones), and zombies that were captured from the monitoring of IRC C&C servers, capturing IP connections to HTTP botnets, or the IP's of Spam relays.
- **Sinkhole HTTP drone report** provides IP addresses of all devices that joined Shadowserver sinkhole server that did not arrive through the usage of an HTTP referrer. Since the Sinkhole server is only accessed through previously malicious domain names, only infected system should be seen in this list.

All these blocklists are provided only to the administrators/responsibles of particular AS networks and also contains the infected machines from this ASN only. Reports are emailed regularly to the administrator email address.

Example of the Command and control report:

```
"IP Address","Port","Channel","Country","Region","State","Domain","ASN","AS Name","AS Description"
"81.211.7.122 69.18.206.194",3267,"#B#t[r2]N#t","RU US","MOSCOW | COMMACK","MOSKVA | NEW YORK",
"GLDN.NET INVISION.COM","3216 12251","SOVAM INVISION","AS Golden Telecom, Moscow, Russia | Invision.com, Inc."
"81.211.7.122 69.18.206.194",3267,"#B#tN#t[r3]","RU US","MOSCOW | COMMACK","MOSKVA | NEW YORK",
"GLDN.NET INVISION.COM","3216 12251","SOVAM INVISION","AS Golden Telecom, Moscow, Russia | Invision.com, Inc."
"81.211.7.122 69.18.206.194",3267,"#B&#65533;t[r2]N&#65533;t","RU US","MOSCOW | COMMACK","MOSKVA | NEW YORK",
"GLDN.NET INVISION.COM","3216 12251","SOVAM INVISION","AS Golden Telecom, Moscow, Russia | Invision.com, Inc."
```

Example of the Drone report:

```
"timestamp","ip","port","asn","geo","region","city","hostname","type","infection","url","agent","cc",
"cc_port","cc_asn","cc_geo","cc_dns","count","proxy","application","p0f_genre","p0f_detail"
"2011-04-23 00:00:05","210.23.139.130",3218,7543,"AU","VICTORIA","MELBOURNE",,"tcp","sinkhole",,,
"74.208.164.166",80,8560,"US",,1,,,"Windows","2000 SP4, XP SP1+"
"2011-04-23 00:00:08","115.166.54.44",,9556,"AU","SOUTHAUSTRALIA","ADELAIDE",
"115-166-54-44.ip.adam.com.au",,"spyeye",,,"94.75.228.147",,16265,"NL","015.maxided.com",1,,,"WINXP",
"2011-04-23 00:00:10","116.212.205.74",48986,9822,"AU","WESTERN AUSTRALIA","PERTH",,"tcp","sinkhole",,,
"87.106.24.200",80,8560,"DE",,1,,,"Windows","XP SP1+, 2000 SP3 (2)"
```

Example of the Sinkhole HTTP drone report:

```
"timestamp","ip","asn","geo","url","type","http_agent","tor","src_port","p0f_genre","p0f_detail","hostname",
"dst_port","http_host","http_referer","http_referer_asn","http_referer_geo","dst_ip","dst_asn","dst_geo"
"2010-08-31 00:09:04","202.86.21.11",23456,"AF","GET /search?q=0 HTTP/1.0","downadup",
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)",,8726,,,,80,"149.20.56.32",,,,,,
"2010-08-31 00:09:06","82.115.28.93",41152,"AF","GET /search?q=0 HTTP/1.0","downadup",
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)",,50499,,,,80,"149.20.56.32",,,,,,
"2010-08-31 00:14:50","180.94.94.3",55330,"AF","GET /?3c851a=7932468 HTTP/1.1","sality",
"KUKU v5.06exp =19026555919",,60564,"Windows","2000 SP2+, XP SP1+ (seldom 98)",,80,"www.kjwre9fqwieluoi.info",,,,,,
```

4 Automatic Conversion and Filtering

We need to convert the reports presented in the previous section to the format suitable for the automatic processing by the monitoring tools, e.g., NfSen or nfdump [8, 7]. Such converted list should be regularly updated and should merge the blacklisted IP addresses to the one final list with all necessary information. Besides the IP addresses and hostnames, this list should contain protocol and port (if available), number of AS network, a description of the infection/type of the botnet, type of primal report, reporting date.

Example of the list:

```
IP_address      hostname       protocol port AS   infection_type  reporter      date
74.208.164.166  -              tcp      3267 3216 irc_cc          shadow_cc     2011-03-20
202.86.21.11    -              tcp      80   8726 downadup        shadow_drone  2011-03-18
87.106.24.200   -              tcp      9556 7543 sinkhole        shadow_http   2011-03-20
94.75.199.163   -              -        -    -    Root.Sirefef    amada         2011-03-20
95.211.130.132  -              -        -    -    Backdoor.Tofsee amada         2011-03-20
-               acidsource.com -        -    -    SpyEye          amada         2011-03-20
```

The conversion itself is performed by the Perl script, which is regularly started, lists all reports in report directory and proceeds the unprocessed ones. The generated output is then stored in the output directory and could be then passed, e.g., for the flow filtering in the NfSen collector.

5 Possible Implementation as the NfSen Plugin

The presented list of aggregated malicious sources could be used with advantage by the network administrator for the filtering flows in the administered network, e.g., using NfSen collector with additional plugin providing such filtering. The network administrator could have a possibility to list all malicious flows in administered network, filter them depending on the type and perform necessary steps to remove the infection.

The scheme of the possible NfSen plugin is following. As the inputs, plugin will ask the network administrator for: on what NetFlow data apply filtering, on what time window, which Internet alert sources to use, type of communication (both infected hosts inside/outside network or only infected hosts inside the network). After querying the NfSen for these data, plugin will process our list of Internet alerts, filter out only particular requested types of infection and query nfdump for such flow data.

The nfdump output is then preformated and passed to the NfSen frontend, where are all malicious flows displayed with a detailed description (type of infection, amount of flows, time window, traffic statistics, etc.).

6 Conclusion

In this text, we have provided the overview of the existing free Internet alerts and we have discussed their suitability for the botnet detection (Section 2). In the following Section 3 we have selected two sources – AMaDa project (Subsection 3.2) and Shadowserver (Subsection 3.3) – suitable for botnet detection and described them in detail. In the Section 4 we have introduced the method for converting and filtering selected reports to suit consequent automatic processing. The possibility of implementing the NfSen plugin for querying botnet data using this generated list is presented in Section 5.

The implementation of the NfSen plugin for querying botnet data using presented list will be a part of work in the Tools subtask of JRA2 T4.

7 References

[1] Abuse.ch. Abuse.ch web page, 2011. `http://www.abuse.ch/`.

[2] BGPmon. BGPMon – BGP monitoring and analyzer tool, 2008. `http://bgpmon.net/`.

[3] Cisco Systems. SpamCop, 2010. `http://www.spamcop.net/`.

[4] Cyclops Team. Cyclops - open eye to your net, 2011. `http://cyclops.cs.ucla.edu/`.

[5] DNS-BH Project. DNS-BH – Malware Domain Blocklist, 2011. http://www.malwaredomains.com/.

[6] Google Inc. Safe Browsing Alerts for Network Administrators, 2010. http://safebrowsingalerts.googlelabs.com/.

[7] Peter Haag. NFDUMP - NetFlow processing tools. http://nfdump.sourceforge.net/, 2011.

[8] Peter Haag. NfSen - NetFlow Sensor. http://nfsen.sourceforge.net/, 2011.

[9] Namestnikov, Y. The economics of Botnets, 2009. URL http://www.viruslist.com/analysis?pubid=204792068.

[10] OpenDNS. PhishTank, 2011. http://www.phishtank.com/.

[11] Shadowserver Foundation. Shadowserver, 2011. http://www.shadowserver.org/.

[12] SORBS. Spam and Open Relay Blocking System (SORBS), 2011. http://www.sorbs.net/.

[13] Team Cymru Inc. Team Cymru Community Services, 2011. http://www.team-cymru.org/.

[14] The Spamhaus Project Ltd. Spamhaus, 2011. http://www.spamhaus.org/.

[15] Wikipedia. Comparison of DNS blacklists — Wikipedia, The Free Encyclopedia, 2011. http://en.wikipedia.org/w/index.php?title=Comparison_of_DNS_blacklists.

[16] Wikipedia. DNSBL — Wikipedia, The Free Encyclopedia, 2011. http://en.wikipedia.org/w/index.php?title=DNSBL.

[17] Wikipedia. IP hijacking — Wikipedia, The Free Encyclopedia, 2011. http://en.wikipedia.org/w/index.php?title=IP_hijacking.