Spam, Real World Numbers and the Value of IP Reputation Lists

Spam has reached the point where more than 95% of all email received at email servers is unwanted, and over 90% of all connections to mail servers are from attackers, bulk mailers, trojans and bots. The most effective way for mail servers to lessen the bandwidth, dictionary attacks* and overhead is to block connections from known IP's that either leak spam, or are used in the above types of abusive behavior.

This study is to examine a typical ISP's real world statistics to show the effectiveness of such reputation lists, and to examine which lists can be used and how effectively in order to lower the overhead and resources that are required to process email, and to prevent the unwanted email that such connections send.

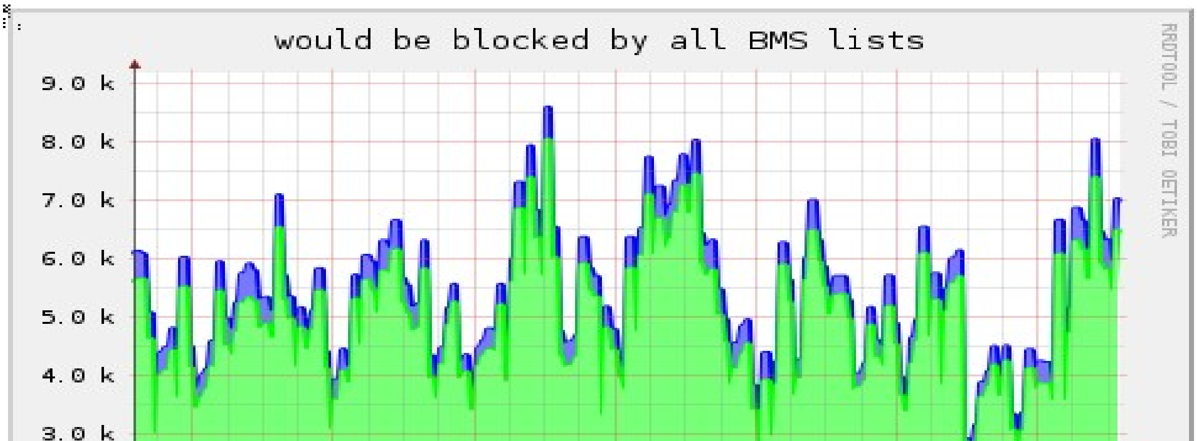
It is obvious to most operators that by blocking such connections (reducing overhead by 90% or more) will mean significant cost savings (1 server is cheaper than 10) and as well it can be used as a 'First Alert' or 'Zero Day' defense to stop the next new wave of attacks from these IP addresses of 'owned' machines (collectively often known as “BotNets”), as their techniques adopt to current email, virus and phishing attacks filters. (which they often do faster than such filters can get updated)

The ISP chosen to reflect these stats shall remain anonymous, however it is a US based ISP of app. 3000 users which historically had problems with Spam before adopting IP reputation and other technologies. Comments shall be made to reflect the differences between it and larger ISP's statistics.

For this study, not all IP Reputation lists are analyzed as some are 'pay for use' lists or otherwise not available for study. It should be noted that two such lists, SpamHaus and SpamCop, industry leaders in this field also report comparable statistics but this study concentrated on freely available IP Reputation Services, (sometimes called RBL's or Real Time Blacklists because they are usually used by ISP's or others to 'blacklist' connections).

(NOTICE: The numbers shown are for a mail server that uses special attack limiters to prevent a single IP from too many connections. Mail servers that do not use this protection can see ***over 99%*** *of all incoming connections belonging to attackers. ISP's often block thousands of IP's that are trying to do dictionary or spam attacks every day, and without that technique of blocking the worst offenders the problem would be a lot worse. Many smaller companies do not have that technology in place, and it is even more important for them to use IP reputation lists. As well, since most dictionary attacks now come from 'BotNets' which may comprise thousands or hundreds of thousands of compromised computers on different IP Addresses, without IP reputation blocking or similar protection, an ISP's complete customer email address listings can be tested or guessed within only a few hours, and sold to the highest bidder for use in Spam attacks)*

<u>It is possible for almost any email server to block over 90% just based on IP Reputation.</u>



**Statistics Indicate Real Time Data as of Apr. 28th, 2008*

Comparative Study of Individual Freely Available Lists Used in this Study.

In this study, the 92.18% represents the amount of email that would be blocked by the use of just a small amount of freely available lists. Normally IP Reputation Lists are used by doing a DNS query on any IP Address that connects to the mail server using special servers that are setup by the list operators. These lists will return whether an IP Address is listed, and often a small 'reason' token leaving it up to the mail server or filtering software to decide what to do with the connections.

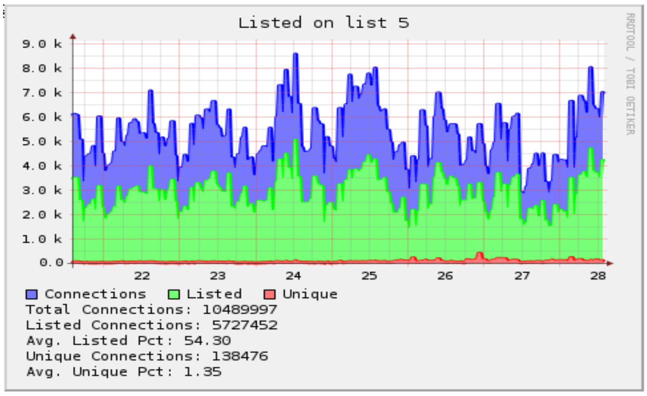
Often, IP addresses are listed for several reasons, and on some lists you can also determine if an IP is listed for one or several of these. Not all IP addresses are listed because they send spam. Many are listed because they are being used to try to 'discover' email addresses or worse; guess the passwords of legitimate email accounts so they can use them to send Spam as well.

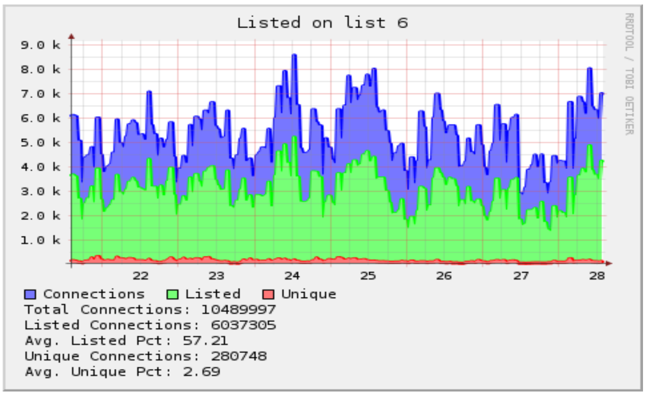
Sometimes other criteria may be used for listing, such as when a mail server is known to be incorrectly configured etc and some IP reputation lists may even go farther and list ISP's that are known not to deal with Spam complaints. Some lists have very good data, and there are some which may have what is known as a 'False Positive', eg listing IP addresses which should not be on the list either by accident or intention.

Most lists have their own way of detecting which IP addresses should go on their lists, but in general it usually done by 'traps'. Spammers often 'steal' email addresses, from listings on web pages etc., just to send them Spam. The 'spamtraps' are false addresses left on web pages on purpose, or unused email addresses left as bait for spammers. Some are from spam emails provided by collections of volunteers who forward spam to list operators. Some lists are easy to get de-listed, and some nearly impossible. When using IP reputation lists, caution should be exercised but this study will focus on reputation lists widely used at ISP's throughout the world.

This study examines the statistics of individual freely available lists that were included as part of the total overall protection shown in the above graph.

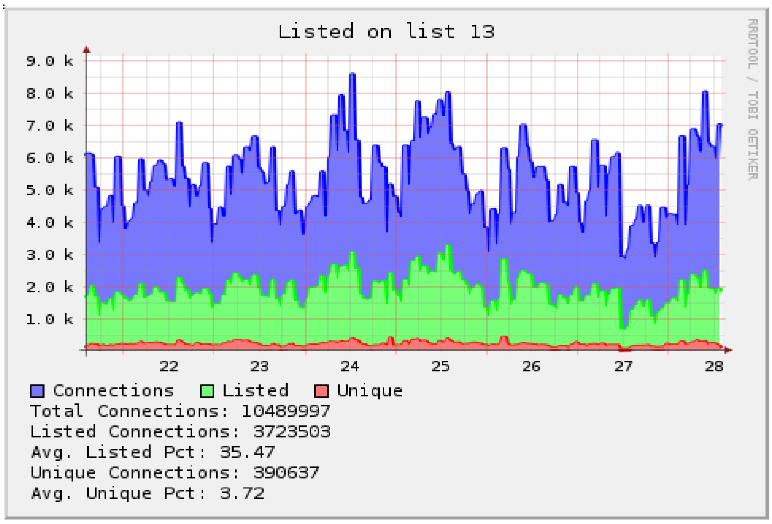
UCE-PROTECT (PROTECT2 and PROTECT3 www.uceprotect.net)





Special Notes: Each list has their own criteria for getting, listed and you should visit their site for a full explanation. UCE-PROTECT uses a 3 Tier system. They have a PROTECT-1 as well, however that was not included as the number of 'Uniques', (IP addresses only listed on that list) was below the number required to be included, eg meaning that the IP address were on other tested lists as well. There has been a few reported cases of 'False Positives' but this could be the result of legitimate mail servers with compromised accounts. UCE-PROTECT2 list does not normally list individual IP's but ranges of IP's where a certain threshold of IP's on that range have been detected as used by Spammers or a repeated pattern is observed. The general theory appears to be that in that case the range is more likely to be owned by Spammers or part of a network with the same problem, ie a range of Dialup IP Addresses etc. The range is usually 255 IP Addresses. UCE-PROTECT3 uses larger ranges where groups of smaller ranges have been detected. The UCE lists have the highest detection percentages of the individual lists tested. This can be the result of it's long history and/or great support by the public community. Typically between 50% and 60% of all IP's connecting to a mail server at ISP's will be on these lists. The surprising low unique count is probably that many IP addresses are listed on both their lists. The percentage and unique counts are expected to be higher if both lists were tested as one.

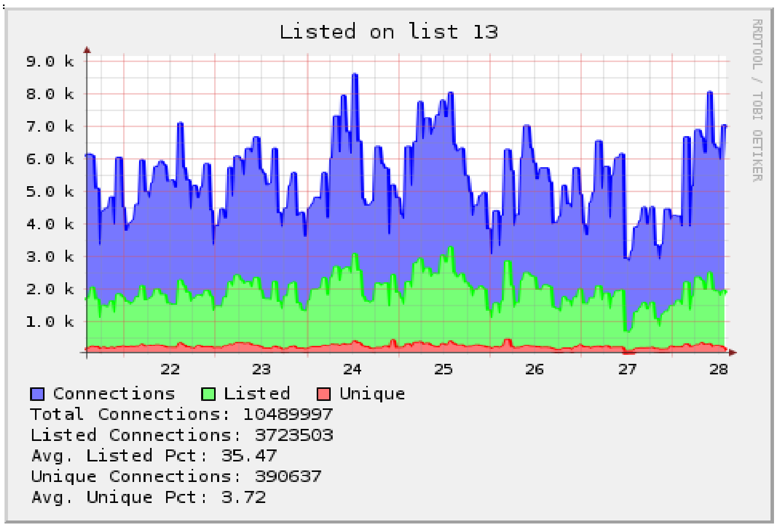
PSBL – PASSIVE SPAM BLOCK LIST (psbl.surriel.com)



Special Notes:

PSBL uses a much simpler mechanism. If you send to their 'Spam Traps' you will probably get listed. You can remove yourself easily if you are a legitimate email provider, and maybe just had a spam leakage problem, which you fixed; they try to 'white list' known good emails and good email servers and they expire their listings quickly to try and avoid false positives. It doesn't mean they don't get any false positives or accidental listings but it can be easily corrected and is not permanent. It is probably because of the quality of it's spam traps that it has such a good success rate and often catches IP addresses before anyone else. It's unique count alone is enough to justify it's use, and with between 30 and 40% detection rates in most ISP environments, that makes this 'recommended' if you want to use free IP reputation lists.

SORBS-DUL (www.sorbs.net)

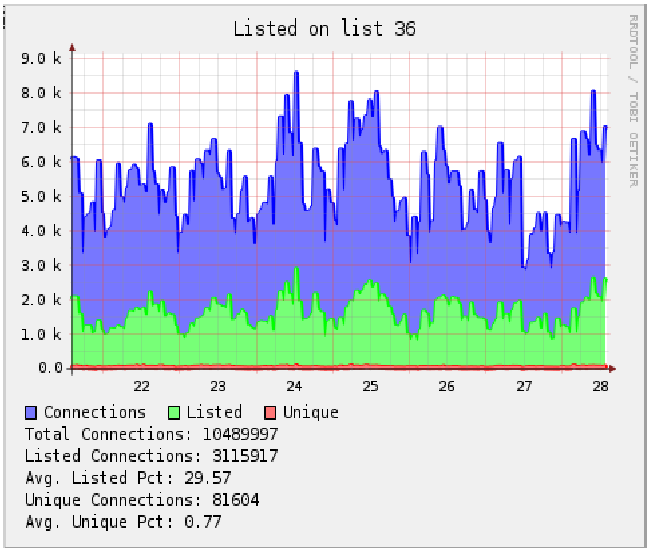


Special Notes:

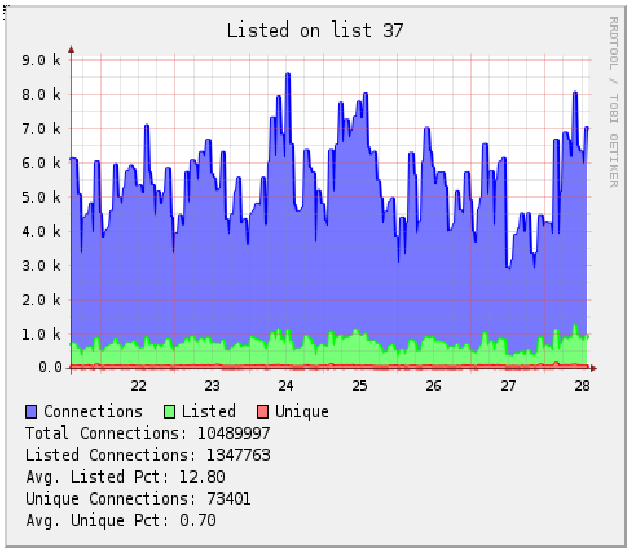
SORBS has a very long history, and has several different IP reputation lists based on different criteria. Some lists are used to list compromised servers, others to list open relays, mail servers with problems, or ISP's which leak spam. It is one of the more controversial lists in our examples, as some people have complained about some problems related to de-listing or removal processes, criteria for getting listed, and/or false positives on some of their lists. However this specific list, SORBS-DUL which is used to list 'DUL' IP addresses (Dynamic/Dialup) has seen very good results with minimal negative feedback, and can be considered when looking at IP reputation lists to use. With it's unique counts, and app. 35% blockage rates this can be a good addition to your arsenal.

(NOTICE: However, as with any IP reputation list, DUL Lists such as SORBS-DUL work best when used with a system to white list known good IP addresses as well as a system to make sure your own customer don't get stopped from sending email when they are the lists. Most mail servers can be configured to only check these lists for inbound connections from the outside world and not your own customers. SMTP authentication by your users should make these easier as well, so they can send email when they are on the road or at a remote location that might be on these DUL lists. Email servers should never be on this normally, unless they are using a network that is meant for DUL customers. Often the IP addresses will change for these networks, so an infected machine could have many different IP address for each time they boot up. And sometimes they will be wireless access points where any machine can log on, and be used in an attack, accidentally because they have been compromised, or intentionally. An infected laptop on such a network can quickly send out hundreds of thousands of attacks in a single day.)

SPAMRATS (RATS-DYNA and RATS-NOPTR www.spamrats.com)



🟦 Connections 🟩 Listed 🟥 Unique
Total Connections: 10489997
Listed Connections: 3115917
Avg. Listed Pct: 29.57
Unique Connections: 81604
Avg. Unique Pct: 0.77



🟦 Connections 🟩 Listed 🟥 Unique
Total Connections: 10489997
Listed Connections: 1347763
Avg. Listed Pct: 12.80
Unique Connections: 73401
Avg. Unique Pct: 0.70

Special Notes:

“SpamRats” has several lists as well, but for this study we have included only the 2 most effective ones. “SpamRats” is a relative newcomer to the IP reputation space, but in only 8 months they have created a highly successful database. RATS-DYNA and RATS-NOPTR owe their success to a unique data collection grid at ISP mail servers to detect IP addresses involved in abusive patterns, and then classifying them by type. RATS-DYNA is based on signatures that indicate the IP address is more likely to be an access point for PC's than an email server location. It checks to see if the sender or connection is not from a correctly configured mail server, according to 'Best Practices' documents for email operators before allowing the IP address to be collected, and in only 8 months have detected enough information to list app. 20 million IP Addresses as sources or potential sources of attackers that may be part of BotNet infections, or other forms of attack. They allow IP's to be easily deleted from the database in the case of false positives, provided the operator of an email server has set up their email server properly. The main difference between RATS-NOTPTR and RATS-DYNA is that the IP addresses of RATS-NOPTR have no reverse DNS. This is a requirement for most internet services to work properly, and especially for a mail server. Email from that location will be marked as Spam anyways by most technologies, so why let it into the server at all. RATS-DYNA uses pattern recognition and other tools, but in both cases reverse DNS is tested, which is not normally under the control of a BotNet owner/attacker, only the network owner and should be correctly configured in any case, so that if Spam does leak from that location, we know who the responsible party is to notify. This is a list to watch, blocking over 40% between the two lists already in less than 8 months of data collection.

Summary and Conclusions:

ANY operator of an email server should be able to block over 90% of all inbound connections using freely available IP reputation lists. And this is so important to stop attackers from stealing your customer list via dictionary attacks, as well as the cost savings. And as Sorbains/Oxsley and CALEA require more and more data retention of any email that you accept into your network, whether you mark it as Spam or not. And by adding a few simple extra tools like rate limiters, validation, and other controls that can be done at the connection level, there is no reason why you can't reach 95% blockage rates. It makes any final filtering you might want to apply so much easier, and less expensive. Some email filtering software may charge per message received or by volume, and by reducing that volume with little or no risk by 90% you can save even further money. And it will make a lot happier customers who have less 'Junk mail' to sort through in their quarantines. New forms of attacks are being made daily to thwart email filters, but they send it the same way they always have, and there are a limited number of IP addresses out there.

*Notice: There are other IP reputation lists that are available and you might want to use some of those in 'test mode' as well. Some are 'pay for use', some are targeted at email marketing companies , companies that are not on most spam orientated IP reputation lists, but as email marketers start reaching up to 60% of inbound email** that passes other IP reputation checks and spam filters, IP Reputation is even extending to those.*

* * * * *

The information and statistics herein were gratefully provided LinuxMagic.

For more information about this press release, or other information provided, please contact the Sales and Marketing Manager, Howard Yu at (604) 589-0100, or email info@linuxmagic.com

LinuxMagic is a software development company, located in Vancouver, British Columbia.
Makers of the MagicMail Mail Servers for the telecommunications and Internet Services industry, LinuxMagic has been a member of the Canadian Anti-Spam Task Force, and a recognized leader in anti-spam and email technologies.

http://www.linuxmagic.com
http://magicmail.linuxmagic.com

For more information about the IP reputation lists described herein, visit..

SpamRats -- http://www.spamrats.com
SpamHaus -- http://www.spamhaus.org
SpamCop -- http://www.spamcop.net
UCE-Protect -- http://www.uceprotect.net
PSBL -- http://psbl.surriel.com
SORBS -- http://www.sorbs.net