

In The Boxing Ring



Network Box Technical News from Mark Webb-Johnson, CTO Network Box

IN THIS ISSUE

1. ON-GOING DEVELOPMENT

This month we continue to work behind-the-scenes in Box Office and NOC support systems (ready for new product feature launches in 2010Q3).

2. SPAM TRAPS

Submissions to spam@network-box.com system are useful, but real-time spam trap feeds are proving to be the most effective mechanism for being able to (a) improve accuracy of Network Box anti-spam, and (b) precisely measure the performance of the Network Box Anti-Spam solution.

3. JULY 2010 FEATURES

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBR3.0 customers.

3. JULY 2010 HINT

Our July hint relates to setting up a real-time spam trap feed with your local support NOC.

Welcome

Welcome to the July 2010 edition of 'In the Boxing Ring'. In June, we have continued to work behind-the-scenes on the new Box Office and NOC support systems (ready for new product feature launches in 2010Q3). More on this in the upcoming Q3 newsletters.

On page 2, we discuss how Network Box uses real-time spam traps. Submissions to spam@network-box.com system are useful, but real-time spam trap feeds are proving to be the most effective mechanism for being able to (a) improve accuracy of Network Box anti-spam, and (b) precisely measure the performance of the Network Box Anti-Spam solution. Spam traps are deployed by redirecting mail from unused mail boxes into a centralised spam trap. In this way, statistics can be automatically generated on the effectiveness of the solution, and spam samples which are currently undetected as such can be submitted, in real-time, to Network Box so that our security response teams can release protection signatures and heuristics as quickly and effectively as possible.

On page 3, we present the usual monthly hint (this month regarding how best to work with the NOC for deployment of a real-time spam trap), and outline the software updates delivered as part of this month's software release.

As usual, if you have any feedback, or comments, they are always appreciated. You can contact us here at HQ via eMail (nbhq@network-box.com). Or, drop by our office next time you are in town.

You can also keep in touch by following our Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
July 2010



Network Box Spam Traps



A Spam Trap is an email address (or domain) that always receives 100% spam.

Usually, such spam email is representative of other spam that the owner receives, and as such it is extremely useful in that it provides for:

- A straightforward mechanism for determining the effectiveness of an anti-spam solution. By analysing all the messages that come into the spam trap, the percentage of messages that are detected as spam is equivalent to the percentage accuracy of the anti-spam solution in detecting spam.
- A real-time stream of ‘misses’ (messages that are not identified as spam). By knowing that all such missed messages are indeed spam, the stream can be used to improve detection rates and in some cases to automatically raise signatures to detect future similar spams.

Network Box offers a Spam Trap facility, integrated into our eMail scanner technology. The Spam Trap works by monitoring a configured list of eMail addresses. Once an email arrives inbound to one of those addresses it is blacklisted as spam (as it is known to be spam) and then a copy transmitted (via eMail) to our centralised Spam Trap facility. This approach means we get the spam in real-time, while only requiring minimal resources on the customer box.

Once the spam eMails arrive at our centralised Spam Trap facility, they are analysed using exactly the same anti-spam technology and signatures rules as on customer boxes. The result of this scan is stored for statistical purposes. In addition, any missed spams are forwarded on to our Outbreak spam system for analysis and release of protection signatures, and any executable attachments are analysed for viruses (and suspicious attachments are forwarded on to our Outbreak virus system for further analysis).

The table opposite shows the results of the centralised Spam Trap analysis since January 2009. While we commit to 95%-98% accuracy, you can see that we are typically achieving an average 98%-99% accuracy in spam detection (on a monthly basis).

By being able to closely monitor the accuracy of our anti-spam solution, Network Box has implemented various alert triggers that escalate spam outbreaks to our security engineers. These include heuristics such as:

- Monitoring the overall spam accuracy, on an hourly basis, and alerting if it drops below 98%.
- Monitoring the digital fingerprints (such as message fragments, urls, email addresses, etc) of spam samples, and correlating these in real-time. If an increase of a particular fingerprint is detected, undetected as spam, engineers are alerted to respond.
- Comparing the rates of digital fingerprints (eg: past hour vs past day) and alerting engineers to changes.

These heuristics effectively alert our engineers to new mass spam outbreaks, and allow us to respond faster to the problem.

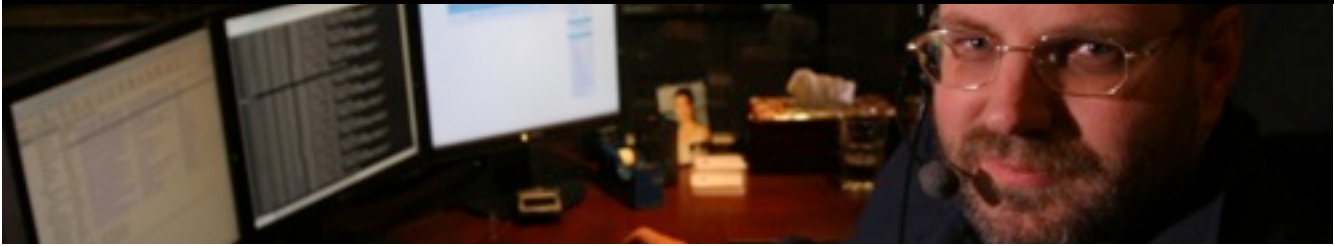
New Spam Traps are setup by identifying unused / incorrectly harvested candidate eMail addresses. With the customer permission, we then setup the trap on these addresses and redirect to a ‘cleansing’ address on our centralised system. We manually monitor that address for several months, to ensure that the Spam Trap is clean, and unsubscribe the address from any mailing lists or non-spam sources. Once the address is deemed clean, it is move it over to the live Spam Trap systems. This process is done with the customer co-operation, and requires little or no involvement.

The process of getting spam samples in real-time from Spam Traps is orders of magnitude better than the spam@network-box.com mechanism. The samples come in with better accuracy and in real-time (rather than delayed by several days) and allow us to better monitor and respond to new spam outbreaks (even those targeted at a single customer).

We currently operate several hundred spam traps, and always welcome new submissions.

Network Box Spam Trap Accuracy		
Month	Spam Accuracy *	% Viruses
January 2009	98.67%	1.39%
February 2009	99.12%	1.99%
March 2009	98.77%	1.78%
April 2009	99.24%	1.42%
May 2009	99.47%	0.21%
June 2009	98.89%	2.07%
July 2009	99.39%	1.19%
August 2009	99.10%	2.63%
September 2009	99.46%	3.12%
October 2009	99.55%	3.16%
November 2009	99.40%	2.14%
December 2009	99.22%	0.56%
January 2010	99.31%	0.88%
February 2010	99.21%	2.70%
March 2010	98.90%	0.83%
April 2010	98.24%	1.46%
May 2010	99.20%	0.79%
June 2010	99.37%	17.13% #

* Spam accuracy is percentage of emails (excluding viruses) detected as spam.
 # Increase due to a global outbreak of HTML script based email spams blocked as malicious viruses.



July 2010 Features



On Tuesday, 6th July 2010, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Further enhancements to the Box Office portal, related to service contracts and their visibility on customer views. We are conducting a phased deployment of our new customer contracts system, over the next two months, which will improve this further.
- A fix to the periodic PDF reporting system related to duplicate counts of spam emails marked but not quarantined on the Network Box. This affected customers not using spam quarantine, and has now been resolved.
- A fix to the my.network-box.com Mail Trace Message function to correctly show delivery status when the delivery date is outside the date range selected in the search.
- Support optional reporting of ISP information to the Global Monitoring System, to allow us to better benchmark ISP and Internet link performance.
- Improvements to the web proxy system to better cope with high workload situations.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

July Hint: Deploy a Spam Trap

As discussed on page 2 of this newsletter, Spam Traps are a very effective tool in the fight against spam. While we already operate several hundred of these traps (both in co-operation with existing customers, as well as our own addresses), we are always looking for new traps.

The process of getting spam samples in real-time from Spam Traps is orders of magnitude better than the spam@network-box.com mechanism. The samples come in with better accuracy and in real-time (rather than delayed by several days) and allow us to better monitor and respond to new spam outbreaks (even those targeted at a single customer).

If you have any old unused, or know of incorrectly harvested, eMail addresses, we recommend you to consider this as an option. The setup of a Spam Trap requires very little resources, and allows us to serve you better (as well as having the altruistic benefit of improving the anti-spam accuracy for all users of Network Box).

Please talk to your local support NOC to discuss how this can best be done for your organisation and how we can best serve your anti-spam requirements.

Mark Webb-Johnson,
CTO, Network Box Corporation

JUNE 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	694	-36.1
Signatures Released	185,792	-25.9
Firewall Blocks (/box)	708	+5.8
IDP Blocks (/box)	147,759	+4.9
Spams (/box)	53,830	+18.3
Malware (/box)	1,389	+104.0
URL Blocks (/box)	90,995	+18.0
URL Visits (/box)	3,585,910	+4.3

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley

Jason Law

Nick Jones

Production Support

Network Box Australia

Network Box Hong Kong

Network Box UK

Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com

or via mail at:

Network Box Corporation

16th Floor, Metro Loft,
38 Kwai Hei Street,

Kwai Chung, Hong Kong

Tel: +852 2736-2078

Fax: +852 2736-2778

www.network-box.com