

# In The Boxing Ring



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

### IN THIS ISSUE

#### 2 & 3.

#### **MAIL PORTAL & MY.NETWORK-BOX.COM ENHANCEMENTS**

Now out of public beta, the new Mail Portal and MY.NETWORK-BOX.COM systems are being deployed globally. The new systems are 3 to 5 times faster for common operations and support a revised workflow (including tick-to-release). More options are now available to give the user finer control over the appearance of their reports. The reports can now be ordered by spam score (as an alternative to the received time of the email).

#### 4.

#### **SEPTEMBER 2009 FEATURES**

We will be globally releasing the enhanced Mail Portal and MY.NETWORK-BOX.COM systems, and also the ongoing deployment of our recently released features and enhancements.

#### 4.

#### **MICROSOFT MAPP**

Network Box has joined the Microsoft Active Protections Program (MAPP), and will be provided with vulnerability information in advance of Microsoft's monthly security update release to offer protections to customers efficiently and effectively.

### Welcome

Welcome to the September 2009 edition of 'In the Boxing Ring'. In this edition, we focus on the global release of the enhanced Mail Portal user and MY.NETWORK-BOX.COM administrative systems. These new features offer improvements in both performance and usability, as well as to the interface for key administrative functions. These new systems (together with the revised Mail Portal User and MY.NETWORK-BOX.COM Administrative Guides) are being globally released this month. Turn to Pages 2 and 3 for details.

Network Box statistics show that 92.43% of our customer base is using Microsoft Windows on their workstations and servers. Within the Microsoft Windows user base, 59% use XP and 25% Vista. This month, we're excited to

be able to announce a new technology partnership between Network Box security response teams and Microsoft under their MAPP program. Turn to Page 4 for further details.

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](mailto:nbhq@network-box.com)). Or, drop by our office next time you are in town.

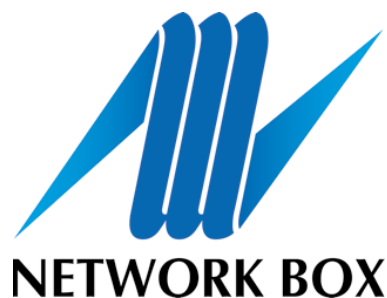
You can also keep in touch by following our new Network Box Security Response twitter feed at:

**[twitter.com/networkboxhq](https://twitter.com/networkboxhq)**

Mark Webb-Johnson

CTO, Network Box Corporation

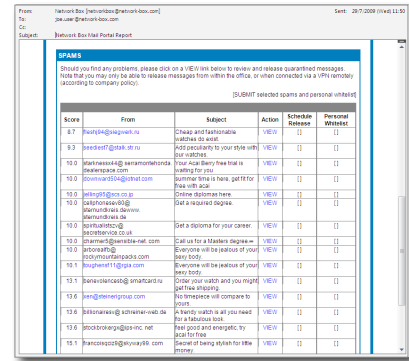
September 2009





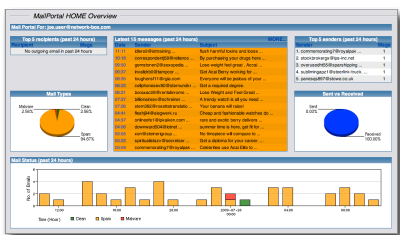
# Mail Portal & MY.NETWORK-BOX.COM Enhancements

In last month's *In the Boxing Ring*, the Mail Portal and MY.NETWORK-BOX.COM were still in beta and we highlighted the enhancements made to both systems — both technical and aesthetic.



Now with both systems out of public beta and deploying globally, the new Mail Portal and MY.NETWORK-BOX.COM systems are 3 to 5 times faster for common operations and support a revised workflow (including tick-to-release). The administrator now can also support the user through the MY.NETWORK-BOX.COM interface as well as through the Mail Portal. More options are now available to give the user finer control over the appearance of his reports. The reports can be sorted by spam score (as an alternative to the received time of the email).

## Mail Portal



As a quick reminder, the homepage of the Mail Portal has been simplified while the search function now includes a *Specify Period* option.

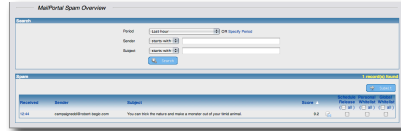
Other improvements included icons indicating whether emails were



*Quarantined, Not Quarantined, or Released.*

Specifically, the major change in the Mail Portal was to the *Anti-Spam Overview* section: the following areas were improved prior to global deployment:

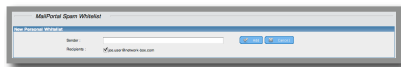
### ANTI-SPAM > OVERVIEW



By default, the *Overview* provides an hourly summary of the the spams received and the score for each spam. Using the pull-down menu, the user can select the range of information they want to review.

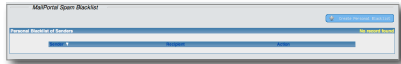
Previously, this section did not offer users the choice of sorting information by spam score: the lower the score, the more likely the mail is genuine; conversely, the higher the spam score, the more probably the mail is spam.

### ANTI-SPAM > WHITELIST



As before, the white list allows users to enter the *Sender* name and select the intended *Recipients* via checkboxes.

### ANTI-SPAM > BLACKLIST



In the same vein as the *Whitelist*, the *Blacklist* functionality allows users to add the *Sender* name and choose the *Recipients* who should not be receiving the specified sender's emails.

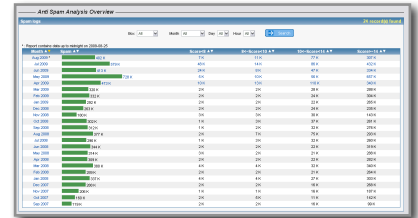
Much of this month's enhancements were, however, made to the MY.NETWORK-BOX.COM system:

## MY.NETWORK-BOX.COM

All the enhancements to both the Mail Portal and MY.NETWORK-BOX.COM systems not only improved their functionality, speed and responsiveness, they have also helped make it possible for the Administrator to help the user manage their mail account via the MY.NETWORK-BOX.COM interface.

The major changes within the MY.NETWORK-BOX.COM system are in the management of spam and viruses in the *Anti-Spam* and *Anti-Virus* sections.

### ANTI-SPAM > ANALYSIS > OVERVIEW



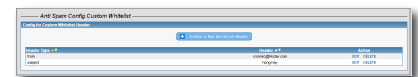
Those emails that contain viruses may have originated from known senders, but the emails' risk to users has resulted in the emails' quarantine.

Individually managing all emails in this list is time-consuming and requires unnecessary effort. To facilitate the management of the *Release Quarantine* list, we have implemented a *Release (all)* functionality.

The *Overview* provides a monthly summary of the number of spams received and the number of emails that fall into each Spam Score range.

Previously, this section did not offer the Administrator the choice of sorting information by spam score. To correct that oversight and provide more flexibility, users can now sort received spam by spam score: the lower the score, the more likely the mail is genuine; conversely, the higher the spam score, the more probably the mail is spam.

### ANTI-SPAM > CONFIG > CUSTOM WHITELIST

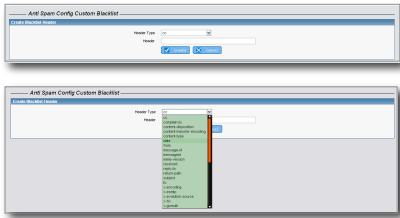


The customisable white list allows the Administrator to enter the *Header*, *Sender* and *Body* information of email types that you wish to receive across the company.

### ANTI-SPAM > CONFIG > CUSTOM BLACKLIST

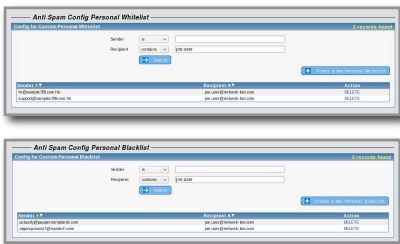
In the same vein as the customisable white list option, the customisable blacklist functionality provides users with

more control over which and whose emails they elect to block across the company. Again, you can enter the *header*, *Sender* and *Body* information of email types that you do not wish to receive.



**ANTI-SPAM > CONFIG > PERSONAL WHITELIST / BLACKLIST**

However, while the *Custom Whitelist* and *Blacklist* are company-wide, the *Personal Whitelist* and *Personal Blacklist* are users-centric and do not influence the wider corporate list.

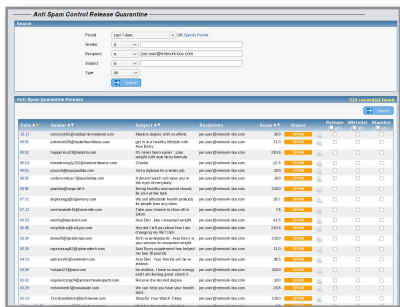


Here, the Administrator can search for the *Sender* or *Recipient* information that they require.

If the *Sender* or *Recipient* is not found in the database, or does not yet exist, the Administrator can *Create a New Personal Whitelist* or *Blacklist*.

To help clean up the personal whitelist or blacklist, the Administrator can help delete the record.

**ANTI-SPAM > CONTROL > RELEASE QUARANTINE**



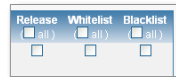
To facilitate the management of Spam in the *Release Quarantine* section, we have reorganised the columns to provide

more meaningful data to the Administrator. You can now sort by *Date*, *Sender*, *Subject*, *Recipients* and *Score*. Clicking on the time in the *Date* column will bring up more information about that particular spam email.

Each email is colour-coded in the *Status* column: Spam is Orange, Virus is Red and Clean Emails are White.

Included in the *Status* column are the Status Icons, denoting *Quarantined*, *Not Quarantined* or *Released*.

In managing the list of email, you can select individual emails, or *Select All*, also known as *tick-to-release*. Instead of just selecting emails to release to the recipient(s), you can now choose whether to *Release* all or some of the emails to the recipient, *Whitelist* or *Blacklist* the email; you can also choose all three *Release Quarantine* options.

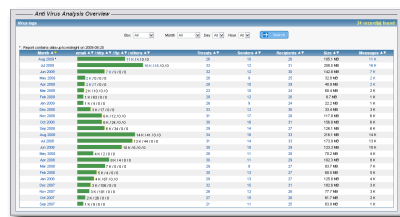


The *Release Quarantine* functionality allows the Administrator to search for a specific email or a set of emails within a certain period, and also to release the emails individually or all at once.

And to help clean up the personal whitelist or blacklist, the Administrator can help delete any record(s) as required.

The Administrator can also release spam from quarantine on request.

**ANTI-VIRUS > ANALYSIS > OVERVIEW**

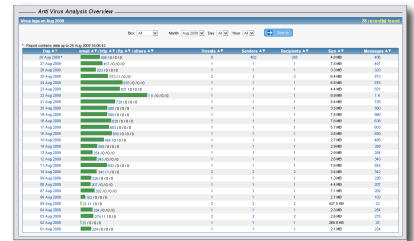


With the new interface, the *Anti-Virus Analysis Overview* provides at-a-glance information via a bar chart. The graph shows the number of viruses detected and blocked in each month.

A closer inspection of the interface reveals a slight reorganisation of the columns and some renaming to further clarify what is being shown. In addition, the Administrator can sort data according to each column.

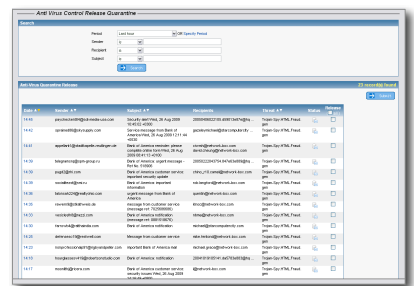
Most useful is the second column where you can view how the virus reached your network: Email, HTTP, FTP or Others.

Clicking the month in the *Month* column brings up the daily records of the number of viruses detected and blocked on any given day within that month.



A search function also allows the Administrator to specify a time period and the Box ID when searching for particular sets of emails, or any one email.

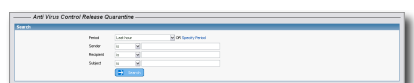
**ANTI-VIRUS > CONTROL > RELEASE / QUARANTINE**



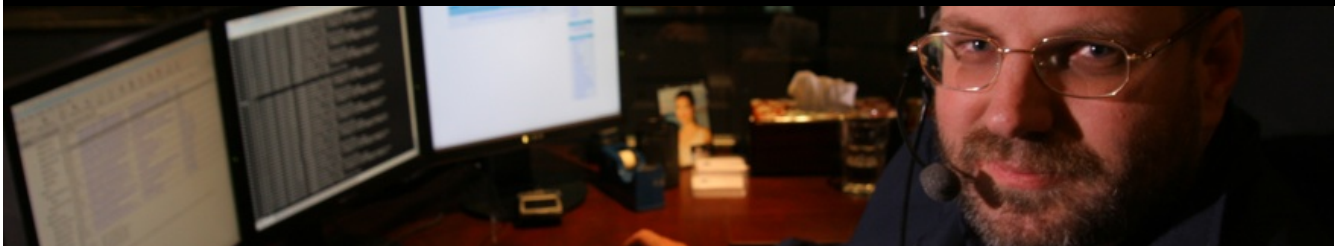
Those emails that contain viruses may have originated from known senders, but the emails' risk to users has resulted in the emails' quarantine.

Individually managing all emails in this list is time-consuming and requires unnecessary effort. To facilitate the management of the *Release Quarantine* list, we have implemented a *Release (all)* functionality.

As with the *Anti-Spam* functionality, the *Anti-Virus Control Release Quarantine* functionality allows the Administrator to search for a specific email or a set of emails within a certain period, and also to release the emails individually or all at once.



Both the Mail Portal and MYNETWORK-BOX.COM systems will be globally deployed on 2 September 2009.



**September 2009 Features**

On Tuesday, 1 September 2009, we will be globally releasing the enhanced Mail Portal and MY.NETWORK-BOX.COM systems. These new systems offer improvements in both performance and usability, as well as to the interface for key administrative functions.

We will also be releasing some further enhancements to our mail scanning systems, including:

- More options for aggressively handling bounce (NDR) messages.
- Improvements to the handling of HTML text sections in email, particularly regarding anti-spam analysis.
- Revisions to the email relationships system to make it SPF aware.

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. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

**Microsoft MAPP**

Network Box has joined the Microsoft Active Protections Program (MAPP), and will be provided with vulnerability information in advance of Microsoft’s monthly security update release to offer protections to customers efficiently and effectively.

We plan to roll-out our support of this in two phases:

Commencing with Microsoft Patch Tuesday, 8 September 2009, Network Box will be releasing a new security bulletin synchronised to Microsoft’s own Patch Tuesday bulletins. This bulletin will summarise the latest vulnerabilities, how they affect our customer base, our recommendations and what protections Network Box has in place to assist our customers with these new issues.

Starting with Microsoft Patch Tuesday, 14 October 2009, Network Box will be releasing activate protections synchronised to Microsoft’s MAPP program and Microsoft Patch Tuesday.

By Network Box receiving vulnerability information earlier, customers benefit from additional possible improvements that provide security protection, such as, Active Intrusion Detection and Prevention, as a part of the Network Box managed UTM+ services.

For more information on Network Box and MAPP, please visit <http://www.network-box.com/managedservice/mapp>.

Mark Webb-Johnson  
CTO, Network Box Corporation  
September 2009

**AUGUST 2009 NUMBERS**

Key Metric)	#	% difference (since last month)
PUSH Updates	1,487	+48.9
Signatures Released	414,475	+243.1
Firewall Blocks (/box)	633,205	+1.4
IDP Blocks (/box)	194,931	+7.2
Spams (/box)	63,694	-10.4
Malware (/box)	2,124	-32.5
URL Blocks (/box)	116,654	+11.0
URL Visits (/box)	3,182,389	+6.8

**NEWSLETTER STAFF**

**Mark Webb-Johnson**  
Editor

**Pauline Chiu**

**Michael Gazeley**

**Jason Law**

**Nick Jones**

Production Support

**Network Box Australia**

**Network Box Hong Kong**

**Network Box UK**

**SUBSCRIPTION**

Network Box Corporation  
[nbhq@network-box.com](mailto: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](http://www.network-box.com)