

In The Boxing Ring



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

Welcome

Welcome to the August 2009 edition of 'In the Boxing Ring'. In this edition, we focus on the enhancements made to the Network Box Mail Portal. Chief among the changes is the increased speed and a tidier user interface. Also tweaked were the workflow, and complementary Mail Report. Turn to Page 2 for details.

Page 3 details enhancements made to the Mail Scanning system. We also provide information on recent vulnerabilities announced by Adobe and Microsoft.

In our August features, we have the usual allotment of updates to the NBRS-3.0 system, and enhancements to the scanning engine, revisions to the email relationships system and components to further support the Mail Portal system.

We also have some core component updates to address recently-announced vulnerabilities. Turn to Page 4.

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 new Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation

August 2009

IN THIS ISSUE

2. MAIL PORTAL ENHANCEMENTS

The Mail Portal is undergoing a public beta of revisions. It is now 3 to 5 times faster for common operations and supports a revised workflow (including 'tick-to-release' on the Web interface). More options are now available, giving the user finer control over the appearance of reports. The reports can be ordered by Spam Score (as an alternative to the received time of the email).

3. MAIL SCANNING ENHANCEMENTS

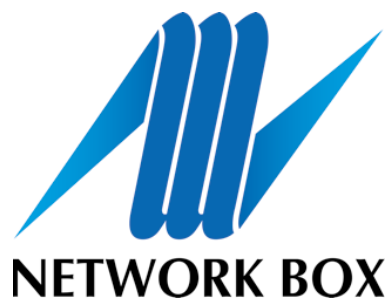
This month there are three major enhancements to the system: Relationship Age and Count Score; SPF Aware Whitelists; and Own Domain Protection for Whitelisting.

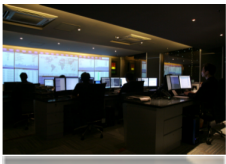
3. RECENT VULNERABILITIES

The announcement of an unusually large number of zero-day vulnerabilities has kept Network Box Security Response at Threat Level Alert Condition #4 for almost a month.

4. AUGUST 2009 FEATURES

The ongoing deployment of our recently released features and enhancements.





Mail Portal Enhancements

Even though the Network Box Mail Portal went live two years ago, we have continued making improvements to the system: it is now 3 to 5 times faster, particularly when searching; and also has a simplified and more user-friendly home page, as well as clarified presentation of data in various sections and improved workflow.

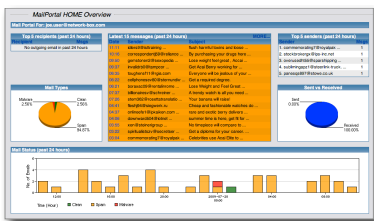


Figure 1 – Home Page

On the home page gone are the lists of *Latest Spam* and *Latest Malware*. Instead, these can be found in their respective sections. The simplified home page now presents:

- Top 5 email senders in the last 24 hours,
- Top 5 email recipients in the last 24 hours
- Latest 15 messages sent in the same period,
- Type of mail (pie chart)
- Sent emails against received emails (pie chart), and
- Mail status for the past 24 hours (bar graph)

Clicking the time in the *Date* column on the list, *Latest 15 messages (past 24 hours)*, will take you to a screen that provides more information on that particular email (also viewable from the *Spam* section).



Figure 2 – Mail Search: Specify Period

For the *Mail* section, the first obvious change is the additional *Specify Period* option for *Search*.

The *Search Results* table has also undergone some house cleaning; we have retitled the columns to be more descriptive – *Received*, *Sender*, *Subject*, *Type*

and *Status* – and added *Status* icons to show if the email is *Quarantined*, *Not Quarantined* or *Released*. All emails also have a colour-coded background letting users know that orange means Spam, red is virus and white is okay.

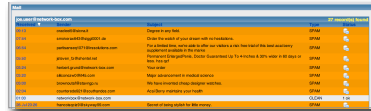


Figure 3 – Mail: Column Titles



Figure 4 – Icons: Quarantined; Not Quarantined; Released

In the *Spam* section, the overview interface has been given a face-lift, particularly in ease of use. For instance, as for the *Mail* section, we expanded the *Search* functionality to include *Specify Period*; *Search* is also faster now.

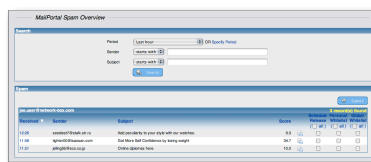


Figure 5 – Spam: Overview

Email scanning time has been reduced to help improve the system's speed. The scanning engine reports whether or not a virus is present.

We have also added *Spam Status* icons and a *Select All* ('tick-to-release') functionality for each column to save on time and effort. In addition, you can click the time in the *Received* column to view details of the selected email.

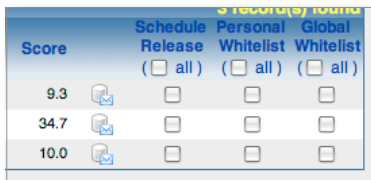


Figure 6 – Select All

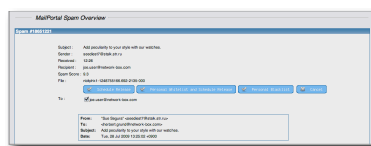


Figure 7 – Spam: Detailed View

The detailed information screen of the selected email also presents data in a

simplified format. Primary information that the user needs to determine whether or not the email is Spam are:

- *Subject*
- *Sender*
- Time the email was *Received*
- *Recipient* and
- *Spam Score*.

More changes have also been implemented in the *Settings* section of the Mail Portal. You are now able to select your own mail client using the pull-down menu next to *Mail Client*. Options currently available include:

- Microsoft Outlook 2007 or later
- Lotus Notes 6.5 or older and
- Other Email Reader



Figure 8 – Settings: Overview

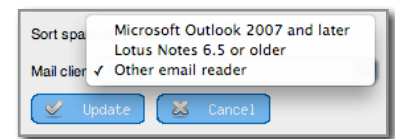


Figure 9 – Settings: Email Client

For this phase's improvements, we have also made aesthetic enhancements found in the accompanying Mail Report: *Malware* is now listed first. And to help you determine if the flagged email is truly Spam, you can also set your Mail Report to list the Spam emails by ascending / descending Score.

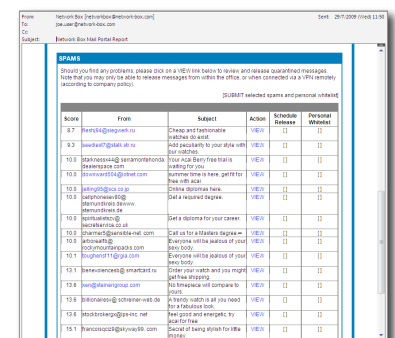


Figure 10 – Mail Report: Listing by Spam Score

The beta software will be available on August Patch Tuesday with a full release targeted for the September Patch Tuesday.



Mail Scanning Enhancements

This month, we are releasing three significant enhancements for our Mail Scanning engines:

1. Relationship Age and Count Score (for Spam Score Adjustment)

Looking at the feedback from the past six months of live deployments of the Network Box eMail Relationship technology, we've implemented an improvement to the algorithm to account for relationship age and activity volume. This can now be used to strengthen (or weaken) an established relationship, based on the two new factors:

- The age of the relationship
- The number of email messages exchanged

2. SPF Aware Whitelists

We've implemented an extension to our whitelisting system to allow whitelists to be fine-tuned according to whether an SPF (Sender Policy Framework) test passed or failed.

After implementing this optional system:

- Failed SPF whitelisted senders will not be whitelisted
- Neutral SPF whitelisted senders will be treated as less likely to be spam (but not whitelisted)
- Passed SPF whitelisted senders will be whitelisted as usual

3. Own Domain Protection for Whitelisting

This optional mechanism now allows the whitelist of a domain to be suppressed if the sender and recipient are in the same domain. In such cases, a negative spam score can also be applied, to make the message more likely to be treated as not spam.

All three of these new features will be released, and available, on Patch Tuesday, 4 August 2009.



Recent Vulnerabilities

This month, an unusually large number of zero-day vulnerabilities have been announced, and patches released. Here is a short summary of the major ones.

Vulnerability in Microsoft Video ActiveX Control Could Allow Remote Code Execution

Microsoft Security Advisory 972890

A zero-day vulnerability in the msvidctl.dll component of Microsoft Video ActiveX. There were widespread attacks exploiting this vulnerability using a large network of compromised websites. The attacks used Internet Explorer as the attack vector and installed a Trojan downloader onto compromised machines. Microsoft released a partial fix on their July Patch Tuesday, but this was later shown to be ineffectual and protection was revised in the Microsoft July 28 out-of-cycle release.

Vulnerability in Microsoft Office Web Components ActiveX Controls Could Allow Remote Code Execution

Microsoft Security Advisory 973472

A zero-day vulnerability in Microsoft Office Web Components ActiveX controls. There were originally limited targeted attacks exploiting this vulnerability using a network of compromised websites, but as expected, the scale of the attacks continues to grow. The attacks used Internet Explorer as the attack vector and installed a Trojan downloader onto compromised machines.

Adobe Flash-in-PDF Attacks

Adobe Security Advisory APSA-09-03

Later in July, Network Box Security Response started to see exploits of a zero-day flaw in Adobe Flash Player 9 and 10, with the exploit delivered by a flash object embedded in an Adobe PDF document (rendered by Adobe PDF Reader / Acrobat). The flaw was acknowledged by Adobe (and labelled CVE-2009-1862). Adobe proposed a workaround (involving the manual deletion of the affected

component) and scheduled to release patches on July 30.

Sun Java XML Signature HMAC Truncation Authentication Bypass

US-CERT Vulnerability Note VU#466161

Sun announced a vulnerability that would allow an attacker to bypass the authentication mechanism provided by the XML Signature specification. Patches were released.

Microsoft Out-of-Cycle Patch 28th July MS09-034 and MS09-035

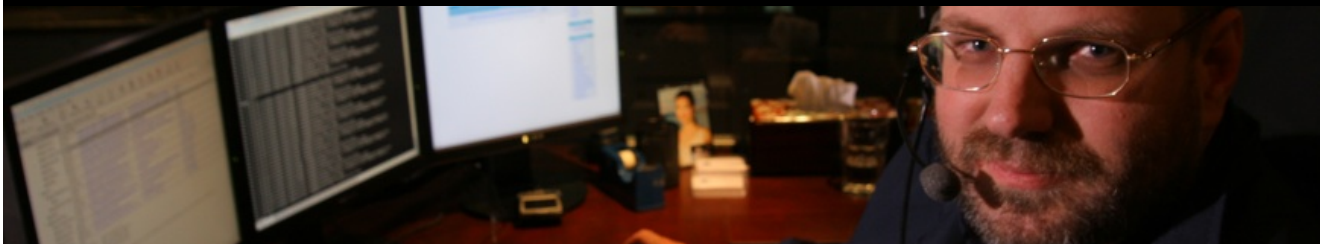
Following on from their work on the ActiveX control vulnerabilities, Microsoft announced that the cause of these vulnerabilities was far deeper than originally expected, and went to the unusual step of releasing out-of-cycle patches for both Internet Explorer and development libraries used by third parties. The patches were released on 28 July, but third parties may take some time to incorporate the changes in their code.

BIND Dynamic Update DoS

CVE-2009-0696 / CERT VU#725188

Following disclosure on a Debian bug-tracking system, the ISC has released urgent patches to their BIND DNS name server code. Exploitation of this vulnerability would result in a crash of the DNS server, and could lead to a Denial of Service (DoS). Analysis by Network Box Security Response and others indicate that this is not currently exploitable to gain remote access. However, the attack is possible against vulnerable ISC BIND DNS servers hosting MASTER zones (i.e., slave-zone-only DNS servers are not affected by this). Network Box, and several other vendors, released patches and protection signatures / instructions.

Overall, it has been an incredible month, and has kept Network Box Security Response at Threat Level Alert Condition #4 for almost the whole month. We, and our OEM partners, have pushed out over 350 signatures, as well as two out-of-cycle patches, specifically to protect against exploitation of these vulnerabilities. We continue to closely monitor the situation.



August 2009 Features

On Tuesday, 4 August 2009, we will be releasing a number of improvements to the mail scanning system. These enhancements include:

- Revisions to the email relationships system to track relationship age and activity
- Integration of SPF to whitelisting (to allow whitelisting to be controlled by successful SPF)
- Own domain protection (protection of whitelisted messages to/from the same domain), and
- Other miscellaneous improvements

We will also release the foundational components to support the new Mail Portal system entering beta this month.

Additional releases are updates to some of our core components to address recently-announced vulnerabilities. These updates include:

- DNS resolution
- DHCP, and
- Web Server

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. 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.

August Hint

In February’s “In the Boxing Ring”, we highlighted a new and powerful anti-spam technology based on email relationships.

The system monitors your SMTP email traffic and builds a statistical database of relationships between the senders and recipients. When your Network Box scans a new message, the system accounts for the previous history and relationship strength of the sender and recipient pair, IP address and domain. It then adjusts the score based on these important parameters. These eMail relationships can also be combined with Challenge/Response for a close-to-100%-accurate anti-spam system.

Together with the new SPF and whitelist integration, plus own-domain-protection features released this month, it is time to re-visit and implement a challenge-response system (if you haven’t already).

Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager. Please don't hesitate to contact us for assistance.

Mark Webb-Johnson
 CTO, Network Box Corporation
 August 2009

JULY 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	998	-7.8
Signatures Released	170,469	-16.7
Firewall Blocks (/box)	624,287	-2.0
IDP Blocks (/box)	181,789	+15.4
Spams (/box)	71,075	-2.8
Malware (/box)	3,148	+42.1
URL Blocks (/box)	105,091	+27.5
URL Visits (/box)	2,979,650	-3.3

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
 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