

In The Boxing Ring



IN THIS ISSUE

1.

WELCOME

The December 2010 'In The Boxing Ring' newsletter.

2.

NESTED '.BIN' BLOCKS

With the growth in migration to office 2007 file formats, we have seen an increasing number of policy blocks on nested '.bin' file extensions.

3.

BOX OFFICE NOTIFICATIONS

We revisit the topic of Box Office Notifications (that we deployed last month)

3.

KASPERSKY V8

We present our latest anti-virus engine update - Kaspersky v8. This update is in its final month before global deployment, with a scheduled global release on the January 2011 Patch Tuesday.

4.

DECEMBER 2010 FEATURES AND HINT

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBR3-3.0 customers.

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

Welcome

Welcome to the December 2010 edition of 'In the Boxing Ring'.

This month, we devote a full page 2 to the topic of policy blocks on nested '.bin' file extensions. With the growth in migration to office 2007 file formats, we have seen an increasing number of these blocks, and feedback from NOCs is that there is confusion amongst our customer base on what these are and how to avoid them. This article should help to clarify the purpose of these blocks and how they should be effectively used for policy enforcement.

On page 3, we revisit the topic of Box Office Notifications (that we deployed last month). The new system is working well, but only about 1/5th of our customers appear to be using it to its full potential. In this article, we concentrate on two aspects of the system (notification methods and time-based control) to help you to better use this new facility.

Also on page 3, we present our latest anti-virus engine update - Kaspersky v8. This update is in its final month before

global deployment, with a scheduled global release on the January 2011 Patch Tuesday.

On page 4, we present our monthly hint (this month on the importance of effective policy configuration), 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
December 2010





Nested '.bin' Blocks and Office 2007

Network Box offers two optional facilities for blocking of eMail attachments:

1. File Extension Blocking (based on the last extension of the filename of attached files).
2. File Content Blocking (based on analysis of file content type).

Each of these policies can be applied to both standard attachments, and attachments within archives (such as ZIP format files). The usual filters can also be applied (e.g.; exempted senders, inbound mail only, etc). The default behavior of Network Box is not to apply any such restrictions, unless explicitly configured (under customer instructions) to do so.

A large proportion of our customers use these policy blocks to restrict executable attachments coming into their networks (irrespective of the result of anti-virus scans). Often, the (configurable) list of file extensions to block include '.com', '.exe', '.pif', '.scr', '.bin' and others.

The problem

This has worked for many years, with little false positives. However, with their release of Office 2007, Microsoft have started to use a new document format (with extensions '.xlsx', '.docx', etc). As this article explains:

<http://www.arstdesign.com/articles/office2007bin.html>

the new Microsoft format is actually just the ZIP file format, and it is not possible to differentiate between the two. A Microsoft document and a ZIP archive are one and the same.

This is made problematic by the fact that Microsoft Office 2007 programs sometimes write printer settings files, Macros, and other such objects with the '.bin' extension (eg; vbaProject.bin, printerSettingsxxx.bin, etc), and if the customer has chosen to blocked nested (ie; within archives) '.bin' files, these Microsoft Office 2007 documents will be blocked as per company policy.

A suggested solution is to have an exception for nested '.bin' files, if the container is an Office 2007 document. As we've explained, there is no way to tell a Microsoft Office document apart from a ZIP archive, except by file extension (eg; '.docx', '.xlsx', '.pptx', etc), and Network Box does offer such an option. However, this is not 100%, as:

- Sometimes, the sender may not name the document with one of the standard extensions.
- Sometimes, the sender will be using a non-English system, and that will result in non-English character set filenames that encode these extensions in hundreds of different formats.
- Such an arrangement could lead to policy bypass - a malicious sender could just name their ZIP archive 'sample.docx' and bypass the extension policy.

The solution

As has been shown opposite, the solution is not easy. There is no 100% effective way to differentiate Office 2007 documents from ZIP archives, and thus no way to exclude '.bin' files in Office 2007 documents from such a policy (and given the use of '.bin' for Macros, embedded objects, etc in Office 2007, it is debatable whether they constitute executable content anyway). But, let's take a step back and think about why we are blocking '.bin' files in the first place.

1. Looking at current lists of possible executable extensions (eg; <http://antivirus.about.com/od/securitytips/a/fileextview.htm>), we don't even see '.bin' listed. It used to be used (in the early days of windows), but that is no longer the case with modern operating systems and applications. A simple solution is to just remove '.bin' from the list of extensions to block.
2. Years ago, operating systems decided which application to launch when a file was clicked by the file extensions. Nowadays, it is common for operating systems to use file content analysis, or mime types, to make the decision. If the goal is to block executable attachments, it is generally more effective to use Network Box file content blocks (either mime or file type) to block executables that to blindly rely on the file extension (which is effectively just a comment, nowadays).
3. As all attachments (including those within archives) are thoroughly scanned by all the engines of the Network Box mail scanning Anti-Virus system, policy extension blocks against executable content, are useful but not essential (especially when they are causing unwanted policy blocks).

The recommendation

Given the problem with Office 2007 documents and nested '.bin' policy blocks, Network Box Security Response recommends that customers don't just blindly block nested '.bin' attachments.

- For customers that don't require executable attachment blocks, turn them off or at least remove '.bin' from the list of extensions to be blocked for nested attachments.
- For customers that do require executable attachment blocks, implement a multi-defence approach - block known executable file extensions (but not '.bin') but also block by content analysis (primarily Microsoft executable content).

The above approaches will improve overall security, while avoiding unintended blocks of nested '.bin' files.

As usual, please discuss this with your regional NOC, who are there to help you effectively implement your policies.



Box Office Notifications

The Network Box Office Notifications system was released on the November 2010 Patch Tuesday, and since then we've seen approximately 1/5th of our customers customise it beyond the defaults provided, with more non-default changes being made day by day. In this article, we concentrate on two aspects of the system to help you to better use this new facility.

1. Notification Methods

Notification methods are mechanisms used to deliver a notification to you. When we deployed the Box Office Notification system, we migrated your existing 'want ticket email' setting into a default eMail-type notification (so that you can continue to receive notifications). However, you can (and should) extend this default behavior. Here are some ideas:

What is the arrangement if your Network Box or mail server becomes unreachable and there is a problem outside office hours? By creating another out-of-office notification eMail address (for example, with a gmail or other such external email address), you can continue to receive notifications even if your internal mail system is not reachable/functioning.

If you have an Apple iOS device, installing and logging in to the Network Box iOS App will create an iOS PUSH Notification helper that will use Apple's notification service to deliver alerts to you.

We also offer the SMS notification method, for delivering SMS alerts directly to your phone.

2. Time Based Control

Each notification contact point you create can have filters attached to restrict notifications to limited time ranges. For example, you probably want your out-of-office notification contact point to only be active out-of-office-hours (which you can do by configuring notifications to only be sent Mon-Fri 09:00->18:00).

Note that on your Box Office My Account page, there is a Time Zone setting. This defaults to UTC, but you can set it to the closest time zone to you, and the rest of Box Office will change to show dates/times in your desired time zone (even if the box or NOC is in a different time zone).

The Box Office Customer Portal manual (downloadable by clicking HELP at the top right of Box Office) is available for your reference, and we encourage you to investigate the options available for notifications.



Kaspersky v8

In co-operation with Kaspersky Lab, Network Box is pleased to announce that we will shortly be releasing a free-of-charge upgrade to all our NBR3-3.0 customers to the new v8 Kaspersky engine.

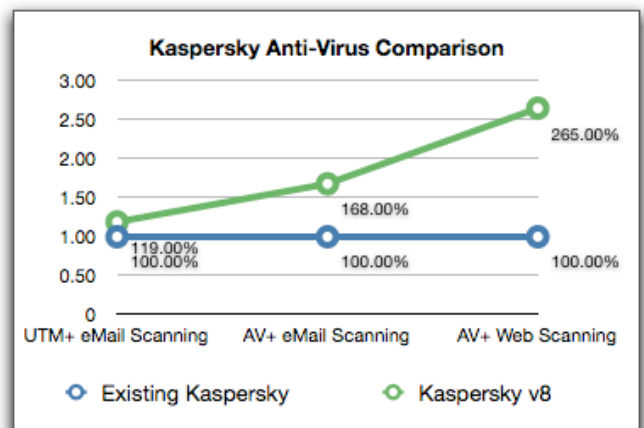
This new v8 engine is the same engine as used in Kaspersky desktop and server products (on Windows and Linux), but is optimised for use at the gateway. As well as welcome performance and memory improvements, the engine brings improved heuristic detection capabilities and application sand-boxing technologies.

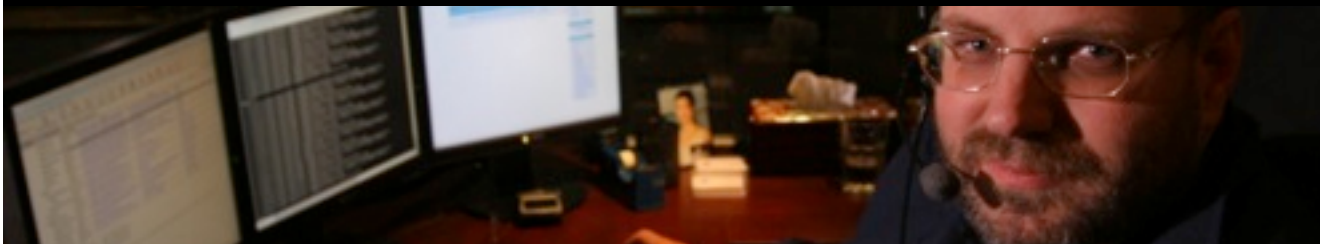
As part of our extensive testing of the new engine, we conducted extensive performance and memory usage tests. We are pleased to say that the new engine gave us an average 19% performance boost for UTM+ mail scanning, 68% for AV+ mail scanning, and an impressive 165% for AV+ web scanning - more than 1.65 times as fast for scanning web traffic when compared to the existing version.

All this, while improving detection capabilities and reducing memory and other resource consumption - the new Kaspersky engine currently requires 30% less flash space for signatures, and uses under half the RAM of its predecessor.

The new Kaspersky engine will be released to all customers on the upcoming January 2011 Patch Tuesday, and the plan is to complete migration of all existing customers to it within two weeks of that date.

The new engine is, however, complete and ready to go, and limited deployment has already started. We are offering this as an early option to all customers, starting from the December 2010 Patch Tuesday.





December 2010 Features



This month, we emphasise our continued work on the Network Box Global Monitoring System, and Box Office integration. There will be minimal changes to the box firmware itself. While the Box

Office changes will be deployed on the Patch Tuesday itself, NOCs will be conducting staged releases of device firmware updates over the next 7 days. The changes include:

- Enhancements to the health reporting system, particularly regarding reporting of large health metrics.
- Enhancements to NTP monitoring and synchronisation.
- Relaxing of temperature sensor sensitivity on some S-series models.
- Relaxing of case fan sensor sensitivity on M-385 model.
- Geo IP updates (for more accurate mapping of IP address to geographic location).
- Improvements to GMS reachability criteria and monitoring of passive (not actively reachable) network boxes.
- Improvements to information presentation in GMS tickets within Network Box Office.

The above changes should not require a device restart, but may impact running services at some sites, so NOCs may contact affected customers to schedule a deployment timeframe.

The enhancement work will be handled by the regional NOCs and will not require any action on your part. Only minimal service interruption is expected to be required.

December Hint: Organisational Policy

As discussed on page 2 of this newsletter, your organisation policy is defined by you, configured by Network NOC engineers, and enforced by the Network Box devices protecting your network.

Network Box NOC engineers can (and will) make recommendations, but it is your organisational policy and we will follow your decisions.

It is important that you review these policies (in particular by looking on my.network-box.com under Mail / Status / Policy Summary for mail policy, and Web Proxy / Config / Rules for web policy). While functions such as anti-spam and anti-virus are largely automatic (albeit controlled and tuned by hundreds of configurable options), the policy functions merely implement what they are told to do.

Upon first deployment, you should ensure that the policy implemented on your Network Box devices conforms to your requirements.

But, to meet industry best practices, you should also periodically review your policy and enforcement blocks that have occurred. You should find the weekly reports and on-line my.network-box.com helpful for this task.

As always, if you need assistance with recommendations or implementation details of your organisational policy, and the many techniques Network Box can offer to help, please talk to your regional support NOC, who are there to help.

NOVEMBER 2010 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	793	-4.8
Signatures Released	485,045	+8.8
Firewall Blocks (/box)	773,496	+10.2
IDP Blocks (/box)	123,662	-3.7
Spams (/box)	28,850	+1.4
Malware (/box)	279	-66.4
URL Blocks (/box)	145,662	+14.4
URL Visits (/box)	4,365,586	+22.0

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley

Jasmine Arif

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