

JUL 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the July 2016 edition of In the Boxing Ring

This month, we are proud to announce the release of the latest engine for the Network Box 5 mail scanning system – **Network Box 5 Mail Scanning Pattern Engine**. The engine scans signatures (lists of patterns) and applies them to the different component parts of email messages, in order to classify email content. This has resulted in improved performances, and a reduction in email scanning times. We discuss this and the approach in greater detail on pages 2–3.

Also this month, we have introduced a new email scanning classification for emails that appear to be going to multiple recipients, as part of a mailing list, newsletter, or such mass distribution services – ‘bulk’. This is highlighted on page 3.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, Network Box won two awards at this year's **PC3 Platinum Brand Awards**, Network Box Germany was at **TAROX Inside 2016**, and Network Box Managing Director, Michael Gazeley, was interviewed by **CNN**. In addition, the Network Box Mobile App is now available on the Google Play Store and Apple iTunes Store. *Please use the links to download the FREE App.*



Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 2016

You can contact us here at HQ by email (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

twitter <http://twitter.com/networkbox>

facebook <http://www.facebook.com/networkbox>
<http://www.facebook.com/networkboxresponse>

Linked in <http://www.linkedin.com/company/network-box-corporation-limited>

Google+ <https://plus.google.com/u/0/107446804085109324633/posts>

In this month's issue:

2–3

Network Box 5 Mail Scanning Pattern Engine

After 8 months of development and testing, we are now ready to release the Network Box 5 Mail Scanning Pattern Engine. The primary goals of this new engine were to improve performance and accuracy.

4


Network Box 5 Features

The features and fixes to be released in this month's patch Tuesday for Network Box 5.

5

Network Box Highlights:

- Network Box Mobile App
- PC3 Platinum Brand Awards 2016
- TAROX Inside 2016
- CNN Interview



Network Box 5 Mail Scanning Pattern Engine

At the heart of the Network Box 5 mail scanner is a pattern engine. It takes signatures (lists of patterns) and applies them to the different component parts of email messages, in order to classify email content as *spam*, *phishing*, *malware*, *pornographic*, etc. There are many different sorts of signatures present in the mail scanning signature sets, but by far the most common are pattern matching rules.

Rules that say things like 'look for a part of the message that contains words starting with advert', or 'find the letter p, followed by a small number of optional symbols, followed by the letter e, etc'. For a typical email, out of perhaps 250,000 signatures, 10,000 to 20,000 such patterns would be run during the classification phase. A simple string search would be fast and efficient, but not powerful enough for effective content classifications; so it is this powerful pattern matching engine that permits complex and accurate classification in Network Box 5.

We are proud to say that after 8 months of development and testing, we are now ready to release the latest pattern engine for the Network Box 5 mail scanning system. The primary goals of this new engine were to improve performance and accuracy.

To achieve these, we've implemented the following changes:

1. There are several hundred thousands patterns in the signature set - corresponding to known aspects of current email seen on the Internet. Running all those patterns over every single component part of the email is not required, as certain pattern checks are only required for certain types of email component. So, the new Network Box 5 mail scanning rules engine allows for specific sets of patterns to be run for specific types of email component - dramatically reducing the total number of pattern checks that we need to perform.
2. We've now got a facility whereby the matching of one particular rule can now enable another set of rules to be run. For example, certain trigger patterns can be used to enable an extended set of rules for further in-depth scanning.
3. The core pattern matching engine itself has been replaced with one optimized for the task at hand. Previously we used a standard backtracking *regex engine*, but our new replacement is based on an optimized finite-state machine using automata theory. Our new engine provides very predictable memory and CPU resource utilization, with a typically linear relationship between size of object to be scanned and scan time. This replaces the previous backtracking *regex engine* we used, which suffered from exponential CPU usage as the size of the object to be scanned increased.
4. The signature set we use has also been optimized, based on feedback from real world spam campaigns we are currently seeing.

The overall performance improvement of the new engine is hard to quantify, because it depends on the size and composition of emails to be scanned. But, in general, we are seeing a two to three times performance improvement, and corresponding reduction in email scanning times, with the new engine when compared to the old.

This new mail scanning pattern engine is being released to all Network Box 5 customers, in the July 2016 patch tuesday.

Network Box 5 Mail Scanning 'bulk' Classification

A large proportion of the submissions to spam@network-box.com or from our spam traps, are newsletters. Messages sent to a large number of people, who may or may not have subscribed to the newsletter perhaps years previously. The problem is that we have no way of knowing whether the recipient subscribed himself, was subscribed by someone else, or merely added to the list by unscrupulous senders. A large number of bulk email delivery services and users seem to subscribe to the notion of it being easier to beg for forgiveness rather than ask for permission. Opt out, rather than opt in.

We cannot simply mark such newsletters as spam, as the emails are required by many of our customers.

We cannot simply blacklist the bulk email delivery services, as many are used by legitimate senders as well as unscrupulous ones.

So, in the July 2016 patch tuesday, we have introduced a new email classification '**bulk**'. When we detect an email which appears to be going to multiple recipients, as part of a mailing list, newsletter, or such bulk distribution service, we will classify it as '**bulk**'. Customers can now use this to be aggressive against such bulk email, or to control it by whitelisting.



Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th July 2016, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features July 2016

This month, for Network Box 5, these include:

- Improvements to email quarantine search in Administration web portal
- Re-organization of Configuration/Control menu in Administration web portal
- Release of Network Setup system in Administration Web portal (this system provides a facility for authorized administrators to change the basic network configuration of ethernet ports)
- Facility to view system conditions, and change status of external conditions, in Administration web portal
- Improvements to sorting of user lists in Administration web portal
- Improved international UTF8 support in entity attributes
- Improvements to search filters in mail server queue view
- Support for IP prefixes in network DDoS dynamic and permanent blacklists
- Support for IP based local and remote IDs in IPSEC VPNs
- Support for subnet technology in SSL VPNs
- Support ACL based routes in SSL VPNs
- Improvements to synchronization between Box Office and boxes
- User portal report is not case insensitive for both user and domain part of email addresses
- Performance improvements in mail message scanning, due to introduction of new pattern matching engine
- Support for original filename and extension extraction in gzip archives, during mail message scanning
- Support a new classification 'bulk', during mail message and envelope scanning

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 SOC will contact you to arrange this if necessary.

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

Network Box ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.



Network Box Mobile App for Android and iOS



The Network Box Mobile App is now available,, on the *Google Play Store* and *Apple iTunes App Store*. Please use the links below to download the **FREE** App.

The App provides access to real time status of your Network Boxes, as well as the ability to create and respond to Box Office tickets directly from your smartphone. Fully integrated with the PUSH notification system, you are in control of what notifications are sent for what boxes and when. For the first time, the App is now available on the Android platform as well as iOS (iPhone and iPad).



Google Play Store
Network Box Android App



Apple iTunes App Store
Network Box iOS App



Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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 2736-2083
Fax: +852 2736-2778

www.network-box.com

Network Box wins PC3 Platinum Brand Awards 2016



Network Box won two **PC3 Platinum Brand Awards** in both the *Unified Threat Management* and *Managed Security Services* categories. The awards ceremony took place on the 10th of June 2016, at the Luxe Manor, Hong Kong.



The purpose of the award is to acknowledge those brands which have brought the best quality products to the markets in 2016 and the winners voted by the public. Network Box is extremely proud to have won this award and would like to thank everyone who voted.

Network Box Germany TAROX Inside 2016

Network Box Germany was at **TAROX Inside 2016**, held at the Signal Iduna Park, in Dortmund. During the event, Network Box Germany Director, Dariush Ansari, was interviewed by **CRN-TV** to talk about Network Box's next generation security technologies and managed services.



TAROX 17.06.2016
TAROX Inside
Dortmund

LINK:
<http://www.crn.de/server-clients/artikel-110688-7.html>

Network Box CNN Interview



Michael Gazeley, Managing Director of Network Box, was interviewed by **CNN**, about the Singapore government's plan to cut off all Internet access for government employees, in order to improve cyber-security.

LINK: <http://edition.cnn.com/2016/06/08/tech/singapore-internet-access/>