MAR 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the March 2017 edition of In the Boxing Ring

This month, we discuss the subject of **Spam Traps**. These are email addresses, or domains, that always receive 100% spam. With Network Box 5, the spam trap facility is finely integrated into the Network Box eMail scanning technology. This and how the spam traps enhances the Network Box anti-spam engine are discussed further on pages 2 to 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 Germany has partnered with *PROKOM* to expand their reach and service offerings in Germany, Network Box HQ also welcomed members of Network Box Germany to receive technical training on the Network Box 5.3 platform.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2017

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

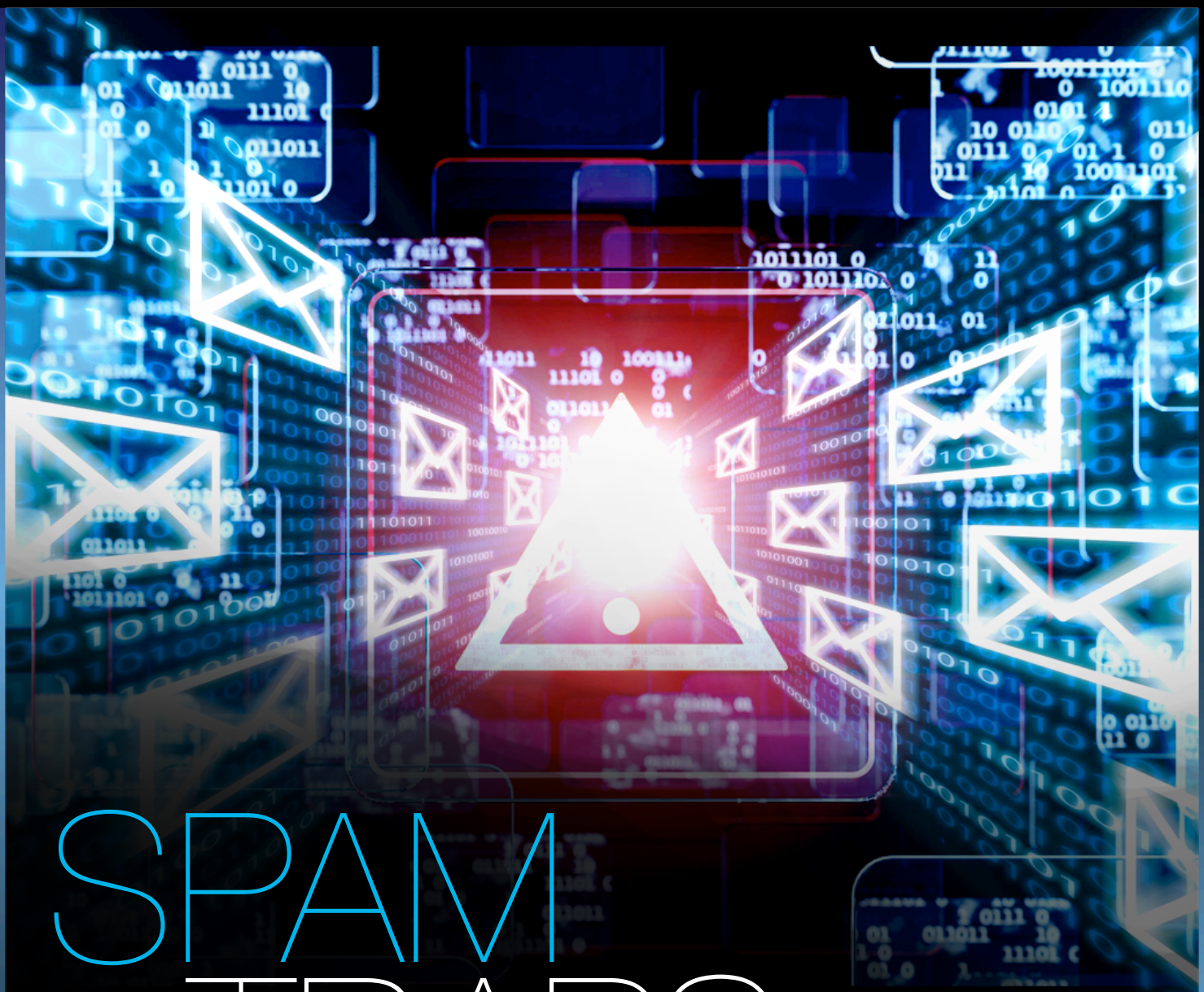
facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

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

In this month's issue:

NETWORK BOX



SPAM TRAPS

We last talked about Spam Traps six years ago, and in that time the technology has improved and has become an integral part of the Network Box 5 anti-spam scanning system. This month, we talk about spam traps in more detail, and show how they can be used to both improve anti-spam performance, as well as provide accurate and real-time benchmarks for that performance.

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 analyzing 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.

Of course, the key requirement here is that the email addresses making up the spam trap must always received 100% spam. Non-spam incorrectly sent to such addresses will both pollute the statistics and lead to false-submissions in the real-time stream of 'misses'. For this reason, we normally recommend to use mis-scraped or invalid eMail addresses as candidates for spam traps. We don't recommend using previously-valid eMail addresses or those manually seeded to spammers.

Network Box 5 offers a Spam Trap facility, integrated into our eMail scanner technology. The Spam Trap works by monitoring a configured list of eMail addresses. Messages arriving on those addresses are accepted and scanned as usual so that statistics can be recorded on success/miss rates and automatically transmitted to our centralized Spam Trap facility. The eMails are then blocked (classified both 'spam' and 'trapped'). This approach means that we get the spam in real-time, while only requiring minimal resources on the customer box.

Once the spam eMails arrive at our centralized Spam Trap facility, they are analyzed 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 Security Response Outbreak spam system for analysis and release of protection signatures. Any executable attachments are analyzed for viruses (and suspicious attachments are forwarded on to our Security Response Outbreak virus system for further analysis).

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 than setup the trap on these addresses and redirect to a 'cleansing' address on our centralized 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 moved over to the live Spam Trap systems. This process is done with the customer co-operation, but 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 thousand spam traps of our own, but these do not necessarily reflect the types of spam you may be receiving. Setting up spam traps on your eMail domains effectively allows us to see the missed spams you are receiving, and respond in real-time. They also allow you to see real-time statistics on the anti-spam effectiveness being achieved on your Network Boxes with your eMails.

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 SOC to discuss how this can best be done for your organization and how we can best serve your anti-spam requirements.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th March 2017, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
March 2017

This month, for Network Box 5, these include:

- Improvements to performance and memory usage in geolocation of IP addresses
- Kernel level support for advanced QOS features
- Performance improvement in web client logging, for bulk vs realtime logging option
- Minor change to show expired CA certificates in red color
- Enhancement to show tx and rx queue sizes in detailed network interface status display
- Improvements to DNS resolver for host based ACLs with huge numbers of hosts
- Improvements to consistency of network input rule ordering
- Provide a new COPY function to permit cloning of a report
- Improve precision on KPI summary comparison figures
- Allow use of @ and space in username for User Portal login
- Support entity names with spaces (mapped to underscore character) in authentication modules
- Provide facility for optional custom text on user portal report
- Improve handling of multiple classifications in KPI report
- Add Record ID to Web Client Block Page
- Provide configurable section limits for mail scanning
- Introduce support for spam trap statistics at envelope scanning stage

This month, we are releasing a new kernel for Network Box 5 (primarily to provide support for our Network and Proxy QoS security modules). This will require a device restart, but it will be up to the SOC's discretion as to whether to conduct this now or postpone to a later more convenient time. 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

Network Box HQ
Network Box Germany Visit

Network Box HQ welcomed our team from Network Box Germany, to be updated on the latest features and functionalities of Network Box 5.3.

Network Box Germany
Technology Partner – PROKOM

Network Box Germany signed a partnership agreement with PROKOM (Professionelle Bürokommunikation), to expand their reach and service offerings in Germany.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	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