# In The Boxing Ring

## IN THIS ISSUE

**1.
ON-GOING DEVELOPMENT**
We continue to work behind-the-scenes on the new Box Office and NOC support systems (ready for new product feature launches in September and October 2010).

**2.
NETWORK BOX SENTINEL**
This month, we are pleased to be able to announce the release of the Network Box Sentinel Anti-Virus engine. As Network Box PUSH technology is concerned with reducing the time from signature release to validated deployment, Network Box Sentinel focuses on reducing the time taken to obtain samples and produce the signatures themselves. Bringing that time down from the current industry standard of several hours, to less than 1 minute.

**3.
SEPTEMBER 2010 FEATURES**
As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBRS-3.0 customers.

**3.
SEPTEMBER 2010 HINT**
Our September hint relates to deployment of spam traps.

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

### Welcome

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

This month, we are pleased to be able to announce the release of the Network Box Sentinel Anti-Virus engine. While heuristic, reputation and relationship technologies continue to improve (and are an important tool in the fight against malware) signature based systems continue to be the primary technology used in malware protection.

As the industry leading Network Box PUSH technology is concerned with reducing the time from signature release to validated deployment on all managed devices, Network Box Sentinel focuses on reducing the time taken to obtain samples and produce the signatures themselves. Network Box Sentinel aims to bring that time down from the current industry standard of several hours, to less than 1 minute.

Network Box Sentinel is not concerned with protecting against millions of different viruses, but concentrates on the handful (typically less than 100 at any one time) that form emerging outbreaks. More on this important new system on page 2.

On page 3, we present the usual monthly hint (this month a repeat of the recommendation to deploy a spam trap), 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
September 2010

NETWORK BOX

## Network Box Sentinel

This month, we are pleased to be able to announce the release of the Network Box Sentinel Anti-Virus engine.

While heuristic, reputation and relationship technologies continue to improve (and are an important tool in the fight against malware) signature based systems continue to be the primary technology used in malware protection.

The core problem facing the industry is the shear volume of malware now seen, and the restriction of having to obtain samples, analyse them, produce signatures, and then validate those signatures prior to the release process.

While Network Box PUSH technology leads the industry with reducing the time from signature release to validated deployment on all managed devices, Network Box Sentinel focuses on reducing the time taken to obtain samples, produce and validate the signatures themselves. Just like the Minutemen of the American revolutionary war, Network Box Sentinel aims to bring that time down from the current industry standard of several hours, to less than 1 minute.

*August 2010 saw another huge upswing in the number of malicious viruses spreading via eMail (up 296.6% from July, with a global box average of 2,358 malware blocks for the month. Technologies such as the Network Box Sentinel system are at the fore-front of the fight against such outbreaks.*

*Mark Webb-Johnson, CTO Network Box Corporation*

Network Box Sentinel is not concerned with protecting against millions of different viruses, but concentrates on the handful (typically less than 100 at any one time) that form emerging outbreaks. It operates by leveraging all the threat information that Network Box Security Response receives (such as spamtraps, virustraps, customer submissions, mail and http statistics, suspect samples, etc) to (a) determine that a particular object may be malicious, and (b) maintain a confidence level for how certain we are that the given object is malicious. This confidence level is used in three ways:

1. Multiple samples, from different sources, of the same suspicious object are correlated in real-time, in order to dynamically adjust the confidence level.

2. Once the confidence reaches a pre-set limit, suspicious samples are automatically escalated to security teams for in-depth analysis of the outbreak and formal signature release.

3. The confidence levels are published in a global real-time database and queried by a module on each Network Box in real-time.

The confidence levels are expressed as a percentage 0 through 100% (with 0 being a new sample, and 100 being absolute certainty that this is malicious), and only executable (or objects with the capability to embed executable) code have confidences assigned by the system. It is common to see a new outbreak enter the system with a low confidence level, but for that level to be rapidly escalated upwards as more samples from more sources are seen, and then for the level to reach 100% once analysis is complete and a formal signature released.

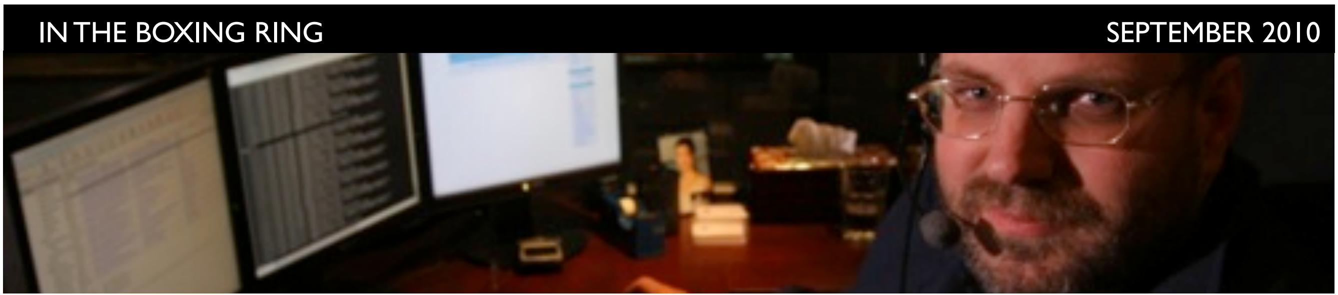
However, the key point of Network Box Sentinel is the system merely publishes the confidence level - it is up to individual per-box configuration to set the threshold at which blocking will occur. The default threshold is 50%, but this can be configured from 1% (for the paranoid) to 100% (for the conservative), on a per-box basis.

Network Box Sentinel works 24 hours a day, 7 days a week, without sleep. Continuously examining, classifying, and assigning confidence levels to in-the-wild suspicious objects, the system is already proving its effectiveness in the first few minutes of new outbreaks. You can identify sentinel blocks by the threat designations nb.sentinel.* (for signature based blocks based on 100% confidence level) and nb.rsentinel.* (for real-time blocks based on dynamic confidence levels).

Testing over the past month has shown the response time for Network Box Sentinel to be under 30 seconds for response to a single new suspicious sample, and 15 seconds for subsequent confidence level changes. Signature release time, globally, is under 3 seconds (including validation). We continue to work to improve these speeds, but they are already orders of magnitude faster than other comparable signature-based systems.

If you require more information on Network Box Sentinel, or other aspects of Network Box Anti-Virus threat protection, please don’t hesitate to contact your local support NOC.

*The Concord Minuteman*
*(Source: Wikimedia Commons)*



## September 2010 Features

This month, we are glad to say that there are no known vulnerabilities to be addressed by package update (as all the vulnerabilities have been able to be addressed by signature update). We do, however, have a number of enhancements to our internal systems, to be deployed this month, including:

- Further enhancements to the Box Office portal, related to service contracts and their visibility on customer views. We are conducting a phased deployment of our new customer contracts system, over the next two months, which will improve this further.
- Revisions to some internal health metrics to improve health monitoring and reduce false positives for environmental sensors in the GMS system.
- Revisions to the GMS reachability tests to add more test points and improve redundancy of the checks.
- A small revision to the readability of the charts on the weekly PDF report (affecting pie charts with several components)

The above changes are internal only and should not impact running services or require a device restart.

The enhancement work will be handled by the regional NOCs and will not require any action on your part. No (or minimal) service interruption is expected to be required.

## September Hint: Deploy a Spam Trap

The July 2010 Hint was 'Deploy a Spam Trap', and that was so successful that we're repeating it as this month's hint. Spam Traps allow a precise measure of the effectiveness of the Anti-Spam system and allow malicious samples (both spam and malware) to be submitted to the Network Box Security Response Team in real-time. As such, they are an invaluable tool in the fight against both spam and malware.

While we already operate hundreds of these traps (both in co-operation with existing customers, as well as our own addresses), we are always looking for new traps.

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).

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

## AUGUST 2010 NUMBERS

| Key Metric | # | % difference (since last month) |
|---|---:|---:|
| PUSH Updates | 1,021 | +5.8 |
| Signatures Released | 178,825 | +36.1 |
| Firewall Blocks (/box) | 721,796 | +4.5 |
| IDP Blocks (/box) | 145,418 | -5.7 |
| Spams (/box) | 44,974 | -7.4 |
| Malware (/box) | 2,358 | +296.6 |
| URL Blocks (/box) | 107,257 | +31.6 |
| URL Visits (/box) | 3,848,865 | +16.0 |

## NEWSLETTER STAFF

**Mark Webb-Johnson**
Editor

**Michael Gazeley**
**Jason Law**
**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