In The Boxing Ring

IN THIS ISSUE

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

Welcome

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

This month, we are pleased to be able to give an update on progress with the Network Box Sentinel AV engine released last month. During the first week following its launch, Sentinel correctly identified and blocked 39 new emerging threats missed by other Anti-Virus engines. Over 150,000 malicious threats were blocked by Sentinel engines in the first week alone (and remembering that Sentinel is only used in the time from outbreak until formal signature release, this is a remarkably impressive figure). Please turn to page 2 for further information on this.

We are conducting final stage testing and pre-deployment familiarisation for several new support systems due for release in Q4 2010. The first of these systems, Network Box Office Notifications, is coming next month (November 2010), so we are taking this opportunity to give you a preview of this system, and show you some of its abilities. More on page 2.

On page 3, we present the usual monthly hint (this month some more information on whitelisting and why you must take care with this facility), 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
October 2010

An Update on Network Box Sentinel

We are happy to report that the success of the Network Box Sentinel Anti-Virus engine launched last month has exceeded our wildest expectations. It is proving to have the ability to set the standard for real-time malware detection, and block emerging threats within seconds of their first appearance.

During the first week following its launch, Sentinel correctly identified and blocked 39 new emerging threats missed by other Anti-Virus engines. Over 150,000 malicious threats were blocked by Sentinel engines in the first week alone (and remembering that Sentinel is only used in the time from outbreak until formal signature release, this is a remarkably impressive figure).

Looking at the top five Sentinel threats blocked in that first week, shows them all to be Trojan style threats, which is to be expected given the current levels of Internet banking and credit card fraud we are seeing in the wild. We continue to closely monitor the performance of Sentinel, and to work on expanding and improving the information sources that feed this key technology for Network Box. Over time, we expect Sentinel to further improve and to become an essential component of Internet Threat Protection (particularly in the first few hours of an outbreak).

Network Box Sentinel AV - First Week Top 5 Threats

#	Sentinel Threat	Kaspersky Threat	% Blocks
#1	nb.sentinel.805769db	Trojan-Downloader.Win32.FraudLoad.hbf	19.2%
#2	nb.sentinel.02988afa	Trojan.Win32.FraudPack.bkfd	8.1%
#3	nb.sentinel.b7083149	Trojan-Downloader.Win32.FraudLoad.xlwv	8.0%
#4	nb.sentinel.2443d998	Trojan.Win32.Oficla.ma	6.3%
#5	nb.sentinel.e991d91e	Trojan-Dropper.Win32.HDrop.sm	5.6%

Notifications - A Preview

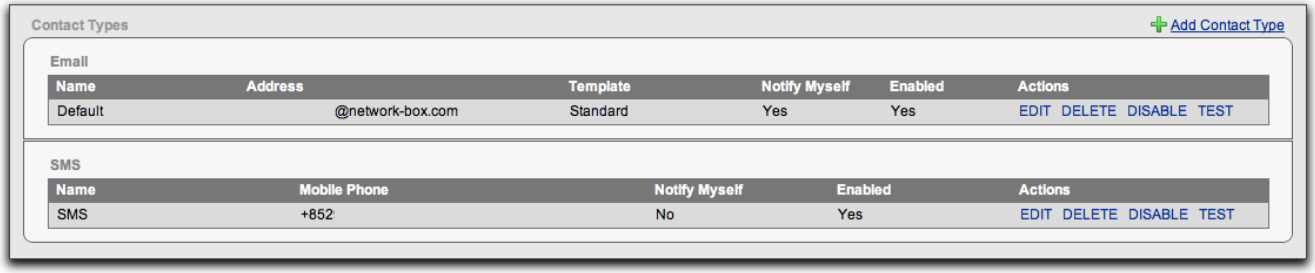
This month, Network Box will be pre-releasing a new Box Office notification system to our regional NOCs, for one months final familiarisation and testing, before formal release to all Box Office users (customers included) in the November 2010 Patch Tuesday.

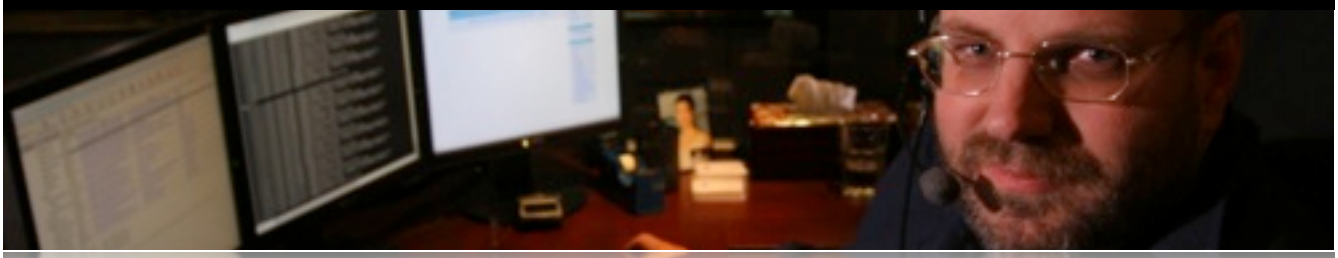
Currently in Network Box Office, each user can choose whether they want to receive notifications of ticket changes to a single registered email address. These notifications can be turned on or off, and a template (notification only, or full ticket email) can be chosen.

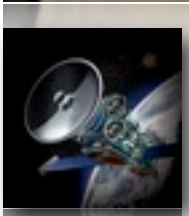
We will be deploying an extensive enhancement to this system, to allow users far finer control over the notifications they receive. In the new system, users can register contact points (multiple contact points such as 'office email', 'gmail email', 'mobile phone', etc) and the time frames they want those contact points to be active (eg; monday-to-friday 9am to 6pm). These contact points can then be selected for different notification types (eg; service ticket updates, GMS tickets creation, etc). We will be supporting contact types for Mail, SMS, Mail-to-SMS gateways, Apple iOS PUSH, as well as several IM services. An 'audit' contact type will also be available, which can be used to record a history of notifications.

Each user has control over their own notifications, and the history of notifications delivered will be available on the Network Box Office web interface and Apple iOS Applications. The new facility offers everything that the previous "want ticket email" facility did, plus so much more, and we have high hopes for its use in streamlining the communication between NOCs and customers.

We have a big month planned for November 2010, and Box Office notifications will be a key part of this.







October 2010 Features

This month, we have a large set of over 50 enhancements and fixes. As usual, the NOC will be conducting staged releases over the next 7 days.

The changes include:

- Enhancements and fixes to the PSP (Protected Service Proxy) sub-system, including work on SMTP and POP3 protocol handlers.
- Revisions to the POLICY engine (used for Web Proxy Content Filtering) related to performance improvements for IP address rules.
- Revisions to some GMS health checks, to reduce false positives in some circumstances and to add support for functionality to be released in Q4 2010.
- Addition of preliminary support for a new Kaspersky anti-virus engine, to be released in Q4 2010.
- Fix to HA subsystem to handle an error condition when issuing eMail notifications to a problematic SMTP email server.

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.

October Hint: Whitelisting Care

We continue to see problems caused by unintended Anti-Spam whitelisting.

The Network Box Anti-Spam system has the ability to perform sender white and black listing. If a particular sender is blacklisted, that instructs the Network Box that the sender only sends spam and all messages from that sender are to be treated as spam. Similarly a whitelisted sender instructs the Network Box that the sender only sends ham and all messages from that sender are to be treated as ham.

The issue comes when administrators whitelist their own or popular domains (in an attempt to avoid mails being blocked as spam). The problem with whitelisting your own domain is that spammers often use your own domain as the sender address (this occurs in approximately 5% of Internet spam). Whitelisting your own domains allows this 5% of spam through, and causes the Network Box to incorrectly 'learn' that spam as ham (resulting in other similar spam being treated as ham as well).

In a similar manner, whitelisting popular domains such as hotmail.com causes problems as spammers often abuse those domains as well.

Whitelisting your own or popular domains is not an affective approach to avoiding false positives and causes many more problems than it solves.

If you have an issue with false positives, please talk to your local support NOC to discuss how we can help, and avoid whitelisting if at all possible.

SEPTEMBER 2010 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	1,044	+2.3
Signatures Released	252,538	+41.2
Firewall Blocks (/box)	708,404	-1.9
IDP Blocks (/box)	121,782	-16.3
Spams (/box)	37,320	-17.0
Malware (/box)	682	-71.1
URL Blocks (/box)	109,064	+1.7
URL Visits (/box)	3,524,915	-8.4

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