

# In The Boxing Ring



## IN THIS ISSUE

### 1. WELCOME

The October 2010 'In The Boxing Ring' newsletter.

### 2. AN UPDATE ON NETWORK BOX SENTINEL

This month, we are pleased to be able to give an update on progress with the Network Box Sentinel AV engine released last month.

### 2. NOTIFICATIONS - A PREVIEW

Several new support systems are 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.

### 3. OCTOBER 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. OCTOBER 2010 HINT

Our October hint relates to antispam whitelisting.

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

### Welcome

歡迎閱讀 2010 十月刊的《In the Boxing Ring》。

這個月，我們很高興能夠對上個月發佈的 Network Box Sentinel AV 引擎進行一次升級改進。在發佈後的第一周，Sentinel 便正確地識別並攔截了 39 種新出現的威脅，而這些對於其它 AV 引擎卻還是漏網之魚。而單單就這第一周，Sentinel 引擎便攔截了超過 150,000 個極具破壞性的威脅（同時別忘了，Sentinel 僅僅只是使用於病毒爆發到產生發佈新的特徵碼庫之間的時間空隙，這才是它最令人興奮的特徵）。請轉到第二頁查看更多的相關資訊。

有幾個支援系統將於 2010 年第四季度發佈，我們現在正進行著最後的測試階段和部署前的熟悉階段。其中，第一個即將發佈的 Network Box Office Notifications 將於下月（2010 年十一月）發佈和部署，因此我們借此機會讓您對這個系統先睹為快，給您展示一下它的一些功能和特點。更多內容請參閱第 2 頁。

在第三頁，按照慣例我們來簡單介紹一下每个月的預告（這個月的是關於白名單篩選的更多的資訊，以及為什麼您必須關注于此項設施），以及概述一下這個月來軟體升級與發佈的情況。

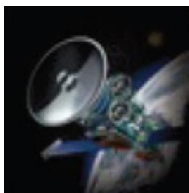
和往常一樣，如果您有任何寶貴的回饋、意見或者建議，我們都非常的歡迎。您可以通過郵箱（[nbhq@network-box.com](mailto:nbhq@network-box.com)）與我們取得聯繫，或者方便的話直接到我們的辦公室來參觀指導。

您也可以加入或者訂閱我們的 Network Box 安全響應 Twitter 和我們保持關注和聯繫，網址為：

[twitter.com/networkboxhq](https://twitter.com/networkboxhq)

Mark Webb-Johnson  
CTO, Network Box Corporation  
October 2010





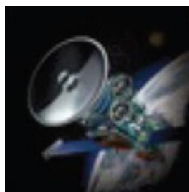
## Network Box Sentinel 的一個升級補丁

我們非常高興地向大家通報，上個月發佈的 Network Box Sentinel AV 引擎所獲得的成功已經超出了我們最高的預期。這充分證明了，對即時的惡意軟體監察以及在新型威脅出現的數秒內進行攔截建立標準的可行性。

在發佈後的第一周，Sentinel 便正確地識別並攔截了 39 種新出現的威脅，而這些對於其它 AV 引擎卻還是漏網之魚。而單單就這第一周，Sentinel 引擎便攔截了超過 150,000 個極具破壞性的威脅（同時別忘了，Sentinel 僅僅只是使用於病毒爆發到產生發佈新的特徵碼庫之間的時間空隙，這才是它最令人興奮的特徵）。

請看下表中排在前五位的 Sentinel 在第一周裡所攔截的網路威脅，可以看出，都是特洛伊類型的威脅，也就是通常我們在外界所瞭解到的被用於對當前安全級別的網路銀行和信用卡所實施的詐騙。我們將繼續更進一步地對 Sentinel 的表現進行跟蹤觀察，並努力擴大和改進資訊的來源，以滿足 Network Box 的這種關鍵技術要求。逐漸地，我們也期望著 Sentinel 能夠進一步提升，並且能成為網路威脅保護必不可少的元件（尤其針對威脅爆發的前數小時）。

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.xlww	8.0%
#4	nb.sentinel.2443d998	Trojan.Win32.Oficla.ma	6.3%
#5	nb.sentinel.e991d91e	Trojan-Dropper.Win32.HDrop.sm	5.6%



## Notifications – 預告

這個月，Network Box 將會向我們的區域 NOC 預發佈一個新的 Box Office 通知系統，以在 2010 十一月份的 Patch Tuesday 正式向所有的 Box Office 的使用者（包括客戶使用者）發佈之前，進行為期一個月的最終的熟悉和測試。

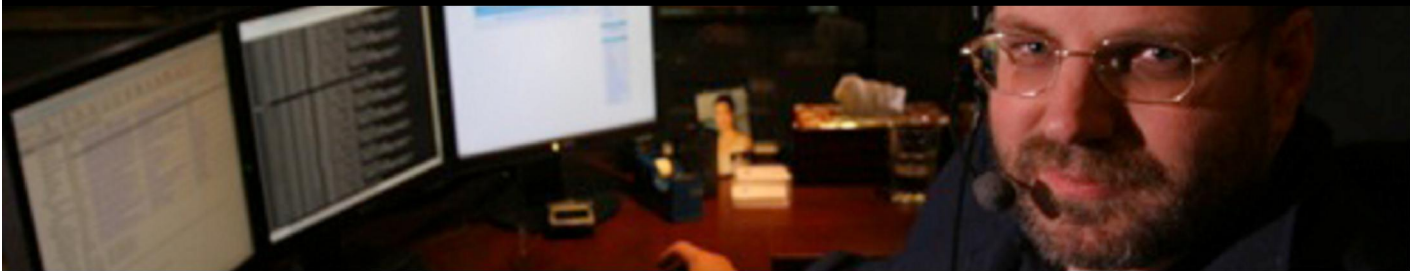
當前的 Network Box Office，每一個用戶都可以選擇是否接收工單狀態變化的通知發送到已經註冊了的郵箱位址。這些通知是可以打開或者關閉的，並且可以選擇通知內容的範本（僅僅通知或者工單的全部內容）。

我們將對這個系統的部署進行廣泛的增強，使用戶能夠通過所收到的通知更好地進行控制。在這個新的系統當中，使用者可以註冊聯繫方式（如辦公郵箱、gmail 郵箱、行動電話等多種聯繫方式）以及使用者所希望的這些聯繫方式方便接收的時間視窗（比如週一到週五的上午 9:00 到下午 6:00）。這些聯繫方式可以選擇不同的通知類型（比如服務工單的更新、GMS 工單的創建等等）。我們還將支援 Mail、SMS、Mail-to-SMS 閘道、蘋果 iOS PUSH，以及幾種 IM 服務工具。還將建立聯繫類型的審計，用於對通知歷史的記錄。

每一個用戶都可以對其自身的通知進行控制，並且所有的通知發送歷史記錄都將可以通過 Network Box Office 的 web 介面以及蘋果 iOS 應用程式進行查看。這個新的機制涵蓋了之前的“want ticket email”機制的功能，並且有更多功能的增加，我們更多地希望它對於 NOC 和客戶之間能夠高效率地進行溝通發揮作用。

2010 年的十一月份，我們的工作重心將著重專注於 Box Office notifications 系統的開發部署和測試等工作。

Contact Types						<a href="#">+ Add Contact Type</a>
<b>Email</b>						
Name	Address	Template	Notify Myself	Enabled	Actions	
Default	@network-box.com	Standard	Yes	Yes	EDIT DELETE DISABLE TEST	
<b>SMS</b>						
Name	Mobile Phone	Notify Myself	Enabled	Actions		
SMS	+852	No	Yes	EDIT DELETE DISABLE TEST		



**2010 年十月 新特性**

在這個月裡，我們進行了超過 50 項的修復和升級。和往常一樣，區域 NOC 將會在未來的 7 天內分階段地進行發佈升級。

所涉及到的改進包括：

對 PSP (Protected Service Proxy) 的子系統進行了修復和增強，包括 SMTP 和 POP3 系統控制器的工作。

·修正了 POLICY 引擎 (用於 Web Proxy 內容過濾) 有關於 IP 位址策略的性能改善。

·修正了 GMS 的一些健康狀況的審查，減少了在某些情況下錯誤的正常指標，並且增加了對 2010 年第四季度即將發佈的功能的支援。

·增加了對第四季度即將發佈的卡巴斯基反病毒引擎的初步支援。

·修正了 HA 子系統在處理 eMail 通知發送到一個有問題的 SMTP 郵件伺服器所產生的錯誤條件。

這些修改並不需要硬體重啓，但可能對某些點正在運行的服務有所影響，不過，我們的區域 NOC 將會與您取得聯繫以確認合適的部署時間。

這些更新的工作將會交由區域 NOC 的工程師進行處理，而不需要客戶方面的任何操作。只需要對相關的服務最小限度的影響。

**十月提示: 白名單篩選的關注**

我們一直都在關注非故意的反垃圾郵件的白名單篩選。

Network Box 的反垃圾郵件系統可以做到對郵件發送者進行白名單和黑名單的區分。如果一個特別的用戶被列入黑名單，這就示意 Network Box 這個發信者只發送垃圾郵件並且其所發送的所有郵件都將被認定為垃圾郵件。同樣的，一個被列入白名單的發信者，對 Network Box 來說，他只發送正常郵件，並且其所發送的所有郵件都將認定為正常郵件。

但是問題來了，當管理員將他們自己的功能變數名稱已經一些常用功能變數名稱放入白名單時 (以試圖避免這些郵件被攔截為垃圾郵件)。將自己的郵箱功能變數名稱列入白名單的問題在於，垃圾郵件發送者通常會使用您自己的功能變數名稱作為他發送的位址 (這種情況占到互聯網垃圾郵件的 5%)。將您自己的功能變數名稱列入白名單的做法將可能導致 5% 的垃圾郵件通過，並且導致 Network Box 錯誤地學習到這類郵件為正常郵件 (從而導致其它類似的垃圾郵件被視為正常郵件)。

同樣的，諸如 hotmail.com 等常用郵箱功能變數名稱被列入白名單，它們和那些功能變數名稱一樣會被那些垃圾郵件發送者所濫用。

因此，將自身的功能變數名稱和常用功能變數名稱放入白名單並不是一種用於避免誤報，甚至所出現的問題可能比起其所能解決的問題要更甚。

如果您正好有關於誤報的一些問題，請與您當地的區域 NOC 工程師取得聯繫，並商討如何可以給予您一定的幫助，以儘量避免白名單篩選多導致的問題。

**OCTOBER 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)	109,06	+1.7
URL Visits (/box)	3,524,91	-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](mailto: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](http://www.network-box.com)

Copyright © 2010 Network Box Corporation Ltd.