

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

歡迎閱讀 2010 九月刊的《In the Boxing Ring》。

這個月，我們很高興能夠宣佈 Network Box Sentinel 防病毒引擎終於發佈了。雖然啓發式技術、聲譽以及相關技術依然在不斷地改善（同時也依然是反惡意軟體的非常重要的工具），但基於簽名的系統仍然是反惡意軟體的最主要的技術。

作為業界領先的 Network Box 的 PUSH 技術是專注於從簽名的發佈到所有被管理設備的驗證部署所耗時間的縮短，Network Box Sentinel 集中關注於減少獲取病毒樣本以及自行產生特徵碼所花費的時間。

Network Box Sentinel 的目的在於盡力減少這樣的時間，從當前行業標準的幾個小時降低到不足 1 分鐘。

Network Box Sentinel 並不是主要針對于數以百萬數量級不同病毒的防護，而是專注於少數（通常在同事間少於 100 種）病毒疫情的爆發。更多關於這個重要的新系統請參閱第 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（這個月的是關於部署垃圾郵件部署的再次建議），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）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

Mark Webb-Johnson
CTO, Network Box Corporation
September 2010





Network Box Sentinel

這個月，我們很高興能夠宣佈 Network Box Sentinel 防病毒引擎終於發佈了。

雖然啓發式技術、聲譽以及相關技術依然在不斷地改善（同時也依然是反惡意軟體的非常重要的工具），但基於簽名的系統仍然是反惡意軟體的最主要的技術。

業界所面臨的核心問題是現在所遇到的大量的惡意軟體，以及必須要先獲取病毒樣本，再進行分析，產生簽名特徵碼，然後使這些特徵碼優先發佈等等一系列過程的局限性。

而作為業界領先的 Network Box 的 PUSH 技術是專注於從簽名的發佈到所有被管理設備的驗證部署所耗時間的縮短，Network Box Sentinel 集中關注於減少獲取病毒樣本以及自行產生特徵碼所花費的時間。Network Box Sentinel 的目的在於盡力減少這樣的時間，從當前行業標準的幾個小時降低到不足 1 分鐘。

2010 年八月份，通過電子郵件進行擴散的惡意軟體也產生了一個非常龐大的增長的數字，相比七月份增長了 296.6%，全球每個 Box 月均攔截 2,358 次惡意軟體的攻擊。而諸如 Network Box Sentinel 系統就是專門針對此類疫情的爆發而走在技術前沿的防護系統。

Mark Webb-Johnson, CTO Network Box Corporation

Network Box Sentinel 並不是主要針對於數以百萬數量級不同病毒的防護，而是專注於少數（通常在同事間少於 100 種）病毒疫情的爆發。它是通過利用 Network Box Security Response 所接收到的所有的威脅資訊（例如：垃圾郵件陷阱、病毒陷阱、客戶意見、郵件和 HTTP 統計、罪犯案例，等等）來做到：(a) 確定某一特定的物件是否具有惡意，(b) 並通過確信等級指數評判保證對該特定物件具有惡意性判斷具有一定的準確度。這一確信等級指數將用於以下三個方面：

1、不同來源的多個相同可疑物件的樣本是即時相關的，將有利於動態調整確信等級。

2、一旦確信等級指數達到預先設定的限度，可疑樣品將會被自動升級為安全性群組，以對疫情進行深入分析，並正式簽署發佈其特徵碼。

3、確信等級指數會發佈於全球即時資料庫中，並且供全球所有的 Network Box 中的相關模組即時查詢。

確信等級指數是用百分比從 0 到 100% 來表示的（0 表示新樣品，100 表示完全確信為惡意），並且只有可執行（或者嵌入式可執行物件）的代碼才會被此系統置信指派。經常可以看到，當一種爆發以一個較低的確信等級指數進入系統後，它便會非常快速地蔓延並增長更多的樣品，產生更多的攻擊源，然後隨著確信等級指數一旦升級到 100% 時，分析便結束了，並且正式簽署發佈其特徵碼。

然而，Network Box Sentinel 的關鍵之處在於它能夠發佈確信等級指數。這取決於每個 Box 均設置了阻擋的閾值。默認的閾值為 50%，但這個值是在每個 Box 的基礎配置中設置為從 1%（開放值）到 100%（保守值）的值。

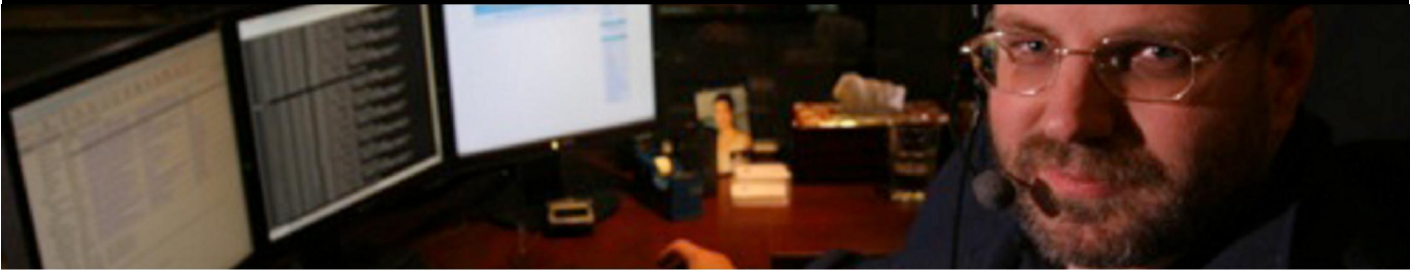
Network Box Sentinel 每天 24 小時，每週 7 天不間斷工作。不間斷地對未知的可疑物件進行研究分析，分類，並評判其確信等級指數，該系統已經證明其在第一時間新病毒爆發時的有效性。你可以通過威脅標示 nb.sentinel.*（用於標示基於 100% 確信等級指數的基礎攔截）和 nb.rsentinel.*（用於標示基於動態確信等級指數的即時攔截）來對 Sentinel 攔截進行定義。

在過去的一箇月中，測試的結果顯示，Network Box Sentinel 在應對單個的疑似樣品時，其回應時間已經低於 30 秒了，其隨後的確信等級指數更新也只需要 15 秒。簽署發佈的時間，全域來看也只需要不到 3 秒鐘（包括確認所耗時間）。而且，我們還依然致力於提高這些速度，但是其數量級與其它同類基於簽名的系統相比卻已經快了許多。

如果您想要獲得更多關於 Network Box Sentinel 的資訊，或者其它方面的 Network Box 反病毒威脅防護的資訊，您可以與您當地的 NOC 支持中心取得聯繫。



The Concord Minuteman
(Source: Wikimedia Commons)



2010 年九月 新特性

在這個月裡，我非常高興地告訴大家，還沒有發現有什麼漏洞需要發佈補丁包加以修補的（因為之前曾發佈的很多補丁包已經足以解決已被發現的漏洞問題）。但在此期間，對我們內部的系統做了一系列的優化和改進，並進行了部署，包括：

·進一步增強了 Box Office 的介面，涉及到服務合同及其對客戶意見的進一步明確。而對我們現有的客戶合同系統進行分階段部署，在未來的兩個月裡，將會得以提高。

·修訂了一些內部健康狀況指標，以提高健康狀況監測以及減少 GMS 系統對環境健康狀況的誤報。

·修改了 GMS 的可到達測試，以增加更多的測試節點以及提高核查的冗餘度。

·修改了 GMS 的可到達測試，以增加更多的測試節點以及提高核查的冗餘度。

·對每週報告的可讀性表格做了一些小修改（有幾個組件影響了直條圖）。

這些修改都只是內部調整，並不會影響到正在運行的服務，也不需要硬體重啓。

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。也不會中斷任何的服務。

九月提示: 部署垃圾郵件陷阱

2010 七月份的提示也是“部署垃圾郵件陷阱”，那次非常成功，所以這個月的提示再次把它拿出來討論。垃圾郵件陷阱可以做到對反垃圾郵件系統有效性的精確的測量，並且可以做到將惡意樣本（包括垃圾郵件和惡意軟體）即時地提交到 Network Box 安全回應組。就其本身而言，這些對於反垃圾郵件和惡意軟體都是非常有意義的工具。

現在我們正在運行的垃圾郵件陷阱已經有幾百個了（包括我們自行建立的以及和我們合作的現有的客戶的），我們也一直不斷地尋找更多新的垃圾郵件陷阱。

通過垃圾郵件陷阱即時獲得垃圾郵件樣本的方式遠遠要好於通過舉報到 spam@network-box.com 郵箱的這種機制。這樣，垃圾郵件樣本來的更加準確且即時（相比於被延遲好幾天的情況），並且給我們更好地監控並對新的垃圾郵件的爆發做出處理回應贏得更多的時機（哪怕只是針對單個使用者的情況）。

如果您有一些老的未使用的，或者意外獲得的郵寄地址，我們建議您考慮將此作為一個選項。垃圾郵件陷阱的建立僅僅需要非常少的資源，並且可以讓我們更好地為您提高服務（這與對所有 Network Box 用戶無私地提高其反垃圾郵件精度的做法是一樣的）。

請與您當地的網路中心（NOC）技術支持取得聯繫，並與之就關於這些如何為您的組織機構做到更好以及根據您的要求我們要怎樣才能做得更好進行交流。

SEPTEMBER 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)	107,25	+31.6
URL Visits (/box)	3,848,86	+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

Copyright © 2010 Network Box Corporation Ltd.