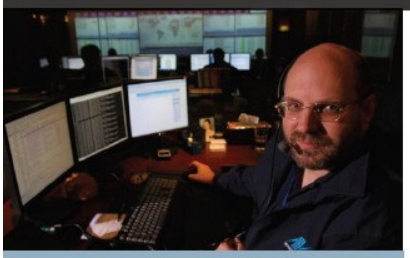
In The Boxing Ring



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

IN THIS ISSUE

Welcome

歡迎來到 2010 年 5 月份的 In The Boxing Ring.在這一期，我們繼續關注漏洞掃描，及對垃圾郵件與病毒的分類問題。

在第二頁，我將花些時間介紹 Network Box 提供一個新的服務。在 2010 的夏天，我們將推出三種類型的網路掃描服務選項，提供針對外部和內部的網路掃描。這個新技術的推出使我們非常興奮。

在第三頁，我將討論是問題是多種混合威脅的分類（尤其是 spam 與 malware 的分類），和深刻理解 Network Box 長期方向上對這個問題的關注。

同樣是第三頁，我宣佈可用于 Network Box iPhone 應用程式的 V3.2 版，包括支持既將出來的 Apple iPad，這個新版本（對 iPad 提供更高解析度的支援）既將發佈。

第四頁，在第四頁，我們介紹通常的每月提示（這個月關注報警政策），並概述部分這個月發佈的軟體升級更新。

和以往一樣，如果有任何反饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發
送郵件到我們的郵件列表：

nbhq@network-box.com

聯繫我們。或者當您下次在香港市區的話來隨時來我公司辦公室進行參觀指導。您也可以加入或訂閱我們的安全響應 Twitter 和我們保持聯繫，網址是：

twitter.com/networkboxhq

Mark Webb-Johnson

CTO, Network Box Corporation

April 2010

網路漏洞掃描

上個月我描述了漏洞掃描的概念和怎麼讓它可有益於遵循和主動保護你的網路。這個月我鄭重的宣佈，2010 年夏天起，Network Box 漏洞掃描服務作為一個選項提供給我們的客戶。

Network Box 這個服務堅持以下原則：

1.安排掃描計畫

2.進行掃描

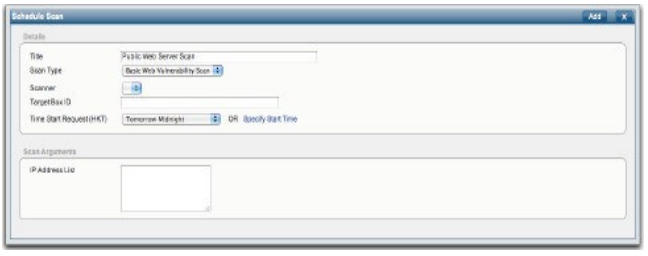
3.Network Box NOC 查閱和分析掃描結果，並作適當的注釋

4.終端用戶查閱掃描報告，並根據報告(有 HTML 和 PDF 格式）進行管理

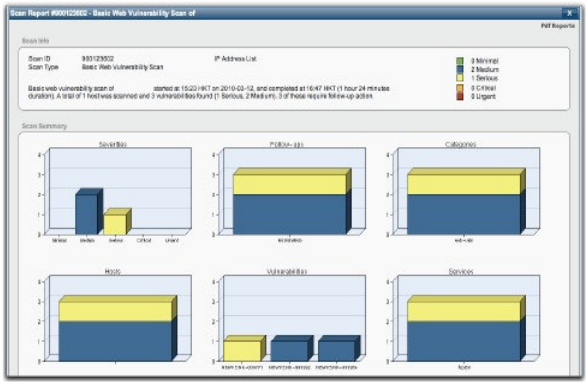
5.為終端用戶提供每個報告結果分類（包括比較掃描期間的報告與重新掃描驗證正確性）。

一旦推行， Network Box 將提供三種掃描方式：
.網路圖（鑒定網路設備，和指紋驗證）。
.綜合漏洞掃描（包括識別已知的漏洞和可疑應用程式）。
.綜合 Web 伺服器掃描（包括掃描專門針對 Web 伺服器和其獨特的漏洞-如 SQL 注入 ）。

NOC 提供掃描模式的檢查，Network Box 專家審查每個掃描的結果，並根據客戶的環境給出建議。這可以在很大程度上解決用戶自動掃描時高假陽性的問題。

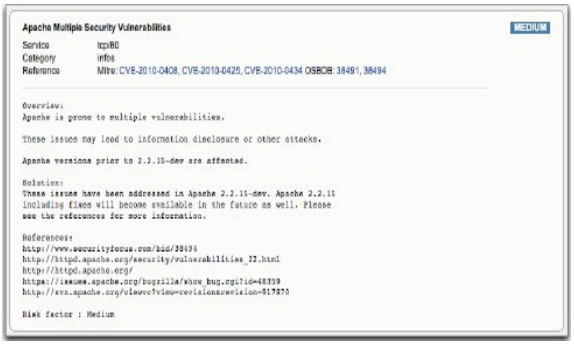


Network Box 將提供外部（掃描者通過在 INTERNET 外的掃描，提供外部網路的查看）和內部（掃描者在客戶網路環境中，提供內部網路的查看）這些服務。兩種類型的掃描其結果都可以在 BOXOFFICE 查閱。



掃描結果被分為六個從 0（資訊）至 5（緊急）的橫向歸類欄中，這些欄目可以作為結果依據去立即有針對性的補救措施。在 Network Box 架構內的用戶圖形介面，可以很快很簡便的分析這個結果。 可以下載 PDF 格式的報告，充分遵和管理報告。

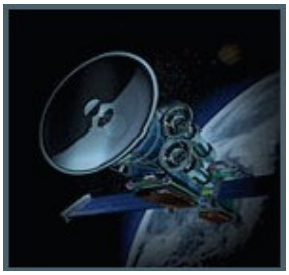
Network Box 的一個重要方法是其後續行為可整合到 NETWORK BOX 架構。每次掃描結果有一個後續行為分配，可以跟進行為跟蹤直到事件結束。這種機制完全支援定期和重複掃描系統，在跟進系統中可讓系統自動突出差異（比如像哪些專案被標記解決了，但仍會出現在以後的定期和重複掃描）。



儘管 NOC 防火牆維護和掃描操作是分開（可以有一個分清維護和查看之間的功能，以上都提供給終端用戶），緊密結合 NETWORK BOX 設備和掃描系統，使掃描行為協調到環境中掃描，提供一個最好的，最精確的，最少的假陽性資料和失誤。

正確使用和熟練的處理，漏洞掃描是一個非常有用於主動保護你網路的工用。我們在這裏非常高興 NETWORK BOX 給我們提供了這個新功能（也為需要這個報告的客戶，及那些誰想使用它的）。

我們預計在 2010 年 6 至 7 月提供開放這項新服務的測試，在夏季遲些時候將有一個完整版的發佈。



垃圾郵件與惡意軟體

粗略的流覽下這個月的統計數，垃圾郵件下降了 23.7%，惡意軟體上升 1789%--這個也許要做些解釋 。

看下這個原始資料：
2010 年 3 月看到每個 BOX 有 45，820 封垃圾郵件和 767 個惡意軟體總共有 46587 條並非客戶想要的資訊。
2010 年 4 月看到 34944 封垃圾郵件和 13791 個惡意軟體，總計 4873 條.因些我們可以看到垃圾郵件在下降 23.7%，惡意軟體增加 1978%，3，4 月總計差異 4.6%。
早在 2010 年 4 月，我們開始看到大量的垃圾郵件推廣廣告鏈結到託管惡意軟體的服務主機（在某些情況下惡意軟體直接附在電子郵件資訊裏）。與合作夥伴的合作下，我們會立即將這些有惡意內容的主機歸類（有些是惡意軟體，有些是垃圾郵件，及其他一些釣魚網站）。因為同一台伺服器上包含有三種威脅，所以很難去歸類這個威脅（因涉及到三種威脅），所以 NETWORK BOX 與我們的合作夥伴採取的做法是把它們歸類為最大危害類（有些是惡意軟體有些是釣魚軟體）。我們的技術可以歸類到 URL 路徑級，但通常個別 URL 上包含了所有這三種類型，這取決於每個 EMAIL 的傳遞參數。
不管電子郵件是否是垃圾郵件，色情的，惡意軟體，病毒或網路釣魚，這些都是不受歡迎有害的。整個月的垃圾郵件數目並沒有多大的變化，是什麼改變每種類型的百分比呢？
主要問題是現在的威脅變得混雜起來，不同的類型的界定變模糊了。一個不安全的 WEB 伺服器有可能是垃圾郵件源，也有可能是釣魚站點，或者是惡意軟體託管主機。
僵屍網路井噴式的大量傳出數十億以上含有惡意軟體和垃圾的郵件，針對這種攻擊提供保護的有效辦法是由 NETWORK BOX 提供多方面的技術，NETWORK BOX 絕大多數客戶用來阻擋的反垃圾郵件和反惡意軟體系統都放在閘道處，當訪問這樣一個包含有威脅的郵件鏈結時，NETWORK BOX 內容過濾系統就可以阻擋這個威脅（阻止網站的訪問，或者通過 Google Safe Browsing 系統阻止已知的惡意網站）。這類網站利用網路漏洞，NETWORK BOX IDPS 系統可以根據地址去處理，最後惡意軟體也會被 HTTP anti-virus 系統阻止。只有在多層次和多個協定安全系統結合起來工作，像 NETWORK BOX 一樣，這樣才能實現對這種威脅的全面保護。
哪個將引領我們的未來，像這種可以讓我們保持和改進我們在技術上領先的混合威脅防護技術在哪里，在 NETWORK BOX 這，我們相信內容歸類的核心技術是正確的，我們的主要目標是改善這種歸類，同時引入系統對一種威脅提供多種分類。
當你訪問 一個網站，這是關於一個個人博客並有涉及到購物，這個就應被歸類為“博客”或者“購物”？我們認為正解答案是兩者都是，像這種做法可以提 供最好的精度界定和準確的政策支持。
引入支持精密多種分類，將使 NETWORK BOX 準確歸類威脅（如：病毒，網路釣魚，垃圾郵件，惡作劇，購物，大郵件，可執行的附件等），然後允許客戶用政策去處理這些分類（如： 阻擋和隔離病毒，或拒絕訪問成人網站的政策）。這就是我們的方向，我們明年在這一架構上將繼續提供越來越多的系統。

APP V3.2

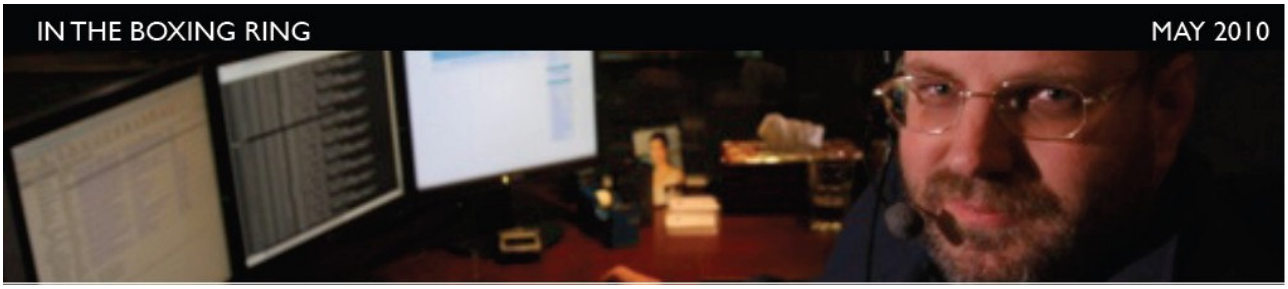
NETWORK BOX 的 iPhone/iPod Touch/iPad 應用程式 V3.2 版將會在 2010 年 5 月分上旬就可以發佈應用。

這個版本是相容性很強的程式，意思是說這個程式支援所有當前蘋果產品（iPhone,iPod Touch 和 iPad)方案。以及對 iPad 1024x768 解析度的支持，新版本還增加對大鍵盤（外部/藍牙鍵盤）的支援。

.V3.2 版本（包括測試過即將發佈的 V4.0）對蘋果作業系統的相容。
.支持蘋果 Apple iPad 1024x768 高清解析度
.支援 ipad 公司特殊的功能（如彈出視窗和資訊輸入屏）。
.改善了 ticket 系統的輸入/更新屏，允許直接輸入 ticket 內容。
.修正本地緩存以提高性能
. 自動刷新改進主頁流覽（之前顯示緩存的內容，刷新顯示伺服器上最新的內容）
.自動刷新改進全球地圖（之前顯示緩存的地圖，刷新顯示伺服器上最新 的地圖）
.完成修復一些 BUG

V3.2 版將更新交付到標準免費更新的蘋果應用程式商店，我們希望這個更新可以在 2010 年 5 月上旬，但是批准發佈時間取決於蘋果公司。

Network Box v3.2 iPhone/iPod Touch/iPad App



展望 2010 年 5 月

週二，2010 年 5 月 4 日，NETWORK BOX Patch Tuesday 將公佈的補丁集改進和修正。區域 NOC 將在下一個禮拜進行該新功能的首次展示。這個月，包括這些：

.對新的架構進行了加固
.增強 TICKET 系統網站對 iPhone/iPad 的支援。
.增強郵件壓縮包掃描功能，支援檢測 ZIP 檔，並可以阻止它們。
.增強郵件掃描系統報警機制
.郵件掃描引入指紋界定資訊結構，可用於反垃圾郵件和反惡意軟體系統。
.改進了 IPSEC VPN 服務的可靠性，能夠更好的應付錯誤匹配參數。還增強了狀態監測系統，把 IPSEC VPN 的狀態加入到監控系統。
.改進了代理服務保護系統，及有關 SMTP 的透明代理。

在大多數情況下，上述變化應該不會影響服務運行或需要設備重新啟動。但是，在某些情況下（需要看配置而定），某個配置可能需要重新啟動。如有需要，當地 NOC 將會與您聯繫並安排時間。

April Hint: Alerting Policy

每個 NETOWRK BOX 包含了一套複雜的處理垃圾郵件和惡意軟體的策略系統，當一個惡意軟體被阻止時，可以打開隔離，可以發送郵件通知到發件人，收件人或管理員。
然而應該十分小心採取這種措施，因為互聯網上這種垃圾郵件太多而導致通知郵件氾濫。

.通知發件人是件麻煩事，當發件者是個偽裝時--將使發給發件人的退件氾濫。
.Mail Portal 報告應該限制在已知有效的接收者（用這樣的信件核查機制避免產生不可達的退件）。

NETWORK BOX 提供一個全球通知限制系統，可以抑制最為常見這些不當警報的通知（例如我們知道發件人是偽造時，就抑制發件人通知）。這個可以在每個 NETWORK BOX 上做配置（及全球默認配置）。

請與你的本地 NOC 去確認你的通知是否已經如你的要求添加進去了。

Mark Webb-Johnson,
CTO, Network Box Corporation

APRIL 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,106	+8.2
Signatures Released	127,140	-50.1
Firewall Blocks (/box)	692,125	+10.1
IDP Blocks (/box)	176,813	+9.3
Spams (/box)	34,944	-23.7
Malware (/box)	13,791	+1,798.0%
URL Blocks (/box)	86,141	+10.1
URL Visits (/box)	3,264,743	+0.2

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