In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

歡迎閱讀2013年1月刊的 In the Boxing Ring

這一期是我們的年終版，我們著重於探討2012年網路威脅的一些數位資料，並且對2013年以及以後進行展望。Network Box的安全回應中心監控並管理著全球數以千計的安全設備，這給予我們對威脅環境以極好的觀察依據。在Network Box，我們堅信，只有在有能力清楚地觀察並分析問題的所在，才能夠拿出解決問題的最佳方案。

在第4、5頁，我們探討了關於NBRS-5.0的一些詳情，並概述了我們近期所發佈的，以及我們具有里程碑意義的一些事件。我們也正在進行著大量的工作，作息不分，在此期間一切如常，緊鑼密鼓而有序順利地進行著。

嚴格來講，我們重新找到了一種實現安全的方法，那就是，從一個既定的威脅攔截裝置，向一個可以靈活對內容進行分類並進行策略執行的一個系統裝置進行轉變。對此，我們有信心將爲客戶提供更加滿意的結果。

在第6頁，是這個月對NBRS-3.0的發佈的新特性和新修復的補丁的詳情。在可預見的未來幾年，我們將繼續NBRS-3.0的開發和提高技術支援。這一頁將讓您瞭解到我們核心產品的動態資訊。

Mark Webb-Johnson
CTO, Network Box Corporation
January 2013

您可以通過郵箱（nbhq@network-box.com）與我們總部取得聯繫，或者到我們的辦公地點親臨參觀指導。您還可以通過以下幾個對外網站對我們保持關注：

http://twitter.com/networkbox
http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse
http://www.linkedin.com/company/network-box-corporation-limited
https://plus.google.com/u/0/107446804085109324633/posts

本刊概述

2012 安全威脅 統計與分析

2012年度Network Box的安全威脅統計資料的概要描述和分析

PUSH 更新 & 簽名特徵碼的發佈

2012期間，Network Box 安全響應PUSH推送了6,328 次更新，，總計 4,484,811 個簽名特徵碼（分別下降11.2%，以及上升15.6%，相比於2011年）。

這就意味著大約每7秒鐘就有一個新的簽名特徵碼產生。繼續來看看2012年度簽名特徵碼的更新資料，我們發現發佈簽名特徵碼的數位增加了許多；也反映出持續地遷移到基於雲端的簽名特徵碼系統的變化（比如Network Box Sentinel Z-Scan和NBCP內容分類系統）。我們預計，這樣的趨勢將持續下去，從深度和廣度上來講，傳統的簽名特徵碼一如是最有效的防惡意軟體的方案，而新興的基於雲端的的簽名特徵碼系統的解決方案對於零日爆發卻是最有效的。

垃圾郵件 & 惡意軟體

2012年期間，Network Box 平均阻擋了163,126封垃圾郵件，以及 7,470 個惡意軟體（相比於2011年兩者分別下降 21.6% 和 6.7% ）。

與2011年一樣，繼續全面地減少了垃圾郵件的數量。然而，垃圾郵件數量的減少在某種程度上或多或少還是要歸功於逐漸增長使用的預掃描過濾（例如在信封階段的RBL阻擋以及收件人地址驗證等）。這樣的信封掃描階段的阻擋非常有效地打擊了大量的垃圾郵件（目前估計在全球範圍內有41%左右）和威脅郵件（包括垃圾郵件和惡意軟體），使之在信封掃描階段即被阻擋掉而不再在我們的“所阻擋的垃圾郵件和惡意軟體郵件”的報告圖表當中。隨著NBRS-5.0的發佈，我們希望在這方面能夠有更大的改觀。在2012年期間，Network Box平均每185秒即會阻擋掉一封垃圾郵件或惡意軟體。

Network Box 安全威脅統計	2011 數字	2012 數字	% 變化
PUSH Updates	7,125	**6,328**	-11.2
Signatures Released	3,880,267	**4,484,811**	+15.6
Firewall Blocks (/box)	9,191,536	**10,497,946**	+14.2
IDP Blocks (/box)	1,420,534	**1,669,242**	+17.5
Spams (/box)	208,081	**163,126**	-21.6
Malware (/box)	8,008	**7,470**	-6.7
URL Blocks (/box)	1,663,284	**1,989,761**	+19.6
URL Visits (/box)	45,838,221	**50,247,987**	+9.6

‣ Network Box2012年相比於2011年的網路威脅統計

與往常一樣，每個月我們都看到越來越多的的網路威脅，而且呈越來越快的趨勢。而Network Box也將繼續在技術上（例如Z-Scan等）加大投入以加快防護手段的發佈週期，同時還會繼續利用我們優秀客戶關係的優勢，使我們能夠齊心協力、協調有效地將網路防禦往前更進一步。

防火牆 & IDP 攔截

在2012年期間，Network Box 平均使用防火牆技術攔截了10,497,946次的攻擊，以及通過IDP技術攔截了1,669,242 次的攻擊（分別上升了14.2% 和17.5% ，相比於2011年）。

隨著全球網路頻寬的不斷增長，網路級的攻擊也在不斷地增長。攻擊者現在可以輕鬆地利用龐大的僵屍網路對企業發動DDoS攻擊。我們的大客戶曾遇到過這樣的攻擊，平均每六個星期遭受一次，這一情況開始於2011年，並一直持續到2012年。因此，爲了不斷提高我們的保護性能，Network Box在這方面也推出了我們的第一個NBRS-5.0的安全模組版本，以滿足達到對網路及攻擊Web應用程式（NBRS-5.0提供了WAF+安全防護服務）的防護要求。

現在的IPv4位址空間被污染得非常嚴重，Network Box的客戶中，平均每2.6秒就會攔截到一次防火牆或IDP網路級攻擊探測。在2012年，我們與微軟的合作不斷深入發展，我們也在我們的安全響應中心網站開設了我們即時的微軟合作夥伴MAPP簽名特徵碼發佈專欄。

URL 地址過濾 & URL 位址訪問

在2012年期間，Network Box根據企業內容過濾政策執行平均阻擋了1,989,761個網站，且全年統計有50,247,987 個網站 URL 訪問位址（分別上升了19.6%和9.6%，相比於2011年）。

正如預期的那樣，不斷增長的貸款（特別是Web使用）。2013年即將推出的Network Box NBRS-5.0的應用識別和包控制，會隨著NBRS-5.0產品的推出也將在Web內容控制方面獲得進一步的改進。這將使我們的客戶能夠更好地擴展他們的出口策略，而不僅僅只是Web訪問，而是包括應用層的所有流量的控制。

那麼2013年及以後 我們所能預見的是什麼呢？

自身設備的可攜帶性（BYOD，Bring-Your-Own-Device）要求，以及與服務產品的需求不斷地增長，那麼即將到來的Network Box的產品和服務，將專門針對於這些要求的滿足。我們將繼續與主要的雲服務提供者建立夥伴關係，以更好地提供我們的雲安全平臺，讓我們所提供的的保護服務更能滿足和接近所需要保護的物件的要求。然而，一個往往容易被人們所誤解的關鍵點是，這並不是要將辦公網路置於保護之外。即使DMZ伺服器遷移到雲端，入站和出站的保護和策略控制仍然需要在辦公區域進行，這裡所涉及到的問題Network Box依然會繼續進行處理。我們也正在爲能提供這種混合部署（分開的辦公區域與在雲端/資料中心等IT實體之間）的服務而不斷地努力著。

全球互聯網威脅源總覽圖（2012年12月），對於即時的統計資料請訪問：http://response.network-box.com/internet-health

Network Box 第5版本
NBRS-5.0

現在我們基於Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) 的NBRS-5.0 (Network Box Reserve Set 5.0)已經正式地發佈了，我們被問及最多的一個問題是：“基於UTM+（Unified Management Plus）的NBRS-5.0什麼時候可以使用？”

那麼最簡單的答案就是，它的一個重要的部分已經完成了。

NBRS-3.0是一個單一的產品，只提供了4中服務套餐（FW+、CT+、AV+和UTM+）。而相比之下，NBRS-5.0卻擁有了大量的安全模組。在近期的一次統計中，其中的57個模組就可以建立起NBRS-3.0基本同等的產品。這些模組中，有些相對比較小，而有些則相對比較大，比如基本安全模組，或者基於Web的管理系統，這些基本上都有幾百M的大小。

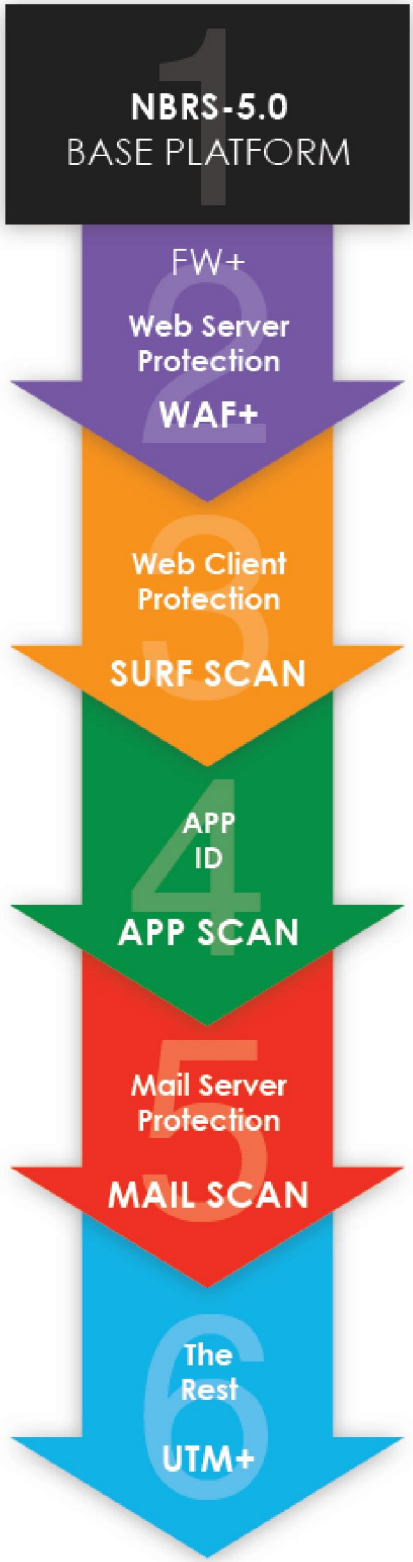
截止到今天，我們已經發佈了25個NBRS-5.0的安全模組，這些都是WAF+以及它所涉及到的支援系統的模組。除此之外，還包括了非常重要的安全基礎模組，還有防火牆模組，DDoS保護模組，代理模組，報告分析模組，以及基於Web的使用者管理介面介面。這些也僅僅是UTM+所有安全模組的小於50%的數量，但是超過90%的模組均已經完成了代碼的開發階段。

我們也已經發佈了我們整個的基礎環境和支援平臺，以更好地支持NBRS-5.0，包括Box Office的增強，代碼套裝軟體資源庫的內容分發網路，全球的前面特徵碼的發佈系統，以及全球NOC，授權認證和配置系統等。

我們也在作息不分地做著大量的工作和努力，在此期間一切如常，緊鑼密鼓而有序順利地進行著。嚴格來講，我們重新找到了一種實現安全的方法，那就是，從一個既定的威脅攔截裝置，向一個可以靈活對內容進行分類並進行策略執行的一個系統裝置進行轉變。當然，在完成我們的研究走出實驗室並且對外進行發佈之前，一切都還需要經過我們非常嚴格的產品生產標準的認證。這就意味著包括大量的程式設計，文檔的製作，模組測試和微調，這些都還需要大量的時間和精力。當然，這些也都是一些非常辛苦和嚴格的工作，但是，這一切都是非常值得的，要不然，如果我們採取任何可能的捷徑的話，也許就會因小失大而得不償失。

NBRS-5.0 路線圖

下面是一個線路圖，給出了一個非常清晰的關於我們最近都有哪些發佈的概述，以及最終的里程碑，最終的產品和服務，這一切都遠遠地超出了目前的NBRS-3.0 UTM+的所有功能。



1

早在2012年的夏天，我們就已經完成並發佈了NBRS-5.0的基礎平臺和基礎設施的支持。這些使得我們大部分產品的代碼的開發有了基礎的平臺，並未我們NBRS-5.0所有產品和模組的形成提供了基礎。

2

接下來的，就是2012年的冬天，NBRS-5.0 的WAF+服務包的完成。這個功能包提供了全新的功能（這是NBRS-3.0所沒有的），它用於保護DMZ區/基於雲的Web伺服器，免於遭受來自互聯網的攻擊。它還提供了網路防火牆，Web應用防火牆，DDoS防護和協定轉換（IPv4與IPv6，IPv6與IPv4的橋接）功能等，集於一身的服務包。

3

此前，爲了建立一個Web應用防火牆，我們首先必須要設計並建立一個能夠理解網頁的HTTP協定的代理模組。而現在，我們轉向了另外一個思路，將其與我們先進的掃描技術進行完美結合，也就是即將與我們NBRS-5.0的下一個版本同期發佈的SURF SCAN。這將提供用於針對基於Web的內部網路使用者的保護，以安全流覽互聯網上的Web伺服器。它還將支援病毒掃描，還有網站和內容分類，以達到更加全面的策略控制。同時它還提供了廣泛的統計報告功能。

4

再接下來，我們將推出APP SCAN，也就是應用識別系統，這個系統我們也爲之忙活了有一段時間了。它不論是獨立運行，或者還是與SURF SCAN相結合，都能很好地在網路層上對應用程式進行識別，並且從資料流程中提取中繼資料和內容。反病毒掃描和策略控制技術均可以同時運用。

5

到達這個階段之後，我們將有全面的針對Web伺服器和內部用戶端保護的支持，因此，我們將發佈我們針對郵件伺服器保護的MAIL SCAN。這將提供針對使用SMTP、POP3和IMAP4協定的郵件流量進行掃描。

6

最後，我們將爲UTM+整體功能畫上一個圓滿的句號，屆時將會發佈一系列安全模組和元件，包括QoS功能、VPN功能、集群功能、高可用性功能等等。當然，其中的有些功能模組可能會在一切都準備好之前，預先提前進行發佈。

版本遷移

在未來的幾個月內，我們將會發佈NBRS-5.0的遷移相關的一些資訊。與之前的NBRS-3.0的升級一樣，我們將爲所有現有使用我們Network Box設備（或者曾經獲批的虛擬系統）的客戶提供升級服務，並且將儘快將所有客戶的設備升級到Network Box第5版本的平臺上來。毫無疑問，2013年將成爲非常振奮人心的一年，這是因爲Network Box在技術進步上又更上了一個臺階。

Network Box Certified ISO 9001 / ISO 20000 / ISO 27001 Security Operations Centre

2013年1月 新特性

在2013年1月1日的星期二這一天，Network Box將發佈這次的Patch Tuesday的補丁包，各區域NOC將會在此之後的7天內安排這些新的功能的發佈和更新工作。這個月的更新補丁包包括：

- 各種內部NOC系統的改進；
- 針對管理介面my.network-box.com的一些小修改；
- 對郵件掃描系統的信封接受黑名單進行了一些小的修改；
- NBRS-5.0在Box Office系統中的進一步支援；
- 一系列針對Box Office和支援系統的（主要是內部）功能增強。

在多數情況下，以上的修改並不會影響到正在運行的服務，也不需要硬體重啓。但在某些情況下（取決於具體配置），可能需要重啓設備。必要時您當地的區域 NOC 將會與您取得聯繫。

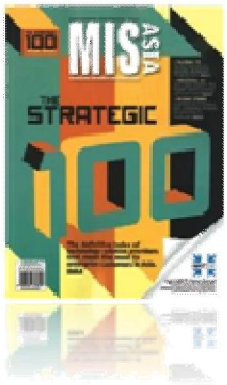
如果您還需要要關於這些的更多的資訊，請與您當地的區域NOC取得聯繫。他們將會進行相關的諮詢和安排。

NETWORK BOX | 2012年12月份所獲獎項

IT 類專業

2012企業最佳選擇獎

Network Box非常榮幸地宣佈，我們餓S-Scan和WAF-Scan均在所述類別的2012年IT類專業的企業最佳選擇獎。S-Scan是Network Box的高性能Web內容過濾引擎，而WAF-Scan是Network Box的Anti-DDoS Web 應用防火牆的增強系統。



MIS 亞洲 | *戰略100強企業*

Network Box最近榮獲了MIS亞洲|戰略100強企業殊榮。這也是Network Box第五次獲得這一殊榮，同時獲得此項殊榮的知名企業還包括Google公司，蘋果公司，Adobe系統公司以及三星電子公司等。

DECEMBER 2012 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	597	+11.8
Signatures Released	559,906	+46.5
Firewall Blocks (/box)	950,627	-1.1
IDP Blocks (/box)	122,782	+1.1
Spams (/box)	12,497	+9.2
Malware (/box)	807	-44.0
URL Blocks (/box)	158,749	-18.8
URL Visits (/box)	4,168,066	-14.6

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box Australia
Network Box UK
Network Box USA
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