In The Boxing Ring

IN THIS ISSUE

2.
2009 THREAT ROUNDUP
We discuss the threat numbers for 2009 and performance metrics of the threat landscape.

3.
2009 ENHANCEMENTS
A look at the software enhancements and features delivered in 2009 and planned for 2010.

3.
DEFAULT POLICY CHANGE
An important change to the Network Box recommended default policy regarding SCRIPT, IFRAME and OBJECT tags in eMails. Please take the time to read and understand this change, and discuss any special requirements you may have with your local support NOC.

4.
JANUARY 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.

4.
JANUARY 2010 HINT
Software vulnerabilities don't just affect Microsoft, and other popular software and platform providers are releasing security patches.

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

Welcome

歡迎您來閱讀2010年1月版“In The Boxing Ring”期刊。在這個版本中，我們回顧和總結2009年的威脅環境，以及在過去的一年中Network Box爲客戶提供的保護情況。

在第2頁，我們將討論2009年的威脅數字。Network Box安全回應團隊監控和管理著全球成千上萬的設備，這給我們極佳的視野去審視威脅環境。在Network Box，我們堅信，只有能夠清楚地看到和認識問題所在，才會提供可實現的解決方案（並獲得可衡量的控管目標）。

轉到第3頁，我們將回顧在2009年業已交付的軟體增強功能和特點，以及2010年的計畫。在過去的一年，我們一直在努力提供增強，修復，補丁和新的功能——這一計畫將在2010年持續進行。

在第3頁，我們也留下一些空間來討論Network Box建議的默認策略方面的一個重要改變，這個策略主要是針對電子郵件的中的腳本SCRIPT、框架IFRAME和物件OBJECT標記。請花些時間閱讀和理解這種變更，如果您有特殊要求，請和你本地的NOC進行討論，尋求進一步的支持。

打開第4頁，按照慣例將提供關於月度總結和使用技巧的小提示。

和以往一樣，如果您有任何的回饋，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。

您也可以通過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
January 2010

NETWORK BOX

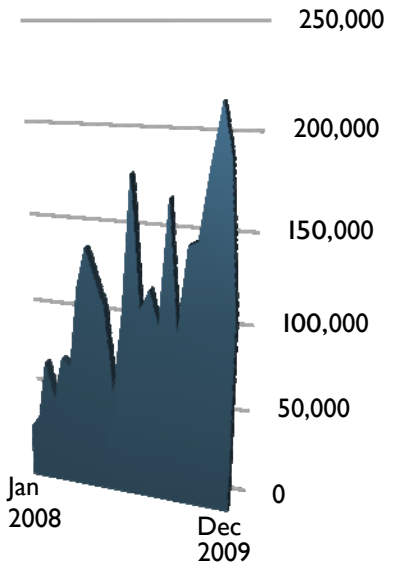
2009 Threat Round-Up

2009年，Network Box安全響應推進了14969次更新，共計2，905，697個簽名（與2008年的兩項指標相比，分別跌10.0%，和增長6.9%）。

平均計算的結果是大約每十點八秒就有一個新的簽名產生。

注：以上簽名只包括推進到客戶的Network Box中的，但不包括基於雲計算服務的簽名，和停止的已經過時的NBRS-1.1系統相關更新，以及許多遷移到“雲”計算的類型（主要包括反垃圾郵件和內容過濾），真正的推進式更新的增長並不是很清晰的。

反病毒特徵碼的增長速度仍然保持最大。僅看防病毒更新（見下圖表），我們看到了從2008年下半年開始不斷加快的顯著增長，我們希望這種趨勢將在整個2010年繼續下去。



2009年，平均每台Network Box阻止了621302封垃圾郵件和20251次惡意軟體（分別比2008年跌36.4%和42.2%）。

儘管如此，垃圾郵件和惡意軟體（特別是電子郵件群發）仍然是一個重大的問題，範圍廣大、不斷蔓延的開放代理意味著絕大多數的垃圾郵件和惡意軟體的來源已經轉移到僵屍網路和被攻破的主機。全球性合作，即時黑名單（它又名“信譽”），端掉大型僵屍網路指揮和控制中心老窩，如此一系列的行動確保了這種威脅的增長得到了有效的控制。

儘管如此，Network Box的客戶平均每49秒仍收到一封垃圾郵件或惡意軟體。

2009年，平均每台Network Box使用防火牆技術阻止了5，854，972次攻擊，使用的IDP技術阻止了1，572，211次襲擊（分別比2008年增長19.8%和47.9%）。

在2009年我們看到的最大變化是大規模的針對一個目標或有漏洞的系統進行溢出攻擊和利用，包括發送大量垃圾郵件和惡意軟體。可執行檔篩檢程式（例如通過 Network Box提供的）非常有效地阻止了它們。“黑帽”駭客已改變了戰術，重點利用那些應用程式中的漏洞，網路流覽器和伺服器（而不僅僅是郵寄出可執行代碼）。

“黑帽子”駭客行動的主要動機也已從“樂趣”和個人的滿足感，轉向商業金錢利益。如今，接管一個網站或工作站（不論用於進一步分發惡意軟體或建立僵屍網路）具有真正的貨幣價值，越來越多的大型犯罪團夥要來借助于這個利潤豐厚的業務。

我們預計這種趨勢會持續到2010年及以後更久。

2009年，平均每台Network Box由於執行公司的內容過濾政策封鎖了821，983個網站與27，132，231個網址，比去年訪問（分別比2008年增長高達131.7%和37.9%）。

這些統計數位清楚地表明，IT系統方面所面臨的壓力在帶寬和網路使用上都有所增加，以及對內容過濾政策的強制執行的反應。我們看到了比去年有兩倍以上政策執行阻斷的數量。

2010年，Network Box安全回應中心將繼續努力保持和佔據反病毒和反垃圾郵件的前沿地位。同時，增加的重點也將放在弱點或漏洞這一邊。

隨著同微軟建立MAPP夥伴關係，新產品如NBIDPS系統的發佈，脆弱性掃描服務的提供，Network Box將繼續努力致力於保護我們客戶的網路。

Network Box Threat Statistics	2008	2009	% Change
PUSH Updates	16,636	14,969	-10.0%
Signatures Released	2,718,770	2,905,697	+6.9%
Firewall Blocks (/box)	4,885,567	5,854,972	+19.8%
IDP Blocks (/box)	1,063,056	1,572,211	+47.9%
Spams (/box)	976,374	621,302	-36.4%
Malware (/box)	35,044	20,251	-42.2%
URL Blocks (/box)	354,757	821,983	+131.7%
URL Visits (/box)	19,668,707	27,132,231	+37.9%

2009 Enhancements

2009年一季度我們重點發佈了高度有效的電子郵件關係系統，引入了基於電子郵件的關係的垃圾郵件評分調整機制。我們還繼續在白名單，發件者框架協議SPF和有效的郵件外發政策上取得了改進。

在第二季度，我們採取了積極的辦法來幫助客戶應對Conficker問題，方法是在閘道層面從Network Box遠端掃描我們客戶的網路以發現存在漏洞的機器。這種主動掃描技術是第一次被Network Box使用，並奠定了未來掃描服務產品的基礎，進一步的漏洞掃描服務將在2010年第一季度得到公佈。通過檢測已知的漏洞，並協助客戶自己的補丁部署計畫，Network Box可以幫助我們的客戶更積極主動地保護網路（通過提前處理主要的弱點，而不是等候攻擊到達後再做響應）。

夏季（第二季度末，第三季度初）我們看到了Network Box客戶門戶系統得已發佈，給客戶提供了一個進入多台Network Box內部系統的視窗。該系統提供所轄範圍內即時的Network Box設備運作狀態，並允許正式和雙向的同Network Box網路運營中心NOC的溝通，NOC負責監測和配置客戶的設備和網路系統。

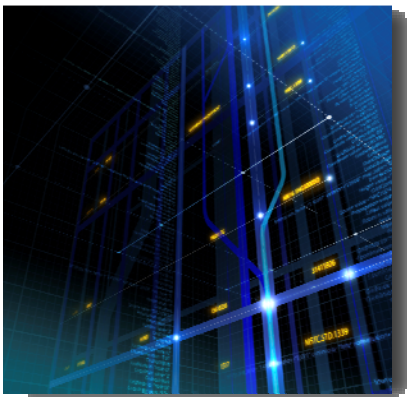
第四季度看到了NBIDPS的正式發佈及我們與微軟達成了MAPP合作夥伴關係。MAPP會讓我們在微軟的月度安全更新之前從微軟安全回應中心（MSRC）獲得相關漏洞資訊。

由於Network Box可以更早些地收到相關的漏洞資訊，客戶可以從中得到附加的安全主動保護改進方面的收益，諸如主動入侵檢測和防範，它是Network Box UTM+管理服務的一部分。建立夥伴關係如同微軟MAPP，Mitre CVE，和其他一些，會使Network Box收到漏洞的資訊會早和更好一些，使我們能夠更早獲得和釋放推進更新，以更好的更好地保護客戶。

第四季度也看到了支援加密的SMTP電子郵件的增強得已宣佈。

整個這一年，對my.network-box.com管理介面和郵件門戶網站的用戶介面添加了許多增強功能。其中的功能包括遠端關機/啓動，詳細的網路位址資訊，DHCP租約資料，跟蹤路由和Ping測試功能，改進隔離檔釋放，以及支持內置的SSL證書頒發機構，它整合了Network Box的SSL VPN，允許通過郵件門戶和電子郵件管道進行證書和VPN用戶端的分發。高潮時是9月份，我們發佈了大量的關於Web介面的美化改進，和以提高性能及易用性的改進，這些功能強大並使管理介面更有親和力。.

整個2010年，我們打算繼續不斷地改善我們的工作。



Default Policy Change

從2001年開始，Network Box已經建議客戶部署一個過濾郵件的默認策略，這些郵件包含特定的屬性（和可執行檔附件一起被阻隔），它們包括：

- CAN-2002-1121 消息/部分
- NBH-BHIDIFM 隱藏的內部框架
- NBH-BHIDOBJ 隱藏的物件
- NBH-BHIDSCR 隱藏的腳本
- NBH-BIFRAME 內部框架
- NBH-BOBJECT 對象
- NBH-BSCRIPT 腳本

注意：它總是，而且將繼續作爲關於拒絕/允許的客戶策略。Network Box公司只是負責執行客戶的政策。

最近，越來越多的HTML格式的郵件被更多的商業客戶採用，轉發網頁（而不是鏈結）的實際操作也越來越普及。我們看到越來越多的這些電子郵件從隔離區中被加以釋放。

據此，2010年2月週二補丁，Network Box將改變其默認建議的政策，具體如下：

1. 對於CAN-2002-1121，我們將繼續建議默認情況下封鎖消息/部分。
2. 對於內部框架，物件和腳本塊，我們會改變默認建議的政策阻止從“阻止所有”到“阻止隱藏”。

沒有對這些政策進行特別設置的客戶將遷移到新的默認建議的設置。你可以通過my.network-box.com的郵件/策略中看到你現在運行的的郵件策略。

如果你對此有任何疑問，請與您當地的NOC取得聯繫尋求幫助。

January 2010 Features

On Tuesday, 5th January 2010, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Refinements to the logging system, to better handle logging of disconnections of VPN clients under some circumstances.
- Enhancements to the logging system, to better handle logging of mail client disconnections during scanning (but before final mail delivery).
- Enhancements to the health monitoring system, to include monitoring of sub-services such as individual VPN links and multiple dynamic routing protocol services.
- Minor fixes to the my.network-box.com administrative web interface, relating to trace web usage with extremely large log queries, web proxy config groups with large numbers of group members, and improved validation of *@*.domain.com anti-spam sender whitelists.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

January 2010 Hint

軟體漏洞不僅僅只是影響微軟，其他流行應用軟體和平臺的供應商也正在發佈安全補丁。

在過去的一年，一些主要的軟體公司已經宣佈在其產品中，包括如下嚴重的漏洞：

- Adobe已經宣佈他們的PDF閱讀器和Acrobat軟體系統中存在多個漏洞。
- Adobe已經宣佈在其SWF Flash軟體中存在多個漏洞。
- WordPress博客已被發現存在容易導致管理員密碼失竊等多個漏洞。
- 幾個主要的Web框架（包括流行的Drupal web CMS）存在多個漏洞，會導致遠端執行代碼及SQL注入攻擊。
- 流覽器如蘋果Safari流覽器，Mozilla Firefox和Opera都有重要的漏洞宣佈。

在2010年1月小提示就是，一件非常重要的事情，你需要檢視你的組織中正在使用的所有軟體系統的更新政策和程式，而不僅僅是微軟。微軟可能是最大的目標，但它不是唯一的目標。

Mark Webb-Johnson,
CTO, Network Box Corporation

DECEMBER 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,394	+11.9
Signatures Released	146,314	-38.0
Firewall Blocks (/box)	635,866	-1.1
IDP Blocks (/box)	177,906	-15.6
Spams (/box)	47,738	-26.4
Malware (/box)	1,956	-32.7
URL Blocks (/box)	104,333	+3.6
URL Visits (/box)	2,901,600	-9.0

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