In The Boxing Ring

IN THIS ISSUE

Network Box 技术新聞

作者： **Mark Webb-Johnson**，首席技术官

致辭

歡迎您來到 2009 年 1 月版 'In The Boxing Ring' 。我打算使用此版簡單地總結一下我們在 2008 年的所作所爲以及我們 2009 年的計划概況。我也將第 3 頁使用一些頁面空間來討論最近的 CVE - 2008 - 4844 （ MS08 - 078 ）漏洞，這個 12 月份出現的嚴重漏洞影響着多個版本的 Microsoft Internet Explorer 瀏覽器。

在本通訊的第 2 頁，我們將粗略的回顧一下在 2008 年的增強性改進點，以及 Box 的功能和重要開發項目的交付情況。在過去一年里，我們處理了超過 300 個增強性改進點的要求及軟硬件修復任務；我們也在前進的道路上取得了非凡的成就，在若干個關鍵技术上也到達了新的里程碑。這些已經或者正在提供的增強功能將作爲 2009 年及以后我們的服務交付平台的一個基礎。對于已經使用了 NBRS - 3.0 的客戶，這一切增強性的功能都是免費提供的，是我們爲您服務的一部分內容。

在本通訊的第 2 頁，我想給您一個我們 2009 年工作計划的概況，包括我們的技术戰略規划以及增強性功能開發計划，這些都是您希望了解到的。由于篇幅空間有限，在這里我只能做一個簡單的概況性總結，我會強調和標識出我們的產品方向的要點，在未來几個月內我們會逐漸提供更詳細的內容給到您手上。對于已經使用 NBRS - 3.0 的客戶，這些功能仍將爲您免費提供。

2008 年是充滿挑戰的一年，我們已經看到了垃圾郵件，惡意軟件和其他威脅的不斷增加。在未來，新的威脅也會不斷地出現，我們也會一直忙碌着去應對，無論如何，我們期待 2009 年，爲您提供更多的高質量服務。

和以往一樣，如果您有任何的反饋，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 nbhq@network-box.com 聯系我們。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。

Mark Webb-Johnson
CTO, Network Box Corporation
January 2009

NETWORK BOX

NETWORK BOX

回顧 2008

年初，我們開始了 Network Box 網絡運維中心 NBRS - 3.0 平台的遷移工作。這一工作可使客戶獲得更爲快速的推送式更新，并可提供更好的工具給我們網絡運維中心的工程師們，以便更好地支持我們的客戶。在第一季度，我們還完成了一套電子郵件掃描系統的測試和部署的變更，以便支持一個新的（更快）的反垃圾郵件簽名系統，包含自動貝葉斯訓練的更新，以及開始發放含垃圾郵件發送者使用的電話號碼和電子郵件地址的反垃圾郵件簽名。

在第二季度，我們發布了我們的 E-x 系列的機型 (E-1000x ， E-2000x 和 E-4000x)。這些新機型采用了英特爾 ® 至強 ® 多核心技朮（提供 2 個， 4 個和 8 個核心分別），取代了基于 Opteron 的 E 系列機型。新機型還提供了更大的內存和硬槃容量，以及遷移到 PCI Express 架搆以及 12 千兆以太網端口的擴展能力。

在第二季度我們也發布了增強性的 my.network-box.com 管理界面功能更新，在 Web 代理服務器，防火牆， IDP 和郵件模塊支持 ' 跟蹤 ' 的功能（包括實時查看的跟蹤功能）。我們還發布了我們的郵件掃描系統的功能性增強，包括支持 Office 2007 文件和微軟智能標簽（同 .bin 附件過濾相關的策略更新和有對象標簽的 HTML 郵件） 。

6 月下旬出現了大量的針對 WEB 服務器的攻擊，尤其是惡意代碼和普通的 SQL 注入攻擊到有后端 SQL 數據庫的 WEB 服務器。 Network Box 安全響應中心發布了一個新的 IDP 攻擊防御模塊（名稱爲 HTTP-SSQLINJWORM ）。雖然沒有網關設備可以 100 %防止這類型的應用層攻擊，我們還是很高興地看到我們的新模塊有效地阻止了這種病毒蠕蟲攻擊我們的客戶（我們的全球蜜罐跟蹤系統使我們能夠在它成爲全球問題的前几天就更新好攻擊防范代碼）。

7 月份我們看到 Network Box 遷移到了一個以星期二補丁爲形式的發布周期（第一個星期二補丁是 2008 年 7 月 1 日） ，并發起了 “ In The Boxing Ring” 時事通訊。該時事通訊還宣布推出几項新的 NBRS - 3.0 平台的功能性增強，包括 NBCS 內容過濾引擎，匿名代理的增強性分類，未歸類網址的反饋，并支持新推出的 E-1000x ， E-2000x 和 E-4000x 機型。

8 月份公布的 NBLDAP 系統，使 Network Box 內容過濾政策可與 Active Directory 的群組進行集成。爲了客戶能快速進入工單支持系統，我們在北美，歐洲和亞洲建立了區域網站鏡相，以提供本地快速的接入。新的鏡相支持英文，繁體中文，簡體中文和韓文語言（后續會慢慢加入更多的語言）。

在 9 月份，我們開始支持谷歌安全瀏覽和谷歌 / 雅虎安全搜索。我們還發布了多語言支持，使郵件門戶 Mail Portal ，系統管理界面 my.network-box.com 和每周報告可以支持繁體中文，簡體中文，韓文（除了標准的英語，后續會慢慢加入更多的語言）。

10 月份是最繁忙的一個月，我們發布了工單系統用戶界面門戶和防垃圾郵件的關系管理系統。

工單系統用戶界面門戶是一個正在進行的項目，它即將在 2009 年第一季度正式發布。該項目整合網絡中的監測系統，庫存，許可，部署，工單和工作量統計到一個單一的以網絡爲基礎的框架內，系統運作在云端。

電子郵件關系系統用一個以改變游戲規則的做法來處理垃圾郵件和帶病毒的電子郵件。 Network Box 的關系管理系統采用了前期數據挖掘、后期打開挑戰及響應的功能，這樣做的好處很明顯，使它對于寶貴的系統資源來講，只增加了最少的系統開銷（在某些情況下實際上是減少了開銷）。

對于垃圾郵件發送者，他們將不得不重新設計他們的整個數據庫系統。我們的以關系為基礎的系統是在 11 月向客戶發布第一版的，我們會陸續推進和完善此功能（預估 09 年上半年完成）。

同樣在 11 月，我們推出了一種新的反垃圾郵件引擎——模糊指紋，它能夠檢測和攔截垃圾郵件的文字 / 附件中極微小的變化。

12 月公布的全球網絡監控系統已經應用到所有客戶的 Network Box 。隨着遷移到全球網絡監控系統的是，我們能夠提供給我們的客戶一個真正有用的資源進入渠道，它可確保網絡，設備和服務的可用性。我們爲每個 Network Box 監測 100 多個指標，這個系統爲客戶提供了進入和了解 Network Box 狀態信息的一個窗口，實時狀態與全球概覽功能對于在多個國家擁有多台 Network Box 的客戶非常有實用價值。

除了上述的功能增強， 2008 年是以往任何時候中忙碌的一年。我們統計的結果是， 2008 年，平均每個 Network Box 有生成 630 萬條防火牆記錄和 130 萬條入侵防御記錄， 120 萬封垃圾郵件掃描結果，其中有 4.4 萬封包含病毒 / 惡意軟件或釣魚郵件，2400 萬網頁對象被掃描，其中含惡意 / 病毒和策略阻止訪問的不良網站有近 50 萬。
此外， Network Box 總部有通過超過 16800 次推送更新分發給每台 Box 近 270 萬個保護簽名。

然而，我們做的不僅僅只是提供一套固定的功能和更新的簽名來識別威脅， Network Box 在該領域投入了眾多型號的產品和基礎設施來發揮作用，不僅保持對最新出現的威脅的識別，也形成了一套有效隔離那些威脅的戰朮。隨着時間的推移，黑客，病毒作者和垃圾郵件會不斷改變策略，只有一個同樣充滿活力，以服務爲基礎的如 Network Box 的解決方案，才可以跟上這一需要自適應的安全格局。

展望 2009

Network Box 在 2009 年的路線圖強調在五個主要領域內做強化，讓我們現在一個一個講給您聽。

1. 提高每個 BOX 的管理和監測系統的數據和統一矩陣的能見度。

該項目將統一整合工單客戶門戶系統及 BOX 管理信息的監測，庫存，許可，部署，工單和工作量統計系統。它也將統一通過工單系統生成按由 Box 爲序的報告，這樣產生的數據可以與其他國家相比，比如類似的位置，組織類型，大小或行業。

2. 提供一個整體單一的 GUI 界面。

用于鑒別用戶和服務的網絡流量（統一的 Mac ， IP 地址，電子郵件地址和用戶名）。這是我們的產品發展方向的一個關鍵組成部分。 Network Box 產品將連接和配合現有的 DHCP 及 LDAP 目錄，以及在 Box 上運行的系統，以提供一個單一的有整體觀的用戶和機器的活動。不同地址的概念（如 Mac ， IP 地址，電子郵件，用戶名）將統一爲一個報告 ' 實體 ' 。目前按每個模塊進行統計的方法將融合成一個多層面的服務和其它的實體（或實體的群體）于一個軸心的報告框架。

3. 用一個統一的報告和數據輸出框架改進的現有的報告和分析功能。

現有的 my.network-box.com 、郵件報警和定期報告機制將被統一到一個單一的框架，使用基于 Web 的 AJAX ， PDF 文件，電子郵件和數據輸出功能。所有的報告將通過這一新的框架來實現。

這將允許數據的輸出，打印，和報告（通過 HTML 或 PDF 格式），并允許檢索以前產生的報告。該框架將允許自定義地通過電子郵件，網頁或文件傳輸機制等方式發送定期報告。

4.Network Box 設備配置和管理集群的統一和細粒度改進。

配置將能夠在全球范圍加以界定，可按每簇，每方塊，每個域或每用戶進行配置管理。配置更改將能夠集中進行，并且可以跨廣域網進行相連接的 BOX 之間配置的復制和同步。群集的支持將是這個改進的核心所在，同時將允許同本地或廣域網上的 Network Box 之間自動負載均衡地處理網絡流量。

5. 擴展更多的協議支持。

這里的大部分工作涉及到客戶端和服務器端對 SSL 加密協議支持，主要協議包括： POP3S ， SMTPS ， IMAP4S 和 HTTPS 。而且我們也正在努力添加一些功能使 BOX 可以分析新的協議（特別是在點對點通訊和即時消息領域）。

上述這些將會有一個全面的基于整個全球網絡的 Network Box 的曆史檢視界面，配置粒度會細到按每個用戶的水平。如果您有 1 個或 100 個 Network Box 的網絡，系統的配置將可以大致一樣的安全水平，而且有很強的可擴展性。

首先要滿足的需求是提供用戶報告的改善。目前我們已經設計出來了一個全新的報告和數據存儲的框架，用以滿足對大多數法律法規的遵從和管理報告的要求（包括使用標准格式進行數據導出的功能）。

我們希望能夠在 2009 年底之前免費地爲大家提供上述軟件增強性改進。

CVE 2008-4844

2008 年 12 月，微軟發布了關于 Internet Explorer 7 和早前版本 IE 的零時差漏洞公告，這個漏洞允許遠程攻擊者對受害人的計算機執行惡意程序。 Network Box 網關設備能夠防止用戶遭受利用此漏洞的惡意程序攻擊。它會在互聯網網關處分析和隔離出惡意代碼的負載——即在它們到達客戶端計算機之前就阻止——使用內容過濾和 HTTP 病毒掃描技术。

由于攻擊的載體是 Internet Explorer 本身，攻擊者可以有不同的有效載荷的攻擊，因此不可能給一個通用的識別此漏洞的有效載荷。

使用 Network Box 的 PUSH 推進更新技术，我們可以在几分鐘內將我們的反病毒合作伙伴卡巴斯基實驗室新開發的病毒和惡意代碼的簽名發送到顧客的 Box 中。

使用 HTTP 的防病毒，當關于這個漏洞的有效載荷首次被發現時， Network Box 就能爲其用戶免受惡意代碼的有效載荷攻擊提供保護，由于它保持了不斷變化的防守抵擋機制以應對這些不斷變化的攻擊。

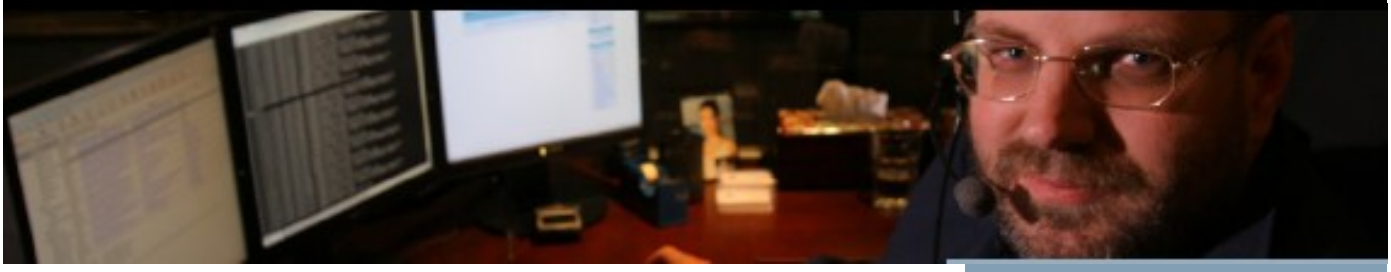
Network Box 建議客戶應采取以下措施，以便對漏洞 CVE-2008-4844 有更強的防護：

1 、確保 Network Box 網關設備中的內容過濾功能是啓用的。 Network Box 默認已經將一些惡意的網站列爲限制性的不良分類 nb-malware 。因此，在瀏覽請求離開該客戶網絡之前內容過濾就已經限制了惡意網頁的瀏覽請求。

2 、確保 Network Box 網關設備 HTTP 防毒掃描功能是啓用的。這使得有效的威脅在進入用戶端電腦之前就被 Network Box 發現和阻隔。

3 、確保您的內部網絡計算機的配置是將 HTTP 請求提交給 Network Box 網關設備，無論是直接地通過瀏覽器設置代理，或間接地通過在網絡中或網關處做重定向。同樣，如果您不確定當前的使用狀況或希望啓用，請聯系您的 NOC 支持人員。

4 、保護您的內部網絡計算機免受此漏洞，直接下載并安裝微軟 Internet Explorer 的安全更新，或者客戶應按照自己的補丁管理程序進行關鍵更新的安裝。



January 2009 Features

本月看點

由于聖誕及新年假期的原因，我們即將舉行的星期二補丁定在 2009 年 1 月 6 日，是一個比較輕微几乎無影響的補丁。我們將推出一些小的增強功能，其中包括：

外發郵件聲明封裝支持 Lotus Notes 郵件系統和超過 999 個字符的可打印引述編碼。

對客戶端服務器模式的內容過濾分類系統進行了優化（對小型、輕量的 Box ），以便更好地（更快地）檢測和解決網絡連接故障。在過程中將需要重新啓動一些 Box 的內容過濾服務，但影響會被降到最低，具體的應用是對上網瀏覽和電子郵件掃描會有輕微及短暫的影響。

我們已經做了一些對 NOC 的工程師的日常 Box 維護工作進行審計的改善。再加上 NOC 自己對工作的審計，可使我們能夠更好地滿足法規遵從要求，并對維修工作負責。

最后，我們已經改進了內核模塊對 H.323 協議的連接跟蹤和 NAT 支持（適用于使用 H.323 協議的 VoIP 裝置）。

這項工作并不需要給您的用戶帶來明顯的服務停用時間，也不會需要重新啟動您的 Network Box —— 所以影響應該是微乎其微。

如果您需要關于上述情況的任何進一步的資料，請聯系您當地的 NOC 。他們將和您聯絡并安排相關的部署工作。

Patch Tuesday

星期二補丁

Network Box 已進入一個以星期二補丁爲形式的軟件增強釋放機制。這是爲了讓 NOC 向我們的客戶發布和安裝新的軟件和增強功能，并在全球范圍內以統籌的方式進行。所有 NOC 都有相同的星期二補丁日程表。這并不影響正常的實時推送更新，國爲這些更新的只是新功能和增強功能而已。

對于 Network Box 的客戶來講，星期二補丁就是每月的第一個星期二。第一是星期二補丁是 2008 年七月一日。

其它的關鍵的軟件補丁，簽名和日常（或每分鐘）更新發布將仍時有發生的周期，在每一個月，我們通常會發布新軟件功能和增強功能的星期二補丁，并每月初進行分批分階段地部署到所有客戶的 Network Box 中。

對我們的客戶來講，這份 “ In The Boxing Ring” 通訊月刊是用來隨時向你通報我們一直在爲您做什么，以及您即將看到的在每月星期二補丁中發布的新功能 / 改進功能。

結束語

感謝您的支持 Network Box ，并繼續將您的網絡安全托付給我們的管理服務。我希望這份通訊月刊對您有用。如果您有任何建議，我們都非常歡迎，您可以向當地的 NOC 或客戶經理反映；如果您有其它需求，也請別猶豫，馬上與我們聯系，尋求協助。

Mark Webb-Johnson
CTO, Network Box Corporation
January 2009

DEC 2008 NUMBERS

Key Metric	#
PUSH Updates	1,232
Signatures Released	214,664
Firewall Blocks (/box)	556,622
IDP Blocks (/box)	131,137
Spams (/box)	54,643
Malware (/box)	1,991
URL Blocks (/box)	54,773
URL Visits (/box)	2,364,433

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jasmine Arif
Jason Law
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