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 2 月版 'In The Boxing Ring' 。在這一版，我將用一整頁來談論即將發布的第三個基于電子郵件關系管理的防垃圾郵件技术。

如果您還記得， Network Box 電郵關系所關注的是跟蹤外部發件人、發件人的屬性和內部收件人之間的關聯，使用所產生的數據庫來以提高防病毒和防垃圾郵件的准確性。首先發布的是電子郵件關系跟蹤引擎本身（其中包括分析收到和發出的電子郵件，以建立關系數據庫）。第二個發布的系統是挑戰 / 響應系統（挑戰此前沒有建立關系的電子郵件發送者）。第三個系統，也就是即將在本月初發布的系統，在關系管理的力量基礎上，使用關系數據庫自動調整反垃圾分數。本通訊的第 2 頁會更詳細的告知您這一新功能。

在第 3 頁本通訊將重要討論兩個安全政策相關的問題，因爲我們最近看到我們的一大批客戶一次又一次的碰到這個問題。首先是白名單的做法，客戶將自己的電子郵件網域加入到白名單（這導致垃圾郵件發送者僞造用戶的郵箱成功發送垃圾郵件）。第二個是缺乏有效的向外訪問（出站）的防火牆 / 內容過濾政策（這會導致信息泄漏和難以執行適當的用戶上網行爲的控制）。我對這兩個問題進行了詳細的討論，并提出解決方案和變通方法。如果這些會給您帶來影響，請考慮馬上修改您的安全政策。

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
February 2009

NETWORK BOX

關系型垃圾郵件打分調整

我很高興能宣布，現在已經准備正式發放第三個 Network Box 電子郵件關系系統。這種新系統基于關系的深度，采用關系數據庫來自動調整反垃圾分數。接下來，這篇文章將討論這一系統的運作方式，以及它是如何來：
（ a ）更積極獲取已知垃圾郵件來源和
（ b ）識辨出及親近已知的有良好來源的非垃圾郵件。

對如下的純技术方面的描述，我感到有些報歉，但重要的是您可以看到該系統在確定垃圾郵件評分的調整方面是如何工作的。

垃圾郵件分數關系的調整通常是應用于入站 SMTP 電子郵件，而不是通過備份 MX 服務器（例如從發件人直接發送）。如果電子郵件已經明確的定義了白名單或黑名單，該系統也將無法正常運行。

對于每封郵件，它首先要確定（使用信封分析和基于地理位置的 IP 地址）發送者的一些基本信息，其中包括：

* 電郵地址
* 電子郵件網域
* IP 地址
* IP/16 地址塊
* IP 地址歸屬國

該系統然后查詢關系數據庫匹配下列元組，并產生一個跨越匹配關系的平均總數記錄：

* 發件人的電子郵件地址，發送國家，接收者（匹配特定收件人地址則定爲 75 %，匹配郵件域則定爲 50 %）。

* 發件人的電子郵件地址，發送人 /16 的網絡塊，接收人（匹配特定收件人地址則定爲 100 %，匹配郵件域則定爲 75 %）。

* 發件人電子郵件地址，收件人（匹配特定收件人以往外發郵件關系建立則定爲 50 %）。

該信心指數是基于上述的比重的重新匹配。例如，如果我們有關系的記錄，以前的電子郵件來自特定寄件者，來自某一特定國家特定的收件人，那么，我們對待這個相信 75 %是相同的發件人。

關系數據庫存儲的關系分數范圍 -100 到 100 （ -100 表示 100 %的惡意， 100 則表示 100 %的非惡意）。這些數據庫爲它們存儲關于每個信任度，垃圾郵件，惡意軟件和政策的數值。

在防垃圾郵件掃描的最后階段，電子郵件與垃圾郵件分數調整機制將：

1. 采用關系垃圾郵件平均打分，乘以信任指數（以百分比表示），以確定調整后的垃圾比重（以百分比表示）。例如，如果關系，記錄了 +100 （即： 100 %不是垃圾郵件），以 50 %的信任指數，調整后的垃圾郵件的比重將是 25 % （即： 0= 正常郵件， 100= 垃圾郵件，我們在一半以下中間的地方不到 50 點）。

2. 映射調整后的垃圾比重到垃圾郵件評分滑動配置表，以確定調整垃圾郵件的評分。例如，如果垃圾滑動規模爲 -7 到 7 ，然后以電子郵件的關系的曆史表明，調整后的垃圾比重爲 25 %，結果調整后的垃圾郵件評分爲 -3.5 （即： 25 %的比重在 -7 到 7 之間 ） 。

3. 提交垃圾郵件的測試結果，調整的總體垃圾郵件評分爲上升或下降，取決于調整后的垃圾比重。這種垃圾郵件測試被命名爲 NB_RELATIONSHIP_SSA 。

注：有一種替代模式（即所謂 ' 比例 ' ，而不是默認的如上所述的“范圍 " 模式）雖然它不是默認啓用的，但是也是可用的。在”比例“模式下，第二階段確定的垃圾郵件評分調整更改不使用滑動窗口，而是使用目前的實際得到的垃圾郵件評分。例如，一個郵件消息目前得分 10.0 ，并有一個調整的垃圾郵件比重爲 25 %，結果調整的垃圾郵件評分爲 -5.0 （和整體垃圾郵件評分因而被減少到 5.0 ）。這種方式的結果比默認的 ' 范圍 ' 模式要敏感很多，所以通常不會啓用。

電子郵件與垃圾郵件分數調整制度對”邊境線“區內的垃圾郵件（一般調整前的分數在 5.0 至 9.0 之間）是非常有效的 ，并能給出相關的標示，以區分它們是垃圾郵件或非垃圾郵件。它會根據以前發送者和接收者的關系情況調整新郵件的垃圾郵件評分，并有試圖驗證發件人的信任挑戰機制，甚至在 SMTP 協議本身沒有啓用發件人身份驗證功能的狀態下也可行。

該系統有強大的可配置性，并且可進行微調，并可以配置為只調整分數上漲或下跌的配置的調整范圍。目前的工作正在取得積極的進展，在防病毒和政策執行方面也有提供同樣的技术。

這一新功能的代碼正在進行最后階段的測試和一些默認的調整。我們計划在 2009 年 2 月 23 日將它作爲一個 PUSHCODE 推進更新到所有 NBRS-3.0 的客戶 BOX 中。

將電子郵件網域加入到白名單

當今市面上的所有反垃圾郵件系統都會有些許誤報，但是我們仍然努力爭取能獲得 100 %的垃圾郵件檢測准確度，和 0 誤報率（即正常郵件不被誤斷爲垃圾郵件），我們永遠不能做到完美無缺（因爲垃圾郵件本身的不確定性質）。極端情況下的例子包括：一個人的垃圾是另一個人的正常郵件列表；如果我向你轉發出垃圾郵件，你收到后它仍然是垃圾郵件？這最后一個例子引出一個關鍵的問題，就是白名單自己的域名的不良后果。

Network Box 使用一些技朮以避免這一問題，用以防止您自己的內部電子郵件在無意中被視爲垃圾郵件，其中包括：

1. 綜合區分“出站、外發”和“入站、流進”的電子郵件。出站的定義是，發件人獲准通過 Network Box 中繼發送郵件，盡管它和發件人的電子郵件地址或域無關。入站電子郵件的定義是，非出站的郵件。中繼能力可通過源 IP 地址（內部工作站 / 服務器和 VPN 客戶端）或 SMTP 認證（對外部用戶通過 Network Box 轉發）。

2. 在默認情況下，反垃圾郵件功能沒有應用于“出站、外發”的電子郵件。這意味着電子郵件從您的工作站，服務器，VPN 客戶端和 SMTP 身份驗證的用戶永遠不會被視爲垃圾郵件。

3. 對使用 Network Box 的外部辦事處，向外發送郵件的數字簽名爲正常郵件，并且默認情況下，將由 Network Box 接收并標識爲信任郵件。這意味着從外部辦事處來的電子郵件也在 Network Box 保護之下，他們也將永遠不會被視爲垃圾郵件。

從上述名單中，您可以看到，如果網絡（及其用戶）得到適合的配置，從您的同事那里發來的電子郵件將永遠不會被視為垃圾郵件，并有機會達到零的假陽性報告。

那么，為什么不把自己公司域名加入到白名單中呢？現在的問題是，垃圾郵件發送者的清單里包含數以億計的電子郵件地址。他們知道您的電子郵件地址，他們也知道在同一郵件域中您的同事的電子郵件地址。他們（一般）不知道和您溝通的其他郵件域。因為沒有對您的電子郵件地址進行認證的單一的標准，所以垃圾郵件發送者很容易假冒您或您的同事作為發件人來發送給您或您的同事垃圾郵件。

在 2008 年 6 月， Network Box 安全響應中心進行了一項垃圾郵件的調查，結果有發現大約 1 %的垃圾郵件中的信封發送地址的網域和收件人地址的網域是相同的。在當時，白名單自己的域名將意味着， 1 %的垃圾郵件將順暢地通過 Network Box 到達您的郵箱（由于您將它列入了白名單）。然而，在 2008 年 12 月新一輪的垃圾郵件開始襲擊人們的郵箱時（與 MSN/ 雅虎即時通訊聯系，并邀請聊天），我們發現，發件人域名和收件人域名相同的比例已經非常之高。實事上我們已經看到一部分受影響的客戶，有 20 %以上的垃圾郵件發送自客戶本身的網域郵件地址。

發件人策略框架（ SPF ）提供了一個可以解決這一問題的方案， Network Box 已經支持這一框架。使用 SPF ，您需要確保您的所有出站郵件都經過界定網關。然后，在您的域名的 DNS 下發布 TXT 記錄，其中列出那些網關。這樣接收郵件服務器（包括 Network Box ）就可以驗證到這一點，并可發現對您的域名的假冒使用。

因此，請避免將自己的域名加入白名單，因為有几個很好的替代辦法，可以用來避免假陽性問題。

向外訪問的安全過濾政策

許多年前，在計算機安全方興未艾之時，防火牆通常配置為允許所有傳入連接，但只攔截某些特定的端口（如遠程登錄 telnet ， rsh 等）。但是很快人們發現這樣做是不夠好的。

現在對我們的大多數客戶來，通常采用的標准做法是確定入站安全政策為“除……之外阻止所有端口” （和以前的出站策略“除……之外允許所有”情況正好是相反的 ）；而出站政策沒有做類似的嚴格設置。

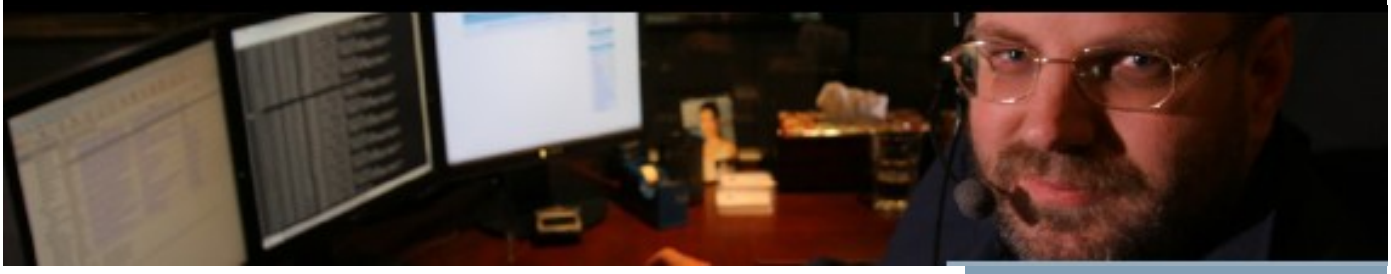
我們得到的其中一個最普遍的要求是“請阻止 Skype” 或 MSN ，或 QQ 或其他一些協議 / 應用程序（而不是端口）。

現在的問題是，應用程序會支持多種協議，這樣用戶就很容易穿透在防火牆上放開（未經過濾）的出站端口，或者可以使用隧道軟件或應用代理，或通過搜索所有可用的端口，直到它找到一個放開的可以利用的。

最好的**解決辦法**是使用和入站安全策略相同的方法，作為出站安全策略。**默認阻止所有的端口，然后在受控制的方式下允許那些被嚴格要求進行放行的。**

對于大多數公司來說，防火牆可以配置為阻止所有出站連接，除了那些非常確定的可以通過 Network Box 的安全代理的應用（如 DNS ， SMTP 電子郵件等），并強制所有的網絡接入通過 Network Box 的 Web 代理（用于上網行爲控制和強制執行安全策略），這樣做也將很少或根本不會帶給用戶工作效率方面的負面影響，但是卻會在安全性和控制管理方法得到巨大的改進。

一旦默認為“阻止所有” ，然后就可以逐漸進行細粒度地控制（甚至會有特定的工作站地址需要開放某些特定的權限），請聯系您當地的網絡安全運維中心 NOC 提供與此有關的進一步的援助。



February 2009 Features

本月看點

2009 年 2 月的星期二補丁，將会推出一些錯誤修復和增強的 Web 代理政策評價引擎，包括如下工作：

首先是技朮上非 DNS RFC 標准的主機名稱問題，但有時會用于解析內部主機名稱。所以我們放松了對這一點驗證確認，并允許它們通過。

一個系統性的增強，可使“可疑網址”分類引擎在必要的時候被禁用或重新排序。

修訂了政策分類緩存，使未分類的結果能更快的顯示出來。

修正了 NBCP 客戶－服務器引擎，以改善高負荷下服務器點的選擇和較差的互聯網連接條件下的查詢速度。

上述變化將需要重新啟動政策引擎，過程中會造成 Web 代理分類的几秒鐘停止，但應該不會造成網頁瀏覽的大量中斷。

我們還將發布擴展我們的全球監控系統監測軟件包，使其支持“抑制”系統健康問題警示。在這種情況下， BoxOffice 客戶門戶將會使傳感器出現爲抑制狀態，但不會被視爲一個錯誤。這主要是針對已經確定下來但是不能由 NOC 來解決的問題，而必須客戶來參與（如系統利用率過高，系統超載，或者環境問題等等）。

如果您需要關于任何上述情況的進一步的資料，請聯系您當地的 NOC ，他們將會安排補丁的安裝部署及必要時同您聯絡。

February Hint

本月小提示

2 月份的一個小提示，別忘了您電腦機房的環境。如果您在南半球，現在正是盛夏；對于那些在北半球的客戶，夏天是僅僅几個月前剛剛離開（盡管現在并不像夏天）。

台式或機架式電腦通常消耗 100-300 瓦的電力，并且會轉換成噪聲，光，熱（絕大部分是熱）。把 3 個或 4 個台式電腦在一起，你就相當于擁有一台 1 千瓦的暖風機。

隨着假期的結束，現在正是來檢查您的空調能力的一個很好時機。在您最近加了一些服務器之后，是否仍然有足夠的制冷能力來支持高峰時期的使用？是否有定期維護？你有經常監測嗎？等等等等。

提示：您可以遠程通過使用管理界面 my.network-box.com 來檢查 Network Box 的溫度，選擇 Box/ 狀態 / 系統健康狀態，查看“系統溫度”，另外某些型號的 BOX 還可以讓您通過前端顯示面板得到這些信息。

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
February 2009

JAN 2009 NUMBERS

Key Metric	#
PUSH Updates	1,223
Signatures Released	356,745
Firewall Blocks (/box)	564,463
IDP Blocks (/box)	139,502
Spams (/box)	69,146
Malware (/box)	753
URL Blocks (/box)	48,300
URL Visits (/box)	2,144,895

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