In The Boxing Ring

IN THIS ISSUE

Network Box 技朮新聞

作者： Mark Webb-Johnson，首席技朮官

致辭

歡迎您來到 2009 年 4 月版 'In The Boxing Ring' 。在這一版中，首先將和大家講講有關 Conficker 蠕蟲和從 Network Box 網關進行遠程掃描，以發現網絡中受感染機器的狀況。

并且我們在業界首次成功地啟動了這一緊急響應行動，時間在 3 月 31 日，僅僅就是愚人節 4 月 1 日 Conficker.C 爆發日期的前几個小時。在這一天，全天候服務的 NOC 工作人員進行了成千上萬次的掃描，大大提高了我們客戶的整體安全性。

這個月，我們將發布大量的軟件更新， my.network-box.com 的管理界面也將有重大的改良，它可以使客戶更方便和快捷地進行查詢，報告和控制 Network Box 設備。

我們將發布功能完備的證書頒發系統，使 NOC 和客戶都可進行相關控制。以及支持 SSL VPN 實時連接狀態查看和日志查詢分析的功能。請轉到第 2 頁查看詳細信息。

在第 3 頁，我將向您展示一個專門針對從特定的僵尸網絡發送垃圾郵件和惡意軟件的郵件掃描框架和目前我們所取得的進展。

我也將向您介紹發件人策略框架（ SPF ）技朮，它只需很簡單的配置，我建議我們所有的客戶都部署它。。

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我們的郵件列表： 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。

您也可以通過加入或訂閱我們的安全響應 Twitter 和我們保持聯系，網址是：

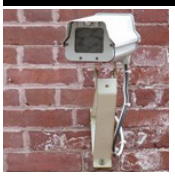
twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
April 2009

Network Box Wins PC3 Platinum Brand Award 2008

Network Box 贏得 PC3 2008 年度白金至尊品牌大獎，這個大獎用來獎勵 Network Box 在 2008 年爲消費者帶來了最優質的產品。

詳細資料請見五月份的 In the Boxing Ring 。



Conficker 蠕蟲網絡掃描工具

Conficker 蠕蟲一直以來都以有非常多的變種而著稱。據估計，受感染的電腦數量有將近 9 至 15 萬台電腦；針對已經測試的計算機的一項調查報告顯示感染率在 6 %。雖然 Network Box 中有反病毒軟件和 IDP 兩種針對所有已知變種的代碼簽名，該蠕蟲病毒仍然可以利用網絡的漏洞進行傳播，比如通過網絡共享和 USB 設備——因此它可能已經感染了您的局域網 / 非軍事區，那里的網絡可能跨越了 Network Box 的網關保護。

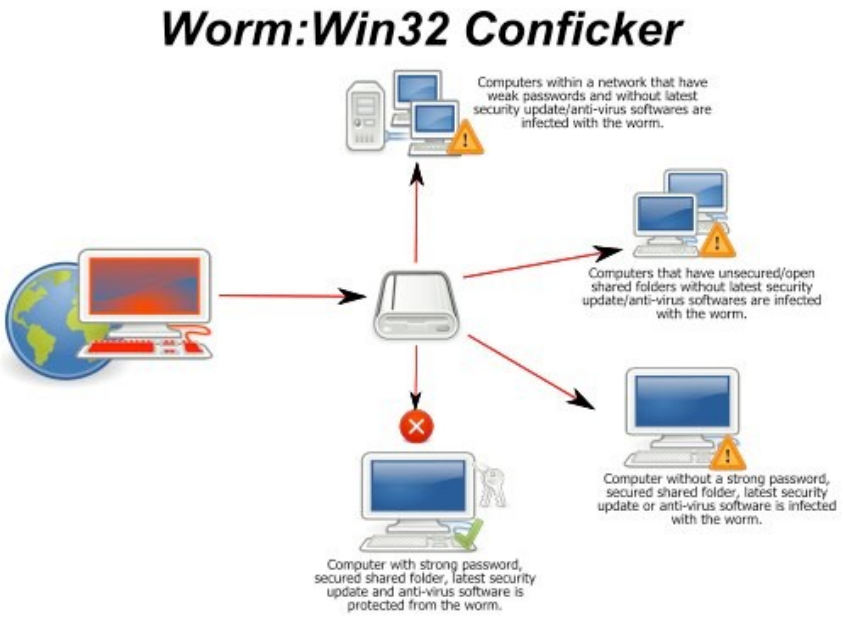
安全分析顯示 Conficker 蠕蟲在全球的肆意活動是在 2009 年 4 月 1 日。在 2009 年 3 月的最后一天，三個安全研究人員（ Dan Kaminsky,Tillmann Werner 和 Felix Leder ）確定了 Conficker 感染的主機的網絡簽名。用 Dan Kaminsky 的話： “我們的發現的確很酷： Conficker 實際改變了 Windows 在網絡上的面貌，這一變化可以被遠端探測發現，而且控測發現的速度非常，非常之快。您甚至可以直接問服務器，它是不是已經感染了 Conficker ，它馬上會告訴你答案。”

Network Box 安全響應即時地打包了這一掃描技朮，以便在 4 月 1 日之前將其提供給我們的客戶。我們爲客戶提供從 Network Box 網關發出的遠程網絡掃描。它將掃描分布于 LAN 和非軍事區網絡中可達的工作站和服務器。該掃描會嘗試連接到 Windows 的 SMB 端口（ tcp/445 ），并且發出 SMB 協議請求給目標主機來確定是否被感染或沒有感染。掃描只能測試已經開通電源的、連接到網絡的 Windows 主機，并且要求 Network Box 可以連接到它們的 tcp/445 端口。

自 3 月 31 日以來，掃描已運行數千次，并且取得了巨大的成功。我們很高興地說，這似乎并沒有造成任何網絡上的重大問題（除了需求極少量的網絡流量和連接開銷之外）。但是，像所有的這類積極主動的掃描探測工具一樣，它可能造成工作站或服務器出現網絡服務問題。

掃描發現了有一些主機已經感染了 Conficker.C ，所有這些被發現受感染的主機都已經使用可公開獲取的安全工具刪除了病毒。

另外請您理解，這種主動的網絡掃描并不是邊界防護設備的常規服務項目，如 Network Box 。然而，由于 Conficker 問題實在太嚴重了，所以我們提供給您的這種服務是完全免費的和建立在 “盡我們最大努力” 基礎之上的。

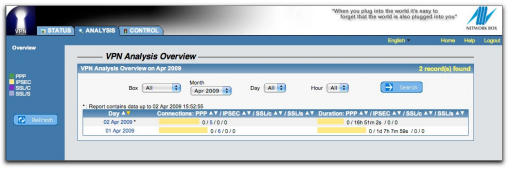


證書授權中心及 SSL VPN

我們在 my.network-box.com 管理界面中增加了一個功能強大的證書頒發機構。您將可以使用它來簽發證書給 SSL VPN 客戶端使用。

認證中心管理局將允許您發放和撤銷證書，以及為您的用戶下載證書。我們也將它納入郵件門戶（ Mail Portal ）中，它就可以當作一種便利的機制來給您的使用者分發證書。

你會從管理 / 配置中發現這個新的功能。



我們也新增了 SSL （客戶端和服務器）虛擬專用網的實時狀態及分析報告，您可以在 VPN / 狀態和 VPN / 分析模塊中發現它。這種功能也包括對現有 IPSec 和 PPTP 的支持。

狀態 STATUS 屏幕可讓您看到所有的虛擬專用網的實時狀態。

對于 VPN 服務器，所有的客戶端的 VPN 信息都將被列出來。

在分析屏幕上，你可以查詢 VPN 連接的曆史記錄，和分析曆史活動。

控制屏幕也可以讓您看到的 SSL VPN 服務的狀態，并且可以讓您按需求進行服務的停止和啓動。

全面支持 NBGMS ，這樣你就可以從 Box Office 中看到 VPN 的狀態，也可以使用最近發布的 iPhone/iPod 的應用程序來查看。

垃圾郵件掃描改進

Network Box 安全響應中心一直跟蹤着新出現的 DHL/ 聯邦快遞等的變種，跟蹤着全球惡意軟件分布趨勢。我們已經在全球推出了兩款新的郵件掃描模塊（ NBH-BGTRACK 和 NBHBBADHDR ）來檢測和阻止這些新出現的變種。

NBH-BGTRACK 啓發式模塊可以尋找可疑的電子郵件特征。它可以阻止新出現的變種甚至包括那些還沒有詳細簽名代碼的垃圾郵件。

NBH-BBADHDR 啓發式模塊可以尋找僵尸網絡發出的電子郵件屬性（特別是有關郵件頭的形成和 SMTP 協議本身的通訊機制），它對從僵尸網絡發出的新變種郵件的檢測是非常有效的。在最初釋放的几個小時內，這一模塊封鎖了超過 25000 封惡意郵件，來源于 16000 個不同的發送地。

因為我們的抵抗目標是僵尸網絡，而不是信息本身，這啟發式掃描也可以非常有效的檢測（和攔截）從同樣的僵尸網絡產生的其他信息（包括“藥丸”垃圾郵件，俄文，中文和含有其他惡意軟件的垃圾郵件）。

此外，本月初我們開始將大量反垃圾郵件簽名遷移到一個新的擁有高性能的規則引擎。新的引擎在針對哪類電子郵件使用哪種簽名方面得到了非常好的調整和優化，（基于文本的，信息結構，內容，啟發式和其他深入的分析）。其結果是減少了掃描時間，用更少的 CPU 周期掃描更多的電子郵件——而對有效性的影響很微小。

如果您有任何問題，或者是其他關于保護模塊或電子郵件掃描系統的，請與您當地 NOC 聯系取得進一步聯系。

發件人策略框架（ SPF ）

維基百科把這定義“寄件人政策架搆 Sender Policy Framework (SPF) 允許軟件在電子郵件發送 SMTP HELO 和 MAIL FROM 命令的階段，識別未經授權使用域名的郵件信息，它建立在域所有者發布的發件人政策信息基礎之上。僞造郵件返回路徑（即發送人地址）是常見的垃圾郵件發送方式，結果導致虛假的“退信”。 SPF 被定義在 RFC4408。”

SMTP 協議允許任何一台計算機發送一封電子郵件，聲稱是來自任何人。因此，很容易被垃圾郵件發送者用僞造的電子郵件地址來發送郵件。這使人們難以追溯真正的垃圾郵件源頭，并使垃圾郵件發送者很容易隱藏自己的真實身份，以逃避相關的責任。

使用發件人策略框架，通過允許電子郵件域名所有者有效地列出其域名郵件地址的發送源范圍就可以解決這個問題，它的實施方法是在要被保護的郵件域的域名 DNS 注冊記錄中加入一個特殊的格式的 TXT 類型記錄。

這里舉個例子， network-box.com 的 SPF 記錄如下：

```
V=SPF1
IP4:218.189.244.64/27
IP4:203.174.43.16/29
IP4:202.177.22.160/27
IP4:203.198.45.104/29
?ALL
```

上述記錄聲明，我們正在使用的 SPF 的第一個版本，并列出了郵件從何而來的四個地址范圍。然后它用了一個“?ALL”，這意味着該清單并不是非常詳盡， network-box.com 電子郵件也可能來自其他地址。

現在，當郵件服務器收到一封從 user@networkbox.com 來的電子郵件時，它就可以查找 SPF 的記錄并且比較電子郵件的真實來源 IP 地址，來確定是不是被允許的。這可以用來確定（一）正面的，來自一個可信賴的地址的正常電子郵件，（二）反面的，這是僞造的來源，或（ 三）中立的（無意見）。

發布一個 “?ALL” 的風格 SPF 記錄，并不是很生硬的。它的意思是，當某人收到電子郵件，來源正好是您列出的地址時，他們肯定知道，它來自于你。如果他們獲得從另一個地址來源收到您的電子郵件，結果是“中性” ，這和沒有 SPF 相比不好也不差。要發布 “ ? ALL” 的記錄，您只需大多數的出站郵件最有可能的源地址名單即可。

發布 “ -ALL” 的紀錄可就會更嚴格了，但是它提供了巨大的反垃圾郵件優勢，尤其是當您 100 % 確定您的郵件地址的來源地址時。使用這種 SPF 可以積極地確定電子郵件是否來自您。他們可以檢測僞造，也會大大地減少郵件反彈和更好地保護域名。

要發布 “ -ALL” 的記錄，您需要確保您的所有出站郵件經過列出的服務器。 Network Box 可以協助您，通過使用 SMTP 認證或 VPN 的連線，以及在多個站點的情況下使用 SMTP 郵件路由規則來幫您規划和實現。

下面是一些很有用的網絡鏈接，您可以用來幫助發布您的記錄：

Kitterman 網站有一個很好的 SPF 記錄測試工具，您可以在正式發布記錄之前使用它：

http://www.kitterman.com/spf/validate.html

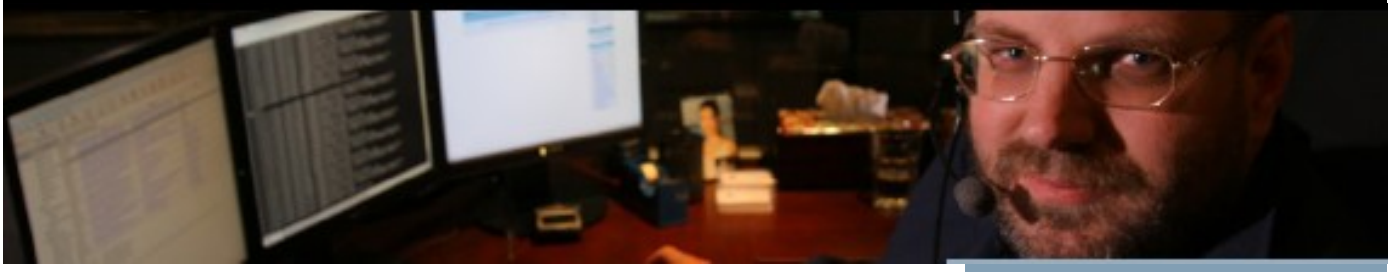
OpenSPF 網站是 SPF 的主頁，它有提供方便的向導工具幫您建立 SPF 記錄：

http://www.openspf.org/

互聯網整體的統計結果是大約有 9.9 %的網域正在使用 SPF 。

大約 10.3 %的 Network Box 客戶發布了他們域名的 SPF 記錄，所以我們是比較超前的，但是也可以做到更好。

我們看到 SPF 實施對抵抗垃圾郵件的影響情況，這里有 3 月份的統計數據，我們發現應用 SPF 后，至少要有 1.4 %的垃圾郵件可以在信封掃描階段給丟棄掉。



April 2009 Features

本月看點

2009 年 4 月 7 日的星期二補丁，我們將爲 NBRS-3.0 系統發布大量的錯誤修復和改進工作。

這些變化包括如下：

•功能齊全的證書授權中心，用戶可以從 my.network-box.com 管理界面進行操作。

•在 my.network-box.com 管理界面查看 SSL VPN 的實時狀態，并且可以進行曆史記錄的分析和查詢。

•新的 Housekeeping ，日志記錄和郵件掃描代碼，可以同時改善功能和提高性能。

•高速 WEB 代理引擎的改進，允許在極高的工作負荷下進行更快速的日志記錄。

•其它的几個關于用戶界面的改進，改善 my.network-box.com 的外觀和性能 / 兼容性。我們還新增加了對微軟 IE8 的支持。

上述變化將不會對正在運行的服務產生任何影響，也不需要設備重新啟動，所以不會造成任何設備運作的重大中斷事故。您當地的網絡安全運維中心 NOC 將以分階段的方式進行新功能的推出。

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

April Hint

本月小提示

Network Box 現在有 iPhone 手機 / iPod 的觸摸應用程序了。由于它的發布定在 2009 年 4 月 7 日，到時您會在全球所有蘋果應用程序商店發現它。您可以下載它并安裝到任何 2.2 版蘋果 iPhone 或 iPod 觸摸裝置中。

這個應用程序可以使您移動地接入到 Network Box Office 客戶門戶和進一步地管理您的 Box 資產（包括健康狀態，合同，虛擬專用網，網絡可達性等）和工單服務（查看，創建和回應工單）。

它也將被免費地提供給 Network Box 用戶，應用程序還提供一個屏幕，用于顯示來自 Network Box 安全響應網站的安全實時狀態。

輸入您的 Network Box Office 的用戶名和密碼，再選擇鏡像網址：
https://beta.boxoffice.network-box.com/
接着就會訪問您的 Box 和工單。

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進行管理服務。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
April 2009

MAR 2009 NUMBERS

Key Metric	#
PUSH Updates	1,386
Signatures Released	242,326
Firewall Blocks (/box)	568,147
IDP Blocks (/box)	123,231
Spams (/box)	54,882
Malware (/box)	821
URL Blocks (/box)	53,925
URL Visits (/box)	2,535,093

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
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