來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2012 年 8 月刊的《In The Boxing Ring》。

在本期的第 2、3 頁，我們詳細描述了資料流程向的重要性。

如果一台安全設備採用一系列的簽名特徵碼對網路流量進行平淡無奇地掃描，那麼流量的方向是無關緊要的。這樣的設備也只能做一些簡單的模式匹配而已。

而對於我們來說，資料流程的方向是最重要的相關性物件之一。比如，這是否是我們的局域網用戶端訪問 Internet 伺服器，或者還是有人在互聯網上訪問我們的 DMZ Web 伺服器。相關的協議是可以相同的（例如在這個例子中的是 HTTP 協議），但從傳輸的方向上來看，我們便知道這意味著什麼，從而使我們能夠準確地針對特殊的問題應用相應的保護技術、簽名特徵碼和啓發式技術。

在第 4 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。

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：

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

Mark Webb-Johnson
CTO, Network Box Corporation
2012 年 8 月

本 刊 概 要

資料流程向的重要性

在我們回應客戶的請求技術支援的過程中，一直都有一個相關的主題排位居高不下，那就是關於資料流程的方向問題。那麼在這個月的期刊當中，我就關於資料流程向的重要性的問題在這裡花一些篇幅來討論一下。

簽名特徵碼與啓發式

如果一台安全設備採用一系列的簽名特徵碼對網路流量進行平淡無奇地掃描，那麼流量的方向是無關緊要的。這樣的設備也只能做一些簡單的模式匹配而已。

然而，這些基本的基於簽名特徵碼的模式匹配的技術，隨著時間的推移越來越顯示出其是一種基本無效的安全技術。當然，話又說回來，含有 1,000 萬個簽名特徵碼的設備肯定比只含有 3,150 個簽名特徵碼的設備要好，而且相比而言未被發現的惡意軟體的數量相比而言要少很多，但是，這樣的數字遲早也是會被突破的。這純粹只是一個數字的遊戲。安全設備必須要在 100%的時間裡面防禦成功，而那些壞傢伙卻只需要又一次機會就足夠了。

那麼，如何取勝？這不同於電影裡面的那些劇情，我們沒有權利選擇不玩這樣的遊戲。而 Network Box 推出了一套廣泛的啓發式技術加入到它的安全保護軍火庫裡面。

簽名特徵碼的目的是爲了精確地與一個特定的威脅進行匹配，而啓發式技術卻有很大的不同，它更加的廣泛，它幾乎是要與所有的威脅相匹配（包括已知的簽名特徵碼樣本以及未來未知的一系列變種）。啓發式有的時候是利用已知的漏洞代碼，而有的時候是爲了檢測異常的行爲。

但是，啓發式技術很重要的一點是它們需要知道流量的前後相關性，這樣才能夠有效地發揮效用。

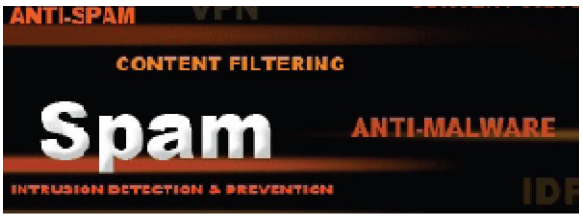
相關性對象

相關性物件可以是一些簡單的檔案類型（例如，一個針對自解密行爲進行搜查的啓發式，應該僅用於針對本質上可執行的一些檔，而將這樣的啓發式僅僅運用於當作原始資料檔案來進行搜查的話，就有可能會出現誤報的情況）。

而對於我們來說，資料流程的方向是最重要的相關性物件之一。比如，這是否是我們的局域網用戶端訪問 Internet 伺服器，或者還是有人在互聯網上訪問我們的 DMZ Web 伺服器。相關的協議是可以相同的（例如在這個例子中的是 HTTP 協議），但從傳輸的方向上來看，我們便知道這意味著什麼，從而使我們能夠準確地針對特殊的問題應用相應的保護技術、簽名特徵碼和啓發式技術。

示例一 反垃圾郵件

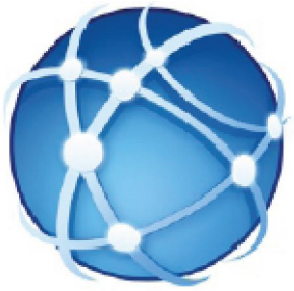
在這個例子中，讓我們來看看我們所獲得的最普遍的請求之一，關於流量的方向的問題。客戶經常會要求我們打開出站的反垃圾郵件功能。



從表面上看，這似乎是一個近乎可笑的要求。客戶爲什麼會關注從他們的受信任的使用者和網路發出去的垃圾郵件呢？那麼原因就在於，可能用戶的機器已經被侵害了，並且可能正在發出垃圾郵件，然後導致用戶的公網 IP 地址段被列入了垃圾郵件黑名單。

而問題就在於，Network Box 的 SMTP 郵件掃描系統是一個真正的合二爲一的系統。一個是針對用戶往互聯網發送的出站郵件提供保護，另一個是針對從互聯網發進來的郵件對郵件伺服器（或者郵件接收用戶）提供保護。方向就是區別所在。針對這兩個不同的服務，我們也採用了不同的啓發式和保護演算法。出站反垃圾郵件功能的開啓將有助於威脅排查，可以將所作的許多的假設都推翻掉，不過這要求將部分入站保護引擎和啓發式引擎停用掉。

再來看看開啓出站反垃圾郵件功能對請求初始化的檢測的作用，從中我們可以更好地從根本上解決在 LAN/DMZ 區已經受到危害的的主機進行檢測和攔截的問題。一旦我們理解到這一點，而不是盲目地啓用出站反垃圾郵件功能（甚至也不顧及會造成怎樣的不良後果），一個更好的解決方案就是對 LAN/DMZ 區出站的連接數進行限速。通過對 LAN 區工作站所能發送的郵件連接數以及郵件數進行出站數量的限制，並且進行合理的限制，那麼我們就可以檢測到可能已被受到危害的主機，並對他們進行相應的處理。



示例二 Web 伺服器的保護

另外一個經常被提交過來的例子就是，客戶經常會要求 NOC 開啓針對他們 DMZ 區的 Web 伺服器的 HTTP 反病毒保護功能。

但是這裡的問題就在於，Network Box 的 HTTP 反病毒系統只是用作爲一項 Web 代理服務，並且旨在保護 LAN/DMZ 區的用戶免受互聯網 Web 伺服器的危害。而不是用於保護客戶 DMZ 區的 Web 伺服器免受互聯網的惡意訪問者的危害。暫且拋開保護機制的設計和意圖，一般意義上來講，向互聯網開放一個 Web 代理的安全隱患也是非常嚴峻的。

對於這個問題，一個更好一些的解決方案是開啓 NBIDPS 的 IDS/IPS （入侵偵測與防禦）系統。這個系統是專門爲保護 DMZ 區的 Web 伺服器免受互聯網的惡意訪問者攻擊而設計的。

而還有一個解決方案就是即將發佈的 NBRS-5.0 帶來的，它將會部署一個 Web 應用防火牆。專門用於解決這個問題的反向代理服務。

示例三 向互聯網開放服務

資料流程的方向通常也暗示了一種信任關係。例如，一個從 LAN 區的工作站用戶到 DMZ 的 RDP（遠端桌面）服務的連接，通常是會被允許的。但是，通常 NOC 會經常接到客戶的請求，要求我們將這個服務完全地開放給互聯網（這樣以便他們外出的工程師能夠遠端存取並管理這些伺服器）。

通常來說，這種做法是很不足取的。每向互聯網增加暴露 LAN/DMZ 區一項新的服務，都將會增加一份遭受危害的可能性。況且有些軟體和服務在針對安全性漏洞的跟蹤記錄方面也是非常欠缺的。

一個比較好的解決方案就是，通過使用 VPN 的方法來取代這些來自於互聯網的信任連接。關閉 RDP 對互聯網的開放，但是只允許來自 VPN 的連接，這樣我們就可以將暴露局限於通過互聯網建立了 VPN 的用戶來進行訪問。Network Box 提供了 PPTP、SSL 和 IPSEC VPN 這幾種選擇，並且其中任何一種對於解決這一問題都是非常有效的（而 PPTP 也是通常建議外出工程師使用的解決方案）。畢竟，哪怕是一個與遠端辦公區建立的未加密的 GRE 通道，比起將此服務開放給整個互聯網要安全得多。

需要記住的一點是，當你接入到互聯網時，很容易被忽略的一點是互聯網也同樣接入到您的網路。

結論

當您提交請求到 Network Box NOC 要求爲您提供支援的時候，請花一點時間說明一下您要求的意圖，而不僅僅只是您的要求。我們 NOC 的同事，均是在保護客戶的網路安全方面身經百戰的資深安全工程師，他們將會爲您在如何避免遭受網路威脅方面提供相應的意見和建議。

2012 年 8 月 新特性

在 2012 年 8 月 7 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：

·一系列內部 NOC 系統的功能增強；

·針對最近新出現的垃圾郵件種類，對郵件掃描的防垃圾郵件功能進行了增強；

·關於將來在 Box Office 系統中對 NBRS-5.0 的支援；

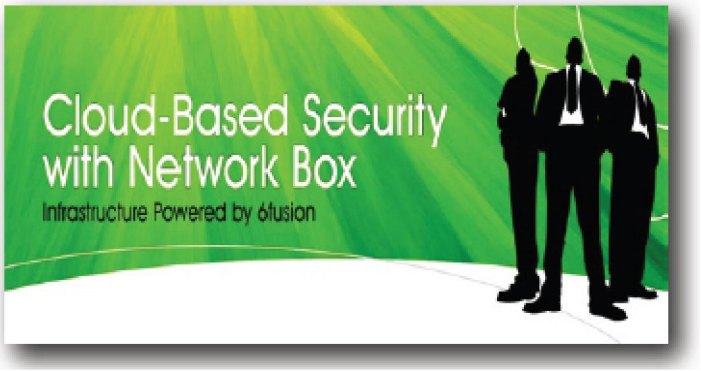
· 一系列針對 Box Office 和支援系統的（主要是內部）功能增強。

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 雲| 基礎設施由 6fusion 提供技術支援

隨著原來越多的關鍵業務應用程式轉移到雲端計算，您需要確保爲基礎設施提供最佳的安全保護。Network Box的安全託管服務，通過6fusion的基礎設施即服務（IAAS）平臺，您即可獲得屢獲殊榮的防火牆功能、入侵偵測與防禦功能以及VPN等服務。



在雲計算解決方案中，Network Box 是唯一一個提供了可被託管管理的、自動配置以及安全監控的的解決方案，並且爲您大量節省了時間和資源。Network Box 與 6fusion 的結合，在優越的雲計算方面提供了業界領先的防火牆服務。而且 Network Box 的防火牆已經獲得認證並且已經直接模組化植入 6fusion 的平臺裡面，通過 6fusion 的平臺，讓解決方案提供商在進行安全部署時更加簡單與輕鬆。

想要獲得更多的關於 Network Box 的資訊，請登錄：

http://www.network-box.com

2012 年 7 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	635	+6.2
特徵碼發包數	242,164	-2.7
防火牆攔截數(每 BOX)	888,490	-1.9
IDP 攔截數(每 BOX)	126,319	+2.3
垃圾郵件數(每 BOX)	13,089	-8.7
惡意軟體數(每 BOX)	632	+93.9
URL 攔截數(每 BOX)	175,734	-4.0
URL 訪問數(每 BOX)	4,461,220	+2.9

月刊工作人員

總編輯：

Mark Webb-Johnson

產品支援：

Michael Gazeley

Jason Law

Nick Jones

撰稿：

Network Box Australia

Network Box Hong Kong

Network Box UK

訂閱方式

您可以些電子郵件到：

Network Box Corporation

nbhq@network-box.com

或者寫信到以下地址：

Network Box Corporation

16th Floor, Metro Loft,

38 Kwai Hei Street,

Kwai Chung, Hong Kong

Tel: +852 2736-2078

Fax: +852 2736-2778