In the Boxing Ring

Network Box 技術咨訊

Mark Webb-Johnson, CTO Network Box

歡迎閱讀2013年7月刊的 In the Boxing Ring

這個月，重點討論的兩個主題是：木馬和開放web應用安全項目（OWASP）的新十大威脅。

CBL（綜合遮罩列表）最近使用http的缺陷來探測被木馬感染的用戶端，只是製作一個HTTP請求就可能將你的IP列入SMTP黑名單。這有些類似於木馬“calling home”的問題。第二頁進一步討論如何防護你網路中的威脅。

在第三頁，我們將這些2010年發行的舊的web應用安全項目十大威脅與當前web應用安全項目發佈的十大威脅做比較。

OWASP是一個開放的社區，專注于爲應用軟體提高安全性。我們包含了關於他們的報告的一個鏈結，方便你進一步閱讀。

最後，我們自豪地宣佈Network Box的網頁內容過濾引擎，S-SCAN，在內容過濾/反病毒方面榮獲了2013年“Computerworld HK Award”獎項。這是連續第三年來Network Box在Computerworld這樣的國際性競賽中獲獎。

Mark Webb-Johnson
Network Box技術總監
2013年7月

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：

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

IN THIS ISSUE

即時檢測和阻止出站的活動的木馬

綜合遮罩列表（CBL － 國際反垃圾郵件組織的一部分）最近加快了他們的動作，現在使用http的缺陷嘗試探測被木馬感染的用戶端，這樣他們就能遮罩那些接入互聯網客戶的IP位址。只要一個HTTP請求就可能將你IP位址列入SMTP黑名單。這有些類似於木馬“calling home”的問題，所以要監測、及早發現、並阻止這樣的活動。

Network Box通常建議一直緊密監視和控制所有出站的連接（LAN -> NET），防火牆策略默認應該阻止所有出站的流量，然後只開放那些必要的或者客戶指定的埠，讓出站流量路由盡可能的通過Network Box代理。默認禁止所有，只允許那些可接受的策略。實施這樣的策略來阻止不受歡迎的出站流量和防止資料洩漏需要花很長時間。這樣的通訊流量也會帶給你很好的實踐經驗。

Network Box安全回應最近提出以下6個建議能更好的針對你網路中未被發現的木馬威脅做防護：

1. 在防火牆LAN ->NET 和Network Box代理這兩者間有效的管理出站策略。尤其是，只允許這些明確要求的，惡意類別例如"病毒/被感染的惡意軟體"應該被默認策略阻止。

2. 允許Network Box在你的網路中開啓入侵檢測和入侵防護系統（NBIDPS）。

3. HTTPS代理"CONNECT"連接到十進位位址（例如：123.456.789.0)默認應該被拒絕，只允許明確要求的。

4. 應該爲入站的電子郵件盡可能的啓用可執行的檢測模組(包括副檔名和檔類型)。

5. 不同的出站代理可以配置使用不同的IP位址。Network Box通常推薦“HTTP/HTTPS”流量和email流量使用不同的IP位址出站。遵循這個建議意味著即使CBL阻止了http通訊而不會影響email服務。

6. RBLMON的服務(http://www.rblmon.com/)將監控你違反RBLs列表的IP位址，並且當有一個或更多的位址被列入黑名單會警告你。這個服務將免費監視3個位址，那些大的客戶需要爲此支付費用。還有其他幾個類似的競爭服務(rbltracker,RBL-check,rblwatch,等)。 訂閱此類服務和密切觀注關於你的位址在RBL中的狀態是有必要的。如果你給HTTP/HTTPS和SMTP的流量使用不同的IP位址出站，那你應該監視兩個IP位址(你會得到一個HTTP/HTTPS傳輸問題的通知，雖然它不會影響你的SMTP流量)。

Network Box繼續密切關注局勢發展，並將進一步推動必要的簽名保護。遵行上述指導應該可以幫助減輕任何木馬感染(例如，一台移動電腦帶進辦公室網路)並提早檢測和阻斷不安全的出站流量。

CBL COMPOSITE BLOCKING LIST

CBL列表展示出各種開放代理的特點(HTTP,socks，AnalogX，wingate，Bagle call-back proxies 等)並專門用於垃圾郵件病毒(類似如Cutwail, Rustock, Lethic等)已經被廣泛地用於發送垃圾/帶病毒的郵件，它們直接以郵件，或者各種類型的木馬或“隱蔽”的間諜軟體，字典郵件捕獲等進行傳輸。

http://cbl.abuseat.org/

OWASP

開放式Web應用程式安全專案

OWASP Top 10 2013

十大最關鍵的web安全風險

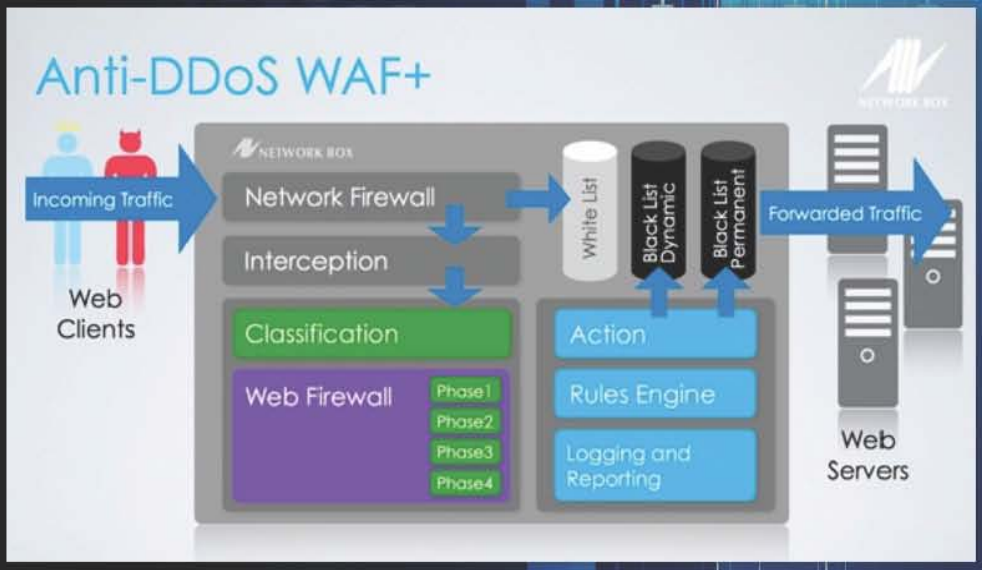
開放式Web應用安全專案(OWASP)是一個開放的、致力於使組織開發、採購、和保持應用程式可以被信任的社群團體。他們最近發佈了他們2013年十大最關鍵的Web應用安全風險。 這篇文檔爲說明這些影響web應用的威脅，以及你如何能最有效的防範它們提供了很好的基礎。

鏈結： OWASP 2013十大安全風險文檔 (PDF)

OWASP Top 10 - 2010 （以前的）	OWASP Top 10 - 2013 （最新的）
A1 – 注入	A1 – 注入
A3 – 被破壞的認證和會話管理	A3 – 被破壞的認證和會話管理
A2 – 跨站腳本	A3 – 跨站腳本
A4 – 不安全物件引用	A4 – 不安全物件引用
A6 – 錯誤的安全配置	A5 – 錯誤安全配置
A7 – 不安全的加密存儲併入A9 →	A6 – 敏感資料洩露
A8 – 無法訪問失效的URL-擴散	A7 – 缺失功能級別的訪問控制
A5 – 僞造的跨站請求	A8 – 僞造的跨站請求
〈A6:錯誤的安全配置〉	A9 – 使用未知易受攻擊的組件
A10 – 未經驗證的重定向和轉發	A10 –未經驗證的重定向和轉發
A9 – 傳輸層保護不足	合併2010-A7到2013-A6

Network Box Anti-DDoS WAF+ 系統 (基礎的 NBRS-5.0 平臺) 是專門被設計用於提供有效和全面防護這些和其他的，以及對web應用程式的攻擊。

更多的資訊請參閱2012年12月的Boxing Ring文檔或者聯繫你當地Network Box的技術支援。



Network Box 第5版
NBRS-5.0

2013年7月2日，星期二， Network Box將發行我們每週二的補丁包進行系統的修復和增強。這些增強功能基本上都已經支持新web用戶端的安全模組 。

NBRS-5.0 特性
2013 7月

各區域的安全操控中心（NOC）將在接下來的7天逐步進行新功能的發佈。這個月,nbrs-5.0發佈的更新包括:

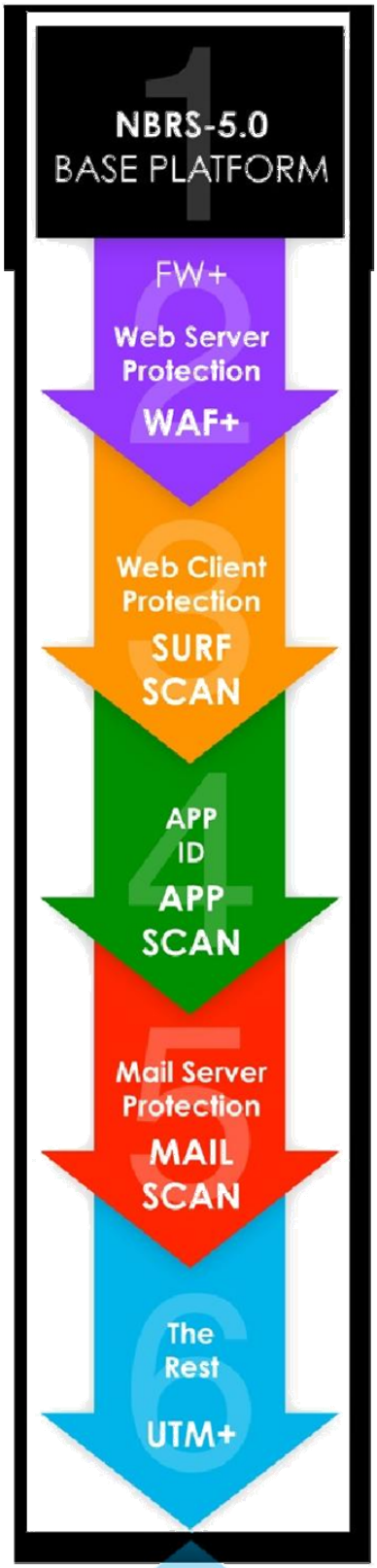
- 終極測試版發佈了7個新的安全模組：
  - 基礎掃描（所有掃描功能的基礎模組）
  - 檔掃描（針對HTTP協定的檔掃描）
  - url掃描（針對HTTP協定的URL掃描）
  - 提供反惡意軟體掃描 (Network Box 的Z-Scan和其他反惡意軟體掃描引擎)
  - 提供卡巴斯基反病毒掃描（卡巴斯基反惡意軟體掃描引擎)
  - 提供分類url掃描 (Network Box的url分類引擎)
  - 提供sscan的url掃描 (Network Box S-SCAN URL分類引擎)
- 添加了支援VLAN的基礎產品。
- 擴展支援web用戶端掃描服務包(包括 URL內容過濾和HTTP 反惡意軟體掃描).
- 爲web用戶端提供web會話跟蹤支援。
- 更改network box防火牆阻止通訊的日誌中記錄的威脅類型'firewall'。
- 更改日誌中記錄的威脅類型,將常見的威脅作爲所有安全模組的名字。
- 在Network防火牆上支援通訊中的源位址和目標位址的國家地理位置識別，以及策略控制。
- 基礎的產品包括一個NTP服務進程。.
- 增強了支援系統日誌消息跟蹤。
- 改進了前面板的顯示和物理硬體功能。
- 新的web管理介面在my.network-box.com中統一展現。
- web管理介面 my.network-box.com 其他的修正和改進
- 在BOX啓動時提升了速度和控制 (冷啓動或者重啓時).
- 各種(主要是內部)Box Office和支援系統的功能增強

大部分情況下，關於更改，不應該影響正在運行的服務或者要求設備重啓。然而，有些情況（取決於配置)，可能需要設備重啓。如果有必要的話你本地的NOC將聯繫你進行安排。

如果你想要瞭解更多關於增強補丁的資訊， 請聯繫你當地的NOC，他們將聯繫你進行安排和部署。

Network Box 第5版

NBRS-5.0



NBRS-5.0 路線圖

我們現在進入NBRS-5.0路線圖的推進階段。大部份開發工作已經完成，我們在進行最後的開發，爲剩餘的安全模組進行打包和測試。

這個月的週二補丁包將發行我們的SURF SCAN產品，將會包括針對web用戶端的反惡意軟體和內容過濾支援，完成我們web內容防護的提供(用戶端和服務端)。在2013年8月的週二補丁裏，我們將發佈我們的郵件掃描產品，和這之後剩下的各種NBRS-5.0的模組，以達到和超過完整的NBRS-3.0的UTM+產品。一旦達到這個階段，我們可以開始將目前客戶的NBRS-3.0升級到NBRS-5.0。

NBRS的主要版本(NBRS-1.0, NBRS-3.0, NBRS-5.0) 包含5年以上的長期支持，所以現在只是NBRS-5.0長途行程中的起點。我們有一些真正令人興奮的新產品，利用NBRS-5.0的新架構將幫助我們保持你們的線上網路安全。

1. 基礎平臺
回到2012年夏天，我們完成並發佈了NBRS-5.0的基礎平臺和支撐架構。成爲這一系列產品的基礎， 並爲所有NBRS-5.0產品的形成提供了基礎。

2. WAF+
我們接著發佈了Anti-DDoS WAF+ 服務包。這個服務包爲防護DMZ和雲基礎的web服務不受互聯網攻擊提供了新功能（以前NBRS-3.0所沒有的）.它整合了網路防火牆，web應用防火牆，DDoS 防護，和 透 明 傳 輸 協 定 (IPv4-IPv6/IPv6-IPv4 橋接)功能，包含在同一個服務包中.

3. SURF SCAN
爲產品提供了一個web應用防火牆，我們設計和構建了一個代理來處理http協定。我們可以嘗試運行，接合我們的高級掃描技術 ， 構成下一代NBRS-5.0產品: SURF SCAN。這將爲基礎的web用戶端在內網提供防護，互聯網上的web伺服器.它將支援反病毒掃描，以及web站點和內容分類，策略控制。它也將支援豐富的報告功能。

4. 應用掃描
以上面爲基礎我們將發佈APP SCAN， 我們使用應用識別系統已經工作了一段時間。通過獨立工作或者與SURF SCAN接合，能夠在網路層識別應用程式，並能從這些資料流程中提取元資料和內容。反病毒掃描和策略控制技術都可以被應用。

5. 郵件掃描
到現在,我們已經有全面的web伺服器和內網用戶端的支持。 所以我們將發佈我們的郵件伺服器防護產品MAIL SCAN。這將爲使用SMTP、POP3、IMAP4協定的流量提供支援。

6. UTM+
最後，我們將發佈一系列的安全模組比如Qos(服務品質控制)，VPN，群集，高可用性等完成UTM+相應的功能。其中一些模組準備好後實際可能隨時和之前的服務一起發佈。

Network Box 通過 ISO 9001 / ISO 20000 / ISO 27001 認證的安全操作中心

NBRS-3.0 特性

2013年7月

2013年7月2日，星期二，Network Box將發佈週二補丁包改進和增強系統性能。各區域的NOC將在之後的7天內安排這些新功能的發佈和更新工作。這個月NBRS-3.0的更新包括：

- 修正SMTP郵件，從掃描器中處理誤報資訊。
- 在HTTP代理系統中提高處理重複無效回應的速度
- 支援爲格式錯誤的SMTP郵件強制添加免責聲明
- 各種針對Box Office支持的增強（主要是內部）

通常情況下，上述的變化不應該影響正在運行的服務或者要求設備重啓，然而，一些情況（取決於配置），要求設備要重啓。如有必要你們本地的NOC將聯繫你安排處理。

除了上面所述，如果你還需要瞭解多的資訊，請聯繫你們本地的NOC，他們將安排諮詢和部署。

Network Box榮獲2013年“Computerworld HK Award”獎項

在內容過濾/反惡意軟體方面

2013.6.21

Network Box非常自豪的宣佈我們的S-Scan Web內容過濾引擎，在內容過濾/反惡意軟體方面榮獲了2013年“Computerworld HK Award”獎項。這已經是Network Box連續三年來在“Computerworld”這樣的國際性競賽中獲獎。

JUNE 2013 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	642	+1.3
Signatures Released	568,821	+4.1
Firewall Blocks (/box)	926,948	+2.4
IDP Blocks (/box)	107,288	+9.1
Spams (/box)	18,008	+8.2
Malware (/box)	603	+19.2
URL Blocks (/box)	186,439	+8.2
URL Visits (/box)	3,298,188	+1.1

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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

Copyright © 2013 Network Box Corporation Ltd.