In the Boxing Ring

Network Box 技術資訊

Mark Webb-Johnson, CTO Network Box

歡迎閱讀 2013 年 8 月刊的《In The Boxing Ring》

這個月，我們發佈了 NBRS-5.0 應用識別框架的公開測試版本。這套系統用於識別 web 應用，並且通過提取資料流程中的中繼資料來實現靈活的報告和策略控制。

在第 3 頁，接著上期《In The Boxing Ring》我們繼續討論 NBRS-5.0 如何解決出站木馬活動的即時偵測和阻擋。

在第 4 頁，我們將詳細介紹本月發佈的 NBRS-5.0 週二補丁及 NBRS-5.0 路線圖的月度進度報告。

最後，是 Network Box 在 7 月份參加的幾個研討會。Network Box 出席了國際酒店業商業技術權威協會 HTNG(Hotel Technology Next Generation)亞太峰會和最近的 ebay PayPal 合作商大會。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2013

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社交網站對關注我們：

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

本 期 摘 要

NBRS-5.0 應用識別框架

這個月，我們發佈了 NBRS-5.0 應用識別框架的公開測試版本

這個框架包括一個叫“applicationid”的代理，用於自動分析網路流量並檢測所屬的類別。接著，這套系統會對檢測到的連接做相應的標記（用於生成報告和實施策略控制）。通過這個方法，你可以方便的識別出如Skype,QQ,FTP,HTTP,Facebook 等超過 1000 種應用的網路傳輸流量——所有這些都是基於流量本身的特徵而不再只是網路位址、埠。

對那些代理原生支援的協定（比如被 web 用戶端代理模組支援的 HTTP），一旦應用被識別出來，相應會話可從 applicationid 代理模組無縫提升到相應協定的專用代理模組中。所以，像運行在 81 埠的 HTTP 流量就可以被識別並轉移到web用戶端模組進行高級別的協定控制（比如認證，策略控制和病毒掃描）。

這套系統的推出對我們來說是非常令人興奮的，因為它建立的基礎能夠用來擴展很多功能。一旦應用被識別出來，中繼資料就可從資料流程中提到出來以用於實現生成靈活的報告和策略控制。

我們會提供這個系統兩個版本的授權：

Lite 簡化版

免費輕量版，用於識別 10 種常見應用，包括在含有代理服務的每個服務包裡。應用檢測是我們的核心協議，SSL 加上幾種音視頻服務。另外，自訂策略可使用 IP 位址、埠、網址等來手動識別其它應用。10 種可識別的應用是：

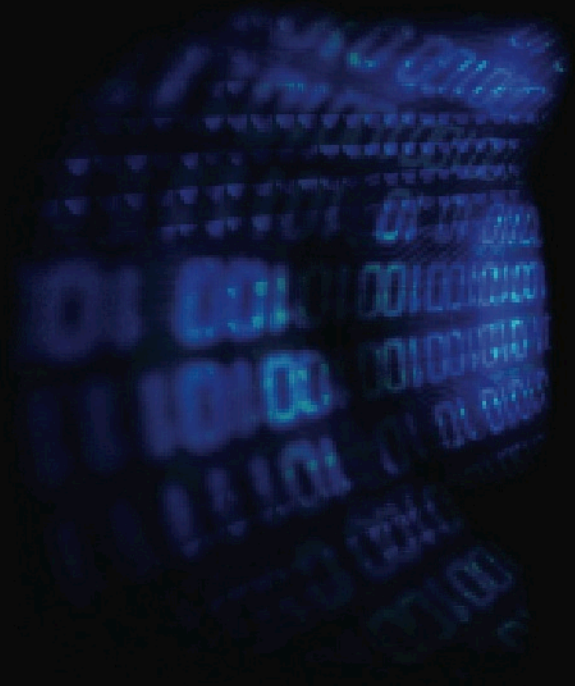
HTTP, SMTP, POP3, IMAP, FTP (包括 FTPCRTL 和 FTPDATA), SSL, SIP, H.323, Facetime, GTALK (包括 GTALKAUD 和 GTALKVID)

Full 完整版

完整版可用於識別超過

1,000 種應用。

上期《In The Boxing Ring》郵刊中我們討論了 NBRS-3.0 中出站木馬活動的即時偵測和阻擋，主要針對最近的 CBL 事件。現在讓來看看我們如何在 NBRS-5.0 解決這一問題的。



NBRS-5.0
出站木馬活動即時偵測和阻擋

NBRS-5.0 有特製的框架和策略，來控制內部及 VPN 連入的網路中僵屍網路的活動。這一功能通過 “infected LAN”這一安全模組來實現。這一框架使用 3 種主要技術秋檢測異常的內部用戶端行為：

1. 試圖連接已知被感染的主控中心。
2. 基於特徵碼和啟發式檢測技術檢測連接僵屍網路主控的資料流程量。
3. 基於比率和反常的回應異常。

如果這樣的流量被檢測到，對應的內部用戶端可以自動隔離並通知管理人員。

這個月我們發佈了這一系統的基礎網路框架，下個月我們會繼續代理層框架上的工作。

Network Box 第 5 版
NBRS-5.0

2013 年 8 月 6 日星期二，Network Box 將發佈一系列週二補丁日更新和修復。這些改進主要用於支援新的 web 用戶端安全模組。

NBRS-5.0 特性
2013 年 8 月

各區域 NOC 會在接下來的 7 日內逐步實施這些更新。這個月為 NBRS-5.0 發佈了超過 50 項改進和修復，主要有：

- 發佈 4 項新的安全模組做最終測試：
  - network-infectedlan (僵屍網路基礎框架)
  - proxy-appid-base (應用識別框架)
  - proxy-appid-navlite (簡化版應用識別，10 個及以上常用應用)
  - proxy-appid-navl (完整版應用識別，1000 個及以上應用)
- 面向客戶發佈 2 項新的安全模組：
  - scan-auth (基礎認證框架)
  - proxy-auth (web 用戶端代理認證)
- 改進 raid 陣列重新同步狀態報告。
- 新 DHCP 伺服器命令，用於使 Network Box 作為 DHCP 伺服器。
- 改進 web 管理介面
- 多項（主要是內部）Box Office 和支援系統改進。

在多資料情況下，上述變更不會需要重啟或影響正在運行的服務。但根據配置的不同，在某些情況也可能需要重啟設備，必要時您所屬的本地 NOC 會同您聯繫安排。

如您需要以上的進一步的資訊，請聯繫您當地的 NOC.他們會安排溝通交流和部署。

Network Box 第 5 版
NBRS-5.0

NBRS-5.0
路線圖

我們現在進入了 NBRS-5.0 路線圖的上升階段。主要的開發工作已經完成，我們在做最後的開發，打包和剩餘安全模組的 beta 測試。

上個月的週二補丁日發佈了我們的 SURF SCAN 產品，包括 web 用戶端惡意軟體防護和內容過濾支援，完成提供完善的用戶端和伺服器內容防護功能。本月的週二補丁日，我們發佈了我們 NBRS-5.0 的應用識別框架的公開測試版。在 8 月底我們將發佈我們的郵件掃描產品，之後是剩餘的其它模組，最終使 NBRS-5.0 達到並超過全功能的 NBRS-3.0 UTM+產品。一旦到達這個階段，我們會開始提供現有 NBRS-3.0 客戶升級到 NBRS-5.0 的服務。

NBRS 主要版本（NBRS-1.0,NBRS-3.0,NBRS-5.0 等）包括 5 年以上的長期支持，所以現在只是 NBRS-5.0 的開始。得益於 NBRS-5.0 新架構我們將提供一些非常令人興奮的新產品來說明我們提升您線上網路的安全。

1. 基本平臺

在 2012 年夏天，我們完成了 NBRS-5.0 基礎平臺和支撐架構的發佈。這成為一系列產品的代碼基礎，並構成了 NBRS-5.0 各產品的基礎架構。

2. WAF+

我們接著發佈了 Anti-DDoS WAF+服務包。這個服務包提供了一些原來 NBRS-3.0 所沒有的保護 DMZ 及雲基礎 web 伺服器倖免於互聯網攻擊新功能。它整合了網路防火牆，web 應用防火牆，DDoS 防護以及協議轉換（IPv4-IPv6/IPv6-IPv4 橋接）功能于一個服務包中。

3. SURF SCAN

為提供 web 應用防火牆，我們需要設計構建一個代理機制來理解 web 的 HTTP 協議。我們現在還在調整並將結合我們先進的掃描技術以構成下一代 NBRS-5.0 產品：SURF SCAN. 它將為基於 web 的用戶端流覽 Internet 上的 web 伺服器提供保護。它也將支援病毒防護及網站、內容分類，並提供豐富的報告功能。

4. APP SCAN

以上面為基礎上我們將發佈 APP SCAN，也是我們開發了一段時間的應用識別系統。通過獨立工作或者與 SURF SCAN 配合，APP SCAN 能夠在網路層面識別應用，在資料流程中提取中繼資料和內容。根據獲取的資訊實施病毒掃描和策略控制。

5. MAIL SCAN

到這裡，我們已經有了完善的 web 伺服器和 LAN 用戶端支持，我們將發佈我們的郵件伺服器防護產品 MAIL SCAN.它將提供對使用 SMTP,POP3 和 IMAP4 協定的郵件的掃描功能。

6. UTM+

通過發佈一系列安全模組來實現比如 QoS（服務品質控制），VPN，集群，HA 等最終完成 UTM+相應的功能。其中一些模組會在準備好時隨同之前的一些服務一起發佈。

NBRS-3.0 新特性
2013 年 8 月

2013 年 8 月 6 日星期二，Network Box 發佈了這次的週二補丁日改進及修復更新包，各區域 NOC 將會在此之後的 7 天內安排這些新功能的發佈和更新工作。這個月的更新補丁包包括：

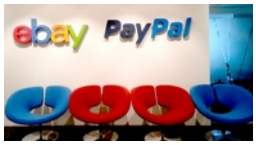
- 修定 Kaspersky 防病毒系統以優化資源使用
- Box Office 和支援系統的多種改進（多為內部）。

在多數情況下，以上的修改並不會影響到正在運行的服務，也不需要硬體重啟。但在某些情況下（取決於具體配置），可能需要重啟設備。必要時您當地的區域 NOC 將會與您聯繫協商。

Network Box
HTNG 峰會

2013 年 7 月 24 日

Network Box 作為演講嘉賓受邀出席了國際酒店業商業技術權威協會 HTNG(Hotel Technology Next Generation)今年在香港舉行的亞太峰會。Network Box CTO,Mark Webb-johnson 做了“保護你的酒店免受全球網路威脅”的主題演講。



Network Box
ebay PayPal 合作商大會

2013 年 7 月 19 日

Network Box 做了網路威脅主題演講，回顧總結最近網路安全威脅並介紹了 Network Box 的綜合 UTM+解決方案。

JULY 2013 NUMBERS

關鍵指標	#	與上月差比（%）
PUSH Updates	522	-18.7
Signatures Released	465,232	-18.2
Firewall Blocks (/box)	900,291	-2.9
IDP Blocks (/box)	97,518	-9.1
Spams (/box)	18,105	+0.5
Malware (/box)	765	+26.9
URL Blocks (/box)	167,010	-10.4
URL Visits (/box)	3,268,582	-0.9

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