

In The Boxing Ring



Network Box Technical News from Mark Webb-Johnson, CTO Network Box

IN THIS ISSUE

1. ON-GOING DEVELOPMENT

We continue to work behind-the-scenes on the new Box Office and NOC support systems (ready for new product feature launches in 2010Q3).

2. SNAKE OIL

In the past month there has been more 'Snake Oil' peddled on the Internet than ever before, so on page 2 I'd like to spend some time presenting our viewpoint on the core goals and advantages of the UTM approach to network security. The true power of UTM comes both from the coverage of the threat landscape and the synergy between the protection - and anything else is, quite simply, Snake Oil.

3. AUGUST 2010 FEATURES

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBRS-3.0 customers.

3. AUGUST 2010 HINT

Our August hint relates to deployment of the Network Box IDPS technology.

Welcome

歡迎閱讀 2010 八月刊的《In the Boxing Ring》。我們一直在為全新的 Box Office 平臺和 NOC 技術支援系統（新產品即將於 2010 年第三季度發佈）而默默地努力著。在即將發佈的第三季度的刊報中，我們將帶來更多的好消息。

在過去的一個月裡，與以往相比越來越多的像“萬靈油(Snake Oil)”一般低劣的網路安全產品在網路上大肆叫賣，所以在第 2 頁中，我非常高興能抽出些時間來分享一下我們對此的主要觀點和看法，並且闡述一下 UTM 運用于網路安全的優勢（尤其是具有 UTM+系統且在網路安全上具有實效的 Network Box 產品）。UTM 並不只有安全方面單一的功能，而是由多重的安全功能融合於一體的精密設備（或者是多個設備組成的集群）。UTM 真正的威力在於兩個方面，一方面是具有廣闊的威脅控制覆蓋面（得益於融合利用多種安全防護的一整套方案），另一方面是多重防護的完美的協同工作（依靠不同的功能模組互相協同互補以達到更好的防護能力）。而其它的同類產品，都是那麼的簡單，就像“萬靈油”一般。

在第三頁，按照慣例我們來簡單介紹一下每個月預告（這個月的是關於 Network Box 的 IDPS 系統的部署情況），以及概述一下這個月來軟體升級與發佈的情況。

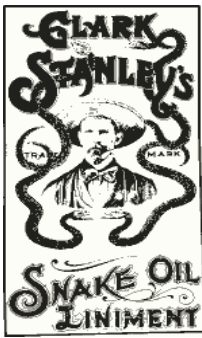
和往常一樣，如果您有任何寶貴的回饋、意見或者建議，我們都非常的歡迎。您可以通過郵箱（nbhq@network-box.com）與我們取得聯繫，或者方便的話直接到我們的辦公室來參觀指導。

您也可以加入或者訂閱我們的 Network Box 安全響應 Twitter 和我們保持關注和聯繫，網址為：

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
June 2010





Security Snake Oil

在美國西部的蠻夷時期，萬靈油 (Snake Oil) 商販們守候著他們的買賣，他們出售的都是一些不太可信的藥物，用於治療小毛病。類似這樣的事情在當今社會卻依然存在（即使是在現代化市場條件之下），而且在網路安全領域更是極其的令人煩惱。鑒於在過去的一兩個月裡，我們清楚地發現，類似這樣的狀況有明顯上升的趨勢，因此，我們覺得有必要抽出些時間讓大伙兒來瞭解一下我們對此的主要觀點和想法，並且闡述一下 UTM 運用于網路安全的優勢（尤其是具有 UTM+ 系統且在網路安全上具有實效的 Network Box 產品）。

那麼，什麼是 UTM？簡單地說，統一威脅管理 (UTM) 就是由多重的安全功能融合於一體的設備（或者是多個設備所組成的集群）。對於需要什麼樣的（或者有多少的）功能應該囊括進去組成一個完整的 UTM 裝置一直存在爭論，但是普遍比較一致地認為，一個最初級的這種裝置應該包括防火牆、VPN、入侵防禦以及防病毒功能。

Network Box 是在 UTM 的基礎上，拓展了一系列額外的功能。例如，除了上面所羅列的 UTM 核心功能之外，我們還提供了 QoS、策略執行、防垃圾郵件、內容過濾、網頁緩存、路由功能、位址轉發、多線路負載、使用分析、郵件介面，以及還有許多其它的功能。

UTM 最重要的優勢，在於其能夠非常有效地解決網路安全問題的多重防護技術的應用。一次又一次地證明，安全隱患發生的主要原因在於需要保護的技術還沒有得到合理的部署。您中了病毒是因為您沒有防病毒系統；您收到垃圾郵件是因為您沒有防垃圾郵件系統；你遭受到蠕蟲病毒侵害是因為你沒有網路級入侵防禦系統；你的頻寬常出現擁塞是因為你沒有做頻寬的控制；等等，等等。

只有通過部署可以涵蓋各類威脅的技術融合，才可以有效的控制不同類型的威脅。單單想依靠某一方面或選擇某幾個方面的防護設備（或軟體）來抵禦各種類型的威脅那簡直是天方夜譚，而且不僅需要高昂的成本投入，日後對不同系統或設備的管理也是一項非常困難的工作。UTM 的最重要的優勢就凸顯於此。

UTM 優越表現的原因，不僅在於其具有了各類威脅的廣泛涵蓋面，還在於其像一把保護傘一樣集成了各類的安全防護技術。如此這般安全防護功能的協同融合（借助不同的元件進行合作和相互合作，充分發揮彼此的防護效能）便是為什麼 UTM 表現如此優越的原因了（儘管可能有一種反面的觀點認為 UTM 是“樣樣皆通卻一無所長”）。

維護方面的重要性。如前所述，安全隱患的重要原因在於缺乏安全技術的運用。其次最常見的原因是不當的配置或過時的保護。換句話說，如果您中了病毒，很可能是因為您沒有防病毒系統，

或因為它沒有被正確打開或隨時保持最新狀態。

我們 Network Box 的方案（我們稱之為 UTM+）採用了我們最核心的技術，並且提供了管理介面（以確保網路防護更方便的配置和管理），還有 PUSH 即時更新技術（以確保防護系統的即時更新）。這有效地解決了安全問題的根本原因，也提供了在當今市場上最全面的 UTM 產品。

與其它同類產品的不同之處。行銷人員在試圖區分他們的產品的時候，他們通常會採用一些“好記的”短語。

有人會說，“我們的是應用層防火牆”。那麼，凡是可以通过應用層協議（如郵箱或網頁方面的協定）來進行惡意軟體掃描的都可以稱之為應用層防火牆。那不同之處到底是什麼呢？

有人會說，“我們的是下一代防火牆”。沒錯，但是區別又在哪裡呢？

有人會說，“我們採用的是應用層資料審計，而不是簡單的針對埠號”。說得也沒錯，但那也只是涵蓋了 5% 的問題（比如出口應用層資料審計），而對其餘的 95% 的威脅卻毫無辦法。它在網路蠕蟲和郵件病毒方面對你來說毫無用處。

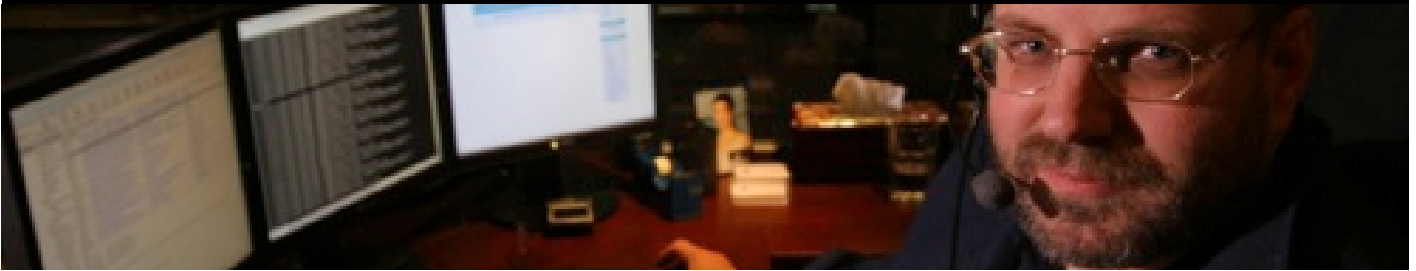
還有人會說，“我們採用了啓發式保護，不再依賴於簽名特徵碼庫”。不過，現在市場上的幾乎所有的防病毒廠商都可以這樣做到（當惡意軟體編寫者已經攻破了同類引擎時，他們可以用於測試新編寫的惡意軟體，以確保在發佈之前可以擺脫啓發式的偵察，因此，這也是毫無說服力的）。

他們未能給到病毒庫的大小數位（曾有一個廠商甚至宣稱說“越簡單便越豐富”）。而現在的 Network Box 有記錄在案的反惡意軟體的特徵碼庫就有 470 萬。對於已知的數位如此巨大的惡意軟體，一個僅有幾千個特徵碼庫的系統又能夠起到什麼作用呢？

正如曾經蠻夷時期的美國西部，那些販賣萬靈油的小商販們還在繼續地吆喝著他們所謂的靈丹妙藥可以包治百病。而問題的關鍵在於要看事實的真相，並確保您遵循最佳安全做法的建議。

如果您想瞭解網路威脅的現狀，您可以參考 [CSI/FBI 電腦犯罪和安全調查](#)（或者通過 Google 搜索關鍵字“CSI/FBI Security Survey”），他們為此以及工作 14 年了，並且提供了一個公平公正的關於電腦犯罪和網路安全現狀的調查報告。這可以說明您認識到網路威脅現狀提供強有力的依據。認識到這些主要的網路威脅只是一些基本的常識，更關鍵的在於要確保您所選擇的電腦安全解決方案是有效而得力的。有的時候，當有些事情聽起來“好得令人難以置信”，其實這一切又都是如此的簡單。

PS：如果您想瞭解有關萬靈油的所有文章，[維琪百科](#)提供了一個很好的起點。我特別喜歡的一個解釋是，“為了促進銷售，藥托（僱傭的騙子）在人群中通常會以自己所謂的切身體驗來忽悠藥物的療效，以抬高人們購買的欲望和熱情”。這種做法，在當今的市場上，我們仍然可以看到推銷網路安全方面的“萬靈油”產品存在。



August 2010 Features

在這個月裡，我非常高興地告訴大家，還沒有發現有什麼漏洞需要發佈補丁包加以修補的

（因為之前曾發佈的很多補丁包已經足以解決已被發現的漏洞問題），因此在八月份裡，我們並沒有發佈任何的套裝軟體給到終端

的 Network Box。

但在此期間，對我們內部的系統做了一系列的優化和改進，並進行了部署，包括：

進一步增強了 Box Office 的介面，涉及到服務合同及其對客戶意見的進一步明確。而對我們現有的客戶合同系統進行分階段部署，在未來的兩個月裡，將會得以提高。

NOC PUSH 更新系統的改進，使更新部署的速度進一步提高。

NOC 硬體管理系統的改善，使系統的管理功能和能力進一步改善。

上述的改進是首屈一指的，而且並不會影響正在運行的服務或者需要重新開機設備。這些改進的工作將只需要區域 NOC 進行處理，而不需要客戶方面的任何操作。也不需要中斷任何的服務。

不過，可以確定的一點是，有個別資料中心需要重組，期間對您設備上的一些防火牆策略會有一些調整。當然這些都會由我們的區域 NOC 進行處理，同時在必要的時候也會與您取得聯繫並作出相關的安排。

August Hint: Deploy IDPS

Network Box 的 IDPS 系統也已經發佈有一定的時間了，並且也已成功為全球範圍內，上萬個網路進行了相關的部署，並為百萬以上的電腦提供保護。

Network Box 還是 [微軟 MAPP](#) 的一個成員，而且我們大部分 [MAPP 簽名特徵碼](#) 的發佈，都是通過我們的 IDPS 網路級保護系統來做到了。當 MAPP 的合作夥伴更早地獲得了漏洞資訊時，他們就會通過他們的安全軟體或硬體為客戶們提供升級保護，比如通過反病毒軟體，基於網路的入侵偵測系統，或者基於主機的入侵防禦系統。而您也只有部署了 IDPS 防護引擎，才能從中獲得保護。

這個月，[微軟](#) 和 [Adobe](#) 宣佈了關於雙方就與微軟的 MAPP 合作夥伴共用 Adobe 漏洞資訊達成了合作。Network Box 也將從中獲益，並且據此積極地為 Adobe 漏洞發佈漏洞防護包，這一切都和微軟的機制一樣。更好更及時的保護，這對於 Network Box 和我們的客戶來說將是一個雙贏的局面，這就更有理由去部署 IDPS 了。

由於 IDPS 引擎需要額外的電腦資源來進行部署，因此，不一定所有使用者都適用（如果不進行硬體升級的話）。具有 6000 多種（且與日俱增）簽名特徵碼的防護，這就是我們主要的防護引擎。

關於入侵偵測和預防系統，要如何才能為您的機構做到最好，以及我們如何才能為您的網路入侵偵測和預防需求提供最好的服務，請您與當地的 NOC 技術支持取得聯繫並進行討論。

JULY 2010 NUMBERS

Key Metric)	#	% diference (since last month)
PUSH Updates	965	+39.0
Signatures Released	131,364	-29.3
Firewall Blocks (/box)	690,756	-2.5
IDP Blocks (/box)	154,221	+4.4
Spams (/box)	48,545	-9.8
Malware (/box)	795	-42.8
URL Blocks (/box)	81,518	-10.7
URL Visits (/box)	3,318,08	-7.5

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley

Jason Law

Nick Jones

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

Copyright © 2010 Network Box Corporation Ltd.