

In The Boxing Ring



本期概要：

1. WELCOME

The December 2010 'In The Boxing Ring' newsletter.

2. 嵌入式 '.BIN'文件的攔截

With the growth in migration to office 2007 file formats, we have seen an increasing number of policy blocks on nested '.bin' file extensions.

3. BOX OFFICE NOTIFICATIONS

We revisit the topic of Box Office Notifications (that we deployed last month)

3. KASPERSKY V8

We present our latest anti-virus engine update - Kaspersky v8. This update is in its final month before global deployment, with a scheduled global release on the January 2011 Patch Tuesday.

4. 2010年12月 新特性與提示

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBR3-3.0 customers.

來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2010 年 12 月刊的《In the Boxing Ring》。

這個月，我們用了第二頁整版的篇幅來講解關於對副檔名為“.bin”的嵌入式文件的策略攔截這一話題。隨著外部檔可以嵌入到 Office 2007 的檔中這一應用的不斷發展，我們也覺察到了這類攔截在不斷增長，區域 NOC 也反映很多客戶對此的困惑與不解，以及需要如何去避免。這篇文章將幫助您瞭解這些攔截的真相，以及它們是如何有效地應用於策略的執行。

在第 3 頁，我們再次提及關於 Box Office Notifications（上個月所開發完成的）的一些內容。這個新的系統現在運行良好，但似乎只有 1/5 的使用者在運用其全部的功能。在這篇文章裡，我們重點圍繞系統的兩個方面（通知的方式和基於時間的控制）進行描述，以幫助您更好地使用此系統。

在第 3 頁中，我們還介紹了我們最新的反病毒引擎的更新——Kaspersky V8。這次的更新還處在最後一個月的開發當中，一個月後，也就是 2011 年 1 月份將進入全球部署的時間表。

在第 4 頁，按照慣例我們來簡單介紹一下每个月的提示（這個月的是關於有效地配置策略的重要性），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，我們都非常歡迎和感激不盡。您可以通過郵箱

(nbhq@network-box.com)與我們總部取得聯繫，或者方便的話直接到我們辦公的地方來參觀指導。

您也可以訂閱我們的 Network Box 安全響應 Twitter 對我們保持關注，網址為：

twitter.com/networkboxhq

Mark Webb-Johnson

CTO, Network Box Corporation

2010 年 12 月





嵌入式“.bin”文件攔截與 Office 2007

Network Box 提供了兩種方式針對郵件附件的攔截：

- 1、根據附件副檔名攔截（基於附件檔案名最後的副檔名）。
- 2、根據內容攔截（基於對檔內容的分析）。

這兩種方式均可應用於標準的附件檔以及內置性附件 檔（比如 ZIP 格式的檔等）。而對於通常的過濾也是適用的（比如，豁免的發件者，僅入站郵件，等等）。在預設情況下，Network Box 是不啓用這些限制的，除非明確配置了要這樣做（根據客戶的要求）。

我們很大部分客戶採用了這種攔截策略來限制可執行的附件流入到他們的網路當中（不論對其進行病毒掃描的結果是怎樣的）。一般情況下，在配置清單中，需要被攔截的檔案類型有：.com、.exe、.pif、.src、.bin 以及其它的一些類型。

問題所在

這項功能已經運行有好幾年了，而且幾乎沒有誤報。然而，隨著 Office 2007 的發佈，Microsoft 開始啓用了一種新的文檔格式（例如副檔名為.xlsx、.docx 等等）。正如以下這篇文章所介紹的：<http://www.arstdesign.com/articles/office2007bin.html>

其實 Microsoft 的這些新的格式就和 ZIP 檔案格式差不多，而且幾乎很難去區別這兩中檔。一個 Microsoft 文檔和一個 ZIP 文檔幾乎是一樣的。

問題的原因在於，Microsoft Office 2007 程式有時會編輯印表機的設置檔、宏，以及其它類似含.bin 副檔名的一些物件（例如 vbaProject.bin、printerSettingsxxx.bin 等等），當客戶已經採用了對嵌入有.bin 檔的文檔進行攔截的策略時，那麼這些 Microsoft Office 2007 的文檔都將因此而被攔截。

如果容器是一個 Office 2007 檔的話，這裡卻也有一種被建議的做法可能導致放行嵌入有.bin 文件的文檔。正如我們先前所描述的，我們很難去區分一個 Microsoft Office 文檔和一個 ZIP 文檔，除非從副檔名（比如.docx、.xlsx、.pptx 等）上來區分，而 Network Box 確實也提供了這樣的選項。但這並非 100%完全如此：

- 有時，發件者並不會按照標準的副檔名來對他的檔命名。
- 有時，發件者所使用的並不是英文作業系統，這將使得使用者可以使用非英文字元給檔命名，包括其副檔名，這樣就可以產生成百上千種的檔案格式。
- 或者這樣一個做法也可以使其繞過策略——惡意的發件者將他們的 ZIP 文檔命名為“sample.docx”，這也有可能導致其繞過副檔名策略的攔截。

解決辦法

正如描述的那樣，解決辦法並不簡單。沒有一種能 100%有效的辦法對 Office 2007 文檔與 ZIP 文檔進行區分，因此這些策略也沒有辦法將正常的嵌入有.bin 檔（鑒於 Microsoft 2007 使用.bin 檔用於宏、內嵌物件等，使用者以任何方式是否使用可執行檔是無法加以影響的）的 Office 2007 文檔區別開來。但是，讓我們退一步來想一想，為什麼我們一開始就對.bin 檔進行攔截。

1、先來看看現有的一個可執行副檔名的列表（比如這裡的：<http://antivirus.about.com/od/securitytips/a/fileextview.htm>），我們並沒有看到.bin被列入其中。因為，它曾經是被應用的（在早期的windows裡面），但是在現在的作業系統和應用程式中並沒有再使用。一個簡單的辦法就是將.bin從擴張名攔截列表中清除掉。

2、幾年前，當我們點擊某一種副檔名的檔時，使用什麼應用程式來打開它，是由作業系統來決定的。而現如今，作業系統卻普遍採用的是檔內容分析，或者採用 MIME 類型來決定。如果目的是為了攔截可執行附件，那麼通常採用 Network Box 的檔內容攔截策略會更有效（不論是 MIME 類型或者檔案類型的），而不是一味地只是依賴於文件副檔名攔截策略（這也是最近的一些評論所認為的）。

3、由於所有附件（包括內置有檔的文檔）都將通過 Network Box 的郵件反病毒掃描系統的引擎徹底地進行掃描，再加上副檔名攔截策略對可執行內容進行過濾，均已可達到目的，但並不是必須這樣做（尤其是當發生不必要的策略攔截時）。

推薦建議

假如存在 Office 2007 文檔和嵌入.bin 的策略攔截問題，Network Box 安全回應組建議您不要盲目地對含.bin 檔嵌入的附件進行攔截。

- 對於不要求對可執行附件進行攔截的客戶，可以將這些攔截關閉或者將.bin 從副檔名列表中清除。
- 對於有要求對可執行附件進行攔截的客戶，可以採用多重防禦的方法——不僅對已知的可執行檔進行副檔名攔截（但不對 .bin 檔攔截），同時也通過內容分析進行過濾攔截（主要針對 Microsoft 的可執行內容）。

以上的幾種方法將即可以提升整體的安全性，又可以避免嵌入有.bin 檔的附件被意外攔截。和往常一樣，您可以與您的區域 NOC 就此進行探討，他們將幫助您有效地執行您的策略。



Network Box 通知系統

Network Box Office 通知系統發佈於 2010 年 11 月的 Patch Tuesday，此後，我們看到將近有 1/5 的用戶在所提供的預設的配置的基礎上進行了定制，而且一天天地越來越多。在這篇文章中，我們重點圍繞此系統的兩個方面進行描述，以幫助您更好地使用此系統。

1、通知的方式

通知的方式是採用機制性的方式發送一個通知給到您。當我們在部署 Box Office 通知系統的時候，我們移植了原有的“want ticket email”的配置資訊到一個預設 eMail-type 通知方式(這樣您就可以繼續通過郵箱收到通知)。而且，您還可以對預設的配置進行擴展。這裡給到您幾條建議：

當您的 Network Box 或者郵件伺服器無法連接，且辦公網路的外出口出現故障的時候，你會怎麼辦呢？創建另外一個外部通知郵箱位址（例如，使用 gmail 郵箱或者其他外部郵箱），您依然可以繼續收到通知資訊，在您的內部郵箱系統無法連接或出故障的時候。

如果您有蘋果的 iOS 終端設備，那麼您可以安裝並登錄到 Network Box iOS App，將會為您創建一個 iOS 通知推送助手，這將可以通過蘋果的通知推送服務發送提醒資訊給到您。

我們還提供 SMS 資訊通知的方式，可以直接發送短信提醒通知給到您的手機。

2、基於時間的控制

您所建立的每一個通知聯繫點都可以有多個用於限制通知的篩檢程式，以對時間區間進行限制。例如，您可能希望下班通知聯繫點隻在下班時間生效（也就是您只是希望在您上班時間的 Mon-Fri 09:00-18:00 收到相關的通知）。

需要注意的是，在您的 Box Office 的“我的帳戶”頁面，有一個時區設置。默認的是 UTC（世界標準時間），但是您可以將其設置為您最近的時區，那麼 Box Office 將會根據您所設置的時區進行時間的顯示（儘管可能 Box 或者 NOC 採用的是其它不同的時區）。

您可以參考 Box Office 的使用者介面使用手冊(您可登錄 Box Office 後在右上方點擊 HELP 下載獲得)。我們建議您最好嘗試一下通知系統的相關功能是否可用。



Kaspersky V8

在我們與卡巴斯基實驗室的合作中，Network Box 很高興向您宣佈，我們將在近期發佈並對所有的 NBR3-3.0 的客戶免費升級到新的 V8 版本的卡巴斯基引擎。

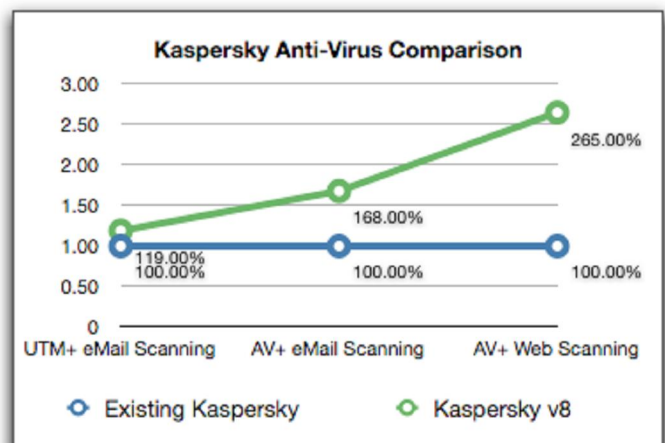
這個新的 V8 版本在使用上與卡巴斯基桌上出版和伺服器版（Windows 或 Linux）是一樣的，但是在閘道上的使用進行了優化。不僅帶來了優越表現及記憶體方面的提高，還在啓發式保護能力以及應用沙箱保護技術上也得到了進一步的提升。

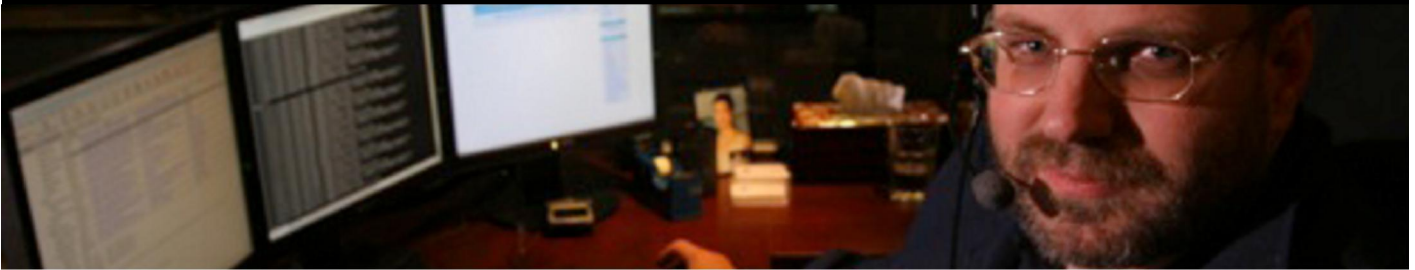
作為新引擎的全面測試的一部分，我們對性能和記憶體使用情況進行了全面的測試。我們非常欣喜地告訴您，新的引擎給我們帶來了對 UTM+郵件掃描平均 19%的性能提高，AV+郵件掃描有 68%的性能提高，還有對 AV+網頁掃描更是提高了 165%——這與現有版本相比在速度上提高了 1.65 倍以上。

所有這些，在檢測能力得到提高以及記憶體和其它資源消耗減少的同時，新的卡巴斯基引擎相對之前版本來說，只需要低於 30% 的快閃記憶體空間用於特徵碼，且只需要不到一半的 RAM 空間。

新版本的卡巴斯基引擎將於 2011 年 1 月份的 Patch Tuesday 的時候發佈給所有的用戶，且此次計畫將在 2 個星期內完成所有用戶 BOX 的移植更新。

新版本的引擎，儘管已經完成並準備好，但是局部的部署已經開始。我們為所有的用戶提供一個早期的版本，這將在 2010 年 12 月份的 Patch Tuesday 開始部署。





2010 年 12 月 新特性

在這個月裡，我們著重致力於 Network Box 的全球監控系統和 Box Office 的整合工作。因此 Box 的固件修改相對要少一些。而對 Box Office 的修改我們將在此次的 Patch Tuesday 自行部署，區域 NOC 也將在 7 天內安排相

關的發佈和升級工作。相關的修改包括：

- 監控報告系統有些增強，尤其關於重要健康指標的報告。
- NTP 監測與同步功能增強。
- 對 S 系列一些產品對其溫度感測器的敏感度有所放寬。
- 對 M-385 產品的主機殼風扇感測器的敏感度有所放寬。
- 對 IP 地理定位有所更新（這將使對 IP 的地理定位更加準確無誤）。
- 對 GMS 可達性準則和被動（而不是主動可到達）Network Box 的監控進行了一些增強。

· 對 Network Box Office 的 GMS 工單的資訊報告有所增強。

以上修改並不需要設備的重啓，但有可能對部分 BOX 的某些服務會有所影響，但區域 NOC 將會在部署時與此部分受影響的使用者取得聯繫。

這些更新的工作將會交由區域 NOC 的工程師進行處理，而不需要客戶方面的任何操作。只有非常少部分的服務可能需要短時中斷。

12 月提示: 組織策略

正如本期刊的第 2 頁所討論的，您組織或企業的策略是由您來定義的，並由區域 NOC 的工程師來幫您配置，然後 Network Box 設備生效後對您的網路提供保護。

Network Box 的區域 NOC 工程師也可能會給您提供建議，但是這是您的組織策略，我們將遵照您最終決定的策略來執行。

審查這些策略對您來說也是非常重要的（尤其是查看 my.network-box.com 中 Mail/Status/Policy Summary 目錄下的郵件策略，以及 Web Proxy/Config/Rules 目錄下的 WEB 策略）。而對於例如反垃圾郵件和反病毒等功能卻是非常自主的（儘管由數百個可配置的選項控制和調整），而策略的功能只是按照它們所被要求的去執行就可以了。

當第一次部署時，您需要確認策略是否已經按照您所要求的在 Network Box 設備裡執行生效。

但是，為了達到企業生產最佳的效果，您還需要定期檢查您的策略以及所發生的強制攔截隔離。您可以參考每週的報告並借助線上的 my.network-box.com 來進行檢查。

和往常一樣，如果您需要哪些建議性說明，或者有關您的組織策略的實施細節，以及 Network Box 所提供的更多的技術，請與當地的區域網路中心（NOC）技術支援取得聯繫，他們將為您提供相關的幫助。

2010 年 12 月份 資料表

關鍵指標	#	與上月 差值百分比
PUSH升級數	793	-4.8
特徵碼發佈數	485,045	+8.8
防火牆攔截數(/BOX)	773,496	+10.2
IDP 攔截數(/BOX)	123,662	-3.7
垃圾郵件數(/BOX)	28,850	+1.4
惡意軟體數(/BOX)	279	-66.4
URL攔截數(/BOX)	145,662	+14.4
URL訪問數(/BOX)	4,365,586	+22.0

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

寫電子郵件到以下郵箱地址：
Network Box Corporation
nbhq@network-box.com

或寫信到以下地址：
Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong
Tel: +852 2736-2078
Fax: +852 2736-2778
www.network-box.com

Copyright © 2010 Network Box Corporation Ltd.