來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2012 年 7 月刊的《In The Boxing Ring》。

在本期的第 2、3 頁，我們詳細描述了引擎、簽名特徵碼和啓發式。

引擎和簽名特徵碼可以被認爲是打擊惡意軟體的兩個最重要的武器，但它們不是完整的解決方案。與傳統的戰爭相比，坦克和大炮都是強大的武器，但它們針對反間諜而言卻是沒有任何用處的。爲此，我們需要更有針對性的解決方案，而這也正是 Network Box 引入 Z-Scan 和啓發式引擎的原因所在。

作爲一個託管服務，Network Box 有義務對 Box 進行安裝，使其能保持正常工作，並且令客戶能夠滿意。簡單地說，這就是 Network Box 的特殊之處與區別所在。

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

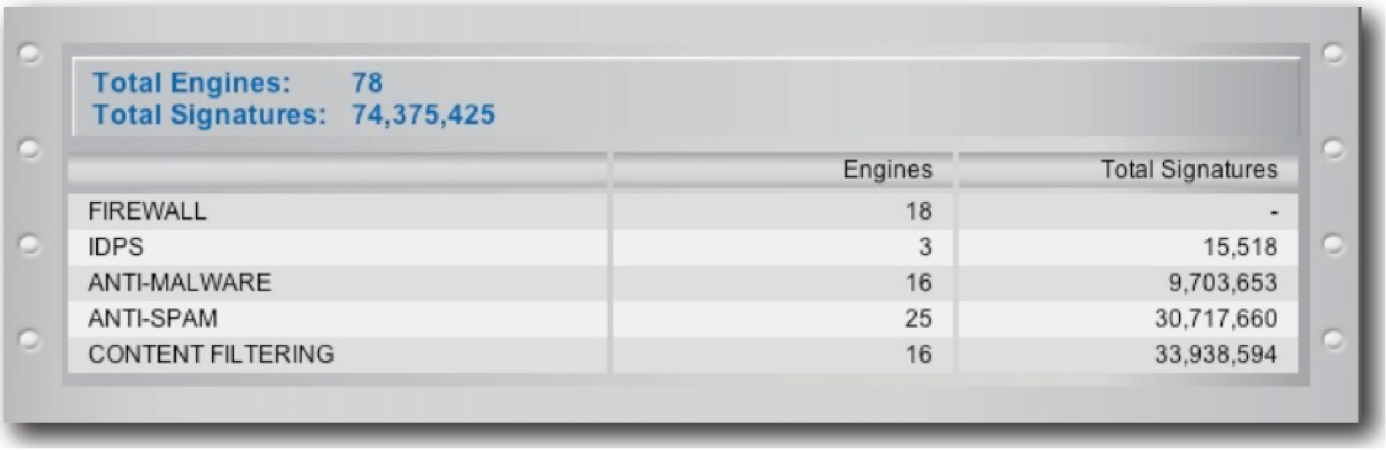
Mark Webb-Johnson
CTO, Network Box Corporation
2012 年 7 月

本 刊 概 要

引擎、簽名特徵碼與啓發式

引擎與簽名特徵碼

以下是當前時刻（2012-7-3 9:30AM）Network BoxNBRS-3.0 產品中的簽名特徵碼與引擎的統計資料，其實，當我記錄下來的時候，其資料已經更新爲更新的資料了：



Total Engines: 78
Total Signatures: 74,375,425

	Engines	Total Signatures
FIREWALL	18	-
IDPS	3	15,518
ANTI-MALWARE	16	9,703,653
ANTI-SPAM	25	30,717,660
CONTENT FILTERING	16	33,938,594

Network Box NBRS-3.0 引擎與簽名特徵碼統計 – 來源：http://response.network-box.com/

若需要查看最新的資料圖表，請登錄 http://response.network-box.com/protection 進行查詢。

這些都是相當可觀的數字。在反惡意軟體方面，我們已經有了 16 個引擎，已接近 1000 萬個簽名。試想一想，這些就是唯一標識將近 1000 萬獨立的惡意軟體威脅的識別簽名。而在 10 年之前，這個數字僅爲 3 萬。

總的來說，我們已經有了 78 個保護引擎，包含超過 7400 萬個簽名特徵碼，所有這些都被應用到掃描您的網路流量問題，並對異常流量禁止攔截。

從同一個基準點來看，在威脅保護的世界裡，引擎的數量確實等同於提供保護的廣度，而簽名特徵碼的數量則體現了保護的深度。

就像是互聯網的蠻夷的西部，人們所兜售的萬靈油（Snake-oil）那樣，當我們對威脅保護系統在一個標準下進行比較時，我們也建議您能忽略炒作的成分並對基本數字進行比較。這樣的話，您將獲得一個正確的判斷，到底是由誰來進行針對性的保護。

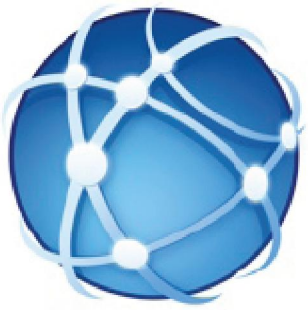
圖例：Kaspersky 物件掃描器（用於電子郵件和檔掃描）

啓發式

引擎和簽名特徵碼可以被認爲是打擊惡意軟體的兩個最重要的武器，但它們不是完整的解決方案。與傳統的戰爭相比，坦克和大炮都是強大的武器，但它們針對反間諜而言卻是沒有任何用處的。爲此，我們需要更有針對性的解決方案，而這也正是 Network Box 引入 Z-Scan 和啓發式引擎的原因所在。

Z-Scan 是 Network Box 獲得多項殊榮的零日防病毒解決方案。比較典型的反病毒的行業實踐模式是在一個病毒首次出現之後的 3 至 12 小時的時間裡面發佈惡意軟體的簽名特徵碼並更新到用戶端。而使用了 Z-Scan 之後，發佈簽名特徵碼的週期卻可以大大地縮短，這是因爲病毒樣本都是通過超過 20 萬個在雲端的病毒捕獲點（Taps）即時地獲取，對病毒攻擊的發生全天候 7*24 小時地進行抵禦。而 Z-Scan 也是基於簽名特徵碼的，那些簽名特徵碼的創建，都是全自動的，並且基於強大的雲端主機的啓發式。Z-Scan 跟傳統的方法相比，它是如此的強大，它所維護的簽名特徵碼的數量相對而言是要小很多的。它純粹是專注於抵禦近期非常緊急的新興惡意軟體。通常來講，其簽名特徵碼的數位會保持在 10 萬個左右，我們會定期地去清理 Z-Scan 中超過 1 天或者更舊的簽名特徵碼，以保持 Z-Scan 盡可能的輕量型、出色而優越的性能。等到傳統的簽名特徵碼發佈了之後，在 Z-Scan 中相對應的特徵碼就可以安全地刪除掉了。

瞭解了 Z-Scan 之後，我們來到啓發式的世界。在這裡，電腦演算法主要被應用於分析可執行程式的特性和其實際的運行代碼，以確定在沒有要求特定已定義的簽名特徵碼的情況下，判斷該程式是一個惡意的軟體。這項技術是非常重要的，可以有效地抵禦緊急的基於 Web 的威脅，同時，Network Box 採用了業界領先的啓發式引擎。



結論

自從成立以來，10 多年以前，Network Box 一直關注于安全防護以及客戶聯網的安全防禦，而不僅僅只是銷售 Box。而我們的競爭對手，他們會賣給你一個 Box，然後隨即便離開了。而作爲一個託管服務，Network Box 有義務對 Box 進行安裝，使其能保持正常工作，並且令客戶能夠滿意。簡單地說，這就是 Network Box 的特殊之處與區別所在。

我們一直都是這樣做的，全天候 360 天 7x24 小時地提供服務，已經有超過 10 年了，而到目前爲止，我們依然 100%將努力集中於威脅防護的問題之上。我們也非常地感謝你選擇了我們，並幫助我們所做的做到最好，因此，您也可以專注於您所做的並做到最好。

2012 年 7 月 新特性

在 2012 年 7 月 3 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；

·對 my.network-box.com 中許可證過期的資料和資訊顯示進行了一些修改，使其在 Box Office 的合同中也能反映相關資訊；

·對郵件掃描中反垃圾郵件進行了針對近期.in 和.ru 功能變數名稱的濫用的增強；

·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 | ISO 認證升級

Network Box非常高興地能夠進行官方宣佈，我們的產品已經升級到了三重的ISO狀態：ISO 9001:2008，ISO 2000:2011，ISO27001:2005。

對於我們的安全運營中心升級到最新的 ISO 標準，我們做出了大量的工作，其中跟很多人的努力是分不開的，所有的人都在這個很重要的時期爲之付出了寶貴而巨大的努力。

毫無疑問，這是一個里程碑式的成就。 Network Box 現在不僅有最新的三重 ISO 認證安全運營中心，而且提供了唯一的 IPv6 核心的就緒階段 2 認證的安全管理平臺，以及獨一無二的可以從一個安全的蘋果 iPhone/iPod Touch/iPad HD app 對其進行監視和管理的功能。

Network Box 才是真正領先世界的安全管理服務。

想要獲得更多的關於 Network Box 的資訊，請登錄：

http://www.network-box.com

2012 年 6 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	598	+24.3
特徵碼發包數	248,813	-29.2
防火牆攔截數(每 BOX)	905,341	+1.6
IDP 攔截數(每 BOX)	123,468	+4.7
垃圾郵件數(每 BOX)	14,327	-3.5
惡意軟體數(每 BOX)	326	-44.7
URL 攔截數(每 BOX)	183,074	+0.8
URL 訪問數(每 BOX)	4,333,709	-3.3

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