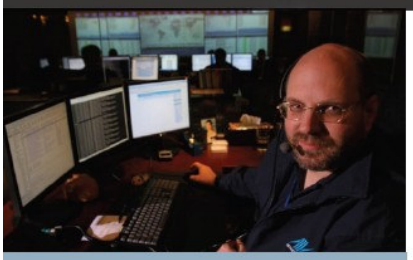
In The Boxing Ring



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

IN THIS ISSUE

Welcome

歡迎來到七月份的 In the Boxing Ring. 在七月，我們將繼續改善 BOX OFFICE 和 NOC 支援系統（準備在 2010 年第三季度推出新產品）。有關更多的消息請關注既將到來的第三季新聞。

在第二頁，我們討論怎麼樣讓 NETWORK BOX 進行即時的 SPAM TRAP（垃圾郵件陷井）。提交給 spam@network-box.com 系統是有益的，另外即時的 Spam Traps（垃圾郵件陷井）機制被證明是可以更有效的去改善提高 NETWORK BOX Anti-spam 的準確性和可以更準確評估 NETWORK BOX 反垃圾郵件解決方案的性能。Spam Traps（垃圾郵件陷井）的部署是重定向那些未經驗證的，來源不明的郵件集中到一塊進行處理。這樣，統計資料可以自動生成有效的解決方案，和即時提交當前未檢測到的垃圾郵件樣本到 NETWORK BOX，以便我們安全響應團隊可以盡可能快和有效的發佈新的保護特徵碼和啟發式簽名。

在第三頁，我們介紹通常的每月提示（這個月關於怎麼樣最好的讓 NOC 配置即時的垃圾郵件陷井系統),並概述這個月發佈的的升級更套裝軟體。

和以往一樣，如果有任何反饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發
送郵件到我們的郵件列表：

nbhq@network-box.com

聯繫我們。或者當您下次在香港市區的話, 隨時歡迎來我公司辦公室進行參觀指導。您也可以加入或訂閱我們的安全響應 Twitter 和我們保持聯繫，網址是：

twitter.com/networkboxhq

Mark Webb-Johnson

CTO, Network Box Corporation

July 2010

Network Box Spam Traps

Spam Trap （垃圾郵件陷井系統）是一個郵件位址（或功能變數名稱），總是接收到百分百的垃圾郵件。

通常，像這個垃圾郵件位址是其他垃圾郵件接收者的代表，所以這樣非常有用，因為它提供:

一個決定 ANTI-SPAM 效率的直接機制。分析所有進入 spam trap（垃圾郵件陷井系統）的郵件，被檢測到為垃圾郵件的百分比相當於 ANTI-SPAM 檢測到垃圾郵件百分比。

一個在即時的資料流程中檢測未被檢測到的（那些沒有被簽定為垃圾郵件的郵件）。可以通過瞭解，這些錯判的確是垃圾郵件，這些即時檢測資料流程可以用於提高檢測成功率，並在某些情況下可以自動增加特徵碼去檢測以後類似的垃圾郵件。

NETWORK BOX 提供 SPAM TRAP（垃圾郵件陷井）工具，整合到我們的郵件掃描技術。SPAM TRAP 的工作是監控一個配置單上的郵件位址，一旦郵件到達且是發到這些位址中的一個，則被判為垃圾郵件（因它是已知的垃圾郵件），然後有一個副本將會傳送到我們 SPAM TRAP（垃圾郵件陷井系統）警告中心。這個方法意味著我們可以即時的抓到垃圾郵件，而且只需要 NETWORK BOX 很小的資源。

一旦垃圾電子郵件到達 SPAM TRAP 中心， 它們將被類似于客戶 NETWORK BOX 上的 anti-spam 技術和特徵碼規則進行非常準確的分析，這個分析結果將被存儲以用於統計。另外，任何 missed 垃圾郵件轉發到我們的垃圾郵件免疫系統進行分析和釋放保護特徵碼，及任何可執行附件中的病毒進行分析（和可疑附件轉發給我們作進一步分析病毒疫情系統）。

左邊的表格是顯示 SPAM TRAP 中心 2009 年一月以來的分析結果。雖然我們保承諾達到 95-98%的準確度，但你可以看到，我們每月通常達到了 98-99%的垃圾郵件檢測精度。

能夠密切監控我們的反垃圾郵件解決方案的準確性，NETWORK BOX 已實施了各種警報觸發器，在垃圾郵件的爆發時發送警告到我們的安全工程師。這些措施包括以下的啟發式，如：

- 監控整體垃圾郵件的準確性，以每小時為單位，如果低於 98%就報警。
- 即時監控這些垃圾郵件樣本的數位指紋（如郵件片斷，URLs，郵件地址等等）。如果檢測到新增了一個特別的指紋碼是未被檢測到的垃圾郵件，將報警到工程師並作響應。
- 比較數字指紋的比率（如：過去一小時 VS 過去一天）並報警給工程師去做修改。

這些啟發式有效的提醒我們的工程師去應對新爆發大規模的垃圾郵件，並可以迅速的對問題進行回應。

新的 SPAM TRAPS 是設置簽定那些未使用/不正確候選郵件位址。在客戶的許可下，我們將在這些地址上安裝陷井，並重定向到我們中心系統上的一個“清洗”的位址。我們將手工監測那些地址幾個月，以確保這些垃圾郵件陷井被清除，和註銷一些來自郵件名單上或不垃圾郵件源的地址。一旦位址被認為是乾淨的，它將會移出垃圾郵件陷井系統。這個過程是和客戶一起合作完成，但要求很少或根本不需要參與。

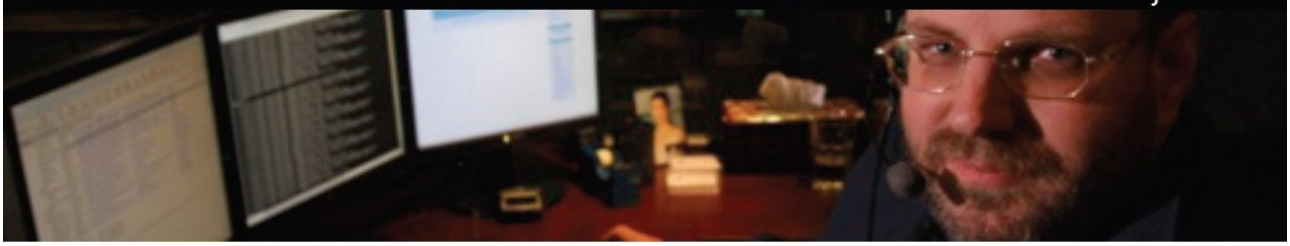
這個過程是即時的從垃圾郵件陷井系統採集垃圾郵件樣本，比 spam@network-box.com 機制有很大優勢。在更好的精度和即時（而不是延遲好幾天）採集進來的樣本，可以讓我們更好的監測和響應新的垃圾郵件爆發（即使針對單個客戶）。

我們當前操作有幾百個垃圾郵件陷井，並隨時接收新的提交。

Network Box Spam Trap Accuracy

Month	Spam Accuracy *	% Viruses
January 2009	98.67%	1.39%
February 2009	99.12%	1.99%
March 2009	98.77%	1.78%
April 2009	99.24%	1.42%
May 2009	99.47%	0.21%
June 2009	98.89%	2.07%
July 2009	99.39%	1.19%
August 2009	99.10%	2.63%
September 2009	99.46%	3.12%
October 2009	99.55%	3.16%
November 2009	99.40%	2.14%
December 2009	99.22%	0.56%
January 2010	99.31%	0.88%
February 2010	99.21%	2.70%
March 2010	98.90%	0.83%
April 2010	98.24%	1.46%
May 2010	99.20%	0.79%
June 2010	99.37%	17.13% #

* *Spam accuracy is percentage of emails (excluding viruses) detected as spam.*
\# *Increase due to a global outbreak of HTML script based email spams blocked as malicious viruses.*



2010 年 七月 新特性

在 2010 年七月的第一個星期二，NETWORK BOX 將發佈補丁包以增強系統的性能。本地的 NOC 將會在七天後進行首次功能配置。這個月，這些包括：

. 促進改善 BOX OFFICE 相關服務合同和客戶查看體驗。我們正在著手部署新的客戶系統，在接下來的兩個月，將有顯著的改善。
. 調整了 PDF 週報系統的相關非 NETWORK BOX 隔離的垃圾郵件標記的計算。 這將會對沒有使用垃圾郵件隔離功能的客戶產生影響。
. 修復了 my.network-box.com 郵件追蹤功能，查詢日期在搜索選定日期範圍之外時可以正確的顯示傳遞狀態
.支援顯示 ISP 資訊選項到全球監控系統中，可以讓我們更好以理解 ISP 和互聯網線路的性能。
.改善網頁代理系統更好的應付高工作量的情況

在大多數情況下,上述變化應該不會影響服務運行或需要重新啟動設備。但是,在某些情況下(需要看配置而定) ,某個配置可能需要重新啟動,如有需要,當地 NOC 將會與您聯繫並安排時間

七月提示: 部署垃圾郵件陷井

在第二頁討論了這個新事項，垃圾郵件陷井系統是針對反垃圾郵件非常有效的工具。儘管我們已經操 作了幾百個這樣的陷井（包括和現有的客戶合作及我們的位址），但我們仍然尋找新的陷井。
這個過程是即時的從垃圾郵件陷井系統採集垃圾郵件樣本，比 spam@network-box.com 機制有很大的優勢。在更好的精度和即時（而不是延遲好幾天）採集進來的樣本，可以讓我們更好的監測和響應新的垃圾郵件爆發（即使針對單個客戶）。
如果你有知道任何老舊未使用的，或已知不正確的郵件位址，我們推薦你考慮這個選項，這個垃圾郵件陷井設置僅僅只需要很少的資源就可以讓我們更好的為您服務（及改善 NETWORK BOX 所有用戶反垃圾郵件系統準確性）。

請與你的本地 NOC 去確認你的配置需求是否已經按你的要求添加進去了，併發點時間去檢測這些選項是否可以工作了。

Mark Webb-Johnson,
CTO, Network Box Corporation

JUNE 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	694	-36.1
Signatures Released	185,792	-25.9
Firewall Blocks (/box)	708	+5.8
IDP Blocks (/box)	147,759	+4.9
Spams (/box)	53,830	+18.3
Malware (/box)	1,389	+104.0
URL Blocks (/box)	90,995	+18.0
URL Visits (/box)	3,585,910	+4.3

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