In The Boxing Ring

IN THIS ISSUE

2.
MAIL PORTAL ENHANCEMENTS

The Mail Portal is undergoing a public beta of revisions. It is now 3 to 5 times faster for common operations and supports a revised workflow (including 'tick-to-release' on the Web interface). More options are now available, giving the user finer control over the appearance of reports.The reports can be ordered by Spam Score (as an alternative to the received time of the email).

3.
MAIL SCANNING ENHANCEMENTS

This month there are three major enhancements to the system: Relationship Age and Count Score; SPF Aware Whitelists; and Own Domain Protection for Whitelisting.

3. RECENT VULNERABILITIES

The announcement of an unusually large number of zero-day vulnerabilities has kept Network Box Security Response at Threat Level Alert Condition #4 for almost a month.

4.
AUGUST 2009 FEATURES

The ongoing deployment of our recently released features and enhancements.

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

Welcome

歡迎您閱覽2009年8月版的In The Boxing Ring。在此版本中，我們將著眼於已經改進了的Network Box郵件門戶Mail Portal。其中最主要的變化是提升了訪問速度及美化了用戶介面。另外還優化及調整了工作流程及完善了郵件報告。請轉到第2頁瞭解更詳細的資訊。

在第3頁我們詳細列出了對郵件掃描系統的改進。我們還提供了Adobe和微軟公司最近宣佈的漏洞資料。

在我們8月的特別欄目中，我們也有通常的針對NBRS-3.0 系統的分配更新，增強的掃描引擎，對關係郵件系統及附件的版本修訂，和性能方面的改進以便能進一步支援到郵件門戶系統。

我們也有一些核心部件的更新，以解決最近公佈的系統漏洞。請轉到第4頁瞭解詳情。

和以往一樣，如果您有任何的回饋，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來隨時來我公司辦公室進行參觀指導。

您也可以通過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
August 2009

NETWORK BOX

Mail Portal Enhancements

儘管Network Box郵件門戶已經於兩年前正式發佈，我們仍然不斷地改進著系統：現在的速度提高了3至5倍，尤其是當使用搜索功能時；另外，我們也提供了一個簡化的和更友好的用戶介面，以及提供各個模組更清晰的資料展示及改進了工作流程。

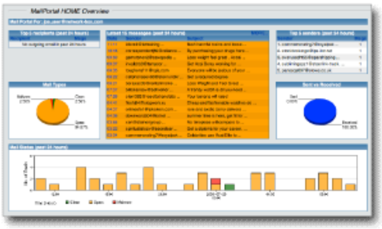


Figure 1 – Home Page

從主頁上我們已經取消了顯示最新的垃圾郵件和惡意軟體的名單。相反，這些可以在各自的欄目部分得到顯示。簡化後的主頁現在可以展示：

◦過去24小時內排名前5的電子郵件發送者，
◦過去24小時內排名前5的電子郵件接受者，
◦同一時期最新發出的15封電子郵件，
◦電子郵件的類型（圓形圖）
◦接收和發送電子郵件的比對（圓形圖），和
◦過去的24小時的郵件遞送狀態（條形圖）

點擊列在名單上日期欄目中的時間，可以顯示出最新的15封郵件（在過去24小時內），您將看到一個提供特定的電子郵件更詳細資訊的螢幕（在垃圾郵件欄目中也可以這樣操作）。

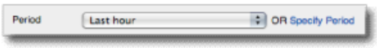


Figure 2 – Mail Search: Specifj Period

在郵件欄目中，最明顯的變化是增加了指定時段選擇搜索。

搜索結果表也發生了一些內部清潔：我們已經改名了欄目描述-接收時間，發件人，主題，類型和狀態-並添加了狀態圖示來顯示電子郵件是否是隔離的，未隔離的或已經釋放了的。所有的電子郵件也有帶顏色的背景，讓用戶知道橙色意味著垃圾郵件，紅色是病毒郵件而白色是正常的郵件。

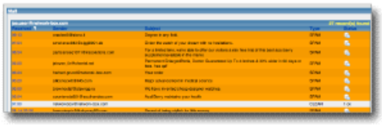


Figure 3 – Mail: Column Titles

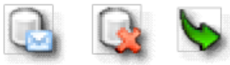


Figure 4 – Icons: Quarantined; Not Quarantined; Released

在垃圾郵件欄目中，概況介面提供了一個整貌，特別的易用。例如，和郵件欄目中的一樣，我們擴大了搜索功能，包括指定期限；搜索的速度也更快了。

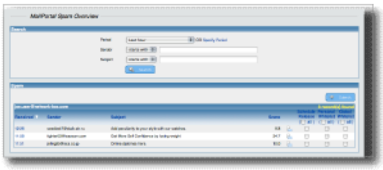
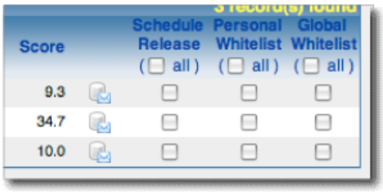


Figure 5 – Spam: Overview

電子郵件的掃描時間減少了，這樣可以幫助改善該系統的速度。掃描引擎會報告當前的郵件是否有病毒。

我們還增加垃圾郵件狀態圖示和全選（勾選及釋放）功能，這些選項是爲了幫助用戶節省時間和精力。此外，您還可以在收信時間一欄中單擊時間查看選取的電子郵件的詳細資訊。



Score	Schedule Release (□ all)	Personal Whitelist (□ all)	Global Whitelist (□ all)
9.3		□	□
34.7		□	□
10.0		□	□

Figure 6 – Select All

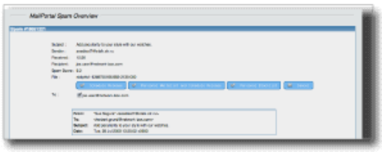


Figure 7 – Spam: Detailed View

於選定的電子郵件的詳細的資訊螢幕上還用非常簡化的格式來展示資料。

用戶可以用來確定電子郵件是否是垃圾郵件的主要資訊包含：

◦標題
◦發件人
◦收到電子郵件的時間
◦收件人及
◦垃圾郵件的分數。

在郵件門戶的設置部分我們也做了很多的變化。現在可以選擇您自己的郵件用戶端，具體方法是選擇使用下拉功能表旁邊的電子郵件用戶端。現有的選項包括：

- Microsoft Outlook 2007或以上
- Lotus Notes 6.5或更老版本
- 其他電子郵件閱讀器

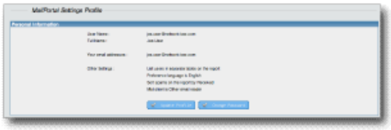


Figure 8 – Settings: Overview

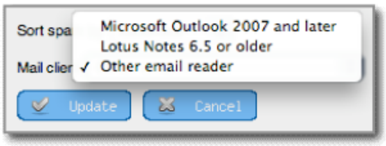


Figure 9 – Settings: Email Client

這一階段的改進中，我們也取得了對郵件門戶中郵件報告的美化：現在列在最前面的是惡意軟體。並幫助您確定標記的電子郵件是否確實是垃圾郵件，您也可以自行設定您的郵件報告，按照升/降分數順序列出垃圾郵件。

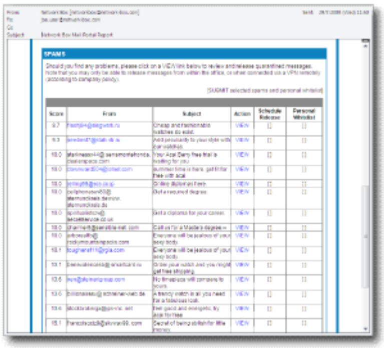


Figure 10 – Mail Report: Listing bj Spam Score

該測試版軟體將在8月的星期二補丁發放，正式的發佈將在9月的星期二補丁。

Mail Scanning Enhancements

這個月，我們將發佈關於郵件掃描引擎的三個重大改進：

1. 關係年齡和計數分數（分數調整爲垃圾郵件）

展望過去6個月的線上部署Network Box郵件關係技術的相關回饋，我們已經實施了演算法的改進，其中會考慮到關係年齡和郵件活動量。這可以被用來加強（或削弱）已經建立的關係，它基於以下兩個新的因素：

- 關係的年齡
- 郵件的交換量

2. SPF白名單的學習

我們已經實施了一項白名單制度的擴展，允許根據SPF（寄件人政策架構）測試結果是成功或失敗而進行白名單的微調。在部署了這一可選系統之後：

- 失敗的SPF白名單發件人將不會被加入白名單
- 中性的SPF白名單發件人將被視爲不太可能是垃圾郵件發送者（但不白名單）
- 成功通過的SPF白名單發件人將像往常一樣被當做白名單

3. 自有功能變數名稱白名單保護

此選用機制現在允許當發送者和接收者都在相同的網域時抑制白名單網域。在這種情況下，消極的垃圾郵件評分也可應用，使郵件資訊更有可能被視爲非垃圾郵件。

所有這三個新的特性將於2009年8月4日的週二補丁中正式發佈。

Recent Vulnerabilities

This month, an unusually large number of zero-day vulnerabilities have been announced, and patches released. Here is a short summary of the major ones.

Vulnerability in Microsoft Video ActiveX Control Could Allow Remote Code Execution

Microsoft Securitj Advisorj 972890

A zero-day vulnerability in the msvidct1.dll component of Microsoft Video ActiveX. There were widespread attacks exploiting this vulnerability using a large network of compromised websites. The attacks used Internet Explorer as the attack vector and installed a Trojan downloader onto compromised machines. Microsoft released a partial fix on their July Patch Tuesday, but this was later shown to be ineffectual and protection was revised in the Microsoft July 28 out-of-cycle release.

Vulnerability in Microsoft Office Web Components ActiveX Controls Could Allow Remote Code Execution

Microsoft Securitj Advisorj 973472

A zero-day vulnerability in Microsoft Office Web Components ActiveX controls. There were originally limited targeted attacks exploiting this vulnerability using a network of compromised websites, but as expected, the scale of the attacks continues to grow. The attacks used Internet Explorer as the attack vector and installed a Trojan downloader onto compromised machines.

Adobe Flash-in-PDF Attacks

Adobe Securitj Advisorj APSA-09-03

Later in July, Network Box Security Response started to see exploits of a zero-day flaw in Adobe Flash Player 9 and 10, with the exploit delivered by a flash object embedded in an Adobe PDF document (rendered by Adobe PDF Reader / Acrobat). The flaw was acknowledged by Adobe (and labelled CVE-2009-1862). Adobe proposed a workaround (involving the manual deletion of the affected component) and scheduled to release patches on July 30.

Sun Java XML Signature HMAC Truncation Authentication Bypass

US-CERT Vulnerabilitj Note VU#466161

Sun announced a vulnerability that would allow an attacker to bypass the authentication mechanism provided by the XML Signature specification. Patches were released.

Microsoft Out-of-Cycle Patch 28th July

MS09-034 and MS09-035

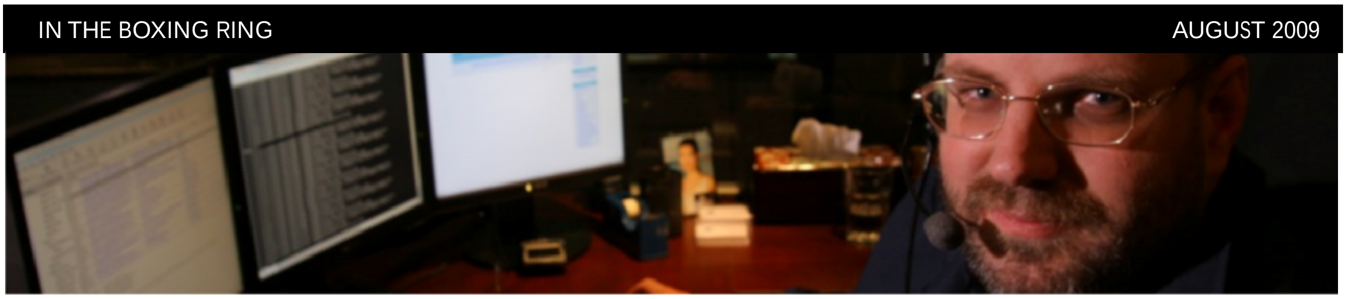
Following on from their work on the ActiveX control vulnerabilities, Microsoft announced that the cause of these vulnerabilities was far deeper than originally expected, and went to the unusual step of releasing out-of-cycle patches for both Internet Explorer and development libraries used by third parties. The patches were released on 28 July, but third parties may take some time to incorporate the changes in their code.

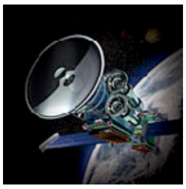
BIND Dynamic Update DoS

CVE-2009-0696 / CERT VU#725188

Following disclosure on a Debian bug-tracking system, the ISC has released urgent patches to their BIND DNS name server code. Exploitation of this vulnerability would result in a crash of the DNS server, and could lead to a Denial of Service (DoS). Analysis by Network Box Security Response and others indicate that this is not currently exploitable to gain remote access. However, the attack is possible against vulnerable ISC BIND DNS servers hosting MASTER zones (i.e., slave-zone-only DNS servers are not affected by this). Network Box, and several other vendors, released patches and protection signatures / instructions.

Overall, it has been an incredible month, and has kept Network Box Security Response at Threat Level Alert Condition #4 for almost the whole month. We, and our OEM partners, have pushed out over 350 signatures, as well as two out-of-cycle patches, specifically to protect against exploitation of these vulnerabilities. We continue to closely monitor the situation.





August 2009 Features

On Tuesday, 4 August 2009, we will be releasing a number of improvements to the mail scanning system. These enhancements include:

- Revisions to the email relationships system to track relationship age and activity
- Integration of SPF to whitelisting (to allow whitelisting to be controlled by successful SPF)
- Own domain protection (protection of whitelisted messages to/from the same domain), and
- Other miscellaneous improvements

We will also release the foundational components to support the new Mail Portal system entering beta this month.

Additional releases are updates to some of our core components to address recently-announced vulnerabilities. These updates include:

- DNS resolution
- DHCP, and
- Web Server

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

August Hint

在今年2月的“In The Boxing Ring”中 ，我們展示了一個新的和強大的在電子郵件關係基礎上的反垃圾郵件技術。

該系統通過監控您的SMTP電子郵件流量進而建立一個發件人和收件人之間關係的統計資料庫。當您的Network Box掃描一封新郵件時，系統會檢查發送者和接收者以前的交往歷史和關係強度， IP地址和功能變數名稱。然後根據這些重要的參數調整評分。這些電子郵件的關係也可以結合挑戰/回應技術，以達到反垃圾郵件系統接近100%的精確度。

連同新的SPF和白名單一體化，再加上在本月發佈的自有功能變數名稱保護功能，現在是時候重新訪問和執行這項挑戰/回應系統了（如果您還沒有用它的話）。

結束語

感謝您支援Network Box，並繼續將您的網路安全託付給我們進行管理服務。我希望這份通訊月刊對您有用。如果您有任何建議，我們都非常歡迎，您可以向當地的NOC或客戶經理反映；如果您有其他需求，也請別猶豫，馬上與我們聯繫，尋求協助。

Mark Webb-Johnson
CTO, Network Box Corporation
August 2009

JULY 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	998	-7.8
Signatures Released	170,469	-16.7
Firewall Blocks (/box)	624,287	-2.0
IDP Blocks (/box)	181,789	+15.4
Spams (/box)	71,075	-2.8
Malware (/box)	3,148	+42.1
URL Blocks (/box)	105,091	+27.5
URL Visits (/box)	2,979,650	-3.3

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
Michael Gazeley
Jason Law
Nick Jones
Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
l6th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2078
Fax: +852 2736-2778
www.network-box.com