In the Boxing Ring

Network Box 技術資訊

Network Box 技術總監 Mark Webb-Johnson

歡迎閱讀2013年 2 月刊的《In The Boxing Ring》

這個月我們將討論兩個主題：DNS和SSL。 名稱解析系統(DNS),可以追溯到1982年。但設計時起，DNS就有一個基礎性問題——它架構在UDP/IP協議基礎上，這意味著回應資料包通常被限制在512位元組以內。我們將在第2頁討論Network Box是如何解決這個問題。

在第3頁，Network Box研發部的Nick Jones將會討論Network Box安全套接層（SSL)安全性原則。這是他一系列有關SSL文章的第一篇，評論 TurkTrust Certificate Authority將給客戶的普通網站證書誤發成為中繼證書這一事件。此次誤發證書不僅顯示出SSL的本質弱點，也突顯了Network Box NBRS-5.0可帶給客戶的保護功能。

在第4頁，是這個月對NBRS-3.0發佈的新特性和修復補丁的詳情。在可預見的未來幾年，我們將繼續NBRS-3.0的開發和支援工作，這一頁將讓您瞭解到我們核心產品的動態資訊。

Mark Webb-Johnson
CTO, Network Box Corporation
February 2013

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
Google+ https://plus.google.com/u/0/107446804085109324633/posts

本 刊 概 要

DNS，電郵和512位元組

名稱解析系統(DNS)，可以追溯到1982年。在此之前，網路中主機互訪要麼是直接使用IP位址，要麼是維護分發一個巨大的“hosts”檔給網路中所有參與的主機。我最早的工作（在有DNS之前），就是管理一個超過1萬行的sendmail .cf設定檔，檔中定義了到上千個電郵伺服器的電郵路徑，多麼可怕的維護工作。

DNS不但解決了名字和IP位址的關聯這一關鍵問題，也進一步使得通過名字可以獲取其它資訊記錄（比如給電郵伺服器的MX記錄）。隨著時間推移，更多的約定出現，來擴展用戶端可獲取的記錄類型和對這些類型作出解釋。現在DNS已無處不在，它已成為全球互聯網的“電話本”。

但是，因為1982年設計時只有有限的幾個記錄，DNS有一個基礎性的問題-建立在UDP/IP協議之上，這意味著查詢回應被限制在512位元組或更小。DNS可以在受到限制後轉面使用TCP/IP協定查詢，但這會減慢速度並且在一些部署中會出現問題（不是普遍啟用，而且常被防火牆阻擋）。如果DNS回應中只有幾個IP位址記錄是沒有問題的。現在，加上MX記錄，A記錄，AAAA記錄，NS記錄和非常重要的DNSSEC記錄，回應已經超過512位元組，DNS運作得很艱難。

一直以來，在防火牆上開放UDP/53（基於UDP的DNS）而阻止TCP/53（基於TCP的DNS）這樣的策略相關普遍，主要因為基於TCP的DNS過去多用來傳輸較大的DNS區域資料。阻止TCP/53可以簡便的阻止敏感的DNS區域資料傳輸。近來，一些主要的DNS提供者進一步限制了某些類型的DNS查詢（比如用來查詢所有記錄的“ANY”查詢）。這兩種防護措施都是違反RFC標準的，其結果就是帶來電郵投遞失敗和網路連接問題。

Network Box一直努力提高效率來平衡DNS帶來的延時，以提高性能和優化網路佔用。很簡單，一次查詢獲取多個記錄比分別查詢各個記錄有效的多。於是我們查詢郵件伺服器MX記錄時使用DNS“ANY”查詢（可以一次獲取所有相關記錄）。這各方式是符合標準規範的，但在遇到不參照標準配置的問題DNS伺服器、防火牆時就會有問題。

在2013年2月的星期二補丁日，Network Box發佈了SMTP存儲轉發服務程式的新修定版本，不再使用“ANY” DNS查詢，而是在需要時用多個單類型查詢代替。這樣可以降低DNS回應包平均大小（只有查詢的那項記錄會返回），缺點時在可能會需要多次DNS查詢（延時較高）以獲得其它類型的記錄。這種方式是完全符合標準規範的，也提升了與那些不合標準的DNS伺服器的相容性，代價是多次查詢增加的開銷。

Network Box 透明模式SMTP系統依賴於發起SMTP連接的主機自己的DNS解析，不受這次變更影響。

和以往一樣，如果您有任何問題和疑問，請與您當地的Network Box NOC聯繫取得幫助。

Network Box
安全套接層安全性原則
(SSL Plus)

Nick Jones
Network Box研發部總監

這是一系列有關Network Box安全套接層（SSL）安全性原則，或者叫SSL Plus的文章的首篇。SSL Plus包含Network Box NBRS-5.0的新技術和Network Box採用的一套商業流程，這給基於SSL的基礎安全增加了新的價值。

這個開篇本準備介紹SSL和SSL Plus的一些重要技術，但最近幾周發生了一件事，不僅顯示出SSL的本質弱點，也突顯了Network Box NBRS-5.0可帶給客戶的保護功能。所我們把解釋這些技術的部分放在了下一個月。

這次事件就是TurkTrust Certificate Authority將給客戶的普通網站證書誤發成了中繼證書。事件的細節，包括起因及是否是惡意行為並不重要，重要的是洩漏的中繼證書可以用來簽發任何網站安全證書，流覽器會當作完美有效的證書接受。這次事件再一次展示了中繼證書以及憑證授權的脆弱性，和流覽器事實上對證書的過份信任--直到這種信任被明確、主動的移除。

這個事件從1月份開始被眾多媒體報導，一個月後主要的作業系統廠商開始發放更新來移除這些中繼證書。雖然一些主要的流覽器廠商反應迅速，但威脅仍要等組織和最終使用者真正更新了他們的軟體後才能解除。

讓我們看看在一個運行著包含用戶端SSL Plus模組的Network Box NBRS-5.0 Web用戶端掃描產品的組織在遇到這咱情況會怎麼樣。用戶端SSL Plus的一個特性就是它個可以檢查組織內部所有流覽器的SSL連接，在閘道上從組織層面執行管理人員制定的存取控制策略。任何被檢測出使用的證書屬於被洩漏中繼證書信任鏈的連接，都可以被NBRS-5.0 Network Box阻止。因為這些中繼證書使用一個獨一無二的SHA1指紋識別，任何其它安全連接都不會受到影響。

在得知這次事件後，Network Box區域SOC員工會聯繫客戶，提供可在客戶NBRS-5.0中立即生效的相關存取控制策略，從而在幾分鐘內保護一個客戶。

在得知這次事件後，Network Box總部會開始一個流程，使這個存取控制策略成為預設配置，並使用NBRS-5.0的配置同步機制在幾個小時內分發這個保護策略到當前的Network Box客戶。

在得知這次事件後，Network Box核心開發團隊會整合這個存取控制策略到NBRS-5.0軟體中，使之成為NBRS-5.0產品的一部分。 更新後的軟體會分發到地區和總部工程團隊，之後發出的所有Network Box產品將會包含這一安全性原則，從而在幾個小時後，有能力保護所有未來的Network Box用戶。

Nick Jones
Network Box研發部總監

Nick給Network Box帶來深層的專業技術。他是自由和開源軟體社區的熱情參與者，這使他參與到Linux內核，OpenSSL和ASIO網路庫等開源專案中。他也是ISO C++標準化委員會網路研究小組的貢獻者之一。

2013年 2 月 新特性

在2013年 2 月5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：

- 各種內部NOC系統的改進；
- 對 my.network-box.com Web管理介面微小修正;
- 電郵服務程式DNS機制修訂;
- NBRS-5.0在Box Office系統中的進一步支援；
- 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 I 網路安全活動

2013年1月30日，Network Box出席了由香港電腦保安事故協調中心、政府資訊科技總監辦公室和香港警務處共同舉辦的“ 應對針對性網路攻擊 ”研討會。Network Box總經理Michael Gazeley做了關於零日攻擊、零日惡意軟體和如何保護電腦和網路安全的演講。

Network Box USA I TechMecca 2013

2013年21-22日， Network Box USA在德克薩斯州沃思堡參加了TechMecca展覽會。TechMecca以舉辦富有活力的，由熟知技術、市場、客戶服務之間微妙平衡的業界專家領導的專業技術研討會為主要特色。

JANUARY 2013 NUMBERS

關鍵指標	數據	與上月差比(%)
PUSH Updates	692	+15.9
Signatures Released	594,462	+6.2
Firewall Blocks (/box)	982,050	+3.3
IDP Blocks (/box)	114,090	-7.1
Spams (/box)	12,020	-3.8
Malware (/box)	369	-54.3
URL Blocks (/box)	169,784	+7.0
URL Visits (/box)	3,975,586	-4.6

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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