Cisco Email Security:瞭解上下文自適應掃描引擎(CASE)

目錄

[簡介](#)
[瞭解CASE，在環境中檢測混合威脅](#)
[誰？](#)
[哪裡？](#)
[怎麼會？](#)
[什麼？](#)
[行動中的案例](#)
[高效能、低成本](#)
[摘要](#)

簡介

混合威脅的數量急劇增加。過去兩年中，許多最重要的病毒爆發都與垃圾郵件傳送有關，也就是說病毒負載會製造一群「殭屍」電腦，用於傳送垃圾郵件、網路釣魚、間諜軟體甚至更多病毒。電子郵件傳播的間諜軟體每六個月就翻一番，垃圾郵件URL安裝竊取使用者名稱和密碼的「鍵盤記錄器」的情況也屢見不鮮。病毒甚至可以用來建立殭屍網路，發動大規模的分散式拒絕服務攻擊，比如[Mydoom.B變種通過協同攻擊讓上合組織的網站下線](#)時。

是什麼在推動混合威脅的突然增加？簡言之，這是錢。隨著第一代反垃圾郵件技術（如黑名單和內容過濾器）的部署越來越廣泛，傳統方法（如從固定伺服器銀行傳送垃圾郵件，在郵件文本中包含「優惠」）的利潤越來越低。隨著使用反垃圾郵件技術的網路越來越多，「簡單」的垃圾郵件也會越來越少，從而會通過垃圾郵件過濾器進入收件人的收件箱。這損害了垃圾郵件製造者的利潤率，迫使他們適應這些變化。

垃圾郵件傳送者通過兩種不同的方式處理這種情況：

1. 他們傳送更多的垃圾郵件，希望他們丟失的郵件遞送率能彌補數量。
2. 他們轉向混合攻擊來掩飾其報文，並提高每條報文的利潤。

第二種方法往往成為犯罪活動。有組織犯罪網路已經建立，可以執行攻擊，並從病毒、網路釣魚和其他威脅中獲利。2004年，一個名叫John Dover的人因交易了超過200萬個信用卡號碼而被捕，這些信用卡號碼是通過網路釣魚攻擊被竊取的。

混合攻擊中使用的技術也變得越來越複雜。[Sober.N病毒使用](#)電子郵件、網路下載、特洛伊木馬和殭屍程式。傳統的內容分析過濾器無法應對這些智慧威脅。許多第一代反垃圾郵件過濾器的使用者發現，他們需要花費更多的時間「培訓」他們的過濾器或編寫新規則。但是，儘管作出了這些努力，它們的捕獲率和吞吐量都在下降。其結果是，隨著需要更多系統來跟上負載，成本會增加，而管理每個系統所需的管理時間會增加。

思科電子郵件安全已經使用稱為情景自適應掃描引擎(CASE)的獨特混合威脅防禦技術來解決這些威脅。 思科電子郵件安全的CASE技術可用於阻止傳統的垃圾郵件和基於殭屍網路的複雜攻擊。這種掃描技術還用於防止病毒和惡意軟體，比簽名可用性提前42小時 — 通過一次統一掃描提高效率。

瞭解CASE，在環境中檢測混合威脅

第一代過濾器被設計用來檢視消息的內容並做出判斷。例如，如果郵件中出現「免費」一詞超過2次，同時出現「草藥」一詞，則可能是垃圾郵件。這種方法相對容易被垃圾郵件傳送者用隱藏的字元或數字代替字母（如「f0r y0u」代替「for you」）擊敗。 第二代技術（如貝葉斯過濾器）試圖通過學習自動區分垃圾郵件和合法電子郵件的特徵來彌補這一限制。但事實證明，這些技術很難訓練，反應太遲，掃描速度太慢。

鑑於當前垃圾郵件使用的高級混淆技術，一流過濾器需要檢查傳入郵件的完整上下文。CASE使用先進的機器學習技術，這些技術模擬人類用來評估消息合法性的邏輯。人類閱讀者以及思科電郵安全的CASE技術提出了四個基本問題：

1. 誰給我發的資訊？
2. 郵件中的連結將我引向何處？
3. 消息是如何構建的？
4. 該消息包含什麼？

下面是對評估的每個邏輯區域進行檢查。

誰？

如前所述，第一代垃圾郵件過濾器主要依靠關鍵字搜尋來識別垃圾郵件。2003年，思科(IronPort)引入了信譽過濾的概念，徹底改變了郵件安全行業。當內容過濾問到「郵件中有什麼？」時，信譽過濾問到「誰傳送了郵件？」問題。這一簡單但有力的概念拓寬了評估威脅的背景。到2005年，幾乎每一家主要的商業安全供應商都採用了某種型別的信譽系統。

確定信譽涉及檢查有關給定發件人（發件人定義為傳送郵件的IP地址）行為的廣泛資料集。 思科會考慮超過120個不同的引數，包括隨時間推移的電子郵件數量、此IP所攻擊的「垃圾郵件陷阱」數量、來源國、主機是否遭到破壞等。思科有一支統計人員團隊，負責開發和維護演算法，這些演算法會處理這些資料以生成信譽分數。然後，接收思科郵件安全裝置(ESA)可使用此信譽得分，然後可以根據發件人的可信度對其進行限制。簡而言之，傳送者出現的「垃圾郵件」越多，傳送速度越慢。信譽過濾還通過在郵件被接受之前拒絕或限制連線，解決了與郵件數量激增相關的問題，從而顯著提高了郵件系統的效能和可用性。Cisco ESA信譽過濾器阻止超過80%的傳入垃圾郵件，大約是競爭對手系統的捕獲率的兩倍。

哪裡？

儘管2003年電子郵件內容分析與聲譽相結合已相當先進，但垃圾郵件傳送者和病毒編寫者策略的成熟程度仍在不斷提高。作為回應，思科(IronPort)引入了Web信譽的概念，這是擴展消息評估環境的重要新載體。與計算電子郵件信譽的方法類似，Cisco Web Reputation會檢視超過45個與伺服器相關的引數，以評估任何給定URL的信譽。引數包括隨時間變化對URL的HTTP請求量、URL是否託管在信譽分數較低的IP地址上、此URL是否與已知的「殭屍」或受感染的PC主機關聯，以及URL使用的域的年齡。與電子郵件信譽一樣，此Web信譽是使用粒度得分來衡量的，這使得系統能夠處理複雜威脅的模糊性。

怎麼會？

思科郵件安全環境分析的另一種新方法是檢查郵件結構。合法郵件客戶端（如Microsoft Outlook）以獨特的方式構造郵件 — 使用MIME編碼、HTML或其他類似方法。對資訊構建的審查可以揭示其合法性的許多問題。一個最能說明問題的例子是垃圾郵件伺服器試圖模擬合法郵件客戶端的結構。這很難做到，不完美的模擬是非法消息的可靠指標。

什麼？

完全的情景分析需要考慮郵件的內容，但是，如前所述，僅靠內容分析不足以識別非法郵件。Cisco Email Security的CASE技術使用最先進的機器學習技術執行全面的內容分析。這些技術會檢查郵件的內容，並將其分為不同的類別 — 是財務的、色情的，還是包含已知與其他垃圾郵件相關的內容？此內容分析與其他屬性（Who、Where、How和What）一起被計入CASE中，以評估消息的完整上下文。

行動中的案例

由於CASE分析資料的廣度，該技術可用於各種安全應用，包括IronPort反垃圾郵件(IPAS)、灰色郵件和病毒爆發過濾器(VOF)。 以下示例重點介紹如何使用CASE來阻止垃圾郵件。該郵件的內容與被遮蔽的組織幾乎完全相同，因此該郵件的內容分析無法識別任何威脅。對於基於內容的過濾器，此消息似乎是合法的通訊。要確定此郵件是否為垃圾郵件，主要依賴於「什麼內容」的過濾器很容易被騙去識別郵件是否合法。但是，對消息整個上下文的分析描繪了不同的畫面。

- 傳送郵件伺服器的IP地址可疑 — 它突然激增了流量，而域則不接受郵件。
- 電子郵件的URL指向似乎位於消費者寬頻網路中的伺服器。
- 消息中通告的URL與按一下連結時使用者導航到的「實際」URL不同。

在情景中考慮上述所有三個因素後，您會清楚地看到，這不是合法郵件，而是垃圾郵件攻擊。

傳統的「內容過濾器」
內容過濾器找到的內容

什麼？郵件內容合法。

裁決：未知

內容自適應掃描
CASE找到的內容

什麼？郵件內容合法。
怎麼會？ 消息構建模仿微軟 Outlook客戶端。
誰？
1)電子郵件傳送量突然激增。
2)作為回報，郵件伺服器不接受郵件。
3)位於烏克蘭的郵件伺服器。

哪裡？
1)一天前註冊的顯示與目標URL網站域不匹配。
2) 在消費者寬頻網路上託管的網站。
3)「Whois」資料將域所有者顯示為已知垃圾郵件者。

裁決:封鎖

在病毒爆發過濾器中使用CASE時，會應用相同的評分和機器學習功能 — 儘管會對單獨調整的資料集進行評分。病毒爆發過濾器是思科提供的基於CASE技術的預防性防病毒解決方案。Outbreak Filters解決方案會根據「即時」爆發規則（由Cisco Talos特定爆發發佈）和「永不中斷」自適應規則（始終駐留在CASE上）掃描郵件，從而在使用者有機會完全形成病毒爆發之前保護使用者。CASE允許病毒爆發過濾器以多種方式準確檢測並防範病毒爆發。首先，CASE可以根據附件副檔名、檔案大小、檔名、檔名關鍵字、檔案幻數（檔案的實際副檔名）和嵌入式URL等引數快速掃描郵

件。因為CASE技術會分析達到這一詳細程度的消息，所以Cisco Talos可以發佈非常精細的爆發規則，以最小的誤報來準確地防禦爆發。CASE可以動態接收更新的爆發規則，確保它針對最新爆發提供保護。

除了根據爆發規則分析郵件外，CASE技術還根據自適應規則掃描郵件。自適應規則是精細調整的啟發式方法和演算法，用於檢查傳入消息是否有表示病毒的偽裝和欺騙特徵。除了這些引數外，自適應規則還根據郵件的SenderBase病毒評分(SBVS)對郵件進行評分。SBVS是一個類似於SenderBase信譽評分(SBRS)的評分，但其排名基於傳送方傳送病毒性電子郵件而不是垃圾郵件的可能性。大多數病毒郵件由以前受感染的「殭屍」電腦傳送，因此識別和評分這些傳送方是捕獲病毒的關鍵因素。

思科電子郵件安全的CASE技術使病毒爆發過濾器能夠在傳統防病毒解決方案之前阻止病毒爆發，因為CASE以多種方式檢查郵件。它能夠分析郵件附件、郵件內容和郵件結構的眾多特徵，並能夠根據郵件發件人的信譽分析郵件。而且，由於CASE還充當IronPort反垃圾郵件和信譽過濾器引擎，因此只需針對所有這些應用程式掃描一次郵件。

高效能、低成本

CASE技術背後的邏輯可能非常複雜，因此處理過程會佔用大量的CPU。為了最大限度地提高效率，CASE採用了獨特的「早期退出」技術。早期退出會優先考慮CASE處理的無數規則的效力。CASE技術首先運行影響最大、成本最低的規則。如果達到統計判定結果（無論是正的還是負的），則不會運行其他規則，從而節省了系統資源。這種方法的優美之處在於充分理解每條規則的功效。CASE自動監控並隨著有效性變化調整規則執行順序。

提早退出的結果是CASE技術處理郵件的速度比傳統的基於規則的過濾器快大約100%。這對於大型ISP和企業具有明顯的優勢。但它對中小企業也有好處。CASE的效率加上Cisco Email Security的AsyncOS作業系統的有效性，意味著使用AsyncOS和CASE技術的ESA可以在非常低成本的硬體上實施，從而降低資本成本。

CASE技術轉變為低成本的另一種方式是消除管理開銷。CASE每天自動調整和更新數千次。Cisco Talos提供經過培訓的工程師、多語言技術人員和統計人員。思科Talos分析師擁有特殊的工具，可突出顯示在任何思科電郵安全客戶網路或全球電郵流量模式中檢測到的郵件流異常。Cisco Talos生成自動即時推送到系統的新規則。Cisco Talos還維護一個大量「垃圾郵件和火腿」語料庫，用於培訓CASE使用的各種規則。自動更新的CASE規則意味著管理員不必調整和調整過濾器，也不用花時間在垃圾郵件隔離區漫遊。

摘要

垃圾郵件、病毒、惡意軟體、間諜軟體、拒絕服務攻擊和目錄收集攻擊都受到相同的基本動機 — 利潤的驅動。這些利潤是通過銷售或宣傳商品或盜竊資訊獲得的。這些銷售帶來的利潤正在推動由專業工程師開發的、日益複雜的攻擊。高級電子郵件安全系統需要在儘可能廣泛的環境中分析郵件以對抗這些威脅。Cisco Email Security的上下文自適應掃描引擎技術問了四個基本問題：從混合威脅中清除合法消息的人員、位置、內容和方式。

- 「誰」是傳送消息的發件人的電子郵件信譽。
- 「Where」是網站宿主源的聲譽 — 分析連結會將您帶到何處。
- 「什麼」是對報文內容的分析 — 報文包含的內容（第一代系統通常僅依賴「什麼」型別的分析）。
- 最後，「如何」是對消息構建方式的分析。

此分析人員、位置、內容和方式的基本框架在阻止垃圾郵件方面與阻止病毒爆發、網路釣魚攻擊、

電子郵件傳播的間諜軟體或其他電子郵件威脅方面同樣有效。資料集合和分析規則集合針對每個威脅進行專門調整。CASE技術使思科ESA能夠在單個高效能引擎上處理這些威脅，從而以最高效率阻止範圍最廣的威脅。