目 錄

本白皮書的目標讀者

企業資訊安全主管與團隊可以透過本文件瞭解新的信譽式安全技術，這種技術可自動辨識並攔截極隱密的惡意程式碼，不需使用者介入，同時還能提升系統的效能。

簡 介

惡意程式碼一直朝更惡毒的方向演進，不斷尋找新的形態、偽裝及管道來接觸、滲透及危害目標。特徵式防毒軟體可有效地防禦已收錄到特徵資料庫的病毒、特洛伊木馬程式和病蟲。雖然特徵掃描對於系統的效能衝擊會隨其掃描檔案的大小、壓縮與否、複雜性和特徵數量而增加，但相對上仍相當有效率。只是，特徵式防禦遇到新的惡意程式時就變得毫無用武之地。

基於這項缺陷，特徵式防禦一般都會搭配其他防禦技術來輔助，例如：可尋找所謂泛型特徵的工具，以及可尋找惡意行為證據的進階啟發式技術。這些工具雖可提升實質防護能力，但是所造成的效能衝擊卻也比特徵式掃描更大。更糟糕的是，由於是啟發式技術 (因此無法實際驗證)，所以準確度較低、誤報率較高，因而可能影響員工的生產力，降低企業使用防護的意願。

結構性的轉變

依據賽門鐵克為其年度網路安全威脅研究報告收集的資料顯示，惡意程式的製作和散佈形態已有驚人的轉變--從廣泛散佈相對少量的威脅，轉變成集中散佈大量的獨特威脅。這樣的轉變打亂了目前特徵式與啟發式防禦之間的平衡，讓兩種方法都變得效果不彰，也讓企業暴露在一大堆獨特的攻擊當中。如果不加以解決，企業可能將被迫在安全與效能之間做出取捨。

這份報告的主要發現如下：

- **更多攻擊**：2011年發生55億次攻擊，比2010年增加81%。
- **更多獨特威脅**：2011年有4億零3百萬個獨特威脅，2010年則是2億8千6百萬個。
- **更多網頁式攻擊**：2011年的網頁式攻擊比2010年增加36%。

大量散發的郵件與其他「傳統」攻擊依然常見，幾年前現身的老惡意程式，至今依然可找到數千台未受保護的電腦可攻擊。但很明顯的趨勢是，不久的將來，網路上將流傳著數以億計讓特徵式防禦難以招架的威脅。若是單靠啟發式技術，全球企業網路的效率和生產力都將大受影響。本報告的目的，就是要發掘新的惡意程式碼偵測方法，並且摘要說明如何讓安全防護更加完整。

偵測的範疇

特徵式偵測能在可執行檔中搜尋已知的程式碼特徵。如果程式碼很新或很少見，就可能沒有可用的特徵來加以偵測。而「泛型」特徵則可偵測與先前發現的程式碼相似的惡意程式，因此類似特徵式偵測，只是較不精確。

進階啟發式技術可測試軟體的行為。但這需要一些時間，因此，主機效能受到影響或是軟體本身因持續或大量的攻擊而癱瘓的可能性將增加。此外，由於啟發式技術的精確度不如特徵式防禦，因此一旦出現大量新的惡意程式碼，將使得誤報率和漏報率雙雙提高。

我們需要一種新的防禦來輔助有效率、但不夠周全的特徵式防毒及較不可靠、需要

耗用更多資源的啟發式技術。這樣的防禦必須要讓防毒層可攔截已知的威脅，甚至讓大多數的新式威脅不需進入進階啟發式技術。

這種新式防禦的關鍵在於情境。所謂的情境，是由檔案本身以外可收集到的所有檔案相關資訊所組成，也就是檔案本身的內容與行為以外的資訊。由於此定義是開放的，因此沒有所謂的完整情境元素清單，但至少應包含：

- **普遍性**--檔案有多少個實例存在？
- **出現時間**--檔案的第一個實例出現於何時？
- **來源**--檔案從何而來？
- **檔案關連**--該檔案與哪些其他檔案有所關連或同時出現？
- **過去經驗**--網際網路上是否有其他電腦掃描過相同的檔案？掃描結果為何？

情境式防禦仰賴的是可信任檔案及網域的白名單，以及可疑檔案及網域的黑名單。然而這些名單並不完整，而且就像特徵一樣無法防範未知威脅：之所以不完整是因為還有一些尚未歸類為惡意或善意的「灰色檔案」存在；而之所以無法防禦全新、獨特或目標式攻擊，則是因為其資訊完全付之闕如，而且還必須將這些檔案送到啟發式技術進行分析，會增加處理器的負擔。

要 求

為了應付未來環境數以億計的新威脅，防禦機制必須使用比白名單和黑名單的情境定義更廣泛的高效率情境式防禦，來輔助特徵式與啟發式防禦。雖然這是一項嚴峻的挑戰，但是我們在下列要求當中描繪出一種利用駭客針對個別企業不斷製造全新獨特威脅的特點，以其人之道還之其身的方法來反制駭客。

1.分析網際網路上可存取的每個可執行檔，收錄到資料庫內

這種方法需要辨識、記錄、測試及評等每個可能包含病毒、特洛伊木馬程式或病蟲的檔案，並為檔案指定一個信任評等。以完整情境進行全方位分析在幾年之前仍是不可行的技術，但現在卻是唯一能個別衡量「普遍性」和「出現時間」的方式，也是唯一能認證低普遍性檔案究竟是否值得信任的方式。

全方位分析也是效能的關鍵，一旦有了檔案可信度評等，防禦機制就不必再檢查已知良好和已知不良的檔案，以免被不斷複製的惡意程式淹沒、浪費時間重新驗證可信任的檔案，或產生不必要的誤報警示。

這項分析必須在全球全面執行，因此需要龐大的偵測器網路和大量的運算效能。這個網路愈大，其偵測結果就愈準確，而且個別偵測器或伺服器的負擔也就愈輕。

2.計算每個獨特檔案的普遍性和出現時間資料

同樣的，這個數量很龐大，但是持續將這些資料收錄到資料庫內，可讓每個檔案在資料庫中的普遍性與出現時間資訊都保持在最更新的狀態。

普遍性與出現時間資料牽涉到檔案可信度，因此佔有重要地位。惡意程式碼的優勢來自於其隱匿性：它數量稀少，且往往以單一企業甚至單一電腦為目標，而且以「零時差」的方式出現來規避特徵式偵測。那些散

佈廣泛、出現已有一段時日的惡意程式碼，則很可能已被辨識，而且有公開的特徵資料。相反的，低普遍性、才剛出現的檔案反而是最危險的。

3.判斷每個檔案的來源和檔案關連

這個步驟對於辨識電子郵件或網址別名的背後玄機，以及辨識可疑來源檔案或辨識與可疑來源檔案關連的檔案非常重要。這方面的技術已經很成熟，資訊安全廠商早已使用這些技術來發掘：

- **指令和控制伺服器(command-and-control server)以及殭屍網路**--伺服器以及伺服器所吸收用來散播垃圾郵件、策劃阻斷服務攻擊和散佈更多惡意程式碼的電腦網路
- **惡意網頁伺服器**--已知會散佈垃圾郵件或惡意程式碼，或利用瀏覽器漏洞在訪客的電腦上植入這類程式碼的伺服器
- **裝置**--USB隨身碟、行動電話，以及其他上傳可執行程式碼到企業網路端點的不尋常媒介
- **檔案分享程式**--用來交換盜版光碟和軟體的應用程式也有很高的機率會植入惡意程式碼

這些彼此之間的關連可能毫不起眼，但是當初為了在大型資料庫當中尋找隱藏的關連性與相依性而開發的資料採礦技術，如今卻非常適合用來發掘電腦感染、網站與檔案之間的關連，規模甚至可以擴大到全球。

4.對每個檔案套用多層式偵測技術

這是原本套用在企業網路、企業內部和消費者裝置上的相同技術。全面套用這些技術的優點是可在全球網路的「雲端」執行大量平行偵測，減輕這些網路和端點的運算負荷。其中涵蓋的技術包括：

- **網路分析**，查看個別封包以發掘攻擊模式
- **特徵式防毒技術**，判斷先前是否已經將可執行檔判定為惡意檔案
- **靜態行為剖析 (啟發式技術)**，尋找檔案內可疑的程式碼
- **動態或即時的行為分析**，在模擬器或「沙箱」中測試程式碼，尋找可疑的活動和目標

情境並非一種獨立的偵測工具，而是為了改善其他偵測技術的準確度和效能而設。普遍性、出現時間、來源和檔案關連等資料，都可作為發掘惡意程式的參考，讓特徵與啟發式掃描能略過已知安全的檔案，讓啟發式技術能更深入地掃描可疑檔案，並讓防火牆能夠攔截已知惡意的連線而不必打擾使用者。

5.提供可採取行動的資料

系統管理員和使用者需要瞭解其所下載和管理的可執行檔中暗藏的風險，而這套方法可提供其需要的完整情境，使其做出正確的判斷。

還有一項附帶的優點是，它能提高安全意識，例如當系統管理員和使用者發現已下載的檔案從未見過、來自不可靠或不明來源，或是含有類似已知惡意程式 (儘管不盡相同) 的程式碼時會有所警覺。

現在的使用者經常必須在情境資訊不足的情況下做出安全決策：是否要造訪網站、安裝檔案或啟動可執行檔。最理想的情況是，在使用者點選連結來安裝程式或者允許程式存取其資料和連線之前，使用者就已獲得

情境和風險資訊。每個下載到企業內的檔案都應隨附風險資訊，讓系統管理員和使用者都能瞭解其所下載及管理的可執行檔是否暗藏風險。

6.根據可承受的風險程度制定政策

在企業 IT 環境中，政策管理非常仰賴自動化來確保政策在整個組織內的執行，並且產生給內部稽核員和外部監理機關查看的法規遵循狀態報告。IT 專家現在應該將新的普遍性、出現時間和檔案關連等資訊也納入其政策當中。可能的政策包括：

- **IT 開發環境**(高風險承受度)--允許安裝低信譽的軟體
- **財務資料**(低風險承受度)--不允許低信譽的應用程式存取這些資料
- **機密資料**(低風險承受度)--不允許中至高風險的應用程式存取付款卡、客戶資料庫或人事檔案
- **財務部門**(低風險承受度)--只能安裝高信譽的軟體

新資訊提供的額外精確度可讓政策準確地區分風險承受度--如此可在需要安全之處提供安全，在需要效能之處亦不犧牲效能。它可讓 IT專業人員根據風險承受度建立端點、Web 或網路攔截政策。例如，當他們知道某個檔案是最近才出現且普遍性很低時，即可根據特定部門、網域或裝置的風險承受度來決定是否提高保護措施。

7. 資訊回報

這樣的一套方法也很容易讓資訊安全廠商與其企業用戶端之間互通資訊，將新檔案的資訊回報至中央資料庫。每一位使用者回報的檔案都讓資料庫更強、更快、更有用。此外，由於此資料庫是全球性的，因此，惡意程式將沒有任何安全的角落可供其窩藏和散布。

這種隨樣本規模而增加的準確度，以及所有參與者共同抵制惡意程式的動力，將形成一種可提高惡意程式辨識率的良性循環，使得漏報率和誤報率降低、掃描速度加快、資源負擔更輕，進而釋放更多的資源來辨識及評量剩餘的程式碼。

這套方法如何改變遊戲規則

相較於時下的安全防護，這套新的方法能以更低的誤報率和更高的效能，提供更好的惡意程式偵測。今日網路罪犯仍佔據上風，因為他們能夠迅速發動客製化目標式攻擊。這套新的方法能徹底改變其模式：一些出現時間與普遍性評等很低的新興客製化攻擊將被所有環境攔截(高風險承受度的環境除外)。而「已成熟」的惡意程式則因為已被發掘並建立特徵，因此特徵式掃描與啟發式偵測也能比今日更輕鬆加以攔截。

同時，這套方法可確認來自信譽優良管道之檔案的合法性以減少誤報，且在永久移除隔離所內可疑軟體之前先檢查軟體信譽。

最後，這套方法還可將運算與評等的作業，以及大部分的掃描工作移到企業用戶端與端點之外，降低惡意程式爆發對系統效能的影響。由於新的評等資訊可減輕特徵式與啟發式防禦的負擔，因此每一種安全技術運作起來都更輕鬆，而且效果更好。

總 結

以企業為目標、專門為了牟利而創造的客製化目標式惡意程式是今日的嚴重威脅。但是建立一套全方位的檔案情境資訊評等機制，卻有機會消除隱密與目標式攻擊的效果，創造一種以更低的負擔即可提升 IT 安全的良性循環。

如何開始

今日賽門鐵克和諾頓的多款產品當中都包含了 Insight 技術。這些產品包括 Symantec™ Endpoint Protection、Symantec™ Endpoint Protection Small Business Edition、Symantec™ Endpoint Protection.cloud、Symantec™ Web Gateway、諾頓防毒、諾頓網路安全大師，以及諾頓 360。

如需更多有關我們偵測技術和企業安全產品的資訊，請洽詢賽門鐵克業務代表，或造訪http://go.symantec.com/insight。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)