可彈性應變的行為式惡意程式防護

目 錄

本白皮書的目標讀者

企業資訊安全高階主管與團隊可以透過本文件瞭解新的行為式安全技術，這種技術可自動識別並攔截極為隱匿的惡意程式碼，不需使用者介入而且對系統效能不會有明顯影響。

內容摘要

新一代的自訂、高度目標性和位元組層級的隱密惡意程式碼(俗稱惡意程式)會偽裝外觀以規避所有種類的被動回應式安全措施，特別是以特徵為基礎的防毒解決方案。不過就算惡意程式「家族」的每個新案例的外觀都不同，其行為是無法偽裝的。

Symantec™ SONAR技術利用此弱點建立新的最終防線，就連最狡猾、最隱匿的惡意程式也逃不過法眼。SONAR會監控受保護電腦上執行的每個處理程序，看看是否出現了在全球進行的詳盡應用程式行為分類期間所識別出的模式，然後即時予以攔截或移除，而不需要任何使用者介入、對效能不會有顯著影響，也不會產生嚴重的誤報警示風險。

SONAR在性質上與模擬和其他行為式方法不同，它每個月會分析超過5,000萬個應用程式執行個體、每天攔截超過73,000個惡意檔案，並且保護著全球超過5,000萬個企業和客戶系統。IT部門應認真考慮將IT安全解決方案升級以包含SONA保護功能，如果還沒真的開始使用，也應考慮啟用SONAR的保護。

全新的威脅環境

如賽門鐵克網路安全威脅研究報告所記載，[1]線上惡意程式碼(惡意程式)正經歷性質上的變化。專為竊取財務資產、智慧財產或敏感資訊而設計的第一代惡意程式會對數百萬個目標廣泛發動威脅，以便在遇到有漏洞的目標時下手。但是，第二代的威脅則採取專門以特定目標為對象進行準確自訂的方式，對於時下的安全技術和依賴這些技術的企業來說，將是更大的挑戰。

這些最新的威脅家族是從既有的惡意程式複製而來，然後透過自動化工具在位元組層級進行隱匿。用來將惡意程式加以偽裝來躲避所有特徵式防毒解決方案的駭客工具號稱是“100% FUD”(也就是完全不會被偵測到的意思)的加密程式，因此在線上罪犯市場中索價很高。

犯罪組織、政治駭客和國家資助的組織會依本身需要使用這些工具來建立最新的惡意程式執行個體，以竊取金錢和智慧財產、誤導使用者購買無用或危險的「假防毒」軟體、滲透或危害重要的基礎設施，或揭露使目標尷尬的資訊。新的企業與消費者威脅會採用的媒介包括：

- 進階持續性威脅(APT)、遠端存取木馬程式、間諜程式和鍵盤側錄程式
- 為了誘騙使用者安裝惡意程式而偽裝成防毒軟體、金鑰產生程式和影片轉碼工具的社交工程攻擊
- Bot軟體和偷渡式下載(drive-by download)，會自動將系統加到傀儡網路
- 會注入到執行中的系統處理程序、讓移除作業變得既困難又危險的非處理程序威脅

1-賽門鐵克公司。第 17 期賽門鐵克網路安全威脅研究報告 (Mountain View, CA，2012 年 4 月)。http://www.symantec.com/threatreport/

- 零時差威脅
- 不需任何使用者動作即可安裝惡意程式的偷渡式下載和網頁攻擊
- 為了規避偵測而設計成安靜掩藏在Rootkit中的惡意程式

位元組層級的隱密或加密會掩藏新的惡意程式變種，以迴避依賴特徵來辨識及攔截每個新加密複本的防毒軟體。自訂的惡意程式能夠在安全廠商發現它正在建立和散佈特徵之前，輕易抵達目標(通常是單一端點)。此外，自訂威脅的繁殖速度極快：賽門鐵克每年都發現數億個惡意程式變種，並攔截數十億次攻擊。

惡意程式的重大弱點以及對付它的新方法

新一代的惡意程式會偽裝其外觀以規避特徵式偵測。但是惡意程式創造者的目標並未改變，也就是詐騙、竊取、破壞及誹謗。因此其「最新誕生的」惡意程式會展現與舊惡意程式相同狹小範圍的行為--鍵盤側錄程式和密碼竊取程式會存取及匯出資訊、垃圾郵件Bot傀儡程式會傳送電子郵件、流氓安全程式會彈出誤導訊息等等。不像自訂惡意程式的特徵多如牛毛，惡意行為數目很少、一直以來都很穩定，而且在惡意程式家族中都很一致。

惡意程式行為的一致性是一大弱點，賽門鐵克就利用此弱點來建立新的防護技術。SONAR主動式行為防禦技術會根據惡意程式嘗試做出的動作，即時攔截和移除惡意程式，而不受其偽裝影響。自2010年起，SONAR就內建於Symantec™ Endpoint Protection 12.1與諾頓360™及諾頓網路安全大師消費性產品當中，並使用即時行為監控來攔截和停用極隱密的惡意程式碼，完全不需任何形式的使用者介入。

SONAR是多層防護的最內層：特徵式防毒功能可針對廣泛散佈的常見威脅提供快速、有效的防護。SONAR則使用及輔助賽門鐵克引擎(例如「網路入侵偵測」和Insight信譽式安全)，建立關鍵最後防線來抵禦以企業端點、桌上型電腦和使用者為目標的新興惡意程式。SONAR技術現在已發展到第四代，採用將Symantec Endpoint Protection 11中推出的早期行為偵測功能完整重新設計的主動式威脅防護。

SONAR 深入解析

SONAR技術會根據威脅的行為來加以偵測，而不是依賴特徵。這種方式連對付精密的惡意程式(例如Duqu、StuxNet和Hydraq/Aurora)以及內嵌惡意程式的Rootkit(如來自TidServ和ZeroAccess來源)的全新複製品種也很有效。為了將對於系統效能的衝擊減至最低，可疑行為定義是在離線實驗室透過詳盡的機器與人工分析來建立，然後透過Symantec™ LiveUpdate派送。

SONAR結合了：

- 在電腦上執行所有處理程序的即時行為監控
- 自動化與人工進行的詳盡行為分類
- 依據威脅行為和可能的系統影響予以移除或攔截

讓我們看看每項元件的運作方式和優勢：

即時行為式防護

SONAR會在處理程序執行時加以監控它們的行為，例如嘗試變更瀏覽器的首頁、安裝瀏覽器工具列、監控按鍵，以及近1,400種的其他行為。它也會藉由考慮處理程序的下列項目，注意每項行為的完整情境：

- **來源**—原始檔案是從可信任的網站下載、從網路共享磁碟複製、或由可攜式媒體安裝等等？
- **內容**—原始檔案是否經過加密和「壓縮」並以high-entropy加密來偽裝？[2]它會匯入哪項Windows®功能？程式碼是以商業解決方案或是以駭客喜歡的低階非主流編譯器編譯的？
- **關係**—處理程序是否產生任何被識別出有惡意企圖的可執行檔？

最後得到的行為清單(以完整情境呈現)可立即用於根據在實驗室所開發分類規則進行評估，而會透過LiveUpdate散佈。SONAR會藉由即時監控處理程序，將應用程式行為(包括極隱密惡意程式複本的行為，甚至是尚未建立之威脅的行為)納入到目錄。情境資訊可協助解決方案更快運作並防止誤報。

應用程式行為的分類

SONAR所監控的大量行為可為用來區別惡意與善意處理程序的規則產生龐大的統計資料庫，但是規則本身的品質與效率同等重要。就嘗試「即時」在用戶端系統內評估處理程序的規則式解決方案而言，品質與效率是互相對立的：準確度越高，需要的運作資源就遇多，而影響的效能越少表示遺漏和(或)誤報的風險越高。

SONAR則採取不同的方法，可發揮最佳效果而不犧牲生產力。系統和專家會在賽門鐵克實驗室中離線分析在線上收集到之應用程式執行個體的行為(到目前為止已有幾億個)，以建立用戶端系統可套用、幾乎對效能毫無影響的分類規則。賽門鐵克已開發超過1,000個這類簡單與複合的規則；基本例子包括：

- “Signed by VeriSign®”(好)
- “Terminates Symantec process”(壞)
- “Modifies Browser Home Page”BUT“Not Developed in Visual Basic”(好)

其他規則會將程式碼分類，例如讀取或寫入系統登錄檔的敏感區域、建立可執行檔、修改DNS設定等等。

收集和分析這一切資訊需仰賴賽門鐵克獨特的強項(包括全球最大的應用程式執行個體儲存庫，和全球各地數億個監聽通訊埠組成的網路)[3]來持續獲得新的執行個體。另外還有兩個強項特別值得一提。

2-Robert Lyda 與 James Hamrock。「使用 Entropy 分析來尋找加密與壓縮的惡意程式 (Using Entropy Analysis to Find Encrypted and Packed Malware)」，IEEE 安全性與隱私權 (IEEE Security and Privacy)，第 5 期第2 號 (volume 5 issue 2) (Piscataway，NJ: IEEE Educational Activities Department，2007 年 3 月)。

3-Christian A. Christiansen、Chris Liebert 及 Charles J. Kolodgy。全球及美國安全服務威脅情報 2011 - 2014 年預測：拋開陰霾並嶄露頭角 (市場分析)。(Framingham，MA: IDC。2011 年 11 月)。

首先，其他賽門鐵克安全技術的廣大普及率，為SONAR的分類工作提供其他來源都無法提供的情境和分析，包括：

- **防毒**—程式碼是否產生可辨識為病毒的可執行檔？
- **入侵預防**—應用程式是否顯示類似Bot傀儡程式的行為，或嘗試建立Bot傀儡程式？
- **信譽式安全**—Symantec Insight信譽系統(會計算所有檔案的社群信譽)的進階分析資料是否將應用程式分類為惡意應用程式？[4]

其次，「賽門鐵克技術與安全應變中心」會以真正有用的方式延伸分類規則，其方法為：

- 識別可定義威脅家族的行為順序，例如"PC Scout"的成員會假冒防毒軟體系列(防毒軟體系列全是都從Temp資料夾啟動)、將"AVE"寫入Windows登錄、建立“hostinfo.txt”檔案，然後修改瀏覽器首頁
- 審查及認可機器編寫的分類規則，以將其分類為IT安全系統管理員更容易瞭解和使用的系列群組
- 發佈惡意程式說明，其中整合來自SONAR、其他賽門鐵克防護技術和賽門鐵克人員智慧的資訊；範例請見RougueAV!gen20和Zbot!gen1

人工分類可加快應變時間，因為針對每個威脅家族來測試、分析及發行規則的速度會比針對每個執行個體的速度快。相較於僅靠機器進行分類，它還可減少誤報，因為每一個規則的背後不僅有更大量的證據來支持，還有經驗豐富的安全專業人員根據知識和經驗進行判斷。

行為式政策鎖定

當最新或變更過的分類規則得到認可且準備好時，賽門鐵克就會派送這些規則，而不會被固定的更新時程或漫長的修補程式發行週期所耽擱。用戶端電腦會立即開始使用這些規則來識別及移除惡意程式。

不過在少數情況下，光是識別和移除是不夠的。非處理程序威脅(如受Tidserv Rootkit控制而嘗試修改分割表的Windows Print Spooler Server)就無法與無害的程式碼區分(也就是說無法被識別出是惡意程式)。此外，移除寄生在主要Windows系統檔案中的威脅會造成系統不穩定。

在這些情況下，SONAR會攔截並反制非法的系統登錄檔變更、檔案刪除、資料夾建立等等來鎖定可疑的程式碼，同時允許不會對系統、使用者或網路帶來風險的作業執行。這種方法可防止因過度反應而降低應用程式效用或系統穩定性，同時仍針對重度加密、單一執行個體自訂的惡意程式或是零時差惡意程式提供優異的防護能力。

即時行為監控、機器與人工分類，以及攔截或鎖定可疑程式碼的結合，可針對為了規避傳統特徵式防毒技術而設計的精密惡意程式，提供極為有效的最後防線。它會在威脅執行的當下就移除或隔離威脅，但不會刪除高度信任的檔案、耗用系統資源在複雜的模擬，也不需讓使用者自行區別真的與假的惡意程式警報，或是區別真實的電子郵件與社交詐騙網路釣魚攻擊。

4-如需 Symantec Insight 的完整詳細資料，請檢閱隨附的白皮書「扭轉惡意程式的形勢：防禦獨特目標性攻擊的全方位方法」。

付諸行動的 SONAR--賽門鐵克的優勢

SONAR是廣泛部署的安全解決方案中，唯一使用即時行為監控來攔截最新和單一執行個體的惡意程式、而完全不需使用者介入的解決方案。它可提供高度的準確性，同時將對於系統資源的影響減至最低，包括在執行開機和關機、啟動應用程式、瀏覽網頁、讀取電子郵件、播放音樂和影片、複製DVD及編輯文件等日常作業期間，使用者幾乎感覺不到任何延遲。

SONAR經驗庫現已涵蓋超過1億3,400萬台電腦，以及對超過13億個應用程式執行個體的分析。此技術光是在2011年就識別及攔截了2,400萬個以上的威脅，同時針對提交評估的檔案維持在0.02%的誤報率。此外，數千萬台已安裝的系統上都自動啟用了攔截功能，為這些系統提供保護而不需要使用者介入或投入IT資源。[5]對賽門鐵克安全專業人員來說，最有價值的就是在線上攔截到數十次駭客通訊，確認這項技術的有效性。

SONAR不只是一點一滴累積進步，而是性質上完全不同的惡意程式碼分類和攔截/隔離方式。當我們逐項和其他技術比較時，就會發現SONAR的優勢非常明顯：

模擬式行為引擎會在啟動或掃描時監控模擬器中的處理程序，而非進行即時監控。這會延誤到合法處理程序的啟動並延長掃描時間。本機模擬對系統資源也會帶來明顯的影響，造成必須在效果和效能之間取捨。單靠機器進行評估和分類，可能會產生安全專家人工監督就能過濾掉的誤報。而駭客也在應變中，知道要對惡意程式加上防模擬功能進行加強，並在發行惡意程式之前對安全軟體測試該防模擬功能。

主機式入侵預防/防護/系統變更監視器會持續追蹤執行中的處理程序，但是會就每個可疑的動作對使用者顯示警示，包括絕對無害的RUN金鑰變更、驅動程式更新、主機檔案修改等等。使用者必須自行評估風險並決定對每個警示的適當回應動作。雖然經驗豐富的使用者會喜歡這種高度自主性，不過對於大多數使用者而言，這樣既礙眼又煩人，因而常常會忽略警示或乾脆關閉整套解決方案。

具有雲端查詢功能的簡單啟發式技術會使用兩階段處理程序在防護與效能之間取得平衡。首先，為了避免查詢作業消耗太多時間，它們會過濾用戶端上具有像是「壓縮」之類簡單特性的檔案。當惡意程式是故意設計成規避篩選，例如以「未壓縮」的形式發行時，威脅可能會順利通過檢查而不會被偵測到。此外，當過濾偵測到風險，並將檔案轉給雲端服務進行深入評估時，這段往返通訊對於處理程序啟動時間會有顯著影響。

偶發特性(例如，特徵、壓縮，甚至信譽)是有助簡化惡意程式之識別和移除的相關根據，但處理程序行為會定義它。SONAR由於會即時監控、攔截和隔離處理程序行為，因此可提供抵禦IT基礎架構與資訊資產威脅的最後防線。由於SONAR分類規則連對“100%FUD”隱密也免疫，這套解決方案可

5-賽門鐵克技術與安全應變中心。STAR 惡意程式防護技術 (網頁)。(Mountain View, CA：賽門鐵克公司。2012 年 5 月 1 日)。http://www.symantec.com/theme.jsp?themeid=star&tabID=4

避免在特徵式、用戶端上啟發式及混合式解決方案中出現的延遲、零時差漏洞，以及防護能力力/效能之間的取捨。

這些駭客都知道－負責監控地下資訊網路的賽門鐵克安全機制應變中心確認了SONAR技術在真實世界中的效果。此外，在已發佈的行為偵測解決方案比較報告中，也證實了SONAR的功能比較優秀。

以賽門鐵克安全解決方案系列領先市場的強項為基礎的SONAR技術在規模上也具有驚人的優勢，包括：

- 全球超過5,000萬個有效參與者貢獻應用程式執行個體給SONAR資訊儲存庫
- 每個月分析超過5,000萬個可執行檔、dll和應用程式
- 每天判定及攔截超過73,000個惡意檔案(至2011年12月為止的90天平均值)[6]
- 與全球使用的其他賽門鐵克防護技術深度整合，這些技術包括網路入侵防禦、防毒和Symantec Insight信譽引擎。

SONAR的成長過程記錄了到目前為止針對時下個人與企業系統的最嚴重威脅的重大防護改進。SONAR技術由於具有彈性應變的能力性，會不斷評估，然後再監控及攔截新的惡意程式變種，因此可持續提供有效的防護，而不需要使用者與IT進行費時或降低效能的介入。此外，賽門鐵克的努力方向是將SONAR技術定位在持續在未來許多年提供更優異的防護與效能。

採取下一步

目前使用Symantec Endpoint Protection 11或其他技術的企業應積極考慮升級至內含的SONAR進階行為式防護功能的Symantec Endpoint Protection 12.1。使用未含SONAR技術之Symantec Endpoint Protection 12.1的企業應評估使用SONAR，在投入較少的使用者和IT資源前提下，改善防護能力。若要深入瞭解SONAR可協助貴公司達到哪些成效，請造訪SONAR 技術網頁或聯絡您所在國家的賽門鐵克業務代表。

6-STAR 惡意程式防護技術。

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)