TRAPS

進階端點防護

Palo Alto Networks Traps 用多重防護方法取代傳統防毒，以獨特方式結合了針對性的惡意軟體與漏洞防護措施，可保護使用者與端點免受已知和未知的威脅攻擊。相較於重要資產已經遭到入侵之後的入侵偵測與事件回應，Traps 可防堵安全漏洞。

Traps 進階端點防護：

- 透過預先阻止已知和未知的惡意軟體、入侵和零時差威脅，預防網路入侵。
- 保護使用者進行其日常活動以及使用網路技術，而不必擔憂已知或未知的網路威脅。
- 利用取自 WildFire 的威脅情報自發地重新設定程式，藉此自動預防。

大多數的組織會部署一個混合式的安全解決方案以保護其端點系統，包括一或多個傳統防毒解決方案。隨著免費與低成本工具的擴散，威脅執行者現在能產出嶄新且獨特的攻擊，藉以避開特徵碼型防毒軟體。目前的端點安全解決方案和防毒無法保護使用者及系統免於遭受迴避、未知或零時差攻擊。

Palo Alto Networks® Traps™ 進階端點防護及其最有效的目的導向型惡意軟體與入侵防護方法的獨特組合，可在已知和未知的威脅危害端點之前加以防堵。

Traps 的多重惡意軟體防護

Traps 能使用獨特的多重預防措施預防惡意執行檔，不但有著最大的惡意軟體防護範圍，還能減少攻擊面，並增加惡意軟體偵測的準確度。此措施結合數種預防方法，能立即預防已知與未知惡意軟體感染系統 (圖 1)。

圖 1：Traps 的多重惡意軟體防護

1. **透過機械學習的靜態分析**：此方法會在允許任何未知的可執行檔執行之前立即提供裁定。Traps 會在不到一秒內檢查數以百計之檔案的特徵，而不需要依賴特徵碼、掃描或行為分析。
2. **WildFire 檢驗與分析**：此方法利用 Palo Alto Networks WildFire™ 雲端式惡意軟體分析環境來快速偵測未知惡意軟體，並自動重寫 Traps 的程式以預防已知惡意軟體。WildFire 能在約 300 秒內將未知威脅轉化成已知，藉以去除威脅。
3. **信任發佈者的執行限制**：此方法讓各組織能夠辨識「未知但良性」的可執行檔案，因為對它們進行發佈和數位簽署的發佈者和實體被 Palo Alto Networks 辨識為具信譽的軟體發佈者。
4. **政策式執行限制**：各組織可以輕易定義出限制特定執行情境的政策，藉此降低環境中的攻擊面。舉例而言，Traps 可以預防 Outlook 「temp」目錄中的檔案或 USB 隨身碟中的特定檔案類型執行。
5. **管理員覆蓋政策**：此方法讓組織能根據執行檔雜湊來定義政策，藉以管控各環境中可以運行以及不能運行的檔案。這個精細的白名單 (或黑名單) 功能可根據使用者定義的條件 (繫結至可以使用 Microsoft® Active Directory® 定義的任何物件)，控制任何檔案的執行。

被視為惡意並防止在端點上執行的任何可執行檔會在受保護的儲存庫中加以隔離，僅可由系統管理員存取。Traps 管理員可以審查、刪除隔離的檔案，或在必要時將其還原至各自端點上的原始位置。

Traps 的多重入侵防護

Traps 使用獨特的嶄新方式來預防入侵。Traps 不專注於數以百萬計的單次攻擊以及其所利用的軟體弱點，而專注在入侵式攻擊中所使用的核心入侵技巧。每次入侵都必須使用一系列這些入侵技巧才能成功破解應用程式。Traps 會在攻擊者嘗試使用這些技術的時刻封鎖它們，讓其失去效用。使用 Traps 的組織可以如常運行任何應用程式，包含在內部開發的應用程式，以及不再有安全性支援的應用程式，而無須為其環境帶來立即威脅。

Traps 採用多種方式預防入侵，結合了數重防護來阻止入侵技巧 (圖 2)：

圖 2：Traps 的多重惡意軟體防護

1. **記憶體損毀防護**：Traps 會針對可開啟含有入侵之武器化資料檔案的應用程式，防止可操控作業系統一般記憶體管理機制的入侵技術。
2. **邏輯錯誤防護**：Traps 會辨識並封鎖允許入侵操控作業系統一般應用程式程序和執行機制的入侵技術。
3. **惡意程式碼執行防護**：在多數情況下，入侵的最終目標就是執行攻擊者內嵌在入侵檔案中的命令。此防護方法能辨識出這種讓攻擊者惡意程式碼得以執行的入侵方式，並在它們得手前阻止之。

新世代安全平台

隨著運算能力的成本不斷減少，威脅執行者可以輕易發動越來越多比以往更多更複雜的攻擊。未整合的安全層，以及依賴過時技術或人工回應警示的單點解決方案，不再足以應對也不再可以擴充。只有對多種預防技術採取合併、自動化以及原生整合的平台才可以確實預防進階、針對性以及迴避攻擊。

Traps 與 Palo Alto Networks 新世代安全平台的原生整合，讓各組織能持續分享來自數千企業客戶處的威脅情報，並跨越網路與端點，協調預防和回應。自動重新改寫程式以及將威脅情報轉於防護用途都消除了攻擊者使用未知與進階惡意軟體感染系統的機會。攻擊者最多只能在世界的某處使用每個惡意軟體一次，並且在 WildFire 將其完全無效化以前僅有數秒時間能執行攻擊。

系統需求與平台支援

Traps 可保護未修補的系統，並在執行 Windows® 的任何平台上都受到支援：桌面、伺服器、工業控制系統 (ICS)、虛擬桌面基礎結構 (VDI) 元件、虛擬機器 (VM) 以及嵌入式系統 (圖 3)。

作業系統	
Windows XP (32 位元，SP3 或更新版本) Windows Vista (32 位元與 64 位元，SP1 或更新版本；FIPS 模式) Windows 7 (32 位元與 64 位元，RTM 與 SP1；FIPS 模式；家用版之外的所有版本) Windows Embedded 7 (標準版與 POSReady) Windows 8 (32 位元與 64 位元) Windows 8.1 (32 位元與 64 位元；FIPS 模式) Windows 10 Pro (32 位元與 64 位元) Windows 10 企業版長期維護 Windows Server 2003 (32 位元，SP2 或更新版本) Windows Server 2003 R2 (32 位元，SP2 或更新版本) Windows Server 2008 (32 位元與 64 位元；FIPS 模式) Windows Server 2008 R2 (32 位元與 64 位元；FIPS 模式) Windows Server 2012 (所有版本；FIPS 模式) Windows Server 2012 R2 (所有版本；FIPS 模式)	
虛擬環境	
VMware ESX Citrix XenServer	Oracle Virtualbox Microsoft Hyper-V
虛擬桌面基礎結構	
VMware Horizon View	Citrix XenDesktop
實體平台	
SCADA Windows 平板電腦	ATM POS
執行階段使用量	
0.1% CPU 負載 50MB RAM	250MB 磁碟空間

圖 3：Traps 系統需求與平台支援

4401 Great America Parkway
Santa Clara, CA 95054

總部辦公室：+1.408.753.4000
銷售專線：+1.866.320.4788
支援專線：+1.866.898.9087

www.paloaltonetworks.com

© 2016 Palo Alto Networks, Inc. Palo Alto Networks 是 Palo Alto Networks 的註冊商標。您可在以下網址檢視我們的商標名單：http://www.paloaltonetworks.com/company/trademarks.html。本文提及的所有其他標誌皆為其各自公司所擁有之商標。

pan-traps-ds-071416