FIREEYE™

惡意軟體分析

360 度視角，全面分析攻擊

圖 1. FireEye 惡意軟體分析 AX 5550 設備。

重點

- 使用 FireEye MVX 引擎，執行完整攻擊生命週期的深度鑑識分析
- 簡化及批次進行可疑 Web 程式碼、執行檔和檔案的分析
- 深入報告系統層級作業系統與應用程式對檔案系統、記憶體與登錄所做的變更
- 提供擬真模式或沙箱分析，以確認零時差入侵
- 透過與 FireEye 中央管理系統整合，動態產生威脅情報以利即時本機防護
- 擷取封包以進行惡意 URL 工作階段與程式碼執行的分析
- 包含 FireEye AV-Suite 以簡化事件回應優先順序的排列
- 支援 Windows 和 Mac OS X 環境

概觀

FireEye 惡意軟體分析是一組鑑識分析解決方案，可讓資安分析人員對於自動設定的強大測試環境進行手動控制，以便用安全的方式執行並檢查網頁、電子郵件附件與檔案中內嵌的先進惡意軟體、零時差與進階持續威脅 (APT) 攻擊。

網絡罪犯會精心設計攻擊來入侵特定的企業、使用者帳戶或系統，因此分析人員需要有容易使用的鑑識工具，來協助他們快速解決目標性的惡意活動。

評估操作系統，瀏覽器和應用程式攻擊

惡意軟體分析利用 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎，讓內部分析人員能 360 度全方位檢視攻擊，從初次入侵、回呼目的地乃至於後續嘗試的二進位檔下載，都面面俱到。

透過預先設定、配備齊全的 Microsoft Windows 和 Apple Mac OS X 虛擬分析環境，MVX 引擎可以完整執行可疑的程式碼，以對常見 Web 物件、電子郵件附件與檔案進行深入檢查。惡意軟體分析使用 MVX 引擎來檢查單一檔案或一批檔案中是否有惡意軟體，並跨多個通訊協定來追蹤出埠連線嘗試。

有效利用時間進行分析，而不僅是行政管理

有了惡意軟體分析，管理員不再需要進行手動惡意軟體分析過程中耗時的虛擬機器環境安裝、基準化與復原作業。藉由內建的自訂功能和承載檔案觸發的精細化控制，惡意軟體分析可讓鑑識分析人員對符合企業需求的攻擊有全面性的瞭解。

選擇擬真分析或沙箱模式

惡意軟體分析為使用者提供了兩種分析模式 - 擬真模式和沙箱模式。惡意軟體分析人員可使用擬真、上網模式進行完整惡意軟體生命週期分析，並允許外部連線。如此一來，惡意軟體分析就能夠跨多個階段和不同媒介追蹤進階攻擊。在沙箱模式中，特定惡意軟體樣本的執行路徑將完全封鎖於虛擬環境內，一舉一動完全透明顯示於報告內。

在兩種模式中，使用者都能夠產生動態、匿名的攻擊描述檔，以透過 FireEye 中央管理系統分享給其他 FireEye 解決方案。惡意軟體分析產生的惡意軟體攻擊描述檔中包含惡意軟體程式碼的識別碼、入侵 URL 以及其他感染與攻擊來源。此外，透過 FireEye Dynamic Threat Intelligence™ (DTI) 也可分享惡意軟體通訊協定特性，封鎖企圖在跨組織中整個FireEye 部署內進行竊取資料的動作。

可自訂以 YARA 為基礎的規則

惡意軟體分析支援匯入自訂 YARA 規則，讓您得以為組織量身指定位元組層級的規則，並快速分析可疑物件中是否有特定威脅。

全球性的惡意軟體防護網絡

惡意軟體分析可以透過中央管理系統將惡意軟體鑑識資料分享給其他 FireEye 解決方案，以封鎖企圖竊取資料的出埠動作，並阻擋入埠的已知攻擊。也可以透過 FireEye DTI 動態威脅情報雲端分享惡意軟體分析的威脅資料，以抵禦新興的攻擊。

預先設定的 FireEye MVX 引擎免除了調整啟發式作業的需要，因此有了惡意軟體分析，管理員即無需再為安裝與設定而費時費心。這是一項解決方案也可以協助威脅研究人員在不增加網絡與安全管理負擔的情況下分析進階目標性攻擊。

表 1. 技術規格。

	AX 5550
效能*	每天最高 8,200 次分析
OS 支援	Microsoft Windows / Apple Mac OSX
網絡介面連接埠	2 個 10/100/1000BASE-T 連接埠
IPMI 連接埠 (後面板)	內含
LCD 螢幕面板和鍵台	內含
PS/2 鍵盤和滑鼠、DB15 VGA 連接埠 (後面板)	內含
USB 連接埠 (後面板)	4 個 Type A USB 連接埠
序列連接埠 (後面板)	115,200 bps、無同位檢查、8 位元、1 停止位元
磁碟機容量	4 個 1 TB 硬碟、RAID 10、3.5 吋、FRU
機殼	1RU、適合 19 吋機架
機箱尺寸 (寬 x 深 x 高)	17.2 x 27.8 x 1.7 吋 (437 x 706 x 43.2 公釐)
DC 電源供應器	不適用
AC 電源供應器	備援 (1+1) 750 W、100 - 240 VAC， 9 – 4.5 A, 50-60 Hz, IEC60320-C14 inlet, FRU
消耗功率 (上限)	292 W
最大散熱量	996 BTU/h

表 1. 技術規格。

	AX 5550
MTBF	54,200 小時
裝置本身/出貨重量磅 (公斤)	33 磅 (15 公斤) / 48 磅 (22 公斤)
安全認證	IEC 60950、EN 60950、CSA 60950-00、CE 標章
EMC/EMI 認證	FCC (Part 15 Class-A)、CE (Class-A)、CNS、AS/NZS、VCCI (Class A)
法規遵循	RoHS、REACH、WEEE
運作溫度	10°C 到 35°C
作業相對濕度	10% 到 85% (非冷凝)
作業高度	1,500 公尺

附註：效能數字是以使用惡意軟體分析時的預設分析次數為基礎，但將依據系統配置和要處理的流量設定檔而有所不同。

要知道更多關於 FireEye，請前往：**www.FireEye.com**

FireEye Taiwan | 台灣火眼有限公司
| 10683 臺北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE
taiwan@FireEye.com

關於 FireEye, Inc.
FireEye 是一間情報主導的資安公司。FireEye 以流暢、可擴充的客戶資安作業延伸，提供了混合創新資安技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平臺。藉由此方法，FireEye 得以讓對於準備、預防及回應網絡攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。