NETWORK FORENSICS (PX 系列)

概觀

妥善維護的周邊防禦機制是所有資安策略的一大重要環節。越來越多的組織意識到自己也必須運用強大的鑑識技術，來改善周邊防禦機制，以便調查並分析攻擊。遭受攻擊時，企業必須要能快速地調查及判斷事件的範圍和影響，以便有效地遏止威脅、保護網路安全。

FireEye Network Forensics 可以極快速度擷取完整封包，並編製索引，讓您更快速地辨識及解決資安事件。您可以透過 Network Forensics 偵測各種資安事件、改善回應品質，並且精準地量化每個事件的影響。

Network Forensics 大幅增強了全方位的 FireEye 威脅防護功能。除了接收精確的警告及相關的威脅資訊外，分析人員還能仔細檢視攻擊發生之前、發生期間及發生之後的特定封包和工作階段，以確認哪些項目可能已觸發惡意軟體進行下載或回呼程序、迅速有效地做出回應，並應用此資訊改良日後的防護策略。

加快擊殺鏈的重新建構速度並影響量化

由於可讓使用者在資安事件發生之前、發生期間及發生之後快速找到並解碼流量和工作階段，Network Forensics 可提供更深入的事件活動相關資訊，讓您更充分地掌控快速事件回應調查的重要情勢。

以超快速度存取網路資料記錄，是縮短解決時間及回答關鍵問題的必備要件，這些問題包括：入侵事件已發生多久、哪些資料可能已流出網路、還有多少主機已遭入侵？

以超快速度擷取、編製索引及搜尋封包

Network Forensics 可以奈秒為單位完成時間戳記，並以高達 20 Gbps 的記錄速度確保封包擷取絕不間斷、毫無遺漏。使用以奈秒為單位的時間戳記與連線屬性，為所有擷取的封包即時編製索引，提供可立即用於鑑識的資料。

儲存及匯出業界標準資料

提供各種內建儲存設定，以及連接 SAS 或連接 SAN 的儲存選項，讓組織享有彈性和成長空間。所有封包都會儲存為標準 PCAP 格式，以便靈活應用於各種分析平台。

重點

- 以奈秒為單位完成時間戳記，並以高達 20 Gbps 的記錄速度實現絕不間斷、毫無遺漏的封包擷取
- 使用時間戳記與連線屬性，為所有擷取的封包編製索引。以 JSON 格式匯出流量索引與連線中繼資料。流量索引可轉換為 NetFlow v9、IPFIX 及 Silk 工具等資料格式。
- 使用正在申請專利的索引編製架構，以超快速度搜尋並擷取目標連線與封包
- Web 型深入查詢 GUI 可用於搜尋及檢查封包、連線和工作階段
- 工作階段解碼器支援，可用於檢視及搜尋 Web、電子郵件、FTP、DNS、聊天、SSL 連線詳細資料和檔案附件
- 使用規則運算式進行封包承載搜尋
- 使用業界標準儲存資料，能以 PCAP 格式匯入及匯出資料以供分析之用
- 快速調查程序的擷取方法是以事件為基礎，藉此找出應集中深入調查的可疑工作階段
- 自動化程序運用專有演算法診斷潛在的異常網路行為，從而辨識出資料竊取活動

FireEye

即時威脅情報特徵碼分析

Network Forensics 與 FireEye iSIGHT 情報網路整合，並自動展開下載新威脅特徵碼的程序，提供即時的威脅特徵碼分析。若偵測到威脅，Network Forensics 便會觸發警示，讓分析人員快速調查威脅。

與 FireEye 威脅防護解決方案整合的工作流程

與 FireEye 解決方案完整整合，可讓您存取我們針對最大型且最繁忙的網路所擷取、編製索引並加以儲存的連線與封包資訊，輕鬆深入地瞭解網路流量與活動。由於可讓使用者在資安事件發生之前、發生期間及發生之後快速找到並解碼流量和工作階段，Network Forensics 可提供更深入的事件活動相關資訊，讓您更充分地掌控快速事件回應調查的重要情勢。

突顯可疑的工作階段

使用者可以建立自訂規則來標記可疑的工作階段資料，以加快調查程序，並與逐漸發生的事件建立關聯性。這麼做可建立深入調查的起點，亦能確保長期保存。鎖定某一特定事件的調查可以單一案例來管理。

技術規格

	擷取連接埠配置	管理連接埠	最大記錄速度	總內建儲存容量	尺寸	電源供應器/一般作業負載
PX 004S	4 x 1 Gbps SFP	2 x 10/100/1000 BASE-T	500 Mbps	6 TB	1.7 x 16.8 x 14 吋 (4.3 x 42.67 x 35.56 公分) 11 磅 (5 公斤)	200 W 降噪 AC 電源 100-240 V、 60-50 Hz 自動量測範圍
PX 1004ESS-16	4 x 1 Gbps、10/100/1000 BaseT、SFP	2 x 10/100/1000 BASE-T	1.5 Gbps	16 TB、可擴充的 SAS 連接儲存裝置	1U 機架吊掛 1.7 x 17.2 x 25.6 吋 (4.3 x 43.7 x 65.0 公分) 46 磅 (20.9 公斤)	650 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍 230-280 W (額定)
PX 1020ESS-16	2 x 10 Gbps、SFP+	2 x 10/100/1000/10G BASE-T	1.5 Gbps	16 TB、可擴充的 SAS 連接儲存裝置		
PX 2004ESS-48	4 x 1 Gbps、10/100/ 1000BaseT、SFP	2 x 10/100/1000/10G BASE-T	4 Gbps	48 TB、可擴充的 SAS 連接儲存裝置	2U 機架吊掛 3.5 x 17.2 x 25.5 吋 (8.9 x 43.7 x 86.6 公分) 52 磅 (23.6 公斤)	1,280 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍
PX 2020ESS-48	2 x 10 Gbps、SFP+	2 x 10/100/1000/10G BASE-T	5 Gbps，可升級至 20 Gbps	48 TB、可擴充的 SAS 連接儲存裝置		
PX 2040ESS-48	4 x 1/10Gbps SFP/SFP+	2 x 10/100/1000/10G BASE-T	5 Gbps，可升級至 20 Gbps	48 TB、可擴充的 SAS 連接儲存裝置		
PX 1004EXT-4G	4 x 1 Gbps、10/100/1000BaseT、SFP	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	4 Gbps	未搭載內建儲存裝置。透過光纖 HBA 連線至外部 SAN 儲存裝置	1U 機架吊掛 1.7 x 17.2 x 25.6 吋 (4.3 x 43.7 x 65.0 公分) 46 磅 (20.9 公斤)	650 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍 230-280 W (額定)
PX 1040EXT-20G	4 x 1 Gbps	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	20 Gbps			
PX 2000SX-24	無	無	無	針對 ESS 型號提供 24 TB 擴充儲存架	2U 機架吊掛 3.5 x 17.2 x 25.5 吋 (8.9 x 43.7 x 64.8 公分) 52 磅 (23.6 公斤)	500 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍
PX 2000SX-48	無	無	無	針對 ESS 型號提供 48 TB 擴充儲存架		
PX 4000SX-264	無	無	無	針對 ESS 型號提供 264 TB 擴充儲存架	4U 機架吊掛 7 x 17.2 x 27.5 吋 (17.8 x 43.7 x 64.8 公分) 75 磅 (34 公斤)	1,280 W 高效率 (1+1) 備援 AC 電源 100-240 VAC、 60-50 Hz 自動量測範圍

附註：所有效能值將依據系統配置和要處理的流量設定檔而有所不同。

如需 FireEye 的詳細資訊，請造訪：

www.FireEye.com

關於 FIREEYE, INC.

FireEye 是一間情報主導的資安即服務領導公司。FireEye 以流暢、可擴充的客戶安全作業延伸，提供了混合創新安全技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平台。藉由此方法，FireEye 得以讓對於準備、預防及回應網路攻擊感到苦惱的組織消除網路安全機制的複雜性和重擔。FireEye 在全球超過 67 個國家/地區擁有超過 5,000 位客戶，其中包括富比士全球 2000 大公司中的 940 家以上公司。

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

www.FireEye.com

© 2017 FireEye, Inc. 保留一切權利。FireEye 為 FireEye, Inc. 註冊商標。
所有其他品牌、產品或服務名稱分屬各該擁有人之商標或服務標記。DS.PXS.ZH-TW.032017