

內網安全威脅獵殺系統



eDetector 主要功能

▶ 惡意程式分析鑑識

eDetector 具備偵測未知型惡意程式功能，讓您面對 APT 的攻擊不再束手無策，更能協助您建構內網安全預警系統，及早發現內網潛伏之殭屍電腦，以便能在最短時間採取必要措施因應，避免資安事件災情擴大。

▶ 資安事件蒐證分析

eDetector 除具有惡意程式分析鑑識功能，亦提供快速蒐證功能，一但發生惡意程式滲透植入資安事件初期時，得以透過蒐證功能深入分析，有助找出這些資安事件發生之源頭，作為未來強化資安架構與政策擬定之參考資訊。

eDetector 惡意程式分析功能

採記憶體動態行為分析，偵測惡意程式植入系統時在記憶體中行為痕跡，包含惡意程式碼注入、程序隱藏/檔案隱藏、核心攔截、連網行為、非正常啟動之服務、偵測互斥...，透過這些行為分析，無論該惡意程式如何隱密躲藏，仍無法避開 eDetector 的偵蒐。

區碼	程序編號	程序名稱	程序型態	程序日期	程序MD5	數位簽署簽署人	程序路徑
90	1040	hhcmaff.e...	動態	2017/07/1...	206ec77b694fb6f3485c9...	null	C:\Users\User\AppData\Local...
40	1560	ClientSearc...	動態	2017/07/1...	8794e63aebfb641b78e3...	IFORENSICS DIGITAL, INC.	C:\Program Files\eDetector\Cli...
40	6976	ClientSearc...	動態	2017/07/1...	8794e63aebfb641b78e3...	IFORENSICS DIGITAL, INC.	C:\Program Files\eDetector\Cli...
30	3048	wmpnetwk...	動態	2017/07/1...	3b40d3a61aa8c21b88ae...	null	C:\Program Files\Windows Me...
0	1256	spoolsv.exe	動態	2017/07/1...	9aea093b8f9c37cf45538...	null	C:\Windows\System32\spoolsv...
0	1376	vmicscv.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicscv...
0	1400	vmicscv.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicscv...
0	1420	vmicscv.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicscv...
0	1448	vmicscv.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicscv...
0	1472	vmicscv.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicscv...
0	1524	iForensicsS...	動態	2017/07/1...	121b064f3ab76a12e41e...	IFORENSICS DIGITAL, INC.	C:\Program Files\eDetector\iFo...
0	1576	vmtoolsd.s...	動態	2017/07/1...	e446c4fd77f926c636115...	VMware, Inc.	C:\Program Files\VMware\VM...
0	1608	wfms.exe	動態	2017/07/1...	5a0859cc41ed459809aaf...	null	C:\Windows\System32\wfmsv...
白名單-0	1668	dllhost.exe	動態	2017/07/1...	a63dc5c2ea944e665720...	null	C:\Windows\System32\dllhost...
0	1816	sppsvc.exe	動態	2017/07/1...	cf87a1de791347e75b98...	null	C:\Windows\System32\sppsvc...
0	2340	dwm.exe	動態	2017/07/1...	505bf4d1cadeb8d4f8bcd...	null	C:\Windows\System32\dwm.ex...

eDetector 除針對記憶體採動態行為分析模式，同時也可選購整合 Metadefender 多合一防毒大數據知識庫，對已部署之電腦/伺服器進行全硬碟檔案完整掃描，協助資安管理員能及早發現儲存於硬碟未被觸發之惡意程式，以避免電腦遭駭淪陷。

eDetector 蒐證分析功能

eDetector 可搜集電腦執行狀態下 20 多種系統狀態資訊，包含上網瀏覽網頁行為、最近開啟之文件、USB裝置使用紀錄、程式執行痕跡、開機自動執行之程式、檔案系統索引表 (\$MFT)，透過這些資訊的蒐證與分析，可以協助資安管理員針對惡意程式植入初期，資安事件發生之原因，此資安管理員藉由分析所獲資訊找到之源頭，便能作為未來強化資安或加強教育訓練之依據。

目前執行程式	Process ID	Priority	Product Name	Version
選擇				
系統安全審核	344	Normal	Microsoft?Windo...	6.1.7600.1638
系統目前之磁碟機資訊	340	Normal	Microsoft?Windo...	6.1.7600.1638
目前正在連線的網路資訊	372	High	Microsoft?Windo...	6.1.7600.1638
目前執行之程式	340	Normal	Microsoft?Windo...	6.1.7600.1638
所有被程式開啟的檔案列表資訊	388	Normal	Microsoft?Windo...	6.1.7600.1638
Internet Explorer 的瀏覽紀錄	386	High	Microsoft?Windo...	6.1.7601.1751
Mozilla Firefox 的瀏覽紀錄	484	Normal	Microsoft?Windo...	6.1.7600.1638
Chrome 的瀏覽紀錄	492	Normal	Microsoft?Windo...	6.1.7601.1844
顯示目前電腦字型的安裝紀錄	300	Normal	Microsoft?Windo...	6.1.7600.1638
檢視電腦中最近開啟的文件	396	Normal	Microsoft?Windo...	6.1.7600.1638
顯示電腦的 USB 設備列表	376	Normal	Microsoft?Windo...	6.1.7600.1638
顯示使用者的用戶資料列表	376	Normal	Microsoft?Windo...	6.1.7600.1638
顯示目前 Windows 的系統資訊	376	Normal	Microsoft?Windo...	6.1.7600.1638
顯示目前 Windows 的安裝資訊	308	Normal	Microsoft?Windo...	6.1.7600.1638
顯示目前 Windows 的安裝 Driver 資訊	340	Normal	Microsoft?Windo...	6.1.7600.1638
顯示目前 Windows 系統中所安裝的軟體或 Patch 資訊	368	Normal	Microsoft?Windo...	6.1.7600.1638
顯示磁碟機傳輸、IP、等相關資訊	100	Normal	Microsoft?Windo...	6.1.7600.1638
系統開機後自動執行之程式列表	256	Normal	Microsoft?Windo...	6.1.7600.1638
Prefetch 列表	1284	Normal	Microsoft?Windo...	6.1.7600.1638
本機使用紀錄	1376	Normal	Microsoft?Windo...	6.1.7601.1751
曾經關聯的資料夾路徑				
User Asses				
100 168 138 103 05 11 WIN7 umicrot.exe				

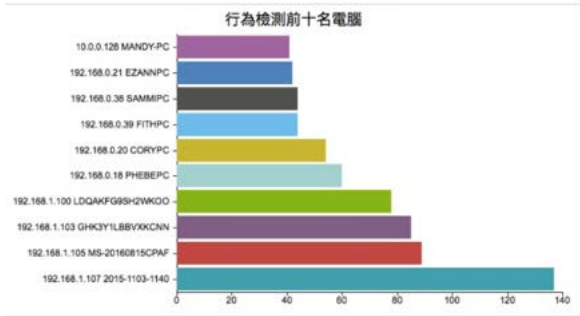
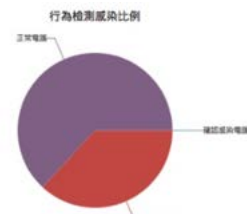
報表功能

當經過分析、確認惡意程式與過濾後，可產出企業/機關之分析報告，報告內容分成三部分

- ▶ 摘要報告：顯示惡意程式感染電腦/疑似感染電腦/正常電腦分佈之圓餅圖，及顯示用戶端電腦惡意程式累計數量排名之橫條圖
- ▶ 惡意程式動靜態分析指標：顯示判定遭植入惡意程式之各類危險指標
- ▶ 惡意程式檔案路徑：顯示該惡意程式檔案實體路徑

eDetector 產品特色

- ▶ 支援中央控管，將程式派送至用戶端之 Windows 作業系統執行後，即可進行用戶端之硬碟檔案搜尋、蒐證及記憶體程序偵測分析
- ▶ 採行為分析，可偵測分析所有執行中程序及其所載入之模組，並定時 email 通知異常情況
- ▶ 針對發現問題之執行程序，可以繪製關聯圖協助人員尋找惡意程式根源
- ▶ 針對執行中之惡意程式可暫停或終止其程序並繪製相關連線 IP 位置地圖
- ▶ 可分析已被刪除之檔案(例如惡意程式下載器)
- ▶ 可檢視開機啟動服務、自我啟動程序及排程任務，供使用者檢視不正常的啟動程序
- ▶ 內建白名單，自動排除微軟發行之應用程式，並可自訂/匯入黑白名單
- ▶ 可搜集用戶端的檔案總管資訊，並對其進行搜尋、篩選及取回檔案
- ▶ 具鑑識級別的蒐證特性，自動將蒐證資訊進行 MD5/SHA 計算以保留原始證據能力



研發原廠

鑒真數位有限公司
iForensics Digital Inc.

台北市中山區松江路 309 號 11 樓之 3
<http://www.iforensics.com.tw>