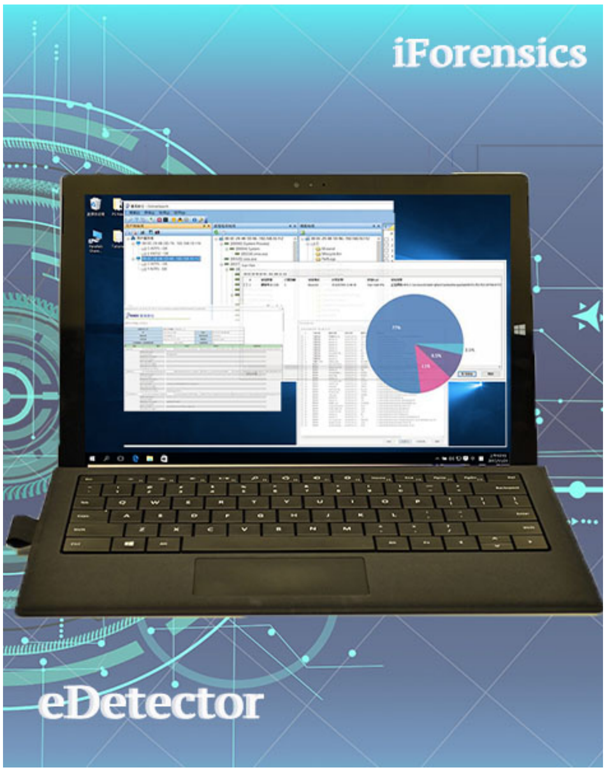
Intranet Security Threats Hunting System



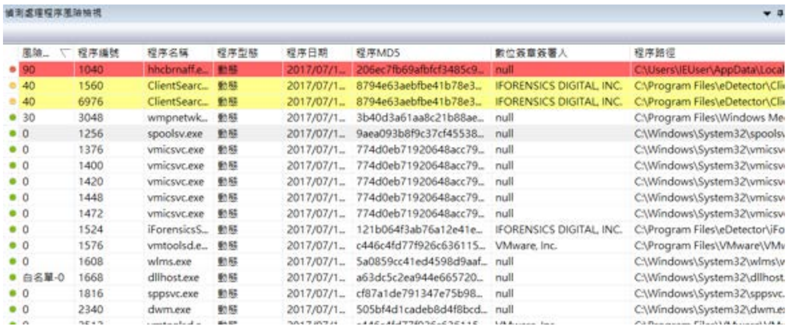
Main Functions

▸ Malware Analysis and Forensics

eDetector has the ability to detect unknown malware. With this function, you would never be helpless against APT attacks. Besides, eDetector can assist you to build an Intranet Security Alarm System, which makes it possible to find the hiding zombie computers earlier. We could hence take the necessary actions against attacks in the shortest time, avoiding the enlarged tragedy of the information security issues.

▸ Digital Traces Collection and Analysis for Information Security Event

eDetector also possesses rapid digital traces collection function. With this function, we could conduct deep analysis in the early stage of a malware penetration event, leading us to the origin of the event. While strengthening the structure of the information security system and formulating policies in the future, these analysis could also be the reference information.



偵測處理程序風險檢視

風險...	程序編號	程序名稱	程序型態	程序日期	程序MD5	數位簽章簽署人	程序路徑
90	1040	hhcbrnaff.e...	動態	2017/07/1...	206ec7fb69afbfcf3485c9...	null	C:\Users\IEUser\AppData\Local
40	1560	ClientSearc...	動態	2017/07/1...	8794e63aebfbe41b78e3...	IFORENSICS DIGITAL, INC.	C:\Program Files\eDetector\Cli
40	6976	ClientSearc...	動態	2017/07/1...	8794e63aebfbe41b78e3...	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	vmicsvc.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicsv
0	1400	vmicsvc.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicsv
0	1420	vmicsvc.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicsv
0	1448	vmicsvc.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicsv
0	1472	vmicsvc.exe	動態	2017/07/1...	774d0eb71920648acc79...	null	C:\Windows\System32\vmicsv
0	1524	iForensicsS...	動態	2017/07/1...	121b064f3ab76a12e41e...	IFORENSICS DIGITAL, INC.	C:\Program Files\eDetector\iFo
0	1576	vmtoolsd.e...	動態	2017/07/1...	c446c4fd77f926c636115...	VMware, Inc.	C:\Program Files\VMware\VMv
0	1608	wlms.exe	動態	2017/07/1...	5a0859cc41ed4598d9aaf...	null	C:\Windows\System32\wlms\w
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.e

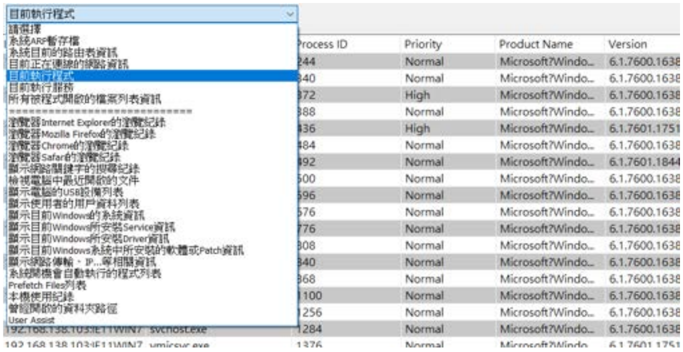
Malware analysis function

eDetector analyzes the dynamic behaviors in the computer memory, and it can detect the behavior traces in the computer memory left by the malware while implanting into the system. The behavior traces include malicious code injection, program hidden/ file hidden, core intercept, Internet connection, abnormal start-up services, detect mutually exclusive…,etc. With the behavior analysis function, no matter how covertly the malware trying to hide, they can't avoid the detection from eDetector.

With optional MetaDefender's Big Data library purchased, eDetector can also be integrated with its library. In this way, the files in the disk of the computer/ server with Agent resided on can be thoroughly scanned, which makes it possible for the information security manager to find the malware undetected in the disk and protect the computers from being hacked.

Digital Traces Collection and Analysis

eDetector can collect more than 20 types of system condition data, including Internet browsing, recent open file, USB usage log, program execution trace, Auto-run program, Master File Table（$MFT）. With the collection and analysis of the information, the information security manager would be able to find the origin of the malware implantation event in the early stage. In consequence, the information security manager can provide the reference information for future information security strengthening and education training.



		Process ID	Priority	Product Name	Version
		244	Normal	Microsoft?Windo...	6.1.7600.1638
		340	Normal	Microsoft?Windo...	6.1.7600.1638
		372	High	Microsoft?Windo...	6.1.7600.1638
		388	Normal	Microsoft?Windo...	6.1.7600.1638
		436	High	Microsoft?Windo...	6.1.7601.1751
		484	Normal	Microsoft?Windo...	6.1.7600.1638
		492	Normal	Microsoft?Windo...	6.1.7601.1844
		500	Normal	Microsoft?Windo...	6.1.7600.1638
		596	Normal	Microsoft?Windo...	6.1.7600.1638
		576	Normal	Microsoft?Windo...	6.1.7600.1638
		776	Normal	Microsoft?Windo...	6.1.7600.1638
		808	Normal	Microsoft?Windo...	6.1.7600.1638
		840	Normal	Microsoft?Windo...	6.1.7600.1638
		868	Normal	Microsoft?Windo...	6.1.7600.1638
		1100	Normal	Microsoft?Windo...	6.1.7600.1638
		1256	Normal	Microsoft?Windo...	6.1.7600.1638
192.168.138.103:IE11WIN7	svchost.exe	1284	Normal	Microsoft?Windo...	6.1.7600.1638
192.168.138.103:IE11WIN7	vmicsvc.exe	1376	Normal	Microsoft?Windo...	6.1.7601.1751

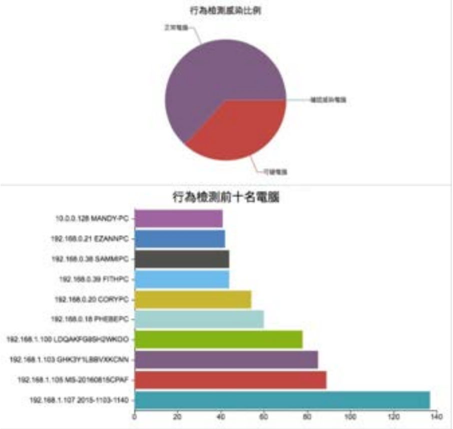
Report

eDetector can export reports for both enterprises and organizations. The report consists of three parts:

- Summary：pie charts displays the distribution of computers infected by malware/ computer seems to be infected/ normal computer; and bar charts shows the ranks of the user computers which is infected by most malware
- Dynamic and Static indicators of malware analysis: display various types of risk indicators used to determine whether there's implantation of malware
- Path of malware: indicate the full path of the malware

Features

- Central control system provided. User can collect digital traces, analyze the processes in the memory and even search the files in client's disk.
- Adopts behavior analysis. Detect and analyze all the processing programs and the modules loaded , and regularly inform the user about abnormal situations via e-mail
- For the suspicious processing programs, draw an interrelationship digraph to assist the users to search for the origin of the malware
- Stop the executing malware to discontinue the activities of the hiding hacker and draw an IP address map
- Have ability to analyze the deleted files (ex: The downloader of malware)
- View all the services, auto-run programs and scheduled tasks to search for abnormal startup programs
- Built-in white list which automatically excludes the Microsoft applications. User can customize/ import the black/white list
- Collect the user computer's windows explorer data to search, apply the filter and get the files back.
- Forensics level Digital Traces collection: automatically calculate the MD5/SHA of the traces collected to ensure the remain of the original



R&D

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 5
http://www.iforensics.com.tw