Filseclab®

費爾智慧防毒 8 創新技術介紹

作者：Filseclab Corporation
網站：http://www.filseclab.com
電郵：info@filseclab.com
時間：2012 年 10 月 8 日

主要技術介紹

行為深度追蹤技術
即時追蹤的快速響應技術
快速存儲與檢索技術（黑盒）
基於人工智慧模型的行為分析技術（威脅鑒定）
I/O 操作的回滾技術
記憶體對象的回滾技術
Windows 內核模擬技術

緩衝區溢出防禦技術
藍屏災難保護技術
增強的自我保護技術
陷阱技術

基因辨識技術
基因特徵庫的自動生成技術
變形病毒辨識技術
縮略微特徵技術
自動誤判排除技術
資源載荷均衡技術
智慧提速技術
斷點續掃技術

虛擬機技術
API 模擬技術
靜態啟發模式病毒檢測技術
基於虛擬機的動態啟發模式病毒檢測技術
虛擬機脫殼技術
巨集病毒啟發技術

靜態變形病毒清除技術
靜態廣譜式清病技術
基於虛擬機的動態清毒技術

雲端快速查詢技術（可比普通資料庫查詢快上百倍）
雲端綜合鑒定技術
雲端智慧分析技術

智慧語音交互控制技術

威脅自動分揀技術
白程式自動分揀技術
病毒碼自動更新技術

程式邏輯追蹤技術 PLT
增強 SVM 人工智算法 EX-SVM

V8 技術亮點之「動態防禦 2.0」

費爾第二代動態防禦開發歷時 4 年，代碼量超過 40 萬行，是費爾最複雜的系統之一，它基本實現一個小型的子系統來模擬和追蹤 Windows 的運作過程。

主要技術亮點

首先用一個比喻來描述新版動態防禦的特色：一個小偷偽裝成客人到家裡偷東西，等巡查員認定它不是客人而是賊時隨即將其拿下，可是家裡卻已經被翻亂了，要還原原樣就比較困難。第二代動態防禦系統不僅可以抓住賊，同時能讓家裡還原如初，並且有能力更早更準確的辨識偽裝更好的賊，包括目前流行的白加黑木馬。主要特點如下：

1. 精確的對象級深度追蹤。
2. 對威脅所產生的破壞進行全面熱回滾。這主要包括威脅對檔案、登錄、HOOK、記憶體的改寫、對象的修改進行全面還原等等。

智慧黑盒

費爾智慧黑盒類似於飛機的黑匣子，它會對電腦中的每個程式單位行為進行精準而細緻的記錄，它不僅可以追蹤程式的檔案、登錄存取，還包括執行緒、記憶體，對象的操作等等。而且它的最小追蹤單位可以精確到 CPU 的執行片斷，以及事件的每一個參與者。比如：一個系統服務執行緒在這個時間段為正常程式 A 服務，而下一個時間段被病毒 B 嫁接並為其服務，此時發生的破壞行為仍然會被準確定位到 B 而不波及整個服務執行緒。再如：當發生一個刪除檔案的事件，此時被追蹤的不僅僅是刪除此檔案的行程，還包括參與此次行動的所有模組以及記憶體，甚至包括父行程、父執行緒都會被一並追蹤。正是這一全新的追蹤架構可以準確定位目前讓主防頭痛的白加黑木馬。

另外，虛擬黑盒具備持久記憶功能，不會隨電腦的重新啟動而歸零，即使重新啟動電腦目的程式曾經發生的行為仍然會被持續的記錄在案，這樣當遇到一種把自己的行為故意打散、分時段來組合完成的潛伏威脅時仍可以準確偵測，從而有能力處理多步式或延時發作的後

門、木馬，並對其進行徹底的清除和回滾。

行為分析系統

採用複雜的邏輯規則及綜合分析系統，對智慧黑盒記錄的行為進行分析並自動判定是否有害，即「記憶式多步智慧主防」。

精準回滾

對有害程式產生的行為實施精準全面的回滾還原。它會對有害程式直接產生的行為以及嫁接到別的程式上間接產生的行為進行還原，而同時不會波及到正常程式。比如：病毒對 Explorer 進行了 HOOK，回滾可以將 HOOK 還原並在不結束 Explorer 的情況下讓其保持乾淨的繼續正常工作。

另外，被病毒修改或刪除的檔案也能夠被完美還原，這包括被感染型病毒感染的檔案。智慧黑盒在追蹤程式行為時會對檔案、登錄、記憶體、對像所有發生的修改性動作進行即時備份，並且採用大量先進算法確保對系統影響不可感知，這樣即使遇到感染性病毒時仍然可以對曾經的破壞進行回滾復原。

黑盒&沙盒（沙盤）

傳統安全軟體中的「沙盒」（Sandbox）的工作機制是：對於任何未知程式進行「有罪推定」，也就是說當一個未知程式在執行時沙盒會先假定它是有害的，然後放入隔離環境中檢驗。這樣做的好處是如果程式真的有害那麼一般不會對系統造成實質影響，但實際情況中用戶遇到的大多數程式都屬於正常安全的，由於沙盒中的正常程式要生效修改時會比較困難（比如在沙盒中安裝遊戲是無法把它真正安裝到電腦中去的），甚至需要全部丟棄讓用戶重新再做一次。所以沙盒比較適合安全廠商進行內部病毒分析或樣本採集時使用，但對於普通用戶來說存在障礙，它目前仍然屬於比較專業的套用。費爾 V8 中的「黑盒」則是一個來源於沙盒思想但與此相反的工作機制，即「無罪推定」。它先假定程式是乾淨無害的，然後完整追蹤每個程式的行為記錄和修改動作，只有當程式表現出惡意行為時才阻止並還原退回當初狀態。這種機制可以和主動防禦系統完美的契合聯動，而且對於用戶來說並不存在任何使用上的門檻，因為整個過程是 V8 內部來自動完成的，不存在要求用戶自動/手動入沙過程，也不存在套用修改的問題，和正常使用沒有區別，所以費爾的黑盒技術更易用也更安全。

V8 技術亮點之「MVM 威脅虛擬機」

威脅虛擬機（MVM）是費爾智慧防毒 8 中又一極為複雜的安全系統。構建此系統的主要目的是為了通過掃描的方式來檢測未知威脅，彌補特徵碼的滯後性，增強對新木馬和加殼變形病毒的防禦能力。經過多年的研發和不斷改進，目前費爾 MVM 虛擬機啟發技術無論從技術層面還是實際效果都已經達到同類系統的一流水平。

為了驗證其效果，曾邀請英國 VB100 評測機構 Virus Bulletin 對虛擬機純啟發引擎進行內部測試，在沒有黑白名單的支援下，其對 WildList 辨識率超過 60%，誤判也控制在極低水平，使得 VB 給其高度評價「Well, it's still doing great considering it's only heuristics and no signatures. It seems to be detecting over 60% of our samples - better than some signature scanners!（它甚至優於某些特徵碼引擎）」。

威脅虛擬機由兩個子系統組成：虛擬機系統和啟發分析系統。虛擬機系統用來模擬程式執行並收集程式行為，啟發分析系統則根據這些行為來判斷目的對象是否有害。

虛擬機系統

MVM 中的虛擬機是一個極度複雜的虛擬仿真系統，它能解析並模擬幾乎全部的 CPU 指令、數千個 API 函式，並對木馬、病毒經常涉及的一些硬體進行仿真，比如：硬碟、網路介面卡等等。它的工作原理是讓目的程式在一個虛擬的隔離環境中執行，並將自己的真實意圖充分暴露，一旦發現有惡意目的即可被偵測，而同時也決不會影響真實系統。目前 MVM 可以脫近 400 種殼，能有效的應對加殼、變形等特徵碼不易對付的病毒。

啟發分析系統

MVM 中的啟發分析系統分為兩部分：靜態啟發，動態啟發。

靜態啟發不需要依賴於虛擬機可以獨立工作。它通過反解目的程式的二進位代碼直接分析其意圖，發現有威脅特點即可被判別，從而達到辨識未知威脅的目的。這種方式的優點是速度快，但無法有效辨識加殼和變形病毒，而動態啟發部分則可以有效彌補這一點。

威脅程式無論是加殼還是變形，最終總要去實現自己的目的，也就是說在執行時它們會自己脫殼。動態啟發就可以讓其在虛擬機中仿真執行，脫掉自己的外衣，誘使它發作，待目的充分暴露出自己的惡意行為時即被判定威脅，實現動態防禦的靜態辨識。

V8 技術亮點之「載荷均衡、智慧解毒與提速、隱私保護與陷阱、緩衝區溢出保護與藍屏災難保護」

智慧載荷均衡

V8 可以根據目前的系統資源佔用狀況自動調節自身能耗，在低配電腦中也能順利執行，既能保障安全又能提高效率。不僅如此，V8 甚至還允許你任意設定病毒碼的使用量和記憶體佔用配額，讓你自由控制它的資源佔用，在「輕量版」與「完整版」之間隨意切換。

智慧解毒

V8 結合虛擬機技術可對某些特定類型的感染病毒進行萬能修復，遇到熊貓燒香、威金病毒後不再只是 「刪除/隔離」，可還原檔案到乾淨狀態。

智慧提速

通過增量快取記憶體技術對二次掃描進行大規模提速，可將掃描速度提高幾十倍甚至上百倍。

檔案隱私保護

電腦中個人文檔、照片等隱私數據是絕不希望被他人窺視的，但在木馬後門、間諜軟體流行的當今，個人隱私被竊取的情況時常發生卻鮮為人知。用戶很難確保自己電腦中沒有隱藏的間諜軟體或別有用心的第三方軟體會在何時拿走自己的檔案。V8 中提供了檔案隱私保護功能，只要把你重要的檔案加入保護，所有試圖存取這些文檔的程式都需要得到你的許可，保障個人隱私不被侵犯。

威脅誘捕陷阱

遇到頑固木馬反覆清除不掉，單純的抑制再生和檔案粉碎往往並不能解決根源。 V8 中新增的陷阱功能可以用來應對這種「疑難雜症」。設定一個虛擬陷阱將有再生能力的頑固威脅的創建者捕獲，實現徹底的清除。

緩衝區溢出保護

安裝 V8 後你的電腦將可以自動免疫各類緩衝區溢出攻擊。即使在沒有安裝 Windows 系統補丁的情況下遇到此類最新威脅也能夠立即偵測並阻止，保護電腦免受 0day 漏洞破壞。

藍屏災難保護

由於病毒攻擊、軟體相衝、系統故障造成的突發電腦藍屏，可能導致你的工作中斷或檔案遺失。V8 中提供的藍屏災難保護將可以阻止某些藍屏的發生，並終止引發藍屏問題的根源遏制故障繼續蔓延，使得電腦可以在一段時間內繼續安全執行，為關鍵時刻及時儲存重要數據提供機會，減少損失。

智慧交互控制

你可以通過語音對 V8 進行控制，並且它也會有自然語言的回應。開啟語音功能後，對著電腦說「費爾」，軟體就會彈出主介面並回答「Hi，我在這裡」，若說：「掃描我的電腦」，軟體自動開始掃描。每個掃描工作都有自己的編號，用戶可以隨時單一（集體）語音控制那些正在進行中的工作，並讓其匯報各自的工作狀態。除此之外，V8 語音還提供了一些友善的日常問候和套用呼叫，比如：新聞、購物，搜索等等。而且語音功能是純綠色的，你不用擔心它會在電腦中安裝任何額外插件。

V8 技術亮點之「雲端人工智慧集群 iRobots」

iRobots - 雲端人工智慧集群 簡介

費爾智慧等級定義
* 初級的自動化處理系統，主要解決重複勞動。
** 帶有初級分析能力和錯誤排除功能的自動化處理系統。
*** 有中度複雜的分析能力和錯誤排除能力的自動化處理系統，能長期無人值守的自動化運作，可作為人力資源的有效替代。
**** 有高度複雜的分析能力和除錯能力，並進行大量複雜運算，可在短時間內提供人力無法完成的分析結果。
***** 高度人工智慧，可在完全脫離人為干預的情況下自我學習，自我完善。

iRobot1 - 病毒樣本自動收集系統

智慧等級：*
服役時間：2003 年
功能簡介：自動從網際網路、樣本提供商、交換商搜集和下載樣本，為病毒碼定義提供資源支援。

iRobot2 - 正常程式自動收集系統

智慧等級：*
服役時間：2005 年
功能簡介：自動從網際網路搜集和下載正常軟體，為排除誤判提供資源支援。

iRobot3 - 樣本分揀系統

智慧等級：**
服役時間：2007 年
功能簡介：自動分析 iRobot1 和 iRobot2 收集到的樣本，對程式的黑白屬性進行快速分揀。

iRobot4 - 自動更新系統

智慧等級：***
服役時間：2007 年
功能簡介：對 iRobot3 和 iRobot5 的結果進行綜合分析，自動生成病毒碼定義和白名單定義並自動發佈更新。
案例：從 2007 年至今 iRobot4 已經成功執行 5 年，為費爾 V7 提供不間斷更新。

iRobot5 - 自動誤判排除系統

智慧等級：**
服役時間：2007 年
功能簡介：自動糾正已知誤判和潛在誤判。

iRobot6 - 智慧基因分析系統

智慧等級：****
服役時間：2009 年
功能簡介：利用人工智慧數學模型構建自動分類算法，從足夠多的樣本中找出區別黑白兩個集合的特徵，從而實現一個特徵辨識整個集合的黑白屬性，並結合 iRobot5 自動排除誤判達到實用層級。

iRobot7 - 行為分析系統

智慧等級：***
服役時間：2010 年
功能簡介：虛擬環境中執行威脅程式並追蹤其行為，綜合分析後判定是否有害。作為 iRobot3 和 iRobot5 的有力補充，增強自動化的自主鑒定能力，有能力辨識出新的未知威脅。同時也為鑒定結果提供切實可靠的證據支援。
案例：目前費爾在給世界最大反病毒組織 WildList 提交的流行樣本均來自於此系統 。WildList 會對提交的樣本做校驗核實，經過 iRobot7 判別的威脅基本 100% 會被 WildList 認可，最終 WildList 再把世界上所有主流殺毒廠商提供的樣本進行綜合篩選、找出重疊部分發佈，作為 ICSA、VB100 等國際認證的測試標準。其中每期 WildList 中來自於費爾的樣本一般都會超過 35%，屬於採用率最高的廠商之一，以此可以反應出 iRobot7 的高度準確性。

iRobot8 - EVANET 中樞神經系統

智慧等級：****
服役時間：2012 年
功能簡介：綜合分析從 EVANET 客戶端傳送來的關於程式的行為、內容等各種特徵資訊，自動判定其是否有危害，客戶端根據 EVANET 的分析結果自動決定處理動作。比如：警告、還原或開放等。

EVANET 計劃 －安全神經網路系統

EVA 取自電影《阿凡達》裡的聖母，電影中聖母 EVA 將潘多拉(Pandora)星球的所有生命連線為一個有機的整體共同抵禦外敵從而實現堅不可摧。

費爾以 EVANET 為名，希望將所有的用戶電腦有效連線起來共同抵禦威脅，從而有效放大抵禦能力。EVANET 計劃分為以下三個階段。

第一階段

通過上傳用戶端有潛在威脅的程式或程式特徵到雲端，利用雲端的更豐富的鑒定方式進行再次鑒定。費爾 V7 在 2007 年初已經完成這一階段。

第二階段

綜合電腦使用者的智慧來判斷未知威脅。比如：根據用戶對程式的不同操作方式進行分析，當很多用戶表現出對此程式反感時，它將被標記為潛在的威脅。費爾 V8 實現了這一階段。

第三階段

智慧聯合防禦階段，當一台電腦受到威脅之後，全體電腦都有感知，並可由 EVANET 中樞發出指令，由就近的電腦對其實施救援，令受威脅的電腦起死回生。也可以脫離中樞的指揮，自動就近尋找救援。此階段正在研發中。

EVANET 首頁：http://www.ievanet.com 正在建設中。