Filseclab®

费尔智能杀毒 8 创新技术介绍

作者：Filseclab Corporation
网站：http://www.filseclab.com
电邮：info@filseclab.com
时间：2012 年 10 月 8 日

主要技术简介

行为深度追踪技术
实时追踪的快速响应技术
快速存储与检索技术（黑盒）
基于人工智能模型的行为分析技术（威胁鉴定）
I/O 操作的回滚技术
内存对象的回滚技术
Windows 内核模拟技术

缓冲区溢出防御技术
蓝屏灾难保护技术
增强的自我保护技术
陷阱技术

基因识别技术
基因特征库的自动生成技术
变形病毒识别技术
缩略微特征技术
自动误报排除技术
资源载荷均衡技术
智能提速技术
断点续扫技术

虚拟机技术
API 模拟技术
静态启发式病毒检测技术
基于虚拟机的动态启发式病毒检测技术
虚拟机脱壳技术
宏病毒启发技术

静态变形病毒清除技术
静态广谱式清病技术
基于虚拟机的动态清毒技术

云端快速查询技术（可比普通数据库查询快上百倍）
云端综合鉴定技术
云端智能分析技术

智能语音交互控制技术

威胁自动分拣技术
白程序自动分拣技术
病毒库自动更新技术

程序逻辑追踪技术 PLT
增强 SVM 人工智算法 EX-SVM

V8 技术亮点之“动态防御 2.0”

费尔第二代动态防御开发历时 4 年，代码量超过 40 万行，是费尔最复杂的系统之一，它基本实现一个小型的子系统来模拟和追踪 Windows 的运作过程。

主要技术亮点

首先用一个比喻来描述新版动态防御的特色：一个小偷伪装成客人到家里偷东西，等巡查员认定它不是客人而是贼时随即将其拿下，可是家里却已经被翻乱了，要恢复原样就比较困难。第二代动态防御系统不仅可以抓住贼，同时能让家里恢复如初，并且有能力更早更准确的识别伪装更好的贼，包括当前流行的白加黑木马。主要特点如下：

1. 精确的对象级深度追踪。
2. 对威胁所产生的破坏进行全面热回滚。这主要包括威胁对文件、注册表、HOOK、内存的改写、对象的修改进行全面还原等等。

智能黑盒

费尔智能黑盒类似于飞机的黑匣子，它会对电脑中的每个程序单位行为进行精准而细致的记录，它不仅可以追踪程序的文件、注册表访问，还包括线程、内存，对象的操作等等。而且它的最小追踪单位可以精确到 CPU 的执行片断，以及事件的每一个参与者。比如：一个系统服务线程在这个时间段为正常程序 A 服务，而下一个时间段被病毒 B 嫁接并为其服务，此时发生的破坏行为仍然会被准确定位到 B 而不波及整个服务线程。再如：当发生一个删除文件的事件，此时被追踪的不仅仅是删除此文件的进程，还包括参与此次行动的所有模块以及内存，甚至包括父进程、父线程都会被一并追踪。正是这一全新的追踪架构可以准确定位目前让主防头痛的白加黑木马。

另外，虚拟黑盒具备持久记忆功能，不会随电脑的重启而归零，即使重启电脑目标程序曾经发生的行为仍然会被持续的记录在案，这样当遇到一种把自己的行为故意打散、分时段来

组合完成的潜伏威胁时仍可以准确侦测，从而有能力处理多步式或延时发作的后门、木马，并对其进行彻底的清除和回滚。

行为分析系统

采用复杂的逻辑规则及综合分析系统，对智能黑盒记录的行为进行分析并自动判定是否有害，即“记忆式多步智能主防”。

精准回滚

对有害程序产生的行为实施精准全面的回滚还原。它会对有害程序直接产生的行为以及嫁接到别的程序上间接产生的行为进行还原，而同时不会波及到正常程序。比如：病毒对 Explorer 进行了 HOOK，回滚可以将 HOOK 还原并在不结束 Explorer 的情况下让其保持干净的继续正常工作。

另外，被病毒修改或删除的文件也能够被完美还原，这包括被感染型病毒感染的文件。智能黑盒在追踪程序行为时会对文件、注册表、内存、对象所有发生的修改性动作进行实时备份，并且采用大量先进算法确保对系统影响不可感知，这样即使遇到感染性病毒时仍然可以对曾经的破坏进行回滚复原。

黑盒&沙盒（沙盘）

传统安全软件中的“沙盒”（Sandbox）的工作机制是：对于任何未知程序进行“有罪推定”，也就是说当一个未知程序在运行时沙盒会先假定它是有害的，然后放入隔离环境中检验。这样做的好处是如果程序真的有害那么一般不会对系统造成实质影响，但实际情况中用户遇到的大多数程序都属于正常安全的，由于沙盒中的正常程序要生效修改时会比较困难（比如在沙盒中安装游戏是无法把它真正安装到电脑中去的），甚至需要全部丢弃让用户重新再做一次。所以沙盒比较适合安全厂商进行内部病毒分析或样本采集时使用，但对于普通用户来说存在障碍，它目前仍然属于比较专业的应用。费尔 V8 中的“黑盒”则是一个来源于沙盒思想但与此相反的工作机制，即“无罪推定”。它先假定程序是干净无害的，然后完整跟踪每个程序的行为记录和修改动作，只有当程序表现出恶意行为时才阻止并恢复退回当初状态。这种机制可以和主动防御系统完美的契合联动，而且对于用户来说并不存在任何使用上的门槛，因为整个过程是 V8 内部来自动完成的，不存在要求用户自动/手动入沙过程，也不存在应用修改的问题，和正常使用没有区别，所以费尔的黑盒技术更易用也更安全。

V8 技术亮点之“MVM 威胁虚拟机”

威胁虚拟机（MVM）是费尔智能杀毒 8 中又一极为复杂的安全系统。构建此系统的主要目的是为了通过扫描的方式来检测未知威胁，弥补特征码的滞后性，增强对新木马和加壳变形病毒的防御能力。经过多年的研发和不断改进，目前费尔 MVM 虚拟机启发技术无论从技术层面还是实际效果都已经达到同类系统的一流水平。

为了验证其效果，曾邀请英国 VB100 评测机构 Virus Bulletin 对虚拟机纯启发引擎进行内部测试，在没有黑白名单的支持下，其对 WildList 识别率超过 60%，误报也控制在极低水平，使得 VB 给其高度评价“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!（它甚至优于某些特征码引擎）”。

威胁虚拟机由两个子系统组成：虚拟机系统和启发分析系统。虚拟机系统用来模拟程序运行并收集程序行为，启发分析系统则根据这些行为来判断目标对象是否有害。

虚拟机系统

MVM 中的虚拟机是一个极度复杂的虚拟仿真系统，它能解析并模拟几乎全部的 CPU 指令、数千个 API 函数，并对木马、病毒经常涉及的一些硬件进行仿真，比如：硬盘、网卡等等。它的工作原理是让目标程序在一个虚拟的隔离环境中运行，并将自己的真实意图充分暴露，一旦发现有恶意目的即可被侦测，而同时也决不会影响真实系统。目前 MVM 可以脱近 400 种壳，能有效的应对加壳、变形等特征码不易对付的病毒。

启发分析系统

MVM 中的启发分析系统分为两部分：静态启发，动态启发。

静态启发不需要依赖于虚拟机可以独立工作。它通过反解目标程序的二进制代码直接分析其意图，发现有威胁特点即可被判别，从而达到识别未知威胁的目的。这种方式的优点是速度快，但无法有效识别加壳和变形病毒，而动态启发部分则可以有效弥补这一点。

威胁程序无论是加壳还是变形，最终总要去实现自己的目的，也就是说在运行时它们会自己脱壳。动态启发就可以让其在虚拟机中仿真运行，脱掉自己的外衣，诱使它发作，待目标充分暴露出自己的恶意行为时即被判定威胁，实现动态防御的静态识别。

V8 技术亮点之“载荷均衡、智能解毒与提速、隐私保护与陷阱、缓冲区溢出保护与蓝屏灾难保护”

智能载荷均衡

V8 可以根据当前的系统资源占用状况自动调节自身能耗，在低配电脑中也能顺利运行，既能保障安全又能提高效率。不仅如此，V8 甚至还允许你任意设置病毒库的使用量和内存占用配额，让你自由控制它的资源占用，在“轻量版”与“完整版”之间随意切换。

智能解毒

V8 结合虚拟机技术可对某些特定类型的感染病毒进行万能修复，遇到熊猫烧香、威金病毒后不再只是 “删除/隔离”，可恢复文件到干净状态。

智能提速

通过增量缓存技术对二次扫描进行大规模提速，可将扫描速度提高几十倍甚至上百倍。

文件隐私保护

电脑中个人文档、照片等隐私数据是绝不希望被他人窥视的，但在木马后门、间谍软件流行的当今，个人隐私被窃取的情况时常发生却鲜为人知。用户很难确保自己电脑中没有隐藏的间谍软件或别有用心的第三方软件会在何时拿走自己的文件。V8 中提供了文件隐私保护功能，只要把你重要的文件加入保护，所有试图访问这些文档的程序都需要得到你的许可，保障个人隐私不被侵犯。

威胁诱捕陷阱

遇到顽固木马反复清除不掉，单纯的抑制再生和文件粉碎往往并不能解决根源。V8 中新增的陷阱功能可以用来应对这种“疑难杂症”。设置一个虚拟陷阱将有再生能力的顽固威胁的创建者捕获，实现彻底的清除。

缓冲区溢出保护

安装 V8 后你的电脑将可以自动免疫各类缓冲区溢出攻击。即使在没有安装 Windows 系统补丁的情况下遇到此类最新威胁也能够立即侦测并阻止，保护电脑免受 0day 漏洞破坏。

蓝屏灾难保护

由于病毒攻击、软件冲突、系统故障造成的突发电脑蓝屏，可能导致你的工作中断或文件丢失。V8 中提供的蓝屏灾难保护将可以阻止某些蓝屏的发生，并终止引发蓝屏问题的根源遏制故障继续蔓延，使得电脑可以在一段时间内继续安全运行，为关键时刻及时保存重要数据提供机会，减少损失。

智能交互控制

你可以通过语音对 V8 进行控制，并且它也会有自然语言的回应。打开语音功能后，对着电脑说“费尔”，软件就会弹出主界面并回答“Hi，我在这里”，若说：“扫描我的电脑”，软件自动开始扫描。每个扫描任务都有自己的编号，用户可以随时单一（集体）语音控制那些正在进行中的任务，并让其汇报各自的工作状态。除此之外，V8 语音还提供了一些友善的日常问候和应用呼叫，比如：新闻、购物，搜索等等。而且语音功能是纯绿色的，你不用担心它会在电脑中安装任何额外插件。

V8 技术亮点之“云端人工智能集群 iRobots”

iRobots - 云端人工智能集群 简介

费尔智能等级定义
*　　初级的自动化处理系统，主要解决重复劳动。
**　　带有初级分析能力和错误排除功能的自动化处理系统。
***　　有中度复杂的分析能力和错误排除能力的自动化处理系统，能长期无人值守的自动化运作，可作为人力资源的有效替代。
****　　有高度复杂的分析能力和除错能力，并进行大量复杂运算，可在短时间内提供人力无法完成的分析结果。
*****　　高度人工智能，可在完全脱离人为干预的情况下自我学习，自我完善。

iRobot1 - 病毒样本自动收集系统

智能等级：*
服役时间：2003 年
功能简介：自动从互联网、样本提供商、交换商搜集和下载样本，为病毒库定义提供资源支持。

iRobot2 - 正常程序自动收集系统

智能等级：*
服役时间：2005 年
功能简介：自动从互联网搜集和下载正常软件，为排除误报提供资源支持。

iRobot3 - 样本分拣系统

智能等级：**
服役时间：2007 年
功能简介：自动分析 iRobot1 和 iRobot2 收集到的样本，对程序的黑白性质进行快速分拣。

iRobot4 - 自动更新系统

智能等级：***
服役时间：2007 年
功能简介：对 iRobot3 和 iRobot5 的结果进行综合分析，自动生成病毒库定义和白名单定义并自动发布更新。
案例：从 2007 年至今 iRobot4 已经成功运行 5 年，为费尔 V7 提供不间断更新。

iRobot5 - 自动误报排除系统

智能等级：**
服役时间：2007 年
功能简介：自动纠正已知误报和潜在误报。

iRobot6 - 智能基因分析系统

智能等级：****
服役时间：2009 年
功能简介：利用人工智能数学模型构建自动分类算法，从足够多的样本中找出区别黑白两个集合的特征，从而实现一个特征识别整个集合的黑白性质，并结合 iRobot5 自动排除误报达到实用级别。

iRobot7 - 行为分析系统

智能等级：***
服役时间：2010 年
功能简介：虚拟环境中执行威胁程序并追踪其行为，综合分析后判定是否有害。作为 iRobot3 和 iRobot5 的有力补充，增强自动化的自主鉴定能力，有能力识别出新的未知威胁。同时也为鉴定结果提供切实可靠的证据支持。
案例：目前费尔在给世界最大反病毒组织 WildList 提交的流行样本均来自于此系统 。WildList 会对提交的样本做校验核实，经过 iRobot7 判别的威胁基本 100% 会被 WildList 认可，最终 WildList 再把世界上所有主流杀毒厂商提供的样本进行综合筛选、找出重叠部分发布，作为 ICSA、VB100 等国际认证的测试标准。其中每期 WildList 中来自于费尔的样本一般都会超过 35%，属于采用率最高的厂商之一，以此可以反应出 iRobot7 的高度准确性。

iRobot8 - EVANET 中枢神经系统

智能等级：****
服役时间：2012 年
功能简介：综合分析从 EVANET 客户端发送来的关于程序的行为、属性等各种特征信息，自动判定其是否有危害，客户端根据 EVANET 的分析结果自动决定处理动作。比如：警告、还原或放行等。

EVANET 计划 －安全神经网络系统

EVA 取自电影《阿凡达》里的圣母，电影中圣母 EVA 将潘多拉(Pandora)星球的所有生命连接为一个有机的整体共同抵御外敌从而实现坚不可摧。

费尔以 EVANET 为名，希望将所有的用户电脑有效连接起来共同抵御威胁，从而有效放大抵御能力。EVANET 计划分为以下三个阶段。

第一阶段

通过上传用户端有潜在威胁的程序或程序特征到云端，利用云端的更丰富的鉴定方式进行再次鉴定。费尔 V7 在 2007 年初已经完成这一阶段。

第二阶段

综合电脑使用者的智慧来判断未知威胁。比如：根据用户对程序的不同操作方式进行分析，当很多用户表现出对此程序反感时，它将被标记为潜在的威胁。费尔 V8 实现了这一阶段。

第三阶段

智能联合防御阶段，当一台电脑受到威胁之后，全体电脑都有感知，并可由 EVANET 中枢发出指令，由就近的电脑对其实施救援，令受威胁的电脑起死回生。也可以脱离中枢的指挥，自动就近寻找救援。此阶段正在研发中。

EVANET 主页：http://www.ievanet.com 正在建设中。