反病毒技术发展趋势的研究

董 雪, 常晓鹏

(河南教育学院 信息技术系, 河南 郑州 450014)

摘要: 从计算机病毒的现状及当前反病毒技术的局限入手, 初步探讨了一些对付计算机病毒新技术和反病毒技术的发展趋势.

关键词: 反病毒; 虚拟机; 发展趋势

中图分类号: TP309.5 文献标识码: A 文章编号: 1007-0834(2008)03-0047-02

1 计算机病毒现状

长期以来, 人们设计计算机的目标主要是追求信息处理功能的提高和生产成本的降低, 而对于安全问题则重视不够. 计算机系统的各个组成部分, 接口界面, 各个层次的相互转换, 都存在着不少漏洞和薄弱环节. 硬件设计缺乏整体安全性考虑, 软件方面也更易存在隐患和潜在威胁. 对计算机系统的测试, 目前尚缺乏自动化检测工具和系统软件的完整检验手段, 计算机系统的脆弱性, 为计算机病毒的产生和传播提供了可乘之机; 全球万维网使"地球一村化", 为计算机病毒创造了实施的空间; 新的计算机技术在电子系统中不断应用, 为计算机病毒的实现提供了客观条件.

安全厂商赛门铁克在 2007年 9月发布警示称: 在过去的 6个月里, 他们发现了 211 201个新的恶意软件样本, 这比 2006年下半年增加了足足 185%, 这意味着每天世界上都有超过 1 100个唯一的病毒被产生. 编写病毒的门槛越来越低, 世界上的病毒数量开始呈爆炸式增长.

2 反病毒软件面临的问题

2.1 病毒在理论上是不可判定的

病毒是一段程序, 不同种类的病毒, 它们的代码千差万别, 任何人都不可能预测明天将会出现什么新病毒. 但有一点可以肯定, 只要出现了一项新的计算机技术, 充分利用这项新技术编制的新病毒就一定离我们不远了. 而由于软件种类极其丰富, 且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术. 所以, 虽然有些人利用病毒某些共有的操作 (如驻内存, 改中断)这种共性, 制作了声称可查所有病毒的程序, 但这种方法对病毒进行检测势必会造成较多的误报情况, 不够可靠, 目前都只能作为辅助的手段配合使用, 无法独立推广.

实际上, 计算机病毒学专家早在 80年代初期就已经提出了计算机病毒的模型, 证明只要延用现行的计算机体系, 计算机病毒就存在"不可判定性". 杀病毒必须先搜集到病毒样本, 使其成为已知病毒, 然后剖析病毒, 再将病毒传染的过程准确地颠倒过来, 使被感染的计算机恢复原状. 因此可以看出, 计算机病毒是不可灭绝的. [1]

2.2 特征码技术的局限

目前的大多数杀病毒软件采用的方法主要是特征码查毒方案与人工解毒并行, 亦即在查病毒时采用特征码查毒, 在杀病毒时采用人工编制解毒代码. 特征码查毒方案实际上是人工查毒经验的简单表述, 它再现了人工辨识病毒的一般方法, 采用了"同一病毒或同类病毒的某一部分代码相同"的原理, 也就是说, 如果病毒及其变种、变形病毒具有同一性, 则可以对这种同一性进行描述, 并通过对程序体与描述结果 (亦即"特征码")进行比较来查找病毒. 而并非所有病毒都可以描述其特征码, 很多病毒都是难以描述甚至无法用特征码进行描述. 使用特征码技术需要实现一些补充功能, 例如近来的压缩包、压缩可执行文件自动查杀技术.

但是, 特征码查毒方案也具有极大的局限性. 特征码的描述取决于人的主观因素, 从长达数千字节的病毒体中撷取十余字节的病毒特征码, 需要对病毒进行跟踪、反汇编以及其它分析, 如果病毒本身具有反跟踪技术和变形、解码技术, 那么跟踪和反汇编以获取特征码的情况将变得极其复杂. 此外, 要撷取一个病毒的特征码, 必然要获取该病毒的样本, 再由于对特征码的描述各个不同, 特征码方法在国际上很难得到广域性支持. 特征码查病毒主要的技术缺陷表现在较大的误查和误报上, 而杀病毒技术又导致了反病毒软件的技术迟滞.

3 最新的反病毒技术

3.1 虚拟机技术

有专家认为, 虚拟机杀毒技术即是在电脑中创造一个虚拟 CPU环境, 将病毒在虚拟环境中激活, 根据其行为特征,

收稿日期: 2008-03-08
基金项目: 2007年河南省软科学项目 (072400450100)
作者简介: 董 雪 (1982—), 女, 河南郑州人, 河南教育学院信息技术系教师.

从而判断是否是病毒. 也有专家认为, 所谓虚拟机技术, 就是用软件先虚拟一套运行环境, 让病毒先在该虚拟环境下运行, 从而观察病毒的执行过程. 这个技术主要用来应对加壳和加密的病毒, 因为这两类病毒在执行时最终还是要自身脱壳和解密的, 这样, 杀毒软件就可以在其"现出原形"之后通过特征码查毒法对其进行查杀. [2]对于未知病毒, 如果能够让病毒在控制下先运行一段时间, 让其自己还原, 那么, 问题就会相对明了. 可以说, 虚拟机是这种情况下的最佳选择. 故此虚拟机当今在反病毒软件中应用范围广, 并成为目前反病毒软件的一个趋势.

目前"临床"应用的虚拟机并不是"高大全"的完整仿真环境, 而是相对比较简单的、易于实现的版本. 因为我们必须解决虚拟机技术面临的两大难题, 一是虚拟运行环境占用资源的问题, 二是如果判断病毒标准的问题.

事实上, 虚拟机技术面临的一个最大的难题就是如何解决资源占用问题. 试想, 虚拟一个 CPU 环境需要占用多大的资源? 在这个环境下激活一个病毒, 让病毒完成其从发作到传播的整个过程, 再分析其行为特征, 又需要多长的时间? 如果全部应用虚拟机技术话, 分析一个加壳病毒需要 3到 5分钟的时间, 而目前电脑中许多压缩加壳的文件, 仅仅分析这些文件耗用的时间和占用的资源, 就足够使一个很有耐心的人放弃这款杀毒软件了.

第二, 在判定病毒的标准上, 仍然会有问题. 尽管根据病毒定义而确立的"传染"标准是明确的, 但是, 这个标准假如能够实施却是模糊的. 一是, 我们要仿真传染条件, 对于那些条件感染病毒, 怎样制造传播条件? 如系统日期、感染对象的文件名等等, 二是这个分析是通过动态执行 (甚至回溯)分支屡试呢, 还是通过反回头进行静态的指令过程分析? 假如我们在对病毒的判定标准上能够通过, 那么, 我们必须检测并确认所谓"感染"的文件确实感染的就是这个病毒或其变形.

故此, 现今的虚拟机技术仍然与传统技术相结合, 并没有抛弃已知病毒的特征知识库. 并非像某些反病毒厂商所宣称的那样, 已经完全进入了"主动防御"的阶段. 目前虚拟机的处理对象主要是文件型病毒. 对于引导型病毒、Word/Excel宏病毒、木马程序在理论上都是可以通过虚拟机来处理的, 但现实实现较难. 目前此项技术运用比较出色的有 NOD32、MCAFEE等.

3.2 沙盘仿真 (虚拟机的继承人)

这项技术最早是系统还原类软件的专利, 例如 Shadow 系统或者 NORTON GOBACK的 safe mode等. 这项技术是说在原有的系统上预先留出一些空间, 然后让用户进行操作, 重新启动后, 原先的数据全部被清除, 还原到原始状态的一种技术. 而杀毒软件也同样看见了这一点. 于是就将此项技术和虚拟机技术进行了整合, 推出了沙盘仿真技术. 技术原理和虚拟机大致相同, 同样是虚拟出一个系统, 然后让病毒运行, 从而进行清除. 此项技术解决了虚拟机的弊端——高资源占用, 与虚拟机技术现在是平分秋色. 目前该技术运用出色的有 Kaspersky 7.0、8.0等.

3.3 主动防御 HIPS

所谓 HIPS (主机入侵防御体系), 也就是现在大家所说的系统防火墙, 当某进程或者程序试图偷偷运行的时候总是会调用系统的一些其他的资源, 这个行为就会被 HIPS检测到然后警告询问用户是否允许运行, 用户根据自己的经验来判断该行为是否正确安全, 是则放行允许运行, 否就不使之运行. [2]一般来说, 在用户拥有足够进程相关方面知识的情况下, 装上一个 HIPS软件能非常有效的防止木马或者病毒的偷偷运行, 这样对于个人用户来说, 中病毒的可能性就基本降到很低了.

杀毒软件具有滞后性, 这是业界公认的一个弊端, 而 HIPS却很好的解决了这个问题, 尤其是卡巴斯基 6.0和东方微点将这一技术推广到了极致. 其优秀的防御系统能够解决 90% 以上的未知病毒. 这不仅能够解决病毒库更新的滞后性, 同时也给技术人员的减负. 在绝大多数情况下 HIPS是需要人为参与的编写规则的, 也就是不能做到完全智能. 自己的规则永远是最好的, 而参看别人规则写自己的规则是一种最好的学习, 去芜存菁是我们需要做的. 但在实际使用中, 因为软件的不同有些特殊的体系变种, 这个需要自己把握和灵活运用, 不适合硬套照搬, 也正因此给大部分初学者造成了很多困难. 目前此项技术运用出色的杀毒软件有: SCS、卡巴斯基 6.0和 7.0、东方微点、终结者 (不完全 HIPS)、SSM、CAHIPS等.

4 反病毒技术的发展趋势

杀毒技术发展的趋势在做从作品对抗到思想对抗的转变, 产品形态在从独立软件产品向操作系统的补丁转变.

(1)从作品对抗到思想对抗

基于对大量的病毒的特征、发作过程、传播变化统计的基础上, 建立控制策略数学模型, 采取分门别类的方法, 有效解决应用同种思想开发出的各种病毒, 可以极大提高对新病毒的反应时间. 由于这种方法是通过抑制病毒设计思想而实现的, 因此, 这是一种病毒制造者与安全专家之间在整体思想层面的竞赛. [3]

因此, 新的杀毒软件不仅仅是依据病毒数据库中的病毒代码对计算机进行扫描, 而是对计算机所运行的各种进程、各种操作进行监控, 如 HIPS, 如果发现某个事件或某项操作存在典型的病毒特征, 或是对计算机存在危害, 那么这些事件或操作就会被阻止, 得以更有效地保护计算机不受新型病毒的入侵.

(2)从独立产品到操作系统的补丁

杀毒软件作为一个独立的软件产品, 已经存在了很久, 但是, 由于病毒制造者越来越多地利用操作系统的漏洞和黑客技术, 因此, 与操作系统的紧密结合成为一种必然: 一方面, 可以帮助操作系统减少漏洞, 另一方面, 也可以进一步提高运行效率和软件兼容度. 从商业角度上来说, 安全技术可以融入各种应用系统, 减少应用系统自身的安全漏洞, 同时, 也可以为用户提供更加个性化的安全服务.

参 考 文 献

[1] 斯泽. 计算机病毒防范艺术 [M]. 段新海, 杨波, 王德强, 译. 北京: 机械工业出版社, 2007.

[2] 韩筱卿, 王建锋, 钟玮, 等. 计算机病毒分析与防范大全 [M]. 北京: 电子工业出版社, 2006.

[3] 秦志光, 张凤荔. 计算机病毒原理与防范 [M]. 北京: 人民邮电出版社, 2007.