文章编号:1009-3907(2007)06-0047-04

病毒检测技术在查杀"熊猫烧香"中的实证分析

任师尊

(长春大学 成人教育学院,吉林 长春 130022)

摘 要:为了更好地查杀"熊猫烧香"病毒,我们研究了常用病毒扫描器对"熊猫烧香"存在的明显不足,并指出改进办法,通过介绍几种病毒检测方法,研究其在"熊猫烧香"中的具体应用。

关键词:病毒检测;特征字扫描;启发式;虚拟机

中图分类号:TP309.5 **文献标识码**:A

0 引 言

"熊猫烧香"病毒的大肆传播和蔓延,给我们的日常工作和生活带来了极大的不便。我们有必要加强反病毒的知识,这样才能与病毒程序进行彻底的对抗。在"熊猫烧香"病毒刚开始爆发时,因它把我们常用的杀毒软件都给关闭了,使得很多人都束手无策。此时此刻研发"熊猫烧香"病毒的专杀工具成为刻不容缓的事情。今天,虽然"熊猫烧香"已经成为过去,但是研究用多种病毒检测引擎技术在查杀"熊猫烧香"病毒过程中的应用的目的是为了在以后使我们更从容地应对大规模突如其来的其它种类的病毒。

1 常用病毒扫描器对"熊猫烧香"存在的明显不足

因"熊猫烧香"病毒具有在定时器时间内搜索常用杀毒软件,并关闭杀毒软件的功能,这使得常用病毒扫描器在应对"熊猫烧香"时存在明显的不足。这也使得专杀工具这种扫描器技术得到了发展空间。因为专杀工具不在常用杀毒软件范围内,"熊猫烧香"虽然能搜索到专杀工具的进程,但是它不能识别出专杀工具的进程具有反病毒的作用,这样,"熊猫烧香"就不会将其关闭。

解决方法:"熊猫烧香"病毒能让常用病毒扫描器的进程结束,是在它对所有的进程名称进行检测后,发现常用病毒扫描器正在使用,就向它发送了令它结束的消息WM_CLOSE[1],扫描器接收到这个消息后,就会运行相应的消息响应函数,这个消息响应函数就是用于处理它本身进程结束时要做的工作。

问题的关键在消息响应函数对消息的处理上,一般的常用病毒扫描器只是简单地进行退出前的确认工作,它会显示退出窗口,问用户是否真的要退出,这时"熊猫烧香"病毒在后台再发送消息WM_QUERYENDSESSION就可以应付进程的确认工作[1],甚至进程的退出前的提示窗口都不会来得及显示,进程就被"熊猫烧香"病毒强迫关闭了。这就要求在处理消息响应函数时必须增加智能判断算法,来区别是用户还是其它进程在发送消息关闭自己。比如用个系统消息监视器,监视系统中近程间相互传递的消息。或者利用双进程,这两个进程可以相互唤醒,即使其中一个被强迫关闭了,另一个进程也会及时把它唤醒。

即使"熊猫烧香"在爆发时没有发送令病毒扫描器关闭的消息,很多病毒扫描器也不会马上能查出"熊猫烧香",因为在扫描器的病毒库中没有"熊猫烧香"的特征码,但是有一些扫描器是能查出病毒的,由于不能确切识别出是病毒的类型,这时候也是不能做杀毒处理的,只能隔离。

2 在扫描器中可使用的扫描方法

检测"熊猫烧香"及其变种病毒可以使用的扫描方法有:校验和法、特征字扫描法、启发式扫描法、虚拟

收稿日期:2007-10-13

作者简介:任师尊(1979-),男,吉林省农安县人,长春大学成人教育学院助教,硕士生,主要从事计算机安全方面的研究。

机技术、专杀工具法。

2.1 校验和法

校验和法是按未被病毒感染文件的内容,计算其校验和(任何校验方法都可以),将该校验和写入特定文件中保存。在使用未被病毒感染的文件过程中,定期地或每次使用文件前,都检查文件现在内容,并算出它的校验和,再与原来保存的校验和比较,是否一致,用此方法来判断文件是否被感染。

使用校验和法遇到如已有软件版更新、变更口令、修改运行参数等情况时都会报虚警。

校验和法在应付"熊猫烧香"病毒时,这种技术的实现方法比较简单,能发现熊猫烧香及其变异,但只能识别出被感染病毒,不能具体识别出感染病毒的具体类型,不能用于具体杀毒操作,这就要求扫描器使用其它技术来识别病毒的类型。同时,也容易引起虚警(文件内容的改变有可能是正常程序引起的),如果在使用校验和法前就感染了"熊猫烧香",那这种检测技术就会失效了。

2.2 特征字扫描法

特征字扫描法是目前唯一能比较准确识别出"熊猫烧香"病毒的方法。

特征字扫描法是在文件和内存中进行检索,与病毒库中每个病毒的特征字节序列进行匹配来判断是否感染病毒。这是杀毒软件最主要的查毒方法。

病毒的特征字序列是从病毒文件中提取出的标示该病毒特征的字符串序列,它不大可能与普通正常程序代码吻合,抽取的代码要有适当长度,一方面维持特征代码的唯一性,另一方面又不要有太大。它们通常可以表示出一种或一类病毒独有的特征。这些字符串序列从病毒中提取出来后,被存入病毒特征字数据库中,供病毒扫描引擎用来在扫描文件或内存时进行字符串序列匹配查找来判断该文件或内存中是否含有该种病毒。

病毒特征字节序列中通常使用了字符串、通配符、不匹配字节数等约束性语法,来定义病毒的特征性。

2.2.1 特征字扫描法中涵盖的技术

特征字扫描法通常按扫描位置不同分为:散列检测法,首尾扫描法,入口点和固定点扫描法。按扫描数据分为:智能扫描法、骨架扫描法[2]。

为了更加精确地识别出病毒,有的在扫描其中使用了双特征字进行病毒文件检测。这种方法可以减少虚警,能更加精确地识别出病毒身份,从而能准确地对该病毒使用相应的清除方法,但是系统开销比较大,通常情况下不使用这种技术。

为了能快速地进行磁盘访问,在扫描器中我们可以绕过系统级 API,直接使用 BIOS 调用来读取磁盘,从而优化了扫描速度,也可以出于对速度和安全性需求,直接与磁盘控制器进行通信,来读取数据。但现在的操作系统和磁盘控制器种类比较多,使这些技术的需要识别操作系统和磁盘控制器的类型,实现起来比较困难,但是要是出于对扫描器通用性的考虑,建议还是使用 API 函数来进行磁盘的读取工作。

2.2.2 扫描位置

散列检测法是指能加速搜索算法的一些技术。散列可以对特征字符串的首字节或第一个 16/32 位字进行计算。通过精心选择字符串的前几个字节内容,就可以更好地控制散列。

首尾扫描法只扫描文件的头部和尾部,而不扫描整个文件,它可以加速病毒的检测。比如在文件开头和结尾的 2kByte、4kByte 甚至 8kByte 内容中进行扫描,检查每个可能出现病毒的位置。

入口点是可执行文件头部能访问到的对象的入口点(EP)。

固定点扫描对每个字符串只在一个位置进行匹配因此就可以设置一个起始位置 M(例如文件的主入口点),然后在距离固定点 M + X 字节的位置匹配每个字符串或散列值。

对"熊猫烧香"病毒具体扫描器在哪个位置进行扫描,要取决于文件的类型,因为文件的类型决定了被感染的具体位置。"熊猫烧香"会在扩展名为 exe,pif,com,src 的文件的头部添加病毒体代码,这样,针对这些类型的文件,我们再进行查杀"熊猫烧香"时在头部和入口点处扫描会取得比较好地效果。熊猫烧香"会在扩展名为 htm,html, asp,php,jsp,aspx 的文件末尾添加一网址,所以在针对这几种文件进行扫描时,在文件的尾部进行扫描效果比较理想。

但是如果要想在品种繁多的"熊猫烧香"病毒的变种中进行查毒,最好这些方法是结合使用。

2.2.3 扫描数据

智能扫描法(smart scanning)是在计算机病毒变异工具包(mutator kits)出现时提出的。这种工具包用于处理汇编语言源文件,并试图向源文件中插入垃圾指令,如 NOP 指令。智能扫描法会忽略宿主程序中像 NOP 这样的指令,也不会把这些指令存入病毒特征(signature)中。

骨架扫描法是针对检测宏病毒时使用的,在"熊猫烧香"中不用这种方法,但是在通用扫描器中是使用的,这里只做简单介绍,不做分析。骨架扫描法是逐行解析宏语句,并将所有非必要语句及一些空白语句字符(如空格、回车换行、制表符等)丢弃,剩下的就是宏代码的骨架,然后对这个骨架做病毒检测。"熊猫烧香"病毒的制作比较简点,但是它的变异就比较复杂了,智能扫描法处理"熊猫烧香"的变种非常实用,但是单用智能扫描不行,因为很多变种可能会加壳,加花指令,所以必须要结合虚拟机技术使用才可以达到理想目的。

2.2.4 特征字扫描法处理"熊猫烧香"病毒的总结

特征字扫描法查杀"熊猫烧香"病毒时,检测准确快速,能识别出"熊猫烧香"病毒及其变异的类型,误报警率低,依据检测结果,可做杀毒处理。但是不能检测出未知的"熊猫烧香"变异病毒;不能检查出已知的经过多态形处理的或隐蔽性处理的"熊猫烧香"变异病毒;随着病毒变异种类的增多,特征字库变大,检索时间会变长,检索速度会变慢。

2.3 启发式扫描法

启发式是指"自我发现的能力"或"运用某种方式或方法去判定事物的知识和技能"[3]。

启发式扫描技术的思想是依据总结的病毒的共性特征来减小文件的搜索空间,提高病毒扫描器的搜索效率。它是在软件系统规模趋于庞大,对常用的特征扫描法的扫描速度要求改进的情况下提出的优化特征扫描法的技术。它是基于专家系统的原理产生的。在判定了文件感染病毒后再对文件进行特征代码扫描或者虚拟机技术处理,这样会明显地提高扫描效率。

病毒的行为可以作为启发式扫描的原理基础。在对病毒行为特征的总结后,我们利用模糊概念计算出某行为的危险系数,通过检测文件中使用的可疑行为的次数和相应行为的危险系数,通过某种的算法来计算出该文件的危险度,再用模糊概念来判断是否感染了病毒[4]。但并不是使用了可疑行为的文件就是被病毒感染了。

可疑行为包含:可疑的内存分配操作,程序代码修改,违规写磁盘操作,改动程序入口地址,对系统文件进行文件操作,可疑的跳转结构,使用非正常堆栈,截获其他软件的加载和装入,内存驻留,在内存中进行搬移,DOS 功能调用等等,然后把可疑行为细化分成相应 API 功能函数用 hook 技术进行监控[5]。

因为"熊猫烧香"及其变异病毒都修改程序或文件,所以启发式扫描技术在查找"熊猫烧香"及其变异病毒上非常有效,不管是多态形的变异,还是隐蔽性的变异,都能一网打尽,而且还可发现未知的"熊猫烧香"变异病毒。但是它不能识别出"熊猫烧香"的具体类型,不能直接进行杀毒处理。它和校验和法一样,都能加快扫描速度,减小特征字扫描的范围,但是它比校验和法更安全有效。

3 虚拟机技术

虚拟机技术的思想是用程序代码虚拟 CPU、内存管理系统、甚至是硬件端口,用虚拟寄存器和标志位来模拟 CPU 指令集,再在内存管理系统中虚拟出数据的内存访问函数,然后由一个庞大的 switch()语句对各个指令集操作码做逐一分析,来模拟代码执行过程。这样,恶意代码就会在扫描器的虚拟机中模拟执行,而不是在真实地 CPU 中执行。

虚拟机技术是一种前沿的反病毒的新技术,主要用来分析未知病毒和查、杀多态变形病毒。

在虚拟机中由于采用动态分析程序变化的技术,使得无论如何变化代码和加密代码的多态形病毒,最终都会露出真实的面目,再用特征字扫描法进行彻底扫描,就会发现病毒的具体种类。"熊猫烧香"也不例外。它能很准确地查出"熊猫烧香"及其各种变异,但是由于虚拟的 CPU 执行速度比真正的 CPU 慢近 10 多倍,所以在采用虚拟机技术前,一定要用启发式或者校验和判断出确实含有病毒,才能再用虚拟机把病毒程序显示出来,然后用特征扫描法来检测。

4 专杀工具法

每当通用的扫描器不能处理某个病毒时,就必须编写新的代码来实现该病毒的特定的检测算法,这就是这种病毒的专杀工具。这种杀毒方法也是现代防毒体系中的一个必要组成部分。

网上有很多"熊猫烧香"病毒的专杀工具,各个大的杀毒软件公司也都推出了相应的"熊猫烧香"病毒的专杀工具。这里不做原理分析了。

采用单一技术是很难把"熊猫烧香"杀灭的,必须各种方法都结合使用才能应对"熊猫烧香"的各种变异。

参考文献:

[1] [美]Jeffrey Richter. Windows 高级编程指南[M]. 王书洪,刘光明,译. 3 版. 北京:清华大学出版社,1999.
[2] [美]Peter Szor. 计算机病毒防范艺术[M]. 段海新,杨波,王德强,译. 北京:机械工业出版社,2007.
[3] 王振海,王海峰. 针对多态病毒的反病毒检测引擎的研究[J]. 微计算机信息,2006,22(3):134 - 136.
[4] 谢金晶,张艺濒. 基于改进的 K-最近邻算法的病毒检测方法[J]. 现代电子技术,2007(3):51 - 53.
[5] 张波云,殷建平,唐文胜. 一种未知病毒智能检测系统的研究与实现[J]. 计算机工程与设计,2006,27(11):1936 - 1938.

责任编辑:钟 声

Analysis of normal methods of detecting viruses for "worm. nimaya." virus

REN Shi-zun
(Adults Education College, Changchun University, Changchun 130022, China)

Abstract: In order to better detect "worm. nimaya." virus , we reseach shortcomings of common virus scanners in handling "worm. nimaya." virus , and raise improved methods. We discuss specific application in detecting "worm. nimaya." virus by introducing several virus detection .

Keywords: virus detection; character scanning; heuristic scanning; virtual machine

病毒检测技术在查杀"熊猫烧香"中的实证分析

作者： 任师尊， REN Shi-zun
作者单位： 长春大学成人教育学院,吉林,长春,130022
刊名： 长春大学学报（自然科学版）
英文刊名： JOURNAL OF CHANGCHUN UNIVERSITY
年，卷(期)： 2007,17(6)
被引用次数： 1次

参考文献(5条)

1. Jeffrey Richter;王书洪;刘光明 Windows高级编程指南 1999

2. Peter Szor;段海新;杨波;王德强 计算机病毒防范艺术 2007

3. 王振海;王海峰 针对多态病毒的反病毒检测引擎的研究[期刊论文]-微计算机信息 2006(03)

4. 谢金晶;张艺濒 基于改进的 K-最近邻算法的病毒检测方法[期刊论文]-现代电子技术 2007(03)

5. 张波云;殷建平;唐文胜 一种未知病毒智能检测系统的研究与实现[期刊论文]-计算机工程与设计 2006(11)

本文读者也读过(9条)

1. 欧春.OU Chun 从查杀"熊猫"烧香病毒谈起——中学图书馆电脑系统防病毒[期刊论文]-农业图书情报学刊 2007,19(11)

2. 陶金 从"熊猫烧香"看新型网络病毒的特点和防御方法[期刊论文]-辽宁师专学报（自然科学版）2007,9(1)

3. 向大为.麦永浩 "熊猫烧香"案件的分析鉴定[期刊论文]-警察技术2009(1)

4. 郑先伟.李荣侠 解剖"熊猫烧香"病毒[期刊论文]-中国教育网络2007(3)

5. 林晨 浅论熊猫烧香类型病毒的防治[期刊论文]-福建电脑2008(1)

6. 安乐 "熊猫烧香"谁被"烫伤"——从"熊猫烧香"看网络信息安全现状[期刊论文]-中国新技术新产品精选2007(3)

7. 赵晓力 从"熊猫烧香"案引发的启示[期刊论文]-信息网络安全2007(11)

8. 刘君博 关于青少年利用计算机犯罪问题的研究[期刊论文]-科技风2008(19)

9. 刘亚 "熊猫烧香"带给教育的思索[期刊论文]-计算机教育2008(2)

引证文献(1条)

1. 马金鑫.袁丁 一种特征代码过滤方法的改进[期刊论文]-计算机应用与软件 2010(8)