浅析360安全卫士及360杀毒软件机制及漏洞

陈素霞 宋斌
(河南省轻工业学校 河南郑州 450006)

摘 要:本文分析了360安全卫士的优缺点以及360杀毒软件的机制和漏洞。对当前有效的免杀手段进行了讨论,并对将来杀软的的发展趋势进行分析。

关键词:木马 杀毒软件 主动防御 360
中图分类号:TP3 文献标识码:A 文章编号:1672-3791(2010)06(b)-0020-01

回顾我国杀毒软件发展的历程,要从1990年说起,当初国内是不存在杀软的,但是当时出现一种叫球球的病毒,深圳一家公司做出了最早的防毒卡,随后瑞星也随着开发出杀毒软件,但因为杀毒软件的单一性,很快就退出了市场。2000年至2004年,网络游戏行业飞速发展,因背后隐藏了一条巨大的黑色产业链,为黑客技术的发展奠定了基础,更为杀软开辟了强有力的市场。现在国内典型的杀毒软件有360杀毒、瑞星、金山毒霸、NOD32、江民等,国外的杀软也陆续进入国内市场,每个杀软都有自己的杀毒引擎,因此在杀毒能力方面各有特色。今天我们对现在市场占有率第一的360安全卫士和360杀毒软件进行分析。

360安全卫士:此软件自2008年以来因为其修复浏览器、修补漏洞、清除插件和云查杀等功能的快捷便利而风靡全国,在短短的一年之中,电脑安装率在90%以上,在国内发展速度之快及安装率之高令人惊叹。然而此软件并非杀毒软件,360安全卫士是一个典型行为报警工具,不能对文件的特征码进行查杀,只对文件运行后某些行为进行查杀,例如:某个木马运行以后要增加系统服务或增加系统启动项,这时360就会根据情况做出提示,报告给用户有可能是恶意程序,提醒用户警觉。360安全卫士自带的云查杀也只能对木马进行简单的行为查杀,对于多数木马来说,并没有真正的清除意义。稍微做一些动作,就可以连提示都没有,下边举例说明如何突破。

首先360的行为监控对文件释放路径有要求,一个文件运行后只要释放文件在C盘后被执行,他就会给客户提示释放文件被执行,如果客户拒绝,则木马不能运行,这样有效的防止了一部分木马。但是现在的木马遥身一变,文件释放在其他盘并运行,这样就简单有效的躲过了杀毒软件的行为监控。然而行为查杀并非这样简单,现在木马运行有两种方式运行,一是注入进程,木马可以注入windows某些特定的开机必启动的进程,这些进程开机被启动后,木马同时也被执行。二是插入windows系统服务和写注册表以保证系统每次启动后木马软件能够执行成功。如果采用以上两种方式运行木马,则木马运行后,360会提示程序被注入,或系统服务被添加或注册表添加启动项目等,提示用户注意,引起用户警觉。如果不采用以上两种方式,则木马运行后360无提示,木马也可以执行成功,但重启电脑后,木马将不随系统启动,无何任利用价值。但现在出现的一种最新的技术——ActiveX技术,使用此技术加载后,使木马不写注册表不写服务就可使木马正常执行且重启之后也可顺利执行,令人欣慰的是,360对于被公布出来的免杀技术免疫的非常快,虽然这种方法很快会被360封闭,但目前这前这种技术还可以使360无提示执行木马。

以上讲述了360安全卫士的优缺点,但360安全卫士做为一个防护软件做的非常出色,虽不具备杀毒软件的特征,但可以有效的防御流行木马,是电脑安全的第一道屏障。下面我们来分析360杀毒软件的杀毒特征,以及如何有效的让木马躲过杀软查杀。

在分析杀软之前,我们要了解主动防御的概念,现在所有杀软都采用了这种技术,简单的说就是文件在未运行之前,杀软就已经将文件放在了虚拟环境中运行,对木马运行后的每个动作进行分析,如果符何木马特征,则会以消息的形式提示用户。那么他是如何来分析其文件是否是木马呢?我们知道,一个程序要在windows系统执行实现自己的功能,就必须要调用dll文件里的API函数,一个进程有怎么样的行为,通过看它调用了什么样的API数,杀软在模拟环境中观察程序对API的调用情况,就可以知道一个进程将有什么动作,如果有危害系统的动作该怎么样处理等等,但这种方法只能够的抵御80%的木马,因为此方法还是有其弊端,目前还是有以下有几种方法就可以绕过杀软的主动防御。

(1)因为杀软监控的是一系列的API函数的运行状况,并不对某一个函数进行查杀,如果发现一系列的函数按顺序执地,那么杀软就会报警,但是如果木马用不同的函数来实现相同的功能,则杀软就不会报警。

(2)如果木马作者在编写木马时,发现木马被查杀,他就会用软件定位出木马的特征码,并根据特征码地址定位到源代码处,在源码上边或下边加一些垃圾函数,这样,函数没有被连续执行,主动防御则不会报警。

(3)如果作者发现杀软查杀了某个函数,他就会将这函数去掉,对于木马来说,失去了某项功能而已,很多功能在木马运行时并不是必须的。

(4)木马被加上生僻壳,杀软无法分析到木马的函数调用情况。

以上是主动防御的优缺点,现在几乎所有的杀软都有主动防御功能,虽然主防能力各不相同,但中心思想大体是不变的。在此我们分析现在最流行的终身免费的360杀毒。

360杀毒是典型的启发式杀毒,这种技术是未来反病毒技术发展的必然趋势,达到80%以上的病毒检出率,而其误报率可以控制在0.1%之下,但是这种杀软的漏洞在于它的启发式杀毒,如果碰见免杀的反调试代码,则会使其沉默,现在的360杀毒盯上木马的版权和图标,现将木马的版权和图标修正为正常程序的版权和图标,再修改其特征码,也可有效的躲避360杀毒查杀。另外,为软件加上数字签名、生僻壳也对免杀360杀毒软件有特效。

综上所述,360安全卫士和360杀软都有其不足之处,360也很清楚这些问题,但是对于目前360的技术而言,解决这些问题并非易事,这些问题也是对所有杀软的考验。杀毒技术的发展永远依附于木马免杀技术的更新,因此对于杀毒软件和木马以后会何去何从我们将拭目以待。