在攻与防的对立统一中寻求突破

黑客防线 3

总第99期
2009

网站全新改版，欢迎访问：http://www.hacker.com.cn

基于有序规则的加密与信息隐藏技术

探索Winlogon进程SAS热键的原理

控制子系统进程间通信监控进程与线程创建

底层函数的进程守护

内核清零杀进程

Windows驱动漏洞的发现与利用

枚举CPU的全局描述符表

CD+书 12.50元

ISBN 7-89462-004-0

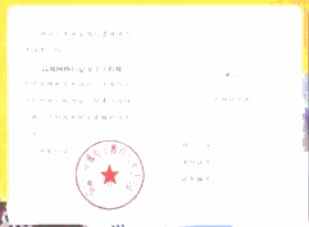
9 787894 620040

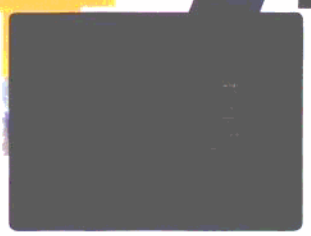
在攻与防的对立统一中寻求突破！

就业培训
证书培训
留学移民培训

强势推出

黑客防线技术奉献强力培训计划





《网络信息安全工程师职业资格培训证书》培训

在线考试，精细辅导，专项强化，资格证书轻松获取，敲开就业大门！

颁发信产部资格证书
采用灵活网络教学
高频考试及辅导
安全技术强化培训
……

保障就业本地网络安全技术培训

找工作难？找网络安全工作更难？
本地培训，保障就业！

合同保障就业，无效退款！
全日制教学，封闭式管理！
短期针对性培训，学有所用！
案例引领，实地操作，全程讲解！
……

课堂

学员

网络安全移民留学培训

网络安全技术，成就留学、移民、高薪之路！

零基础入学
保证留学学校offer
保证留学签证
保证留学实习
符合条件，保证移民
合同保障，无效退款！
……

详情访问：http://www.hacker.com.cn/plant/
培训咨询QQ：1049118405
咨询电话：010-62145877

在攻与防的对立统一中寻求突破

黑客防线 2009订阅方案

攻防对立，技术提升，莫问英雄何处出！
崇尚技术，勇攀顶峰，敢与权威试比高！

作为2001年创刊的中国第一本网络安全技术专业刊物，《黑客防线》与国内网络安全爱好者一起，8年来不懈奋斗，秉承着“在攻与防的对立统一中寻求突破”的核心理念，逐步发展成国内网络安全技术的顶尖媒体。除了《黑客防线》月刊以外，为了将快捷、方便、无地域限制的网络优势发挥出来，黑客防线于2005年10月正式开放了VIP体制，让更多的网络安全技术爱好者能通过网络，交流、学习、讨论最新的网络安全技术问题，极大地提高了国内网络安全技术的普及率和高级网络安全技术人员之间的交流。

为了满足广大《黑客防线》读者对月刊的需求，2009年新的订阅方案在秉承方便、实惠的一贯方针的基础上，融入了全新的、人性化的以往VIP会员回馈方案，以便让长期支持、关注、关怀《黑客防线》的读者朋友们享受到更多的实惠和技术讨论的便捷。

当今时代要求我们，更加专注于最顶尖的技术研究，更加专注于网络安全技术的普及，更加专注于网络安全理念的推广——2009年订阅方案的种种优惠活动，就是为了让更多、更新的新兴血液加入到网络安全技术中来！

2009年超级优惠订阅方案

★《黑客防线》杂志每月月初出版，定价12.5元，全年12期共150元。

★超级至尊

汇款1980元，订阅2009全年12期杂志。

免费赠送

每期杂志快递送出，价值96元；
黑防新一代远控高级个人版（完全免杀，一年服务），价值2000元；
铂金终身会员权限及相关服务，价值1980元；
《黑客防线2008精华本》，价值39.8元；
《黑客防线2009精华本》，价值39.8元；
可开发票。

★钻石恒久

汇款758元，订阅2009全年12期杂志。

免费赠送

每期杂志快递送出，价值96元；
钻石终身会员及相关服务，价值758元；
《黑客防线2008精华本》，价值39.8元；
可开发票。

★金牌惊喜

汇款488元，订阅2009全年12期杂志。

免费赠送

每期杂志挂号邮寄，价值36元；
金牌三年会员及相关服务，价值488元；

★银牌超值

汇款358元，订阅2009全年12期杂志。

免费赠送

每期杂志挂号邮寄，价值36元；
银牌一年会员及相关服务，价值358元。

★快速阅读

汇款246元，订阅2009全年12期杂志。
【杂志款150元＋全年快递费96元＝246元】
汇款204元，订阅2009全年12期杂志。
【杂志款150元＋全年挂号费36元＋全年邮寄费18元＝204元】

★VIP会员2009年订阅方案

即日起，至2008年12月20日，铂金VIP会员、钻石VIP会员、金牌VIP会员、银牌VIP会员订阅全年《黑客防线》杂志，均享受8折优惠！
VIP会员汇款206元，订阅2009全年12期杂志。【杂志款120元＋全年快递费96元＝216元】

★VIP会员升级订阅方案

即日起，至2008年12月20日，特定升级VIP会员，可享受赠送2009年全年《黑客防线》杂志，杂志以挂号方式寄出。
银牌升级金牌：不享受杂志赠送。
银牌升级钻石：370元，赠送2009年全年《黑客防线》。
银牌升级铂金：1622元，赠送2009年全年《黑客防线》。
金牌升级钻石：不享受杂志赠送。
金牌升级铂金：1492元，赠送2009年全年《黑客防线》。
钻石升级铂金：1252元，赠送2009年全年《黑客防线》。

★培训班特惠订阅方案

即日起，至2008年12月20日，加入黑客防线各种培训班，均送2009年全年《黑客防线》杂志，杂志以挂号方式寄出。
脚本培训班：340元
工具培训班：380元
C/C++培训班：1980元，可开发票。
Linux培训班：1980元，可开发票。
漏洞发掘培训班：1980元，可开发票。
Delphi培训班：1980元，可开发票。
Java编程培训班：1980元，可开发票。

注意事项：

1. 除以上方案以外，2009年《黑客防线》不接受其他方式的订阅。
2. 快递方式是每期出刊后立即发送，快捷便利，可以尽快阅读最新技术，但是，县市以下的地区不通快递，请不要选择这个方案。一旦按照这个汇款而又不能通过快递发送，我们将自动更改为通过邮局挂号邮寄。挂号邮寄也安全可靠，但是路途时间较长，一般要15天到20天才能收到。
3. 选择一、二、三、四方案的，因为涉及到会员权限的开通，不管选用什么方式汇款，都要联系客服3的QQ:812712489或者致电010-82145877，或者传真至010-82141360，说明你在黑防网站的注册账户，以便及时给你开通会员权限。
4. 无论选择什么方案，全部都要到网站注册账户，重要的是，要在注册信息准确地写出可以收到邮件的地址，同时，真实姓名和电话也必须不可少。
5. 如有其他疑问，请访问《黑客防线》官方网站www.hacker.com.cn，或[illegible]QQ。

汇款方式：

中国银行
卡号：6013 8201 0000 1361 321
户名：王英
开户地：北京市海淀区知春路支行

中国农业银行
卡号：6228 4800 1030 0147 815
户名：王英
开户地：北京市海淀区大钟寺支行

中国工商银行
卡号：6222 0202 0001 4677 781
户名：王英
开户地：北京市海淀支行

交通银行
卡号：6222 6009 1002 7088 507
户名：王英
开户地：北京市海淀区双榆树分理处

中国建设银行
卡号：4367 4200 1068 0443 876
户名：王英
开户地：北京市海淀区北三环储蓄所

招商银行
卡号：6225 8801 1002 5187
户名：王英
开户地：招商银行北京市中关村支行

中国邮政储蓄所
卡号：6221 8810 0004 0752 651
户名：王英
开户地：北京市海淀区双榆树邮局

汇款地址：北京市中关村邮局008信箱
邮政编码：100080
收款人：黑客防线邮购部

淘宝网店
网址：http://shop35607533.taobao.com/

提示：为了防止与其他读者的汇款混淆，建议在所汇金额后存入一尾数，如39、86、39、92等，以便与他人汇款区别。银行汇款可能需要身份证，邮局不需任何证件即可汇款。如有疑问，欢迎致电010-62145877，您的疑问会得到详细解答。

2009年黑客防线投稿指南

2009年，黑防将继续提升技术高度，力创中文网络安全技术第一月刊，争创世界黑客技术前沿杂志。让我们以此共勉，共同进步！

◆首发漏洞

要求原创必须首发，杜绝一切二手资料。主要内容集中在各种0Day公布、讨论，欢迎第一手溢出类文章，特别欢迎主流操作系统和网络设备的底层0Day，稿费从优，可以洽谈深度合作。有深度合作意向者，直接联系总编辑binsun20000@hotmail.com。

◆本月焦点

针对时下的热点网络安全技术问题展开讨论，或发表自己的技术观点、研究成果，或针对某一技术事件做分析、评测。

◆漏洞攻防

利用系统漏洞、网络协议漏洞进行的渗透、入侵、反渗透、反入侵，包括比较流行的第三方软件和网络设备0Day的触发机理，对于国际国内发布的POC进行分析研究，编写并提供优化的exploit的思路和过程；同时可针对最新爆发的漏洞进行底层触发、ShellCode分析以及对各种平台的安全机制的研究。

◆TCP/IP缺陷研究（新增栏目）

与网络协议缺陷有关的强悍ARP欺骗攻击、隐蔽的XSS跨站利用，深度技术。急征深度技术分析和实例相佐的文章，特别欢迎发包速度变异的ARP欺骗攻击和结合脚本漏洞XSS跨站利用深入技术分析和防范解决方案。同时欢迎利用网络协议缺陷的DDOS攻击、盗链下载等方面的技术研究。

◆脚本攻防

利用脚本系统漏洞进行的注入、提权、渗透；国内外使用率高的脚本系统的0Day以及相关防护代码。重点欢迎利用脚本语言缺陷和数据库漏洞配合的注入以及补丁建议；重点欢迎PHP、JSP以及HTML边界注入的研究和代码实现。

◆工具与免杀

巧妙的免杀技术讨论；针对最新Ant:杀毒软件、HIPS等安全防护软件技术的讨论。特别欢迎突破安全防护软件主动防御的技术讨论，以及针对主流杀毒软件文件监控和扫描技术的新型思路对抗，并且欢迎在源代码基础上实现免杀和专杀的技术论证！最新工具，包括安全工具和黑客工具的新技术分析，以及新的使用技巧的实例讲解。

◆渗透与提权

欢迎非Windows系统、非SQL数据库以外的主流操作系统的渗透、提权技术讨论，特别欢迎内网渗透、摆渡、提权的技术突破。一切独特的渗透、提权实际例子均在此栏目发表，杜绝任何无亮点技术文章！

◆溢出研究

对各种系统包括应用软件漏洞的详细分析，以及底层触发、ShellCode编写、漏洞模式等。

◆外文精粹

选取国外优秀的网络安全技术文章，进行翻译、讨论。

◆网络安全顾问

我们关注局域网和广域网整体网络防／杀病毒、防渗透体系的建立；ARP系统的整体防护，较有效的不损失网络资源的防范DDOS攻击技术等相关方面的技术文章。

◆搜索引擎优化

主要针对特定关键词在各搜索引擎的综合排名、针对主流搜索引擎的多关键词排名的优化技术。

◆编程解析

各种安全软件和黑客软件的编程技术探讨；底层驱动、网络协议、进程加载与控制技术探讨和Virus高级应用技术编写；以及漏洞利用的关键代码解析和测试。重点欢迎C/C++/ASM自主开发独特工具的开源讨论。目前特别欢迎Win32平台的批处理、VBS的技术应用和其他主流平台的解析语言的利用。(此栏目文章一定要在文章最后注明使用的平台和编译程序的准确名称和版本）特色程序可以与我部深度合作，深度合作请直接联系总编辑binsun20000@hotmail.com。

◆密界寻踪

关于算法、完全破解、硬件级加解密的技术讨论和病毒分析、虚拟机设计、外壳开发、调试及逆向分析技术的深入研究。

投稿格式要求：

1）技术分析来稿一律使用Word编排，将图片插入文章中适当的位置，并明确标注“图1”、“图2”；

2）攻防技术操作稿件必须使用文章加录像方式投稿，便于读者在阅读文章后，可通过录像进一步的学习相关技术。作者也可单独采用操作录像投稿。操作录像请务必使用屏幕录像专家制作，录像中桌面务必使用黑防统一桌面（黑防桌面下载地址http://www.hacker.com.cn/down/view_14689.html）。录像制作完毕后，将录像EXE文件、录像中涉及的程序和内容说明文本一起压缩即可；

3）在稿件末尾请注明您的详细联系地址和银行账户，包括你的真实姓名、准确的邮寄地址和邮编、QQ或者MSN、邮箱、常用的笔名等，方便我们发放样刊和稿费。

4）投稿方式和和周期：

采用E-Mail方式投稿，投稿mail：du_xing_zhe@yahoo.com.cn。

投稿后，稿件录用情况将于1～3个工作日内回复，请作者留意查看。每月10日前投稿将有机会发表在下月杂志上，10日后将放到下下月杂志，请作者朋友注意，确认在下一期也没使用者，可以另投他处。限于人力，未采用的恕不退稿，请自留底稿。

重点提示：严禁一稿多投。无论什么原因，如果出现重稿——与别的杂志重复——与别的网站重复，将会扣发稿费，从此不再录用该作者稿件。

5）稿费标准：《黑客防线》实行优稿优酬的稿费评定标准，范围在60－200元／千字。我刊率先尝试改革技术期刊稿费评定办法，一改百年不变的按照字数计酬的制度，将按照如下权重评定稿酬：

完全按照字数计算的基本稿费：60元／千字

按照论坛讨论的反响的公评稿费：0－40元／千字

按照技术水平的高低的技术稿费：0－100元／千字

请发稿作者立即将网站ID注册为发稿笔名，通过投稿信箱通知我们开通权限。从2008年4月开始，论坛不对普通用户开放，仅提供给作者和部分会员技术交流。

6）稿费发放周期：

目前，一般发稿后3个月发放稿费，维持一个周期，主要为了杜绝一稿多投和选题重复抄袭。但是，随着作者队伍的稳定，将会逐渐缩短周期。一旦发现抄袭和向外发布，将扣发稿费，拒绝采用同一作者来稿。特约作者稿费当月发放，稿费从优。欢迎更多的专业技术人员加入到这个行列。

7）稿费发放办法：

采用邮局邮寄和银行卡发放，支持境内各大银行借记卡，不支持信用卡。中国银行卡要提供开户行的具体名称。请准确随稿件附带银行卡号和姓名。更改稿费发放卡号请将文章名、作者名、笔名、刊发期数等信息 发到投稿信箱，勿提供给个人，因为要依据信件凭证到财务备案。稿费发放信息http://www.hacker.com.cn/forum/view_119018.html。

8）关于样刊。一般在出刊当月3日前发出样刊，3日后的时间由邮政当局控制。由于平邮寄出，有时会丢失，所以，从2008年开始，采用挂号方式邮寄。挂号邮寄丢失率较低，但是在邮局邮路滞留时间更长。如果当月收不到，请直洽黑防网站值班客服QQ：812712489。

黑客防线杂志社联系办法：

投稿信箱： du_xing_zhe@yahoo.com.cn

值班编辑： QQ675122680

样刊查询： QQ318569389　**电话：** 010-62145877

稿费查询： http://www.hacker.com.cn/forum/view_118337.html

深度技术合作： binsun20000@hotmail.com

黑防杂志第3期光盘目录

黑防前沿

微软中关村市场反盗版只会铩羽而归?
克服模仿和山寨必须要有创新
提前三年进入"全民笔记本时代"

江湖心声

《十则成功誓言》成功誓言之五
成为编程高手的八大奥秘

黑防集训营

1)编程<编程之声>
使用WININET函数写下载功能
完成端口的部分代码
获取系统目录
2)入侵<兵不血刃>
简单分析IFrame漏洞
编写变形的Shellcode实战篇
冷眼看Wins远程溢出漏洞
3)病毒<毒力毒行>
中美安全人员联合挫败Conficker蠕虫大规模攻击
"犇牛"始作俑者曝光 曾因制作"中华吸血鬼"被捕
警惕:"广告炸弹"木马贼喊捉贼
4)防护<安全防御阵线>
UNIX与类UNIX系统安全检查笔记
一切为了安全——禁用USB设备
为Linux蒙上Windows面纱让黑客自投罗网

兵器天下

旁注入查询器

集成有多个网站的入侵小工具,便于更方便的进行踩点工作。

ZionEdit v2.2.4

一个为程序员设计的语言编辑器,支持C/C++、Java、C#、Perl、Ruby、Python、Lisp、SQL(MySQL)、CSS、HTML(+JavaScript、PHP等)、Fortran77-9X、Makefile、ASM和批处理文件。ZionEdit的编程功能非常丰富,具备体积小、高可靠性和高易用性。告别了传统的工具栏编辑方式,最大化编写界面,从而令编写代码更高效、更轻松。

XP变脸王

XP变脸王能让电脑桌面变得绚丽多彩,极富个人魅力,给您带来与众不同的视觉享受。拥有比XP自身更多更强大的界面定制功能,能彻底改变Windows XP界面内的各个元素,实现超炫系统图标、彩色浏览器、动态鼠标指针、动态桌面、个性开机画面、个性化文件夹、可视风格、XP风格应用程序等,并且还附带了大量的桌面素材,界面直观,使用方便,一个电脑新手都可以轻松打造一个属于自己的Windows! 更重要的是它不会影响电脑运行速度,不占用系统资源!

InstDrv

驱动加载工具。一个比较好用的驱动安装、卸载工具,可以方便的把驱动程序安装或卸载掉,本程序更多的应用于动态调式驱动前的加载操作中。其功能有:执行加载、启动、停止、卸载驱动操作;支持文件拖拽打开;支持程序窗口总在最前显示;操作后有详细的中文提示信息;支持命令行控制台调用;提升程序自身的权限和优先级。

娱乐时空

1)精彩预告
-降临之子
-渺渺
-骑劫地下铁
-天使与魔鬼
-疯狂的赛车
2)热门歌曲
-没有如果
3)语音遨游
-NBA
4)游戏娱乐
-太平洋之战

就业不难，找黑防培训

我第一次也是最后一次用这个广告语来作为卷首标题，希望读者朋友能够原谅并且理解我的用意：黑防真的想在就业难的恐慌之中，带给我们的读者一份镇定、一份从容和一份希望。这就是我们一直倡导的，技术，才是真正的立命之本。作为一种边缘技术之源，黑防责无旁贷地要为刚走出学校大门的朋友分一点忧，尽一点力，做一点实事。这也是黑防积累9年的技术实例，充分体现在技术奉献上的一个走向，不仅仅在今天，而且在未来的漫长岁月。

我们常常说，人不要忌讳把自己当成商品。改革开放之初，就出现的所谓人才市场这个名词，其用意就是把人作为一种商品放到市场上交易。既然是商品就要走向市场，走向市场就要符合市场规律。市场规律的一条经典要义就是：左右市场的是一只看不见的手。这只手，就是供求关系。供大于求的时候，商品就会贬值甚至滞销。这就引发出市场规律的第二条要义：差异化营销。就是说，你要想畅销，就要有差异，与众不同。大学生就业就是这样，一样的教学大纲，一样的教学模式，一样的考试流程，造就出来的人才都是一样的，在市场不好情况下就会出现降价和滞销，就是所谓的就业难。

那么，解开这道难题的唯一方法，就是要想办法产生差异化的特质和知识结构，而这个特质是学校常规的教学体制培养不出来的。你会发现，应聘程序员的队伍如此庞大，你如果没有一点与众不同的特点，很难应聘成功。我曾经在一家公司的人事部看到上百封的求职简历，人事经理几乎一秒钟一份地毫不犹豫地否定着，最终一份被他选中的，就是简历上面×年×月在《黑客防线》上发表xxxxx文章，他毫不犹豫地说，能在这样的杂志上发表文章，说明自学过学校没有教的东西，立即转到技术主管通知面试了。我实在没看出来我在场对他有任何影响，他完全是凭借自己的经验来履行职责。这就说明了要有一个与众不同的知识结构的重要性。大的方面来看，网络信息安全肯定是差异化比较高的领域，我看到这样的公司几乎常年都在招聘，但是适合的很少，究其原因，常规教育没有培养出他们需要的人才。

基于此，我们采取突击式的训练方式，其实就是为学员解决了常规教育所留下来的缺项——这个缺项恰恰就是用人单位所需要的长项。

所以，我们很自信的说，你要是正常的大学相关专业毕业，进过我们10个月的培训，就不仅仅能够就业，而且是高薪就业。为什么？因为没有一所大学把C++、脱壳破解、逆向分析、汇编这几门课程搭配起来教你，而这个知识结构，正是所有安全厂商、反病毒厂商最需要的人才。产品设计前要分析别人的产品，病毒库更新要分析样本，新的防范手段要分析新的病毒木马。总之，就是要分析然后在产品上实现防范程序。这样的人才就会构成公司的核心竞争力，不管市场萧条不萧条，高薪就业没有问题。而且，我们具备权威的推荐和广泛的厂商合作，形成了紧缺人才的就业直通车。

说到最后，希望关注我们的就业培训体系。我们想要做的，就是给追随黑防钻研技术的有志者，找到高薪出路。

总编辑 Binsun
Email: binsun20000@hotmail.com

黑客防线
www.hacker.com.cn
目录 2009/03
——最新攻击与防范技术研究

总 编 辑　孙彬
技术总监　贺生涛
总 编 室　徐生震（主任）
值班编辑　矫若龙 675122680(QQ)
执行主编　吴田锋
技术编辑　刘流 蝴蝶 脚本小子 侯文辉
光盘编辑　猪猪

投稿信箱　du_xing_zhe@yahoo.com.cn
技术合作　binsun20000@hotmail.com

VIP 客服　赵季枝 318569389(QQ)
客服电话　010-62145877

设计制作　李志华 黄婷

发 行 部　王英
电　　话　010-62141359
传　　真　010-62141360
邮购电话　010-62145877

出　　版　齐鲁电子音像出版社
版　　号　7-90044754-7
定　　价　12.5 元（光盘 + 书）

首发漏洞

本月焦点

漏洞攻防

脚本攻防

工具与免杀

渗透与提权

外文精粹

网络安全顾问

CONTENTS 目录

编程解析

密界寻踪

编读互动

本期技术精华

搜狗浏览器特殊URI欺骗漏洞
Windows驱动漏洞的发现与利用
让360的实时监控形同虚设
浅析LxBlog V6变量未初始化漏洞
打造手机通话记录获取木马
枚举CPU的全局描述符表
内核清零杀进程
内核模式简单实现进程监控
SSDT Hook拦截远程线程的创建
基于有序规则的加密与信息隐藏技术
控制子系统进程间通信监控进程与线程创建
DR.COM木马的设计与实现
用Debug API踩点正确注册码

重要通知

1)《黑客防线2009精华本》已经开始发行,在当地买不到的读者,请直接联系网站3号客服812712489办理邮购,或者直接到淘宝站购买。最近加入网站VIP会员就赠送本书。

2)为了应对全国就业难的问题,黑防网站、编辑部、技术团队联合推出的就业培训正在招收学员,请适合自己的读者尽快登录网站,查看详细说明,实现自己的快速就业。

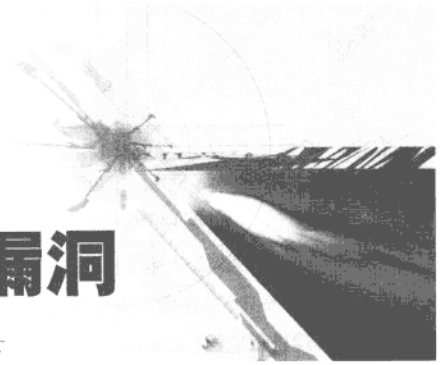
3)对于有些读者提出本刊内容技术水准太高,不易读懂的问题,编辑部建议这样的读者先加入网站的VIP会员,这个会员区相当于一个读友俱乐部,在这里可以广泛交流,很快就能够达到阅读黑防杂志的水平。

4)有些作者反应,刊发稿件后并没有授予网站的技术团队称号,这是因为我们有一个考核机制,首先看技术水平,投稿要有一定数量,还要看在论坛的公开版的活跃程度等等,综合考评后才能开通原创区权限,授予技术团队头衔。总之,这个团队宁缺毋滥。

5)对于购买杂志困难的读者,也建议直接联系网站客服,加入会员会赠送杂志,采用快递和挂号邮寄的方法可以保证每期准时看到最新技术研究信息和成果。

前置知识：VC
关键词：漏洞、搜狗浏览器、URI

搜狗浏览器特殊URI欺骗漏洞



文/图 爱无言

无意中在下载软件的时候，发现搜狗也发布了浏览器，从网页的宣传界面上看，这款浏览器界面还十分另类，于是，抱着极大的兴趣下载安装了搜狗浏览器。

搜狗的大图标形式的浏览器设计风格视觉效果十分不错，安装之后我是爱不释手，虽然这样，我还是比较怀疑这款出色的浏览器是不是存在漏洞，因为在以前的时候，腾讯TT浏览器就被我发现过典型的栈溢出漏洞，其实它还有一堆溢出漏洞，只是危害很小，也就没有再发布了。

简单测试了一下搜狗浏览器对于过长URL地址的处理，还算不错，没有发现什么问题，不过好像在某些情况下会导致浏览器处于忙状态，反应迟钝，暂且不去研究了，估计是内存消耗问题。想到以前测试浏览器的一些方法，我开始由简单到复杂开始检查该浏览器，没想到第一个测试就发现搜狗浏览器出现问题了。这个问题属于一个欺骗形式的漏洞，也就是说浏览器的使用者往往会被浏览器本身的解析行为所误导。我们先不忙着说漏洞的影响，先来看看这个漏洞的具体表现吧。

打开记事本，在里面写入如下一段代码，保存为1.htm文件。用搜狗浏览器打开，从表面来看，这段代码应该的执行方式是，当使用者点击http://www.baidu.com这个超链接时，浏览器应该马上跳转到百度网站的首页上，可是如果你在搜狗的浏览器中点击这个超级链接后，会发现最终访问的不是百度首页，而是我的Blog地址！

```
<html>
<title>Sogouexplorer URI 欺骗漏洞</title>
<head></head>
<body>
POC:
<a href="http://www.baidu.com@hi.baidu.com/digexploit">http://www.baidu.com</a>
</body>
</html>
```

问题就出在代码href后的那段地址链接。仔细看这里的超链接地址写法与以往的不一样，在百度首页地址的后面我们添加了一个"@"字符，这个字符在以往的URI地址中主要是用来产生类似FTP服务器登录的，也就是说往往浏览器会将"@"字符后面的地址当作一个目的地址，然后将"@"字符前面的数据当作发送到目的地址的登录信息。可是浏览器需要适当的正确辨别"@"字符前面的数据信息是不是合法的登录信息格式，不能一股脑的当作信息处理而直接访问"@"字符后面的地址。现在搜狗的浏览器问题就发生在这里，它没有正确鉴别"@"字符前的信息而是一味的访问"@"字符后的地址，这就导致看似一个正确的百度超级链接反而在点击之后变成了访问我的博客地址。

如果将这个漏洞结合在网络钓鱼中利用，那么浏览器的使用者就会被恶意欺骗，那么他的银行账号、密码什么之类的就完全可以被恶意获取到了。

在测试中我还发现，傲游浏览器也存在这个问题，主要原因是无论傲游还是搜狗浏览器使用的都是IE内核，但是IE7以上的版本却不存在该问题，在点击这种欺骗链接后，IE没有任何反应。而同样的测试代码在火狐浏览器中会给出一个警告提示，提示用户该访问URI可能存在欺骗嫌疑。由此可看，这种URI欺骗还没有引起某些开发者的足够重视，也许这种漏洞的性质还没有像缓冲区溢出漏洞那样可怕吧！

前置知识: VC
关键词: 漏洞、驱动、IOCTL

Windows驱动漏洞的发现与利用

文/ Anibal Sacco 译/ riusksk(泉哥)

设备驱动程序是Windows模块的一个基本组成部分,它可以与硬件进行交互,或者执行内核操作。通过用户层接口,用户模式下的进程可以与驱动程序建立一个沟通渠道,从而以预定的方式发送和接收数据。

近来新的驱动程序漏洞不断地被暴出,已经不是什么新鲜事了,毕竟驱动中总是会有漏洞的,只是只有少数人去挖掘它而已。而现在很少有程序员致力于驱动程序和Ring 0软件的开发了,这也是可以理解的,毕竟这是一项有难度的工作。一直以来这方面的官方资料都很不完善,而一些团体组织又常常隐藏他们的研究发现,但还是有很多未公开的函数被发现,并被文档化,这些都是经一些团体组织逆向分析Windows程序后,接着再去寻找一些被泄漏的源代码而得来的。基于这个原因,很长时间里(甚至直至今日),很多驱动程序开发者都把精力投入到程序的稳定性及可靠性上面,以致有时忽略了一些非常基本的安全检测。Windows驱动程序漏洞暴露于一些可在用户模式下正常执行的进程,比如MS Word、MS Messenger,甚至是计算器。这与在Ring0进程下利用漏洞获取执行权限不同,它隐含着最大的可执行权限,通过该漏洞,攻击者就可能控制或破坏整个系统。

本文主要针对Windows驱动程序建立通讯渠道的方式进行讲述,为后面解释如何通过它们具体的设计特点来处理一些常见的驱动程序漏洞作个铺垫。同时,我也将讲述一些利用这类漏洞获得代码执行权限的攻击方式。

驱动程序结构

驱动程序不像用户模式下的进程,它并没有充分利用它所有的功能来执行。通常情况下,它主要是通过DriverEntry()函数来构造的,相当于动态链接库中的DllMain()函数。因为只有当驱动程序被加载时,它才进行内存映射。但当操作系统加载模块时,它仅执行一次。

下面简单看一下这个函数,它主要负责驱动程序的初始化,比如创造符号链接(帮助用户模式下的进程打开句柄),以及"Function Dispatch Table"(在DRIVER_OBJECT结构体中包含的一个指针列表,而DRIVER_OBJECT是用于实现驱动程序的真实功能,用户模式进程通过IOManager来调用这些指针,进而执行在内核中希望执行的代码)的初始化。

DRIVER_OBJECT

每个驱动程序加载时,就意味着内核数据结构需要调用DRIVER_OBJECT。驱动对象指针是驱动程序中DriverEntry()函数的一个输入参数,当DriverEntry()函数被调用时就会被初始化。DRIVER_OBJECT结构如下:

```
typedef struct _DRIVER_OBJECT
{
SHORT Type;
```

```
SHORT Size;
PDEVICE_OBJECT DeviceObject;
ULONG Flags;
PVOID DriverStart;
ULONG DriverSize;
PVOID DriverSection;
PDRIVER_EXTENSION DriverExtension;
UNICODE_STRING DriverName;
PUNICODE_STRING HardwareDatabase;
PFAST_IO_DISPATCH FastIoDispatch;
LONG * DriverInit;
PVOID DriverStartIo;
PVOID DriverUnload;
LONG * MajorFunction[28];
} DRIVER_OBJECT, *PDRIVER_OBJECT;
```

其中,MajorFunction数组指针会被驱动程序初始化,用于指向它自身的函数。这个结构相当重要,因为这些函数将被IO Manager调用,这主要依赖于来自用户模式下的各类IRP请求。例如使用CloseFile()这个API函数关闭驱动程序时,Majorfunction[IRP_MJ_CLOSE]指向的函数指针将会被调用。

IRPs

根据MSDN的说明"Microsoft Windows家族操作系统通过发送I/O请求数据包(IRP)与驱动程序通信。封装IRP的数据结构不仅描述I/O请求,而且在I/O请求经过处理它的驱动程序时维护请求的状态信息。因为该数据结构具有两个用途,所以 IRP 可以定义为: I/O请求的容器,或者线程独立的调用堆栈。"

现在回顾一下前面的内容:用户模式的进程是通过请求包来与驱动程序进行通讯的,这些请求包告诉驱动程序应该调用MajorFunction数组指针中的哪个函数,必要时可对用于发送和接收数据的缓冲区进行管理。这些请求包被称为IRP Major requests。

IOCTLs (IRP_MJ_DEVICE_CONTROL) 请求

这是一个关键请求,驱动程序常通过DeviceIoControl来发送和接收数据,其原型如下:

```
BOOL WINAPI DeviceIoControl(
  _in HANDLE hDevice,
  _in DWORD dwIoControlCode,
  _in_opt LPVOID?lpInBuffer,
  _in DWORD nInBufferSize,
  _out_opt LPVOID lpOutBuffer,
  _in DWORD nOutBufferSize,
  _out_opt LPDWORD lpBytesReturned,
  _inout_opt LPOVERLAPPED lpOverlapped
);
```

当用户层通过已打开的驱动程序句柄去调用DeviceIoControl函数时,它先将一个指向IRP object的指针作为参数,然后调用MajorFunction[IRP_MJ_DEVICE_CONTROL]中定义的函数。这个函数将会通过DeviceIoControl这个数据结构来接收重要数据,比如输入缓冲区、输出缓冲区,及其相应的长度。依靠这些已定义的方式,IOManager可以采用各种不同的方式对缓冲区进行处理。

驱动程序可以使用下列三种不同的I/O方式 buffered、direct或者neither。当使用一个内核模式驱动程序去创建一个设备对象时,可以在设备对象中的Flags域指定想使用的I/O方式。这里可以将DO_BUFFERED_IO与DO_DIRECT_IO中的一个值赋予Flag域,或者也可以不选择指定的方式。在这种情况下,我们称驱动程序将Flag指定为neither方式。通过驱动程序的读写分发例程,这种方式可以影响分配给设备对象的I/O读写请求。

这里讲的主要是METHOD_NEITHER方式。当最后XXX bits被打开时,IO_Manager就会使用这种方法。但这也存在一个特殊问题,与其它I/O方式不同的是(IO_Manager使用其它方式来管理缓冲区,这对驱动程序进行内核缓冲区的分配是相对安全的),在这里IO_Manager并未对缓冲区进行任何检测。这仅需要通过DeviceIOControl去调用指向驱动函数的用户层缓冲区指针,就可以绕过任何检测,对内核区域进行非法访问。

驱动漏洞

我们先不谈用户模式与内核模式请求方式的选择,先来看看这些方式中的相同之处:

1)用户进程打开一个句柄去访问驱动程序。

2)通过DeviceIoControl结构中input buffer存储的数据以及指定的output buffer来发送一个IOCTL请求。

3)驱动程序接收IOCTL,并根据Inputbuffer中的数据进行一些操作,同时返回数据给Output buffer。

4）用户进程接收数据，并继续运行。

当驱动程序并未对来自用户层的指针进行充分地检测时（或者一点也未对其进行检测），问题就出现了。如果检测不当，驱动程序将会检索输出缓冲区中的数据，并直接将其写入用户进程指定的内存，同时依据该地址来发送数据，这可能会写入到一个无效内存地址，从而导致蓝屏Blue Screen of Death（BSOD），或者被攻击者利用。下面将会对此进行讲述，通过修改特定的内核模式结构，从而允许未授权的用户进程在Ring0下执行任意代码，这样做的目的就是为了提升权限。

在各种不同情况下，普遍不一样的是驱动程序在输出缓冲区中返回的地址，但在大多情况下，这个地址并不是都那么重要。有时仅需要一点想象力，就可以将可预测值写入或替换掉内核中的内存数据，从而获得执行代码的权限。

为了更清楚地解释这个问题，下面举个漏洞实例（CVE-2007-5756），是关于Winpacap 4.x的一个驱动程序漏洞（Winpacap是基于Windows操作系统下的一个软件包，为网络链路层的实时访问提供方便）。

看看下面驱动程序例程的主要部分，如前所述，该例程中实现了用于初始化MajorFunctions数组指针的驱动函数。在这里对我们最为重要的是IRP_MJ_DEVICE_CON-TROL entry的初始化，它提供了NPF_IoControl函数，用于处理来自用户层的IOCTLs。

```
    NTSTATUS DriverEntry( IN PDRIVER_OBJECT
DriverObject, IN PUNICODE_STRING
    RegistryPath)
    {
    ......
    // 设置设备驱动程序入口指针
    DriverObject->MajorFunction[IRP_MJ_CREATE] =
NPF_Open;
    DriverObject->MajorFunction[IRP_MJ_CLOSE] =
NPF_Close;
    DriverObject->MajorFunction[IRP_MJ_READ] =
NPF_Read;
    DriverObject->MajorFunction[IRP_MJ_WRITE] =
NPF_Write;
    DriverObject->MajorFunction[IRP_MJ_DEVICE_
CONTROL]=NPF_IoControl;
    DriverObject->DriverUnload = NPF_Unload;
```

漏洞函数代码如下：

```
    NTSTATUS NPF_IoControl(IN PDEVICE_OBJECT
DeviceObject,IN PIRP Irp)
    {
    ......
    IrpSp = IoGetCurrentIrpStackLocation(Irp); ①
    FunctionCode=IrpSp->Parameters.DeviceIoControl.
IoControlCode;
    Open=IrpSp->FileObject->FsContext;
    ......
    case BIOCGSTATS: //function to get the cap-
ture stats ②
    TRACE_MESSAGE(PACKET_DEBUG_LOUD,
"BIOCGSTATS");
    if(IrpSp->Parameters.DeviceIoControl.
OutputBufferLength < 4*sizeof(UINT)) ③
    {
    SET_FAILURE_BUFFER_SMALL();
    break;
    }
    pStats = (PUINT)(Irp->UserBuffer); ④
    pStats[3] = 0; ⑤
    pStats[0] = 0;
    pStats[1] = 0;
    pStats[2] = 0;  // Not yet supported
    for(i = 0 ; i < NCpu ; i++) ⑥
    {
    pStats[3] += Open->CpuData[i].Accepted;
    pStats[0] += Open->CpuData[i].Received;
    pStats[1] += Open->CpuData[i].Dropped;
    pStats[2] += 0;  // Not yet supported ⑦
    }
    SET_RESULT_SUCCESS(4*sizeof(UINT));
    break;
```

在①处，IRP Stack Pointer通过IoGetCurrentIrpStackLocation进行检索，该结构还包含了用户层的其它参数。IOCTL参数存储在FunctionCode变量中，在"switch-case"语句中用于选择将进行的操作。在这里，我们感兴趣的数值是②BIOCGSTATS。

在③处，检测OutputBufferLength参数，以确定是否可将数据写入（四个符号整数），若不行，则跳出"switch-case"语句。

在④处，获取用户层地址，以作为输出缓冲区。接着，在⑤处我们就可以看到漏洞本身了。该驱动程序将16个0写入用户模式下指定的地址，但并未对其做任何检测。在正常情况下，该地址是一个用户地址范围内有效的缓冲

区指针，但这里可以提供一个无效地址，以触发访问异常，从而在Ring0下执行操作，进而导致蓝屏(BSOD)。

在⑥处是一个循环，用于在数组中迭代添加数值。在整个循环中，除了第三个DWORD值，其它值均置0。接下来，离开switch- case语句，继续执行其它操作。

通过上面的讲解，现在大家应该可以利用该漏洞致使整个系统崩溃了。这仅需要发送一个IOCTL去指定一个无效的内核空间地址作为输出缓冲区就可以了，比如地址0x80808080。下面我们更深入地探究一下。

通过该漏洞，我们可以在一些可写的内核地址中修改16 bytes。在这种情况下，我们无法确切地知道是哪个数值，但不需要进一步分析，我们就可以知道第三个DWORD值总为0。那么现在的问题就是，该如何在这一数值中获得代码执行的权限呢？

篡改SSDT

System Service Descriptor Table(SSDT)是内核中的一个数据结构，其中包含了函数指针列表。当一些用户模式下特定的API函数想要在内核空间执行操作时，这些函数指针就会被系统服务分配器调用。例如，当在用户进程中调用AddAtom()函数时，在DLL中的代码就会负责验证一些参数，然后利用Int 2e或者sysenter(依赖于Windows版本)切换上下文到Ring0，从而通过分配表中的索引号来引用函数。接着系统服务分配器转向对应的指针重发(有时终止它，或者甚至修改它)用户模式参数。在内核调试器KD中查看一下SSDT，可以发现指针指向的地址在各Windows版本中始终保持不变，如下所示

```
kd> dds poi(KeServiceDescriptorTable)
.....
8050104c  805e8f86
nt!NtAccessCheckByTypeResultListAndAuditAlarmByHandle
80501050  8060a5da nt!NtAddAtom
80501054  8060b84e nt!NtQueryBootOptions
80501058  805e0a08 nt!NtAdjustGroupsToken
8050105c  805e0660 nt!NtAdjustPrivilegesToken
80501060  805c9684 nt!NtAlertResumeThread
80501064  805c9634 nt!NtAlertThread
80501068  8060ac00 nt!NtAllocateLocallyUniqueId
8050106c  805aa088 nt!NtAllocateUserPhysicalPages
80501070  8060a218 nt!NtAllocateUuids
80501074  8059c910 nt!NtAllocateVirtualMemory
.....
```

通过这个漏洞，利用我们可控制的数据去修改SSDT表中的指针，使其指向用户空间中分配的内存区域，从而发动攻击(被广泛使用的攻击方式之一)。在这种情况下，我们已经知道了作为输出缓冲区的地址，驱动程序将会写入：8 bytes的未知数据(写入的内容实际上很明显，但我们不需要知道它)；4 bytes 0；4 bytes未知数据。

由上可知，可预测值只有4个0，但我们如何通过数值0来篡改指针呢？这里有个小技巧，就是将代码置入在页0中分配的内存里面。这个可以通过1中的基址来调用NtAllocateVirtualMemory，因为这个函数是在低内存页(lower page)中分配数值，它是从0x0开始分配内存的。

```
PVOID Addr=(PVOID)0x1;
NtAllocateVirtualMemory((HANDLE)-1, &Addr, 0, &Size, MEM_RESERVE|MEM_COMMIT|MEM_TOP_DOWN, PAGE_EXECUTE_READWRITE);
```

利用这四个0值，我们就可以篡改需要的入口地址。我们只需发送BIOCGSTATS IOCTL去触发漏洞，然后通过驱动程序来修改函数地址即可。之后被选择的函数指针将会被0值替换掉，从而指向我们分配的缓冲区。

```
DeviceIoControl(hDevice, 0x9031, lpInBuffer, nInBufferSize, (Address of the selected function - 8), nOutBufferSize, &ret, NULL)
```

但是这种方法有个小问题，因为我们破坏了四个连续的函数指针，因此必须精心地挑选好要被修改的函数。这些函数被调用的次数要少，而且并不是很重要的函数才行。我们可以附加调试器去设置一些断点，然后去查找那些最不经常被调用的函数。

最后我们只需调用用户模式下对应的函数，但该函数需要使系统服务分配器去调用kernel-patched- pointer才行。通过这种方法，我们就可以获得我们构造的用户层代码的执行权限了。正常情况下，0x0地址中的代码将会以已知的方式去提升指定进程的执行权限，但这已经不属于本文的主题了。

前置知识：无
关键词：手机、蓝牙、DOS

再谈手机攻防

文／ heiben

手机与我们的生活密不可分。有了手机我们不仅可以打电话、发短信，还可以做许多事情，比如手机上WAP、聊天、蓝牙游戏等。与此同时，随着手机功能的增强，手机也面临着越来越多的各种攻击。

蓝牙攻击

现在许多手机都内置蓝牙功能（小灵通除外）。蓝牙是一种无线通信标准，允许蓝牙装置在一定范围内传输文件、照片与其他数据的协议。因此我们要实施蓝牙攻击就必须熟悉蓝牙通信标准。一般蓝牙通信设置都可以划分为两大类：一种是主设备与主设备连接，另一种是主设备与从设备连接。一般来说主设备都是具有键盘的，例如PDA和电脑就是主设备，而从设备呢？就是没有键盘输入的，例如蓝牙耳机。而蓝牙连接一般的步骤都分为以下几步：

1）发现：设备一方扫描另一方设备。

一般来说手机蓝牙模式分为关、开可发现或全部可见、隐藏等四种模式。一般来说黑客都可以对开可发现或全部可见、隐藏三种模式进行攻击。

2）配对：设备间交换配对码等信息。

蓝牙的配对程序相对于计算机上的TCP/IP协议在互联网上的连接，它允许两个正试图连接的蓝牙设备进行互相交换地址、配对码等重要信息。听起来配对码好像和密码有相同的地方，的确，配对码可被我们看似密码的东西，因为许多时候一些蓝牙耳机都是缺省配对码的。试问一下，假如你的蓝牙耳机的配对码是很复杂的数字，你会愿意输入吗？而且许多时候我们的配对码都是十分短的，例如：0000、1111，或者1234，都是十分容易就被破解的。

3）绑定：设备交换密钥与绑定连接。

当绑定完成后，设备就会自动生成一个密钥并绑定，说明两种设备间的连接只能用于这两个设备，其他设备不能干扰或者窥视这种连接。反而言之，如果两设备建立了蓝牙连接，那么第三设备也就无法窃听数据传输了。

蓝牙攻击的目前主要有以下几种：蓝劫、修改通讯录、蓝牙垃圾短信、蓝窃、蓝牙后门、蓝牙蠕虫、蓝牙打印、蓝牙扫描、其他攻击、短配对码或缺省配对码、随机挑战答案生成器、中间人、信息广播、强暴攻击、拒绝服务（DOS）、单元密钥、拟人化等。

本文将为大家介绍一些容易上手的，且国内外也比较主流的攻击方法。蓝劫攻击有时又被称之为蓝牙对象交换（OBEX）强推攻击，著名的红獠牙就是这种强推攻击工具，大家可从http://www.atstake.com了解。匿名免费短信也属于蓝劫攻击的一种，我们可以使用微软的Outlook Express进行匿名发短信，比如我们可以发恶意短信说什么中大奖，然后拨打什么电话之类（大家千万不要学哦）。这里向大家介绍一些工具，首先是信息收集工具btscanner，它可以在不需要连接的情况下就质询设备。BlueSniff可以在一定范围内发现隐藏的蓝牙设备。BlueSpam在PalmOS上运行，搜索蓝牙设备并向它们发送随机文件。另外还有三款工具推荐给大家，一是Bluefish监视系统，每次发现蓝牙设备都可以描绘出它们的位置，跟踪它们的运动；二是Blueprint，一个识别蓝牙设备的工具；

三是Blooover，一款移动电话安全检查工具，运行在J2ME电话上，可以在一定范围内提取易受攻击的敏感数据，执行BlueBug攻击。

拒绝服务攻击

死亡之Ping是最普通的计算机攻击方式，而手机的L2CAP层允许蓝牙工具向另一工具发出回音，所以和Ping一样的攻击就存在了。我们可以在Linux系统下运行L2ping工具，例如执行"l2ping -f 00:00:00:00:00:00"。我们在这里分为远程畸形字符短信攻击、本地畸形字符短信攻击、非正常MIDI文件攻击、非正常格式化字符串攻击。一般来说，远程畸形字符短信攻击都会发送一些不正常短信，例如"%Hacker"，必须有双引号，且头字母要大写。而本地畸形字符短信攻击则如"hacker"，必须有双引号。非正常MIDI文件攻击则是发送一些含有视频、声频或者图片的MMS。虽然这些只是一些最普通的短信攻击，可能对于一些新的手机类型已经不再适用了。

电话窃听

电话窃听无论在电影中还是在现实生活中，都的确是存在的。许多诺基亚手机其实都有隐藏的听筒菜单，通常它是不可应用的，然而我们可利用短路连接手机的针脚来激活这一功能。先将手机关闭，然后短路连接3、4针脚，激活前面所说的功能，最后重启手机找出新增的菜单，就能实现自动接听功能，只要将铃声设为静音模式，一部间谍手机就出来了。

安全防护

手机虽然存在这样那样的漏洞，但并不能因为一个不好而将其全部抹杀，就像网络一样。那么我们怎样才能像在电脑面前一样，用得游刃有余之余，又以防出身未捷身先死呢？

1）在任何时候都要将蓝牙关闭，只有在迫不得已的情况下才将蓝牙打开或隐藏模式。

2）更改手机名称，在公共场所上，攻击者很容易在你的手机上找到详细的、隐私的信息。

3）不要接收蓝牙传输的不知名的短信或文件，它们可能是病毒蠕虫，也可能是其他攻击，攻击者仅仅使用OE，或在诺基亚上运行Punk SMS这款工具就可以发送匿名SMS到其他手机用户。

4）在进行手机蓝牙配对时，不要在公共场合与不认识的手机配对。

5）设置较长，容易记忆但难猜中的PIN。

手机攻防还有许多许多，未有详尽只心感遗憾，有错误之处还请大家多多包涵。以上所涉及到的工具已随文提供，有兴趣的读者可以测试看看。

（编辑提醒：本文涉及的工具，已收录入本期光盘杂志相关栏目；也可以到黑防官方网站下载）

前置知识：无

关键词：漏洞、Anti-Virus、硬链接

AV之祸

文/图 046569@【8K7】

对于大多数人来说，Anti-Virus（反病毒）程序早已是系统的必备软件了。可把自身的安全完全交给反病毒工程师终究让人有些不放心，于是一个邪恶的想法& 测试诞生了。

试验目标及难点

"最危险的地方就是最安全的地方"。要想隐藏，能混进杀软行列是最好的办法。可如

今杀软早已经告别一个taskkill命令就可以结束掉进程的年代了。无论是主动防御还是自我保护模块，都是不小的麻烦。这时我们有两种选择，一是像硫磺岛战役中的美军，强攻硫磺岛却遭遇顽强抵抗，最后成为太平洋战争中登陆一方的伤亡超过抵抗登陆方的唯一战例；二是如同《超人归来》中那个内裤外穿男一样，混迹于平常人之中，关键时刻大显身手。很显然，我比较喜欢后者。所以我们的任务很简单，写入杀软目录，甚至感染杀软文件以达到潜藏的目的。

测试过程

首先我们需要一个趁手的工具，好在微软已经帮我们准备好了。下面简单说明一下。

Fsutil是唯一由完全了解Windows的高级用户所使用的高级工具。Fsutil是可用于执行多种与FAT和NTFS 文件系统相关的任务(例如管理重解析点、管理稀疏文件、卸载卷或扩展卷)的命令行实用程序。由于Fsutil功能非常强大，因而只有完全掌握Windows XP的高级用户才能使用它。此外，必须作为管理员或管理员组的成员登录才能使用Fsutil。利用Fsutil可以轻松创建硬链接，方法很简单："fsutil hardlink create <新文件名> <现有文件名>"。

Hardlink(硬链接)相当于一个文件的别名。比如硬盘上原来存在一个文件1.exe，你可以为它创建一个2.exe的硬链接。当删除其中任何一个之后，事实上文件内容并不会被删除掉，仍然可以用其他的名称来访问这个文件。只有当最后一个指向这个文件内容的文件名被删除之后，文件内容才会被删除。也就是说，一个文件的hard link跟此文件本来的名称并没有任何本质上的区别。需要注意的是，因为每个分区上都可能有相同的存储位置地址，所以hard link必须跟被link的文件在同一个分区上。

现在大家想到了什么没有？对，AV很可能依靠路径去匹配文件，包括主动防御和自我保护！因此思路很简单，创建一个硬链接，对它进行操作！还记得马奇诺防线是怎么被突破的吗？绕过去的！我们甚至用两条DOS命令就能完成替换工作。我们的杀软终于完成了"从被一条命令干掉"上升到"被两条命令干掉"的高度了。

听起来似乎进展很顺利，可以结束了。可惜事实并非如此，我们要做的工作还有很多。比如我们要替换哪个文件呢？比如用户系统不是Windows XP怎么办？再比如其他可能碰到的意外情况。下面我们来一个一个解决。

问题一：替换什么文件。个人的建议是替换升级文件。杀软一定要升级，替换它可以保证我们狸猫换太子后，狸猫可以做一做太子(被执行)。这点很重要，但一定要注意的是，你的程序要有独占性，不能反复被执行，否则杀软频繁升级，会让用户卡到郁闷继而格盘，那你就前功尽弃了。

问题二：用户系统不是Windows XP。我们可能碰到Vista甚至是Windows 7。这个比较麻烦了，系统的易用性和安全性成反比，Vista+UAC那么难用，确实安全得有些过分，以至于我暂时也没想到好办法突破。但微软接受了用户批评Vista难用的意见，改良了UAC机制，让其在微软最新操作系统Windows 7中不再那么烦人，于是安全性也降低了。我们来看一个微软已知但却打算拖到RC1才发布补丁的漏洞。

"The default UAC setting in Windows 7 is: "Don't notify me when I make changes to Windows settings. What this really means is: "Don't notify me when Microsoft applications require administrator rights."

即Windows 7中UAC的默认设置是当我改变Windows设置的时候不要通知我。而它的真正意思是当微软程序需要管理权限的时候不要通知我。

而问题就出在rundll32上。它处于白名单中，换句话说，它申请高特权不需要UAC确认(权限继承类漏洞)。那么问题简单了，我们只需要编写一个DLL实现相应功能就可以了。在之前的我们已经知道了，Fsutil运行的时候需要管理权限，现在问题迎刃而解了。我们只需要关注以下几个问题：

1) 创建硬链接的API:CreateHardLink，用来代替不好控制的DOS语句。

2) Rundll32的接口标准，以便可以被调用。

3) 硬链接要求处在同一盘符内。