快速通道

文档分类
- 红盟公告
- 新手上路 <=
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- 安全技术
- 业界动态

本类热门
- ftp使用经典
- 一个木马的查杀过程
- 基于arp欺骗的网络攻击程序(BtNet.exe)
- 终端服务全攻略
- 握着你的“手”清除DLL后门
- 巧用asp木马和KV2004得到管理员权限

一个木马的查杀过程

提交文章： galaxy
提交日期： 2003-08-26
文章属性： 原创
文档类别： 新手上路
浏览次数： 今12次/总29430次

galaxy@redtx.net

写这个文章的目的，是让大家知道，遇到木马后应该怎么办
因为这个木马是我第一次接触，我想我杀木马的经历，应该会对大家有帮助的吧
至于这个木马的具体情况，来源，功能等详细内容，我没研究，反正zer说要写一篇文章出来的

昨天（8月25日）晚上，zer4tul给我了个木马（exelinks.exe），让我来试试，呵呵。
收到后，运行，没有任何反应（废话！！）
然后，我查看进程，先把exelinks进程杀掉，然后运行regedit
……
……
……
找不到这个文件！！！
我ft
难道是exe文件被关联无法打开了？
查找，居然是这个文件丢了（zer4tul那里没丢，看来不具备共性）
只好运行regedt32.exe了，呵呵
发现在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run下面多了一个
网络服务 启动程序名字为 svchoost.exe，这个当然是他了，删除，呵呵

这个时候，我重起系统，运行regedt32，发现run里又有了他，杀进程，删除文件

既然又有，说明还有启动的来源，来源是什么？对了，我不是运行了regedt32吗？这个可是exe文件啊。

查看.exe内容，写的exefile，没问题
查看exefile内容，shell\open\command里的内容为
winnt/system32/exelinks.exe %1 %*，呵呵，果然关联了
修改回来，%1 %*
另外根据zer4tul提示，这个程序原始名字是windowssend.exe
我在winnt/system32/start 目录找到了它
估计是想做个自动启动吧，呵呵，这个文件也删除掉
重起系统，看进程，看注册表，一切正常了，这样，木马就杀完了

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net