

Backdoor.Win32.IRCBot.aba分析报告 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/462/2021_2022_BackdoorW_c100_462998.htm 病毒名称：Backdoor.Win32.IRCBot.aba 病毒类型：后门类 文件MD5：

8F6CB8D895E60387FE3E41377D0F0D3F 文件长度：270,848 字节 感染系统：windows 98以上版本 加壳类型：未知壳 病毒描述：该病毒为后门类，病毒运行后复制自身到系统目录，并重命名为mozilla.exe，并删除自身。修改注册表，添加启动项，以达到随机启动的目的。把自身副本文件添加到防火墙默认放行列表。连接到IRC服务器，等待受控。行为分析：1、病毒运行后衍生文件：%System32%\mozilla.exe 2、修改注册表，添加启动项，以达到随机启动的目的：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 键值：字符串："Mozilla" = "C

:\Windows\System32\mozilla.exe" 3、连接网络，下载相关病毒文件信息：协议：TCP 地址：www.tgiweb.com 端口：80 下载文件：radi.exe 4、把自身副本文件添加到防火墙默认放行列表：

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\WINDOWS\system32\mozilla.exe 键值：字符串："C:\WINDOWS\system32\mozilla.exe:*:Enabled

:mozilla" 5、连接到IRC服务器，等待受控，命令说明如下：IRC命令如：/join [该闲聊室的密码] /nick /quit [退出连接的理由] 对目标主机的操作：下载文件 发起拒绝服务

(DDOS) 攻击 执行IRC命令 执行系统扫描 注释： %Windir% WINDODWS所在目录 %DriveLetter% 逻辑驱动器根目录 %ProgramFiles% 系统程序默认安装目录 %HomeDrive% 当前启动系统所在分区 %Documents and Settings% 当前用户文档根目录 %Temp% 当前用户TEMP缓存变量；路径为：

%Documents and Settings%\当前用户\Local Settings\Temp

%System32% 是一个可变路径；病毒通过查询操作系统来决定当前System32文件夹的位置；Windows2000/NT中默认的安装路径是 C：\Winnt\System32；Windows95/98/Me中默认的安装路径是 C：\Windows\System；WindowsXP中默认的安装路径是 C：\Windows\System32. 清除方案：1、使用安天木马防线可彻底清除此病毒（推荐），请到安天网站下载

：www.antiy.com . 2、手工清除请按照行为分析删除对应文件，恢复相关系统设置。推荐使用ATool（安天安全管理工具），ATool下载地址：www.antiy.com

或http://www.antiy.com/download/index.htm . （1）使用安天木马防线或ATool中的“进程管理”关闭病毒进程（2）强行删除病毒文件 %System32%\mozilla.exe （3）恢复病毒修改的注册表项目，删除病毒添加的注册表项

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 键值：字串："Mozilla" = " C

: \Windows\System32\mozilla.exe "

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C：\WINDOWS\system32\mozilla.exe 键值：字符串："C：\WINDOWS\system32\mozilla.exe：*：Enabled

：mozilla" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com