网络安全

安全技巧（三）

小未 主编

目　录

注册机破解法的原理和应对方法.....1
防止黑客用 TTL 值鉴别你的系统.....6
解析危险的特洛伊木马.....7
软件暴力破解的原理和应对方法.....18
关于 Linux 网络安全的内在限制.....23
动态 IP 地址的捕获及其应用.....25
缓冲区溢出与病毒攻击.....36
非法探取密码的原理及其防范.....40
堆溢出的研究.....45
高级扫描技术及原理介绍.....49
利用反弹技术进行 DDoS 攻击的分析.....59
RpcPatch 蠕虫代码点评.....63
Linux 系统下病毒的研究.....73
利用远程注册表加强系统安全.....100
防范网络嗅探.....113

注册机破解法的原理和应对方法

认识注册机破解法

顾名思义，写注册机来破解软件注册的方法，就是模仿你的注册码生成算法或者逆向注册码验证算法而写出来的和你一模一样的注册机。如果被写出注册机，你的软件只好免费了。或者你必须更换算法，但以前注过册的合法用户都得被迫更换注册码了。

Cracker 要写注册机必须详细研究你软件的验证模块，这必须先将你的软件脱壳，再反汇编或者用调试器跟踪。市面上许多加壳和保护软件都吹嘘不可能被脱壳，但到目前为止没有一个软件兑现了自己的诺言。由于 CPU 最终执行的都是有效指令，所以等你的程序自解压完成后再从内存中 Dump 出来就可以实现脱壳。因此不要在壳上面花很多功夫，因为没有这个必要。

第一招：制造假相

反汇编和调试器跟踪都是不可能防止的，因为所有的 Win32 程序都必须通过 API 来调用 Windows 系统中的关键 DLL 的（如 Kernel32.dll、GDI32.dll 等），然而 API 是可以 Hook 的。我们只能从自己的代码着手来保护我们的劳动果实了。

为了自己调试和以后维护的方便，我们一般采用有意义的名字给我们的函数命名，可这给了 Cracker 可乘之机。例如这样的函数是什么意思大家应该一目了然吧? IsRegistered（），IsLicensed（），LicenseVerify（），CheckReg（）……这样 Cracker 就可以轻松地从数千个函数

中找到他的目标——你的注册码校验函数!而且破解 Delphi 编写的软件还有一件 TMG 小组的破解利器——DeDe。它可以轻松地看到你软件里的 Form、Unit 和函数名，还可以反汇编一部分代码，更可以和 Win32DASM 合作反汇编更多的代码，对 Delphi 编出的程序威胁极大。

为了不给 Cracker 创造温馨舒适的破解环境，要故意混乱（Obfuscate）我们的代码，将软件中所有的函数名全部替换成随机生成的函数名。例如 Func_3dfsa_fs32zlfv 这个函数是什么意思?恐怕只有天知道了。网上有现成的代码混乱器，按你使用的编程语言的种类可以找到一些。但要注意，只有当你要发布软件时才使用它，而且一定注意备份源代码。否则，当你看不懂你自己的代码时就着急了 :)

第二招：用公匙，并改名

另外，一定要使用公开密匙算法保护你的软件。RSA、DSA 和 ElGamal 之类的算法都可以从网上找到。但注意：将你算法单元中所有涉及到算法名称的字符串全部改名。避免被 Cracker 发现你用的算法而模仿写出注册机来!你还可以张冠李戴，明明用的 DSA，将名字全部替换成 RSA。

其它算法，如对称算法和 Hash 算法也要注意改名，否则这样：

EncryptedCode=Blowfish（MD5（UserName），MD5（Key））；

//你的加密算法，使用了 Blowfish（对称算法）和 MD5（Hash 算法）

虽然那些 Cracker 不了解 Blowfish 和 MD5 算法的原理，也不会逆向推测它们，但他们了解你的校验算法的

流程和算法名，便可马上从网上找到类似的 Blowfish 和 MD5 算法包，从而模拟你的软件仿造出注册机。

如果你用不常见的，算法如 Skipjack（NASA 美国航天局标准算法）、LOKI、3-WAY、Safer 之类不出名但保密程度很高的算法，并且全部改名，这样就会伤透他们脑筋了。

当然，最好把 Hash 算法也全部改名，会给他们制造更多的困难。但注意，MD5 和 SHA 之类的 Hash 初始值会被 Cracker 从内存中找到，这样他就知道你用的 Hash 了。所以建议同时使用 MD5 的变形算法 Ripe-MD（RMD）128 或 160 或其它的 Hash，如 Tiger、Haval 等算法。

第三招：阻止别人调试

还有一点，调试器对我们的威胁很大，我们不会让 Cracker 们舒舒服服地使用 SoftICE、TRW 或 OllyDbg 来调试我们的程序。除了常用的 MeItICE 方法外，这里我给一个笔者写的方法：

{检查自己的进程的父进程是否为 Explorer.exe，否则是被调试器加载了}

{不过注意，控制台程序的父进程在 WinNT 下是 Cmd.exe!}

{注意加载 TlHelp32.pas 单元}

```
procedureCheckParentProc；
var//检查自己的进程的父进程
Pn:TProcesseNtry32；
sHandle:THandle；
H，ExplProc，ParentProc:Hwnd；
Found:Boolean；
```

```
Buffer:array[0..1023]ofChar；
Path:string；
begin
H:=0；
ExplProc:=0；
ParentProc:=0；
//得到 Windows 的目录
SetString（Path，Buffer）
GetWindowsDirectory（Buffer，Sizeof（Buffer）-1））；
Path:=UpperCase（Path）+'\EXPLORER.EXE'；//得到 Explorer 的路径
//得到所有进程的列表快照
sHandle:=CreateToolHelp32SnapShot（TH32CS_SNAPALL，0）；
Found:=Process32First（sHandle，Pn）；//查找进程
whileFounddo//遍历所有进程
begin
ifPn.szExeFile=ParamStr（0）then//自己的进程
begin
ParentProc:=Pn.th32ParentProcessID://得到父进程的进程 ID
//父进程的句柄
H:=OpenProcess（PROCESS_ALL_ACCESS，True，Pn.th32ParentProcessID）；
end
elseifUpperCase（Pn.szExeFile）=Paththen
ExplProc:=Pn.th32ProcessID；//Explorer 的 PID
Found:=Process32Next（sHandle，Pn）；//查找下一
```

个

end；

//父进程不是 Explorer，是调试器……

ifParentProc<>ExplProcthen

begin

TerminateProcess（H，0）；//杀之!除之而后快也!:）

//你还可以加上其它什么死机代码来消遣消遣这位可爱的 Cracker:）

end

end

你可以在 Delphi 或者 VC 中试试，这样可以把 Delphi 和 VC 杀掉了，因为你现在用的是 Delphi 和 VC 的内置调试器来运行你的程序。调试的时候你还是把它的注释删掉吧，发布时别忘记激活哟!

第四招：保护字符串

最后一个问题，这也是一个非常重要的问题：保护你的字符串!字符串在注册模块中非常重要!当一个富有经验的 Cracker 破解你的软件时，首先做的就是窃取你的字符串。比如他会输入错误的注册码，得到你关于错误注册码的提示，通常是“无效的注册码，请重新输入!”或者“Invalidkey（pleaseinputagain）”等等，然后用 OllyDbg 进行断点调试或者用 WinDASM、IDAPro 等静态分析工具在被他脱壳后的程序中查找那个字符串，找到后进行分析。因此，请一定加密你的字符串!使用时再临时解密出来，而且要尽量少使用消息提示框，避免被 Cracker 找到漏洞。加密字符串不需要太复杂的算法，随便找一个快速的对称算法就可以了。

最后提醒大家一句，不要在加密上花太多的功夫!

你应该把更多的时间和精力都用来完善你的软件，这样会更合算。借用一位前辈的话来忠告大家吧：花点时间考虑你自己的软件,看看它是否值得保护?如果没人用你的软件，保护也就没有意义了，不要过高估计你的软件“对世界的重要性”!

防止黑客用 TTL 值鉴别你的系统

大家都知道，通过 PING 和 TRACERT 程序能判断目标主机类型。ping 最主要的用处是检测目标主机是否连通。TRACERT 利用 ICMP 数据包和数据包头部中和 IP 数据包中 TTL 的值，防止数据包不断在 IP 互联层上永远不终止地循环

许多入侵者首先会 PING 一下你的机子，如见到 TTL 值为 128 就可以认为你的系统为 WINDOWNT/2000，如果 TTL 值是 32 则认为目标主机操作系统是 WINDOWS95/98，如果 TTL 值是 255/64 就认为是 UNIX/LIUX 操作系统。既然入侵者那么相信 TTL 值所反映出的结果，那么我们可以修改 TTL 的值，入侵者就无法入侵电脑了。

操作步骤：

一、打开记事本文件，编写批处理文件命令：

@echoregedit4＞＞changeTTL.reg

@echo.＞＞changeTTL.reg

@echo[HKEY_LOCAL_MACHINE\SYSTEM\CURRENT_CONTROLSET\SERVICES\TCPIP\PARAMETERS]＞＞＞changeTTL.reg

@echo"defaultTTL"=dword:"000000">>changeTTL.reg

@regedit/s/cchangeTTL.reg

二、把编写好的程序另存为为扩展名为.bat **的批处理文件，点击这个文件，你的操作系统这时的** TTL **值会被修改为** ff**，即** 10 **进制的** 255**，也就是说把你的操作系统人为地改成了** UNIX **系统了，同时，在该文件所在的文件夹下会生成一个名为** changeTTL.reg **的注册表文件，如果你想运行完这个批处理文件后而不产生** changeTTL.reg **文件，可以在此处理文件的最后一行加入** deltree/ychangeTTL.reg **就可以无须确认自动删除** changeTTL.reg **文件了。**

解析危险的特洛伊木马

一位客户的 PC **出现了奇怪的症状，速度变慢，**CD-ROM **托盘毫无规律地进进出出，从来没有见过的错误信息，屏幕图像翻转，等等。我切断了他的** Internet **连接，然后按照对付恶意软件的标准步骤执行检查，终于找出了罪魁祸首：两个远程访问特洛伊木马——一个是**CultoftheDeadCow **臭名昭著的** BackOrifice**，还有一个是不太常见的** TheThing**。在这次事件中，攻击者似乎是个小孩，他只想搞些恶作剧，让别人上不了网，或者交换一些色情资料，但没有什么更危险的举动。如果攻击者有其他更危险的目标，那么他可能已经从客户的机器及其网络上窃得许多机密资料了。**

特洛伊木马比任何其他恶意代码都要危险，要保障

安全，最好的办法就是熟悉特洛伊木马的类型、工作原理，掌握如何检测和预防这些不怀好意的代码。

一、初识特洛伊木马

特洛伊木马是一种恶意程序，它们悄悄地在宿主机器上运行，就在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。一般而言，大多数特洛伊木马都模仿一些正规的远程控制软件的功能，如 Symantec 的 pcAnywhere，但特洛伊木马也有一些明显的特点，例如它的安装和操作都是在隐蔽之中完成。攻击者经常把特洛伊木马隐藏在一些游戏或小软件之中，诱使粗心的用户在自己的机器上运行。最常见的情况是，上当的用户要么从不正规的网站下载和运行了带恶意代码的软件，要么不小心点击了带恶意代码的邮件附件。

大多数特洛伊木马包括客户端和服务器端两个部分。攻击者利用一种称为绑定程序的工具将服务器部分绑定到某个合法软件上，诱使用户运行合法软件。只要用户一运行软件，特洛伊木马的服务器部分就在用户毫无知觉的情况下完成了安装过程。通常，特洛伊木马的服务器部分都是可以定制的，攻击者可以定制的项目一般包括：服务器运行的 IP 端口号，程序启动时机，如何发出调用，如何隐身，是否加密。另外，攻击者还可以设置登录服务器的密码、确定通信方式。

服务器向攻击者通知的方式可能是发送一个 email，宣告自己当前已成功接管的机器；或者可能是联系某个隐藏的 Internet 交流通道，广播被侵占机器的 IP 地址；另外，当特洛伊木马的服务器部分启动之后，它还可以直接与攻击者机器上运行的客户程序通过预先定义的端口进行通信。不管特洛伊木马的服务器和客户程序如何

建立联系，有一点是不变的，攻击者总是利用客户程序向服务器程序发送命令，达到操控用户机器的目的。

特洛伊木马攻击者既可以随心所欲地查看已被入侵的机器，也可以用广播方式发布命令，指示所有在他控制之下的特洛伊木马一起行动，或者向更广泛的范围传播，或者做其他危险的事情。实际上，只要用一个预先定义好的关键词，就可以让所有被入侵的机器格式化自己的硬盘，或者向另一台主机发起攻击。攻击者经常会用特洛伊木马侵占大量的机器，然后针对某一要害主机发起分布式拒绝服务攻击（DenialofService，即 DoS），当受害者觉察到网络要被异乎寻常的通信量淹没，试图找出攻击者时，他只能追踪到大批懵然不知、同样也是受害者的 DSL 或线缆调制解调器用户，真正的攻击者早就溜之大吉。

二、极度危险的恶意程序

对于大多数恶意程序，只要把它们删除，危险就算过去，威胁也不再存在，但特洛伊木马有些特殊。特洛伊木马和病毒、蠕虫之类的恶意程序一样，也会删除或修改文件、格式化硬盘、上传和下载文件、骚扰用户、驱逐其他恶意程序，例如，经常可以看到攻击者霸占被入侵机器来保存游戏或攻击工具，用户所有的磁盘空间几乎都被侵占殆尽，但除此之外，特洛伊木马还有其独一无二的特点——窃取内容，远程控制——这使得它们成为最危险的恶意软件。

首先，特洛伊木马具有捕获每一个用户屏幕、每一次键击事件的能力，这意味着攻击者能够轻松地窃取用户的密码、目录路径、驱动器映射，甚至医疗记录、银行帐户和信用卡、个人通信方面的信息。如果 PC 带有

一个麦克风，特洛伊木马能够窃听谈话内容。如果 PC 带有摄像头，许多特洛伊木马能够把它打开，捕获视频内容——在恶意代码的世界中，目前还没有比特洛伊木马更威胁用户隐私的，凡是你在 PC 前所说、所做的一切，都有可能被记录。

一些特洛伊木马带有包嗅探器，它能够捕获和分析流经网卡的每一个数据包。攻击者可以利用特洛伊木马窃取的信息设置后门，即使木马后来被清除了，攻击者仍可以利用以前留下的后门方便地闯入。

其次，如果一个未经授权的用户掌握了远程控制宿主机器的能力，宿主机器就变成了强大的攻击武器。远程攻击者不仅拥有了随意操控 PC 本身资源的能力，而且还能够冒充 PC 合法用户，例如冒充合法用户发送邮件、修改文档，当然还可以利用被侵占的机器攻击其他机器。二年前，一个家庭用户请我帮忙，要我帮他向交易机构证明他并没有提交一笔看来明显亏损的股票交易。交易机构确实在该笔交易中记录了他的 PC 的 IP 地址，而且在他的浏览器缓冲区中，我也找到了该笔有争议的交易的痕迹。另外，我还找到了 SubSeven（即 Backdoor_G）特洛伊木马的迹象。虽然没有证据显示出特洛伊木马与这笔令他损失惨重的股票交易直接有关，但可以看出交易发生之时特洛伊木马正处于活动状态。

三、特洛伊木马的类型

常见的特洛伊木马，例如 BackOrifice 和 SubSeven 等，都是多用途的攻击工具包，功能非常全面，包括捕获屏幕、声音、视频内容的功能。这些特洛伊木马可以当作键记录器、远程控制器、FTP 服务器、HTTP 服务器、Telnet 服务器，还能够寻找和窃取密码。攻击者可

以配置特洛伊木马监听的端口、运行方式，以及木马是否通过 email、IRC 或其他通信手段联系发起攻击的人。一些危害大的特洛伊木马还有一定的反侦测能力，能够采取各种方式隐藏自身，加密通信，甚至提供了专业级的 API 供其它攻击者开发附加的功能。由于功能全面，所以这些特洛伊木马的体积也往往较大，通常达到 100 KB 至 300KB，相对而言，要把它们安装到用户机器上而不引起任何人注意的难度也较大。

对于功能比较单一的特洛伊木马，攻击者会力图使它保持较小的体积，通常是 10KB 到 30KB，以便快速激活而不引起注意。这些木马通常作为键记录器使用，它们把受害用户的每一个键击事件记录下来，保存到某个隐藏的文件，这样攻击者就可以下载文件分析用户的操作了。还有一些特洛伊木马具有 FTP、Web 或聊天服务器的功能。通常，这些微型的木马只用来窃取难以获得的初始远程控制能力，保障最初入侵行动的安全，以便在不太可能引起注意的适当时机上载和安装一个功能全面的大型特洛伊木马。

随便找一个 Internet 搜索网站，搜索一下关键词 RemoteAccessTrojan，很快就可以得到数百种特洛伊木马——种类如此繁多，以至于大多数专门收集特洛伊木马的 Web 网站不得不按照字母顺序进行排列，每一个字母下有数打甚至一百多个木马。下面我们就来看看两种最流行的特洛伊木马：BackOrifice 和 SubSeven。

■BackOrifice

1998 年，CultoftheDeadCow 开发了 BackOrifice。这个程序很快在特洛伊木马领域出尽风头，它不仅有一个可编程的 API，还有许多其他新型的功能，令许多正规

的远程控制软件也相形失色。BackOrifice2000（即 BO2K）按照 GNUGPL（GeneralPublicLicense）发行，希望能够吸引一批正规用户，以此与老牌的远程控制软件如 pcAnywhere 展开竞争。

但是，它默认的隐蔽操作模式和明显带有攻击色彩的意图使得许多用户不太可能在短时间内接受。攻击者可以利用 BO2K 的服务器配置工具可以配置许多服务器参数，包括 TCP 或 UDP、端口号、加密类型、秘密激活（在 Windows9x 机器上运行得较好，在 WindowsNT 机器上则略逊一筹）、密码、插件等。

图一：BO2K 的客户端界面

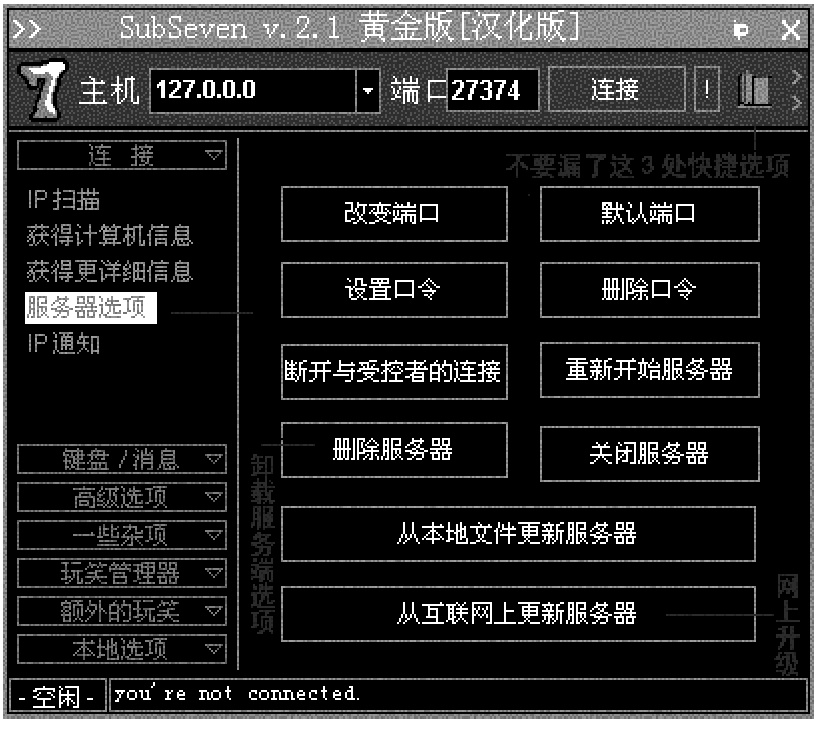
BackOrifice 的许多特性给人以深刻的印象，例如键击事件记录、HTTP 文件浏览、注册表编辑、音频和视频捕获、密码窃取、TCP/IP 端口重定向、消息发送、远程重新启动、远程锁定、数据包加密、文件压缩，等等。

BackOrifice 带有一个软件开发工具包（SDK），允许通过插件扩展其功能。

默认的bo_peep.dll插件允许攻击者远程控制机器的键盘和鼠标。就实际应用方面而言，BackOrifice对错误的输入命令非常敏感，经验不足的新手可能会使它频繁地崩溃，不过到了经验丰富的老手那里，它又会变得驯服而又强悍。

■SubSeven

SubSeven可能比BackOrifice还要受欢迎，这个特洛伊木马一直处于各大反病毒软件厂商的感染统计榜前列。SubSeven可以作为键记录器、包嗅探器使用，还具有端口重定向、注册表修改、麦克风和摄像头记录的功能。图二显示了一部分SubSeven的客户端命令和服务器配置选项。



图二：SubSeven服务器配置

SubSeven 具有许多令受害者难堪的功能：攻击者可以远程交换鼠标按键，关闭/打开 CapsLock、NumLock 和 ScrollLock，禁用 Ctrl+Alt+Del 组合键，注销用户，打开和关闭 CD-ROM 驱动器，关闭和打开监视器，翻转屏幕显示，关闭和重新启动计算机，等等。

SubSeven 利用 ICQ、IRC、email 甚至 CGI 脚本和攻击发起人联系，它能够随机地更改服务器端口，并向攻击者通知端口的变化。另外，SubSeven 还提供了专用的代码来窃取 AOLInstantMessenger（AIM）、ICQ、RAS 和屏幕保护程序的密码。

四、检测和清除特洛伊木马

如果一个企业网络曾经遭受病毒和 Email 蠕虫的肆虐，那么这个网络很可能也是特洛伊木马的首选攻击目标。由于木马会被绑定程序和攻击者加密，因此对于常规的反病毒软件来说，查找木马要比查找蠕虫和病毒困难得多。另一方面，特洛伊木马造成的损害却可能远远高于普通的蠕虫和病毒。因此，检测和清除特洛伊木马是系统管理员的首要任务。

要反击恶意代码，最佳的武器是最新的、成熟的病毒扫描工具。扫描工具能够检测出大多数特洛伊木马，并尽可能地使清理过程自动化。许多管理员过分依赖某些专门针对特洛伊木马的工具来检测和清除木马，但某些工具的效果令人怀疑，至少不值得完全信任。不过，Agnitum 的 Tauscan 确实称得上顶级的扫描软件，过去几年的成功已经证明了它的效果。

特洛伊木马入侵的一个明显证据是受害机器上意外地打开了某个端口，特别地，如果这个端口正好是特洛伊木马常用的端口，木马入侵的证据就更加肯定了。一

旦发现有木马入侵的证据，应当尽快切断该机器的网络连接，减少攻击者探测和进一步攻击的机会。打开任务管理器，关闭所有连接到 Internet 的程序，例如 Email 程序、IM 程序等，从系统托盘上关闭所有正在运行的程序。注意暂时不要启动到安全模式，启动到安全模式通常会阻止特洛伊木马装入内存，为检测木马带来困难。

大多数操作系统，当然包括 Windows，都带有检测 IP 网络状态的 Netstat 工具，它能够显示出本地机器上所有活动的监听端口（包括 UDP 和 TCP）。打开一个命令行窗口，执行“Netstat-a”命令就可以显示出本地机器上所有打开的 IP 端口，注意一下是否存在意外打开的端口（当然，这要求对端口的概念和常用程序所用的端口有一定的了解）。

图三显示了一次 Netstat 检测的例子，检测结果表明一个 BackOrifice 使用的端口（即 31337）已经被激活，木马客户程序使用的是远程机器（ROGERLAP）上的 1216 端口。除了已知的木马常用端口之外，另外还要特别留意未知的 FTP 服务器（端口 21）和 Web 服务器（端口 80）。

图三：检测到激活的 BO

但是，Netstat 命令有一个缺点，它能够显示出哪些