Dvldr32 蠕虫病毒的检测与控制

Detecting and Controlling Dvldr32 Worm Virus

徐雅斌 （辽宁工学院计算机学院 121001）

摘 要：本文着重介绍了新近发现并已对网络造成灾难性危害的蠕虫病毒的危害和传播机理，以及不同级别人员的检测和控制手段。

1 病毒的主要危害

2003年3月7日以来，一种破坏力很强的蠕虫病毒（暂且以攻击程序的名字命名为Dvldr32）开始在网络上传播，控制了大量口令设置不安全的Windows NT/2000/ME/XP系统，对网络造成了很大破坏。目前主要的网络运行商已经在网络上对其传播途径进行了控制，但被感染的系统、可能被感染的系统仍然大量存在，而且类似的蠕虫攻击有可能再度发生。

计算机感染Dvldr32蠕虫病毒后，定期的随机选择两个C类地址进行扫描（TCP 445端口），如果目标机器上存在弱口令帐号（如：administrator账号口令为空），蠕虫便会利用该帐号将自身远程注入到目标系统中。该蠕虫会在感染的系统上留下可以远程控制的后门（TCP 5800,TCP 5900），并通过互联网聊天协议（IRC，TCP 目标端口6667）与境外的服务器进行通信。

该蠕虫的扫描和传播可能造成网络严重拥塞，主要表现为大量 TCP 445端口的扫描、TCP 6667端口的通信。另外，网络流量监测结果表明IP协议字段为 255（IP 头标的第9个字节）的流量增大也与Dvldr32蠕虫的感染有关。

2 病毒传播机理分析

dvldr32.exe,采用ASPASK压缩，该程序由MS VC 6.0编写。

该文件中以资源的形势，包含了2个可执行文件，其中一个为sysinternals所发布的著名行命令网络工具psexec（psexec本身包含一个名为psexesvc的程序，此前版本分析报告有误），蠕虫的制作者使用了最新版本的psexec.exe（Ver 1.31.0.0），但采用了UPX进行压缩，使文件大小从122,880字节缩小到了36,352字节。

另外一个程序为一个不常见安装工具所制作的安装包，该安装包中包括5个文件，其中3个文件(explorer.exe；VNCHooks.dll；omnithread_rt.dll)属于AT&T所发布的网管工具VNC, nc的3.3.3.9版本）。另外两个文件则是rundll32.exe、cygwin1.dll。其中cygwin1.dll由red hat发布，名称是Cygwin(r) POSIX Emulation DLL。用以对Linux移植到Windows下的程序进行支持。

文件之间调用关系如下：

```
explorer.exe
 ├ VNCHooks.dll
 └ omnithread_rt.dll
rundll32.exe
 └ cygwin1.dll
```

我们可以看出，对于explorer.exe；VNCHooks.dll；omnithread_rt.dll由于是VNC的一部分，已经无需分析，而网络上对于sysinternals的psexesvc和Remote process launcher的使用介绍也已经很多。cygwin1.dll是一个正常的动态连接库也无须分析。主要应该分析的是dvldr32.exe的执行部分和rundll32.exe。

dvldr32.exe:该程序运行后，会随机选择2个IP段，连接对方445的网络包，一旦连接成功，则用自身一份字典列表穷举对方超级用户口令，一旦破解成功，则将自身复制到目标系统中。

这个程序主要来实施发包进行网络感染操作。其大量的发包，也是造成网络瘫痪的主要原因。

感染操作需要特别说明一下，这个程序

远程投送两个文件其自身和inst.exe，其提供了两种投送方式，一种是通过psexec命令，一种是通过网络共享copy。通过psexec命令，可以完成文件copy和在远程主机的执行，但有可能投送失败。其对inst.exe还通过网络路径copy到英文windows的启动组下，使开机被执行，因此，inst.exe投送的成功率要比dvldr32.exe更高。这就造成几种情况，从而导致对目标系统的影响有所不同。

一些感染的主机，只发现了rundll32.exe而没有发现dvldr32.exe正是上述原因。

该程序将正常系统管理工作VNC作为后门，安装到用户系统下，通过修改配置，使VNC SERVER图标不在托盘中出现，不过由于VNC在系统锁定状态下不能连接，因此功能有所折扣。但由于该蠕虫有通知机制，即使VNC失效，等于已经告知了蠕虫作者，用户密码为空，或者在小字典档内。仍然可以导致入侵。

rundll32.exe：不是正常的MS系统的RUNDLL32，似乎为一个LINUX移植到WINDOWS平台的程序，目前已经可以分析出该程序的主要功能是向一个irc列表汇报已经感染主机的信息。

3 病毒的检测与控制

3.1 计算机用户的检测手段

如果出现以下特征之一，可以认为系统已经被感染：

（1）如果你的管理员口令为空或者容易猜测的口令，那么你的计算机系统可能已经被感染了，或者很容易受到感染；

（2）登录计算机系统，执行netstat -an命令，如果出现大量对外6667端口的TCP连接，或者正在监听TCP 5800和5900端口，那么你的系统可能被感染了，如下所示：

```
C:\>netstat.exe -n
Active Connections
Proto  Local Address  Foreign Address  State
TCP    x.x.x.x:1043   149.156.91.2:6667   CLOSE_WAIT
TCP    x.x.x.x:1045   198.65.147.245:6667  CLOSE_WAIT
.....
TCP    x.x.x.x:4811   198.65.147.245:6667   CLOSE_WAIT
TCP    x.x.x.x:4887   149.156.91.2:6667    CLOSE_WAIT
```

（3）如果系统目录下出现了以下文件，那么你的系统可能被感染了：

```
C:\> dir /O:D winnt\system32
C:\winnt\system32 的目录
...
2003-03-07  02:23   745,984 Dvldr32.exe
2003-03-08  19:53   61,440 PSEXESVC.EXE
2003-03-08  22:38   684,562 inst.exe
2003-03-08  22:38   36,352 psexec.exe
C:\>dir winnt\fonts /O:D
.....
2002-11-06  17:07   212,992 explorer.exe
2002-11-06  17:58   29,336 rundll32.exe
```

（4）检查注册表，如果增加了如下键值，则你的系统已经被感染了：

```
[HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Winows\ CurrentVersion\ Run
"TaskMan"="C:\\WINNT z\\Fonts\\rundll32.exe"
"Explorer"="C:\\WINNT\\ Fonts\\explorer.exe"
"messnger"="C:\\WINNT\\system32\\Dvldr32.exe"
```

3.2 计算机用户的控制手段

（1）为administrator设定安全的口令，检查其他所有用户口令的安全性；

（2）终止名为dvldr32.exe和rundll32.exe的进程；

（3）删除以下文件(%windir%是windows nt/2000的根目录，比如c:\winnt)：

```
%windir%\system32\dvldr32.exe
%windir%\fonts\explorer.exe
%windir%\fonts\omnithread_rt.dll
%windir%\fonts\VNCHooks.dll
%windir%\fonts\rundll32.exe
%windir%\system32\cygwin1.dll
%windir%\system32\ INST.exe
```

（4）清理注册表，删除3(4)中所提到的注册表中的键值；

（5）重新启动计算机。为防止类似事件发生，我们向Windows用户或系统管理员建议以下最基本的安全措施：

① 为操作系统安装最新的补丁；

② 为所有用户选择安全的、不用易猜测的口令；

③ 安装防病毒软件，并及时更新病毒定义码（最好每天一次）。

3.3 网络管理员的检测手段

如果你管理的网络出现了以下现象，那么网络中可能有计算机系统受感染了。

（1）网络性能显著下降；

（2）用流量分析工具（比如Unix平台的tcpdump、Windows平台的Sniffer pro），可以看到从网络内部发起的大量目标端口为445、6667的TCP数据包；

（3）用端口扫描软件（比如Linux平台的nmap），扫描你所管理的网络，如果有的计算机同时打开了TCP 445、5800、5900端口，则该计算机系统可能被感染了。

3.4 网络管理员的控制手段

在边界路由器或防火墙上配置访问控制规则，可以控制蠕虫传播的途径，起到保护内部网络、控制被感染系统扩散的目的。

例如，可以在cisco 路由器上的配置如下访问控制表:

```
access-list 110 deny tcp any any eq 445
! 用于控制蠕虫的扫描和感染;
access-list 110 deny tcp any any eq 5800
access-list 110 deny tcp any any eq 5900
! 用于防止受感染的系统被远程控制
access-list 110 deny tcp any any eq 6667
! 用于控制 受感染的系统与聊天服务器的通信
access-list 110 deny udp any any eq 1434
! 用于控制 Slammer worm
access-list 110 deny 255 any any
access-list 110 deny 0 any any
! 用于控制 IP Protocol 为255 和0 的流量
access-list 110 permit ip any any
```

4 结论

通过对蠕虫病毒的危害和传播机理进行分析，给出了计算机用户和网络管理员的有效检测和控制手段。通过所提供的方法即可有效消除病毒。但是我们必须注意蠕虫病毒和其他各种病毒还将不断变异，仍有可能在网络上蔓延和泛滥。因此作为用户来说，避免设置弱系统口令，并定期对查杀病毒软件进行升级，就可以在一定程度上预防和消除病毒。而对于网络管理员来说，经常性的检测网络信息流量和查看系统日志，定期扫描常用的网络端口，可及时发现异常情况的出现。如果能够经常进行分析和网上交流，就可以有效预防和解决病毒问题。

参考文献

1 Windows Internet 黑客防范与安全策略，SETH FOGIE.CYRUS PEIKARI，清华大学出版社。

2 http://WWW.20CN.Net。

3 http://www.ccert.edu.cn。