ARP 攻击现象和解决方案

“网吧传奇杀手”这种病毒使用 ARP 攻击方式，对内网的 PC 进行攻击，使内网 PC 机的 ARP 表混乱，导致内网某些 PC 机无法上网。目前路由器无法抵挡这种病毒的攻击，因为他们的攻击方式是攻击内网的 PC 机，只有请用户从内网的 PC 机下手防范。

这种病毒的显现为内网的部分 PC 机不能上网，或者所有人不能上网，最重要的特点是不可以上网的 PC 机的 ARP 表会乱掉，当我们发现内网某台 PC 无法上网时，进入到 DOS 窗体，然后输入命令 ARP -A 可以看到同一个 MAC 地址对应多个 IP 就是有问题了，具体介绍如下。

近期部分网吧反映频繁断线并且网速较慢，经过调查咨询后确认：这种情况是由于一种名为“网吧传奇杀手 Trojan.PSW.LMir.qh ” 的病毒爆发引起的。该病毒破解了《传奇 2》的加密解密算法，通过截取局域网中的数据包，然后分析《传奇》游戏通讯协议的方法截获用户的信息。运行这个病毒，就可以获得整个局域网中传奇玩家的详细信息，盗取用户帐号信息。

现象:

网吧短时间内断线(全断或部分断),在很短的时间内会自动恢复.这是因为 MAC 地址冲突引起的,当病机的 MAC 映射到主机或者路由器之类的 NAT 设备,那么全网断线,如果只映射到网内其他机器,则只有这部分机器出问题.多发于传奇游戏特别是私服务外挂等方面.

解决办法：

1、由于此类病毒采用 arp 攻击。因此在病毒发作时，网络管理员可任找一台机器，开启 DOS 窗口并输入“arp -a” 命令，会发现很多不同 IP 地址有着相同的 MAC 地址表：

2、Interface: 192.168.0.1 on Interface 0x1000004

Internet Address Physical Address Type
192.168.0.61 00-e0-4c-8c-9a-47 dynamic
192.168.0.70 00-e0-4c-8c-9a-47 dynamic
192.168.0.99 00-e0-4c-8c-81-cc dynamic
192.168.0.102 00-e0-4c-8c-9a-47 dynamic
192.168.0.103 00-e0-4c-8c-9a-47 dynamic
192.168.0.104 00-e0-4c-8c-9a-47 dynamic

可以断定 MAC 地址为 00-e0-4c-8c-9a-47 的机器感染了病毒。然后网络管理员在 DOS 窗口中输入“ipconfig /all” 命令，察看每台机器的 MAC 地址：

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO
Physical Address. . . . . : 0-e0-4c-8c-9a-47
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.186.30.158
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.186.30.1
DNS Servers . . . . . : 61.147.37.1

通过以上步骤定位到染毒的机器，予以隔离处理。

2、网吧管理员检查局域网病毒，安装杀毒软件（金山毒霸/瑞星，必须要更新病毒代码），对机器进行病毒扫描。

3、没有完全解决方案出现之前，请停止传奇私服服务及客户端游戏。

4、采用工具软件(或者 arp -s 方法)在服务器上将 MAC 地址和 IP 绑定，或者使用能将 MAC 地址和 IP 地址进行绑定的交换机来避免此类情况发生。

5、补充说明 :这是全国性的问题 ,该病毒从 3 月初开始在全国大面积爆发。

安全建议：

1、给系统安装补丁程序。通过 Windows Update 安装好系统补丁程序(关键更新、安全更新和 Service Pack)

2、给系统管理员帐户设置足够复杂的强密码，最好能是 12 位以上，字母+数字+符号的组合；也可以禁用/删除一些不使用的帐户

3、经常更新杀毒软件（病毒库），设置允许的可设置为每天定时自动更新。安装并使用网络防火墙软件 ,网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻击和病毒的入侵。部分盗版 Windows 用户不能正常安装补丁，不妨通过使用网络防火墙等其它方法来做到一定的防护

4、关闭一些不需要的服务，条件允许的可关闭一些没有必要的共享，也包括 C$、D$等管理共享。完全单机的用户也可直接关闭 Server 服务

5、不要随便点击打开 QQ、MSN 等聊天工具上发来的链接信息，不要随便打开或运行陌生、可疑文件和程序，如邮件中的陌生附件，外挂程序等。

用户解决方案：

1、在路由器做 MAC 和 IP 地址的绑定。有 ARP 广播的路由器可以开启 ARP 广播功能。

2、在 PC 上做 MAC - IP 绑定，将网关 IP 地址与 MAC 地址设为静态。

3、登陆路由器配置界面，在系统状态→联机状态 中查看路由器的 LAN 口 MAC 地址。（例如：LAN 口 IP：192.168.1.254　MAC：00-0f-7a-01-02-03）

4、编写批处理文件 rarp.bat：

1）新建记事本，输入如下

@echo off

arp -d

arp -s 192.168.1.254 00-0f-7a-01-02-03

将文件中的 IP 地址和 MAC 地址修改为您网络中网关的 IP 地址和 MAC 地址即可。

2）选择记事本中的“文件”→“另存为”，文件名为 rarp；并修改文件名后缀为.bat。

3）将这个批处理文件放到每台 PC 机的启动目录：“windows--开始--程序--启动”目录中。如果是网吧可以通过（万象或者美屏等）管理软件发送文件到每台 PC，并退出还原卡保存设置。

4）当您需要修改该批处理文件时，你只需鼠标右键单击 rarp.bat 文件，选择“编辑”即可修改。

注：以上方案在 WIN 2000 和 WIN XP 上经过反复验证，工作正常。