什么是 ARP?如何防范 ARP 欺骗？病毒防护

什么是 ARP?

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC 地址。

什么是 ARP 欺骗?

从影响网络连接通畅的方式来看，ARP 欺骗分为二种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

第一种 ARP 欺骗的原理是——截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 欺骗的原理是——伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

近期，一种新型的“ ARP 欺骗”木马病毒正在校园网中扩散，严重影响了校园网的正常运行。感染此木马的计算机试图通过“ ARP 欺骗”手段截获所在网络内其它计算机的通信信息，并因此造成网内其它计算机的通信故障。ARP 欺骗木马的中毒现象表现为：使用校园网时会突然掉线，过一段时间后又会恢复正常。比如客户端状态频频变红，用户频繁断网，IE 浏览器频繁出错，以及一些常用软件出现故障等。如果校园网是通过身份认证上网的，会突然出现可认证，但不能上网的现象（无法 ping 通网关），重启机器或在 MS-DOS 窗口下运行命令 arp -d 后，又可恢复上网。ARP 欺骗木马十分猖狂，危害也特别大，各大学校园网、小区网、公司网和网吧等局域网都出现了不同程度的灾情，带来了网络大面积瘫痪的严重后果。ARP 欺骗木马只需成功感染一台电脑，就可能导致整个局域网都无法上网，严重的甚至可能带来整个网络的瘫痪。该木马发作时除了会导致同一局域网内的其他用户上网出现时断时续的现象外，还会窃取用户密码。如盗取 QQ 密码、盗取各种网络游戏密码和账号去做金钱交易，盗窃网上银行账号来做非法交易活动等，这是木马的惯用伎俩，给用户造成了很大的不便和巨大的经济损失。

如何检查和处理“ ARP 欺骗”木马的方法

1 ．检查本机的“ ARP 欺骗”木马染毒进程

同时按住键盘上的“ CTRL ”和“ ALT ”键再按“ DEL ”键，选择“任务管理器”，点选“进程”标签。察看其中是否有一个名为“ MIR0.dat ”的进程。如果有，则说明已经中毒。右键点击此进程后选择“结束进程”。参见右图。

2 ．检查网内感染“ ARP 欺骗”木马染毒的计算机

在“开始” - “程序” - “附件”菜单下调出“命令提示符”。输入并执行以下命令：

ipconfig

记录网关 IP 地址，即“ Default Gateway ”对应的值，例如“ 59.66.36.1 ”。再输入并执行以下命令：

arp –a

在“ Internet Address ”下找到上步记录的网关 IP 地址，记录其对应的物理地址，即“ Physical Address ”值，例如“ 00-01-e8-1f-35-54 ”。在网络正常时这就是网关的正确物理地址，在网络受“ ARP 欺骗”木马影响而不正常时，它就是木马所在计算机的网卡物理地址。

也可以扫描本子网内的全部 IP 地址，然后再查 ARP 表。如果有一个 IP 对应的物理地址与网关的相同，那么这个 IP 地址和物理地址就是中毒计算机的 IP 地址和网卡物理地址。

3 ．设置 ARP 表避免“ ARP 欺骗”木马影响的方法

本方法可在一定程度上减轻中木马的其它计算机对本机的影响。用上边介绍的方法确定正确的网关 IP 地址和网关物理地址，然后在 “命令提示符”窗口中输入并执行以下命令：

arp －s 网关 IP 网关物理地址

4.态 ARP 绑定网关

步骤一：

在能正常上网时，进入 MS-DOS 窗口，输入命令：arp －a，查看网关的 IP 对应的正确 MAC 地址， 并将其记录下来。

注意：如果已经不能上网，则先运行一次命令 arp －d 将 arp 缓存中的内容删空，计算机可暂时恢复上网（攻击如果不停止的话）。一旦能上网就立即将网络断掉（禁用网卡或拔掉网线），再运行 arp －a。

步骤二：

如果计算机已经有网关的正确 MAC 地址，在不能上网只需手工将网关 IP 和正确的 MAC 地址绑定，即可确保计算机不再被欺骗攻击。

要想手工绑定，可在 MS-DOS 窗口下运行以下命令：

arp －s 网关 IP 网关 MAC

例如：假设计算机所处网段的网关为 192.168.1.1，本机地址为 192.168.1.5，在计算机上

运行 arp －a 后输出如下：

Cocuments and Settings>arp -a

Interface:192.168.1.5 --- 0x2

Internet Address Physical Address Type

192.168.1.1　　00-01-02-03-04-05 dynamic

其中，00-01-02-03-04-05 就是网关 192.168.1.1 对应的 MAC 地址，类型是动态（dynamic）的，因此是可被改变的。

被攻击后，再用该命令查看，就会发现该 MAC 已经被替换成攻击机器的 MAC。如果希望能找出攻击机器，彻底根除攻击，可以在此时将该 MAC 记录下来，为以后查找该攻击的机器做准备。

手工绑定的命令为：

arp －s 192.168.1.1　　00-01-02-03-04-05

绑定完，可再用 arp －a 查看 arp 缓存：

Cocuments and Settings>arp -a

Interface: 192.168.1.5 --- 0x2

Internet Address Physical Address Type

192.168.1.1　　00-01-02-03-04-05 static

这时，类型变为静态（static），就不会再受攻击影响了。

但是，需要说明的是，手工绑定在计算机关机重启后就会失效，需要再次重新绑定。所以，要彻底根除攻击，只有找出网段内被病毒感染的计算机，把病毒杀掉，才算是真正解决问题。

5 .作批处理文件

在客户端做对网关的 arp 绑定，具体操作步骤如下：

步骤一：

查找本网段的网关地址，比如 192．168．1．1，以下以此网关为例。在正常上网时，“开

始→运行→cmd→确定”，输入：arp －a，点回车，查看网关对应的 Physical Address。

比如：网关 192.168.1.1 对应 00－01－02－03－04－05。

步骤二：

编写一个批处理文件 rarp.bat，内容如下：

@echo off

arp －d

arp -s 192.168.1.1 00－01－02－03－04－05

保存为：rarp.bat。

步骤三：

运行批处理文件将这个批处理文件拖到“Windows→开始→程序→启动”中，如果需要立即生效，请运行此文件。

注意：以上配置需要在网络正常时进行

6.使用安全工具软件

及时下载 Anti ARP Sniffer 软件保护本地计算机正常运行。具体使用方法可以在网上搜索。

如果已有病毒计算机的 MAC 地址，可使用 NBTSCAN 等软件找出网段内与该 MAC 地址对应的 IP，即感染病毒的计算机的 IP 地址，然后报告单位的网络中心对其进行查封。

或者利用单位提供的集中网络防病毒系统来统一查杀木马。另外还可以利用木马杀客等安全工具进行查杀。

7.应急方案

网络管理管理人员利用上面介绍的 ARP 木马检测方法在局域网的交换机上查出受感染该病毒的端口后，立即关闭中病毒的端口，通过端口查出相应的用户并通知其彻底查杀病毒。而后，做好单机防范，在其彻底查杀病毒后再开放相应的交换机端口，重新开通上网。

附录一

清华大学校园网络安全响应小组编的一个小程序

下载地址： ftp://166.111.8.243/tools/ArpFix.rar

清华大学校园网络安全响应小组编了一个小程序，它可以保护您的计算机在同一个局域网内部有 ARP 欺骗木马计算机的攻击时，保持正常上网。具体使用方法：

1、 程序运行后请先选择网卡，选定网卡后点击“选定”按钮。

2、 选定网卡后程序会自动获取您机器的网关地址。

3、获得网关地址后请点击获取 MAC 地址按钮获取正确的网关 MAC 地址。

4、 确认网关的 MAC 地址后请点击连接保护，程序开始保护您的机器。

5、 点击程序右上角的叉，程序自动隐藏到系统托盘内。

6、要完全退出程序请在系统托盘中该程序图标上点击右键选择 EXIT。

注意：

1、这个程序只是一个 ARP 攻击保护程序，即受 ARP 木马攻击时保持自己计算机的 MAC 地址不被恶意篡改，从而在遭受攻击时网络不会中断。本程序并不能清除已经感染的 ARP 木马，要预防感染或杀除木马请您安装正版的杀毒软件！

附录二

Anti Arp Sniffer 的用法

下载地址：http://www.wipe.edu.cn/Files/wlzx/Antiarp.rar

双击 Antiarp 文件，出现图二所示对话框。

图二

输入网关地址（网关地址获取方式：[开始] -->[程序]--> [附件]菜单下调出“命令提示符”，输入 ipconfig，其中 Default Gateway 即为网关地址）；点击获取网关 MAC 地址，点击自动防护保证当前网卡与网关的通信不被第三方监听。

点击恢复默认，然后点击防止地址冲突，如频繁的出现 IP 地址冲突，这说明攻击者频繁发送 ARP 欺骗数据包。

右击[我的电脑]-->[管理]-->点击[事件查看器]-->点击[系统]-->查看来源为[TcpIP]--->双击事件可以看到显示地址发生冲突，并记录了该 MAC 地址，请复制该 MAC 地址并填入 Anti ARP Sniffer 的本地 MAC 地址输入框中(请注意将:转换为-)，输入完成之后点击[防护地址冲突]，为了使 MAC 地址生效请禁用本地网卡然后再启用网卡，在 CMD 命令行中输入 Ipconfig /all，

查看当前 MAC 地址是否与本地 MAC 地址输入框中的 MAC 地址相符，如果成功将不再会显示地址冲突。

注：1、如果您想恢复默认 MAC 地址,请点击[恢复默认],为了使 MAC 地址生效请禁用本地网卡然后再启用网卡；本软件不支持多网卡，部分网卡可能更改 MAC 会无效。

ARP 病毒猖獗不衰，传统的双向绑定的方法不足以应付新的变种，为了探讨和研究解决 ARP 病毒的方法，偶建了一个群给，群号是 27425242，QQ 群共享里有一些文章和软件，欢迎各位网友加入！

各位朋友，偶其实是菜鸟哦，新出来的 ARP 病毒在我所在的校园网还没有出现过，所以我也就不晓得如何对付啦，呵呵，想不到这篇文章受到这么多人的关注，希望能对大家多少点帮助吧。