使用抓包工具把病毒揪出来 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/57/2021_2022__E4_BD_BF_E7_94_A8_E6_8A_93_E5_c39_57634.htm 你是不是有过这样的经历：在某一天的早上你突然发现网络性能急剧下降，网络服务不能正常提供，服务器访问速度极慢甚至不能访问，网络交换机端口指示灯疯狂地闪烁、网络出口处的路由器已经处于满负荷的工作状态、路由器CPU已经到了百分之百的负荷……重启动后没有几分钟现象又重新出现了。你也一定听说过红色代码、Nimda、冲击波以及震荡波这些臭名昭著的网络杀手。就是它们制造了上述种种恶行。当网络病毒出现时，如何才能及时发现染毒主机？下面我根据网络病毒都有扫描网络地址的特点，给大家介绍一个很实用的方法：用抓包工具寻找病毒源。1．安装抓包工具。目的就是用它分析网络数据包的内容。找一个免费的或者试用版的抓包工具并的抓包工具，非常小巧,运行的速度也很快。安装完毕后我们就有了一台抓包主机。你可以通过SpyNet设置抓包的类型，比如是要捕获IP包还是ARP包，还可以根据目的地址的不同，设置更详细的过滤参数。2．配置网络路由。你的路由器有缺省网关吗？如果有，指向了哪里？在病毒爆发的时候把缺省网关指向另外一台路由器是很危险的（除非你想搞瘫这台路由器）。在一些企业网里往往仅指出网内地址段的路由，而不加缺省路由，那么就把缺省路由指到抓包主机上吧（它不下地狱谁下地狱？当然这台主机的性能最好是高一点的，否则很容易被病毒冲击而亡）。这样可以让那些病毒主机发出的绝大部分扫描都自动送上门来。或者把网络的出口映像到抓

包主机上，所有对外访问的网络包都会被分析到。 3．开始抓包。抓包主机已经设置好了，网络里的数据包也已经送过来了，那么我们看看网络里传输的到底是些什么。打开SpyNet 点击Capture 你会看到好多的数据显示出来，这些就是被捕获的数据包。 图中的主体窗口里显示了抓包的情况。列出了抓到数据包的序号、时间、源目的MAC地址、源目的IP地址、协议类型、源目的端口号等内容。很容易看出IP地址为10.32.20.71的主机在极短的时间内向大量的不同主机发出了访问请求，并且目的端口都是445。4.找出染毒主机。从抓包的情况看，主机10.32.20.71值得怀疑。首先我们看一下目的IP地址，这些地址我们网络里存在吗？很可能网络里根本就没有这些网段。其次，正常情况下访问主机有可能在这么短的时间里发起这么多的访问请求吗？在毫秒级的时间内发出几十甚至几百个连接请求，正常吗？显然这台10.32.20.71的主机肯定有问题。再了解一下Microsoft-DS协议，该协议存在拒绝服务攻击的漏洞，连接端口是445，从而进一步证实了我们的判断。这样我们就很容易地找到了染毒主机的IP地址。剩下的工作就是给该主机操作系统打补丁杀病毒了。既然抓到了病毒包，我们看一下这个数据包二进制的解码内容：这些数据包的长度都是62个字节。数据包前12个字节包括了目的MAC和源MAC的地址信息，紧跟着的2字节指出了数据包的类型，0800代表的是IP包格式，0806代表ARP包格式。接着的20个字节是封装的IP包头，包括了源、目的IP地址、IP版本号等信息。剩下的28个字节封装的是TCP包头，包括了源、目的端口，TCP链接的状态信息等。这就构成了一个62字节的包。可以看出除了这些包头数据之外，这个包没有携带其

他任何的有效数据负荷，所以这是一个TCP要求445端口同步的空包，也就是病毒主机在扫描445端口。一旦染毒主机同步上没有采取防护措施的主机445端口，便会利用系统漏洞传播感染。