网络安全:巧妙教你对付路由器蠕虫攻击计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/585/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c98_585085.htm 2009年下半年全国计算机等级考试时间是2009年9月19日至23日。2009年下半年全国计算机等级考试报名时间会在考前两个月开始报名！更多优质资料尽在百考试题论坛 百考试题在线题库。 前些日子，安全研究人员发现了一种称之为psyb0t的僵尸网络蠕虫，它可以攻击DSL调制解调器和路由器。这种蠕虫可以搜索并利用开放端口的特定设备。被攻击的设备还有一个特征，即弱口令。一旦某个蠕虫进入了路由器，它便可以为所欲为，阻止端口，并可以泄露敏感信息，攻击其它网络等。 在本文中，笔者将分析容易受这种特定蠕虫攻击的路由器类型，然后讨论如何防止这类和其它类型的路由器蠕虫的感染。最后，我们将探讨如何清除感染路由器的蠕虫。 蠕虫是怎样进入路由器的 路由器蠕虫是通过用于远程管理路由器的端口进入路由器的。不过，路由器在默认情况下并没有打开这些端口。必须在路由器Web界面的配置程序上手动启用之。 此外，更大的漏洞在于弱口令。换句话说，如果采取了防御措施，远程管理就是安全的。 根据有关媒体的研究，这种最新的蠕虫攻击的基本上需要满足下面的标准： 1.这些设备一般都是使用MIPS处理器的设备，这种处理器运行简版Endian模式(mipsel)运行。这包括大约30种Linksys设备，十种Netgear 型号的设备，还有其它许多种设备。此外，加载其它固件代替品的路由器，如DD-WRT和OpenWRT也易于受到攻击。 2.启用了某种类型远程管理的设备，如启用了telnet、SSH，或是

基于Web的访问，要知道，仅提供本地的访问并不容易受到攻击。 3.远程管理访问的用户名和口令的组合不够强健，易被破解。或者是其固件容易被漏洞利用程序所利用。 保障广域网服务的安全 既然路由器蠕虫是通过远程管理端口侵入的，保障这些端口的安全就成为了防止感染的关键所在。此外，不启用远程管理并关闭这些端口就是最佳方案，因为蠕虫无路可进。不过，如果需要远程访问，遵循下面的指南可以防止蠕虫的入侵： 1.使用强健而安全的口令 要知道，路由器蠕虫依赖于强力字典攻击(不断地努力猜测口令)，所以我们应当使用不易被猜测的口令。不要使用什么“ admin ”、“ router ”、“ 12345 ”等作为路由器的口令，而要使用一种混合性的组合，如rDF4m9Es0yQ3ha等。其中至少要包括大小写字母，并利用数字和字母。虽然这种口令不易记忆，但我们可以将其存放于可以某个文件(如文本文件)中，再用TrueCrypt、Cryptainer LE等软件为各种保存密码的文件加密。 2.保障远程连接的加密 例如，尽量不要使用HTTP方式传送，因为它使用的是明文传送，而可考虑使用HTTPS来传送基于Web的访问。可以打开路由器配置程序的远程访问设置，选择“ https ”选项。如果需要命令行才能访问路由器，可使用SSH。因为SSH是一个加密的协议。使用加密的连接并不是防止路由器蠕虫的必须措施，但它可以加强路由器的总体安全性。 3.改变默认端口 蠕虫僵尸可通过这些远程连接的默认端口侵入，如通过HTTP Web 访问的80或8080端口、加密Web访问的443端口、SSH的22号端口等。因此，一台在非默认端口上接收连接的路由器更为安全。很多路由器在紧挨着远程连接设置功能的位置有一个端口(Port)字段，在此输入

想要使用的端口号码。例如，键入路由器所在位置的面向互联网的IP地址，加上一个冒号，然后是端口号。如果是通过SSH进行连接，你需要在SSH客户端程序的连接设置中指定端口号。 4.使用入站过滤器 其实我们可以对有些路由器进行配置，使其过滤哪些IP地址或范围准许使用进入的连接，如此便可以阻止不在列表中的任何IP地址的蠕虫。为此，首先，可以看一下是否可以在路由器的远程管理设置中定义IP地址或IP地址范围。然后，检查路由器是否可以设置入站的连接设置。 保障路由器的固件最新 前面我们提到,路由器固件所所使用的软件也使路由器易于受到蠕虫攻击，因此保持路由器总是加载最新的固件版本可有助于防止这种漏洞。路由器的制造商们和固件替换项目会定期发布这些固件的更新，用以修补已知的安全漏洞。 要更新路由器的固件，应从厂商的网站下载新的镜像。然后登录进入路由器的配置程序，打开“ Admin ”/“ Misc ”或“ System ”部分，选择最新的固件，并加载它即可。 清除蠕虫：还路由器的清洁之躯 我们前面所讨论的预防性措施可防止路由器受到蠕虫的攻击和危害。记住，如果你不需要远程访问就不要启用它。如果有必要采用此功能，我建议你把用户名和口令复杂一些，多用一些大小写、数字等混合的口令，并要通过SSH或HTTPS传输，还要考虑使用非默认端口，并尽量采用任何的入站过滤器。 如果路由器已经受到感染，肯定会发生一些不可思议的事情。例如，据报告，Psyb0t会阻止22号端口、23号端口、80号端口的通信。 要清除蠕虫，最彻底的解决方法是将路由器恢复到出厂默认值，这样做可以保证清除蠕虫。按下路由器背面的复位按钮，并且过上几秒钟(不同的厂商要求不一样，如笔者

的路由器要求按下30秒钟以上才可以)，就可以恢复到出厂状态。一旦清除了蠕虫，一定要记得采用本文所介绍的方法哟。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com