抵御Conficker攻击保护Windows系统安全Microsoft认证考试
 关于Conficker 微软公司在2008年10月23日发布了一个重要的安全更新MS08-067以解决windows服务器服务中的漏洞，因为当时正面临着有针对性的攻击威胁。该漏洞可以让匿名攻击者通过网络攻击完全掌握对漏洞系统的控制，而攻击最终要的载体通常都与网络“蠕虫”有关。自从发布MS08-067后，微软恶意软件保护中心(MMPC， Microsoft Malware Protection Center)已经确定了Win32/Conficker的两种变体： 蠕虫病毒：Win32/Conficker.A于2008年11月21日被发现。 蠕虫病毒：Win32/Conficker.B于2008年12月29日被发现。 Conficker大事记 2008年11月21日MMPC发现了蠕虫病毒Win32/Conficker.A，该蠕虫病毒试图通过网络攻击利用MS08-067漏洞来散播自身，同日，MMPC对微软Forefront、Microsoft OneCare以及Windows Live OneCare Safety Scanner增加了签名和检测功能。2008年11月25日MMPC通过其博客公布了有关这个病毒的信息。 2008年12月29日MMPC发现了第二个变体Win32/Conficker.B，并于同日对其 Microsoft Forefront、Microsoft OneCare以及Windows Live OneCare Safety Scanner增加了签名和检测功能。蠕虫病毒Win32/Conficker.B通过以下方式传播自身： 1. 通过网络攻击利用MS08-067漏洞来散播自身从而攻击计算机系统。 2.将自身复制到目标机器的ADMIN$\System32文件夹并通过时间表设置让该文件每天执行，首先它会尝试利用登录用户的登录证书，只要该帐户

具有管理权限，用户在网络的不同电脑环境使用这些相同的登录证书。如果这种方法失败，它就会尝试不同的方法：在目标机器上保护使用者帐户列表，并试图使用每个用户名和猜测的简单密码来进行登录，如果这样做登录成功的话，并且帐户还有写入权限的话，病毒就能将自身复制到ADMIN$文件夹中。 3.将自身复制到可移动媒介(如USB驱动)和其他使用自动播放功能启动自身的移动存储设备。 注意：上面列举的第二种和第三种放啊并没有利用MS08-067涉及的安全漏洞，因此安装了该漏洞安全更新的系统就可以成功阻止这两种攻击方式。 2008年12月31日MMPC通过其博客公布了有关conficker.B的信息。 2009年1月13日，MMPC在其恶意软件移除工具(MSRT，Windows Malicious Software Removal Tool)加入了移除Win/Conficker.A和Win/Conficker.B的功能。 2009年2月12日，微软公司重金奖励提供关于在网上非法传播Conficker恶意代码犯罪分子信息的人，该公司认为这种conficker蠕虫病毒确实属于恶意非法行为。 如何保护计算机免受conficker攻击 1. 安装安全更新MS08-067，了解关于该漏洞的详细信息、受影响软件、检测和部署工具和指导方案和安全更新部署信息等。 2. 请确保你运行的防病毒软件已经安全最新安全更新，并请选择有良好信誉的供应商。 3. 检查安全软件或者设备(如防病毒网络入侵检查系统或者主机入侵检查系统等)更新保护功能。 4. 将未打补丁的系统或者感染系统与网络其他设备隔离开来。 5. 部署强度高的密码。 6. 使用组策略或者注册表功能禁用自动播放功能，微软公司告诉用户允许用户禁用自动播放/自动运行已经通过自动更新方式部署了。 注意：Windows 2000、Windows XP和Windows Server

2003客户必须部署安全更新才能够成功禁用自动播放功能，而Windows Vista 和Windows Server 2008客户则需要部署MS08-038更新才能成功禁用自动运行功能。 如何清理受感染的系统 1. 手动下载MSRT到未感染的计算机上，然后部署到已感染的计算机上来清除病毒。 2.不能在自己环境中使用MSRT的用户可以阅读微软知识库文章(链接为http://support.microsoft.com/kb/962007)来了解如何手动移除Win/Conficker.B。 更多优质资料尽在百考试题论坛 百考试题在线题库 微软认证更多详细资料 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