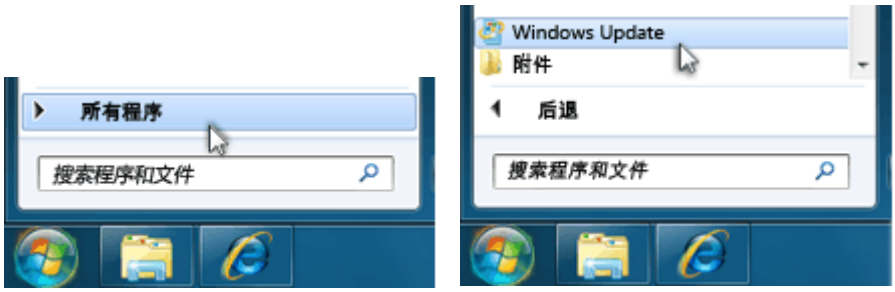
附件 3. GANDCRAB 勒索病毒防范指南

一、 使用 Windows 系统自动更新功能更新补丁

使用 Windows 系统“开始”菜单检查更新：Windows 更新包含在“控制面板”中。要检查更新，请执行下列操作：

单击“开始”按钮，单击“所有程序”，然后单击“Windows 更新”。



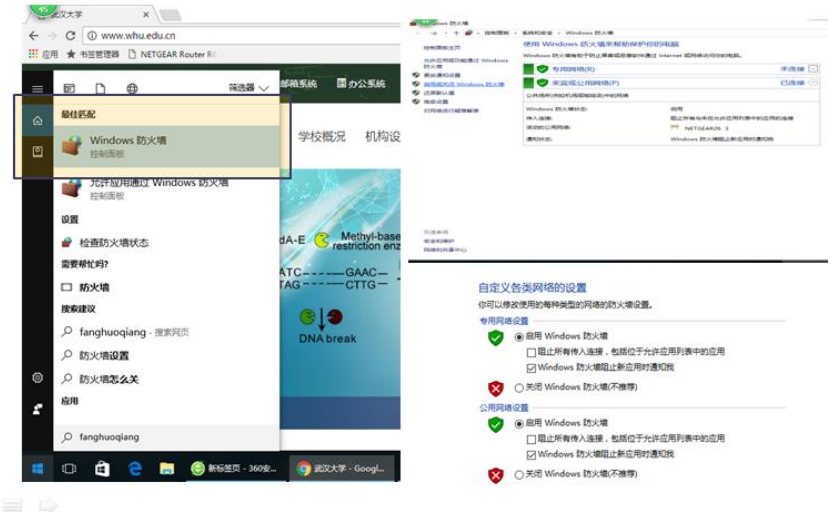
二、 个人电脑的系统防火墙设置（关闭个人电脑的相应端口）

提示：以下指南以 **Windows10 操作系统**为例说明供参考，因个人电脑的操作系统版本存在细节差异，师生参照本文操作时应酌情调整操作，如遇疑问请联系信息化建设与网络安全办公室具体咨询。

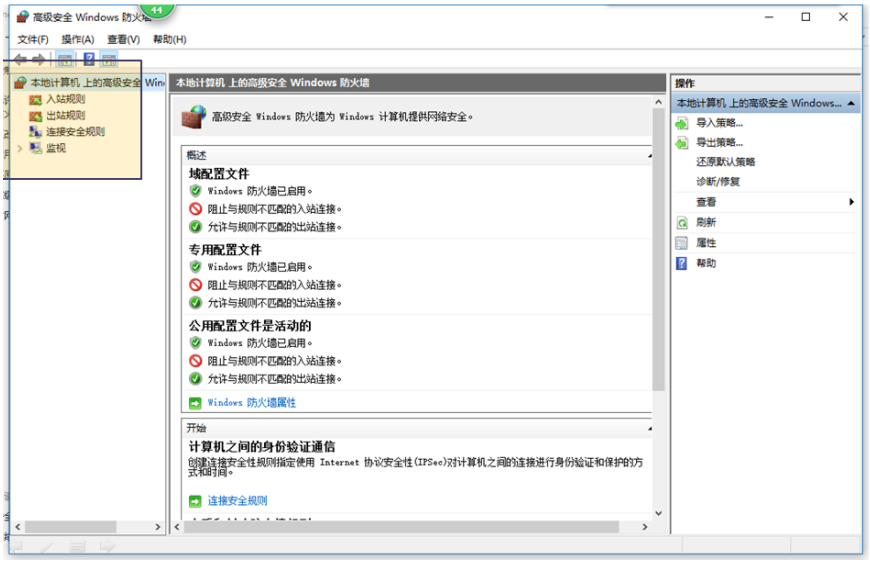
现在，开始关闭电脑的 445、135、137、138、139、3389、5900 等端口。按照以下步骤操作（以 445 端口操作为例,请按透明橙色标注框体的设置内容具体操作）：

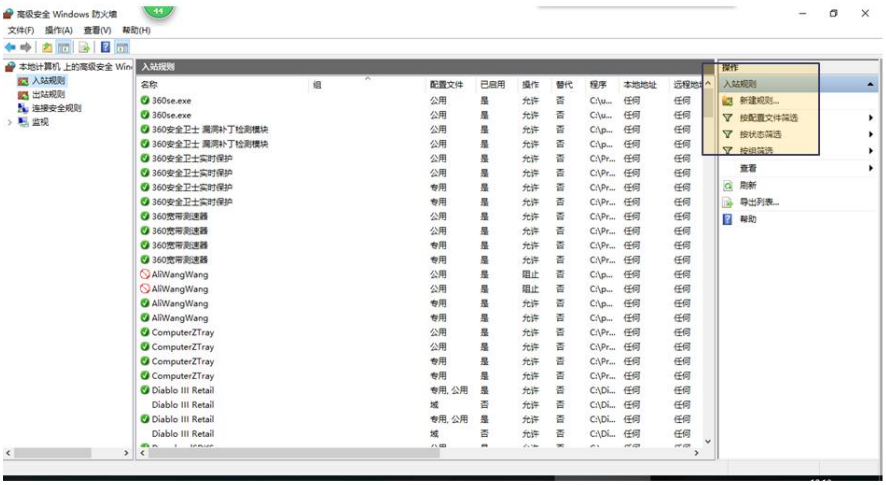
在开始之前，请先将电脑断网。

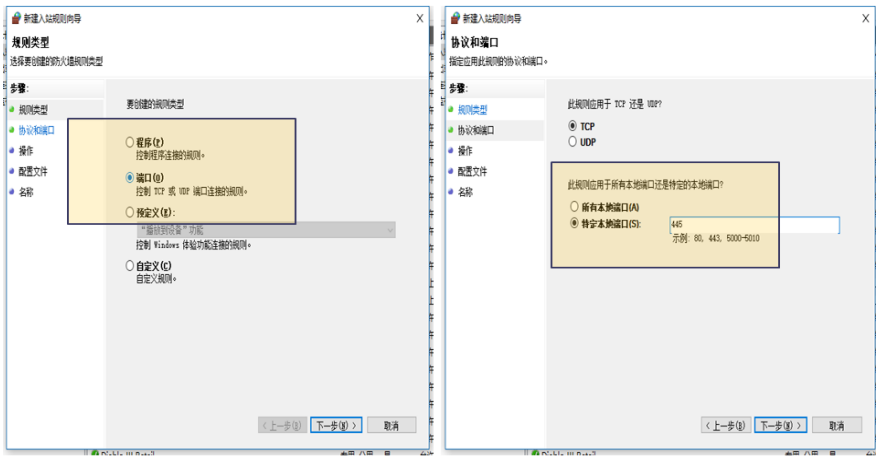
在电脑上查找系统自带防火墙(路径在“控制面板”中)并设置为启用。

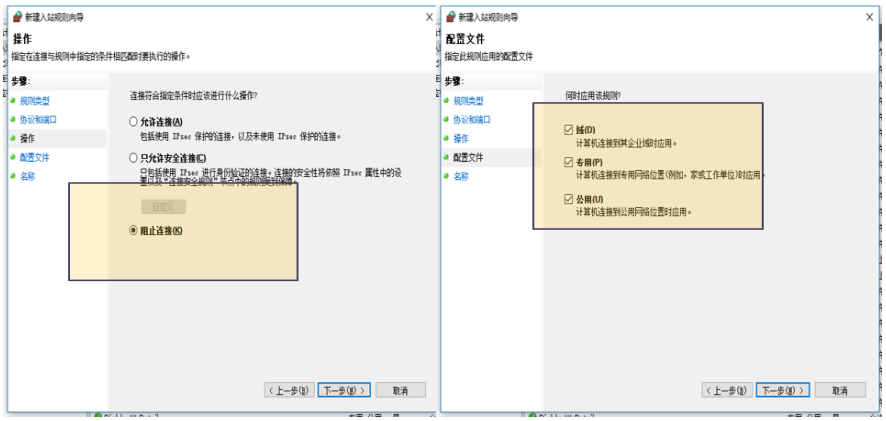


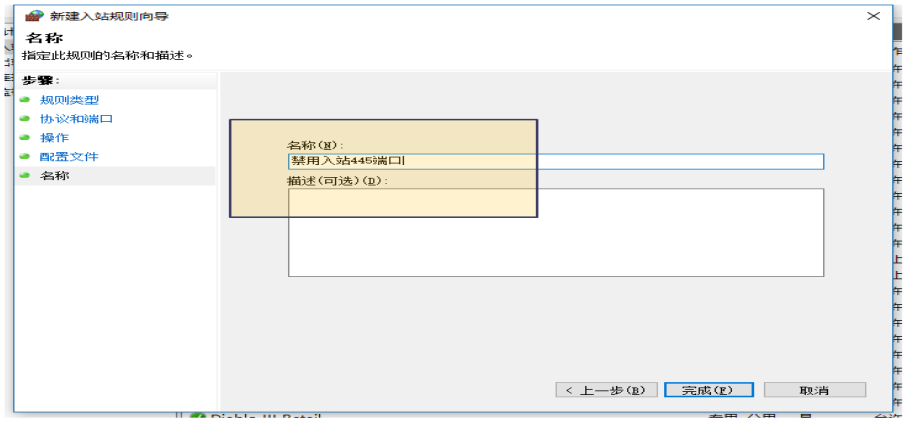
1）点选入站规则项，并新建入站规则：禁用本机 445 端口。



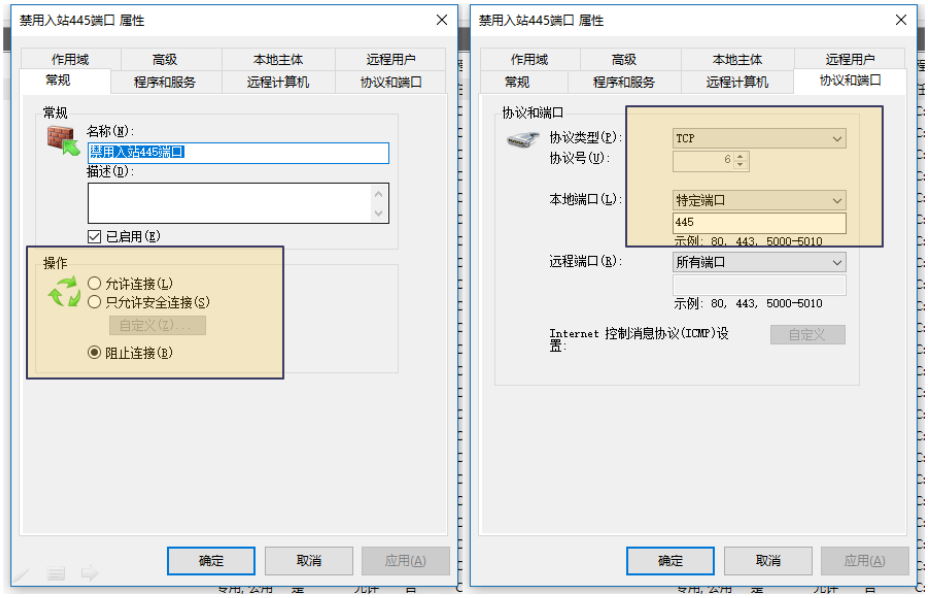








2）核实关闭 445 端口访问的规则已经正确添加并且生效。



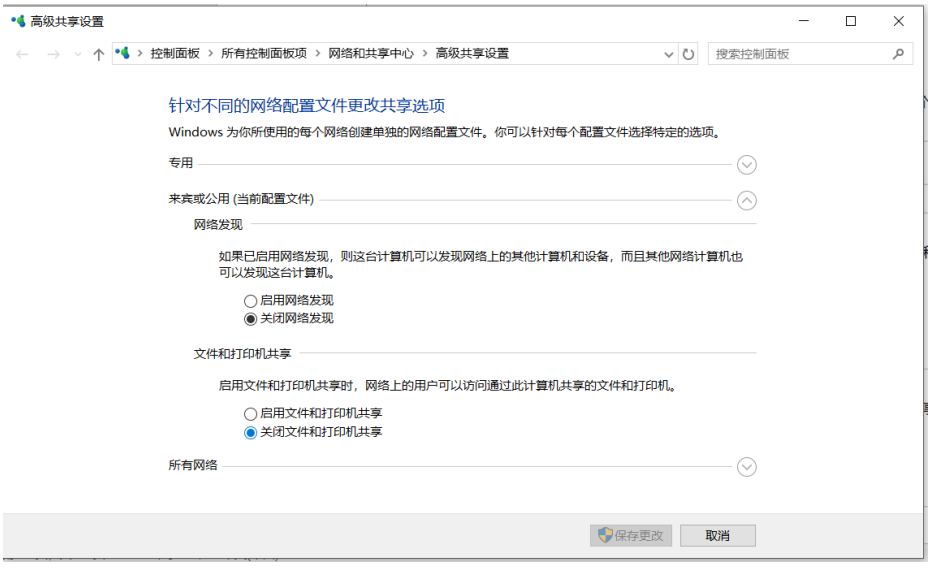
3）还须关闭 135、137、138、139、3389、5900 端口，操作与上述关闭 445 相同。

三、 关闭网络文件共享

Windows10 操作系统：

1）桌面右下角状态栏，点击网络连接图标后显示网络连接状态，点击“网络和 Internet 设置”。

2）点击“共享选项”后，在“高级共享设置”页面选择“关闭网络发现”和“关闭文件和打印机共享”，然后点击“保存修改”。

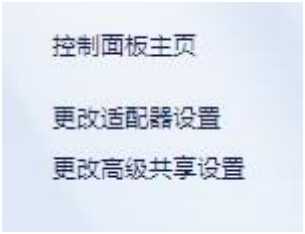


Windows7 操作系统：

1）打开桌面上的“网络”

2）点击“网络和共享中心”

3）点更改高级共享设置

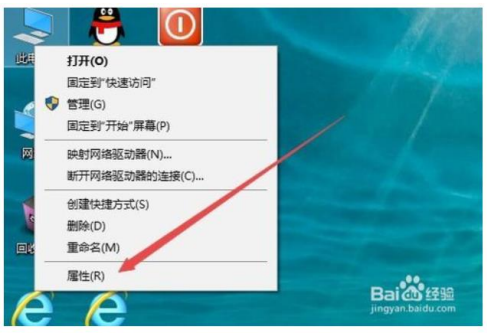


4）选中关闭网络发现，选中关闭文件和打印机共享，选中关闭公用文件夹共享，点保存修改。

四、 关闭远程桌面连接服务

Windows7 操作系统：

1）打开开始菜单，右键计算机选择属性栏，点击打开，或者右键点击桌面左下角的“此电脑”图标，在弹出菜单中选择“属性”菜单项。如下图所示：



2）在打开的计算机属性页面，我们找到页面左边的“远程设置”点击打开。如下图所示：

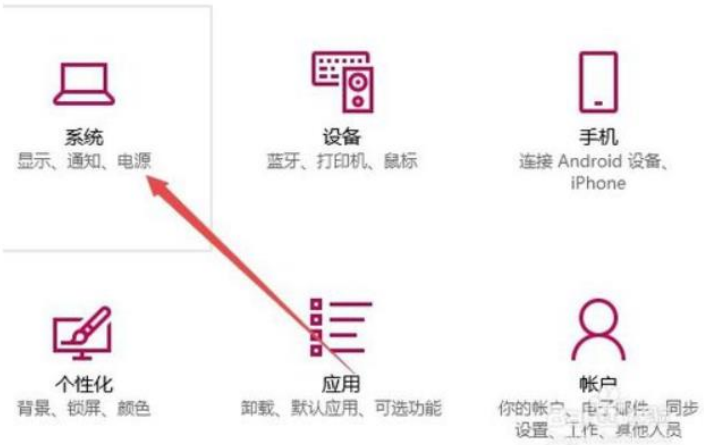
3）接着将“允许远程协助连接这台计算机”选项勾选取消，在下方选择“不允许连接到这台计算机”选项，如下图所示：

4）完成以上操作后点击“应用”再点击“确定”完成操作。如下图所示：

Windows10 操作系统：

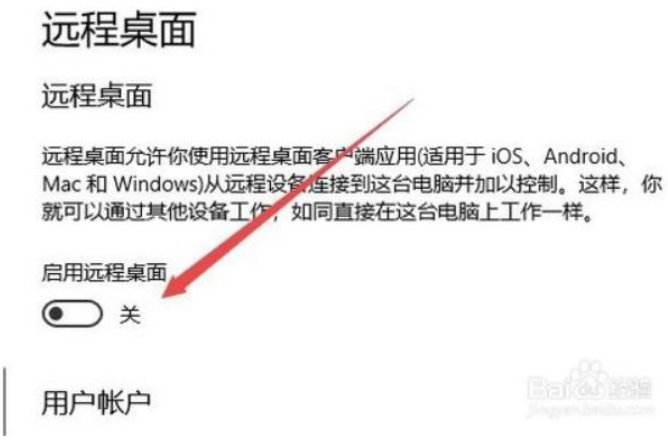
1）右键点击桌面左下角的开始按钮，在弹出菜单中点击“设置”菜单项。

2）这时会打开 Windows 设置窗口，在窗口中点击“系统”图标。



3）在打开的设置窗口中，点击左侧边栏的“远程桌面”菜单项。

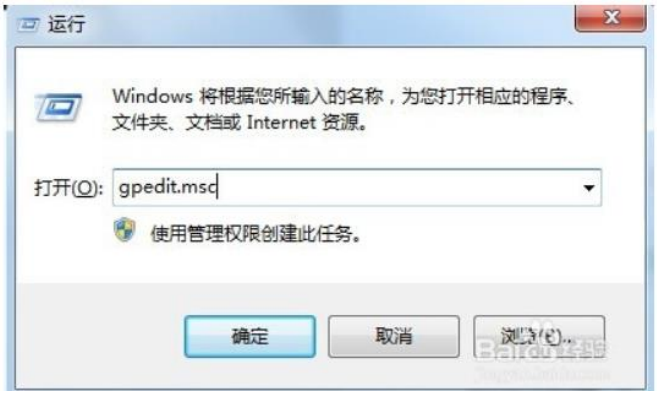
4）这时在右侧窗口中找到“远程桌面”设置，找到“启用远程桌面”一项，把其开关设置为“开”即可打开远程桌面，如果不使用了后可以把其设置为“关”即关闭了远程桌面了。



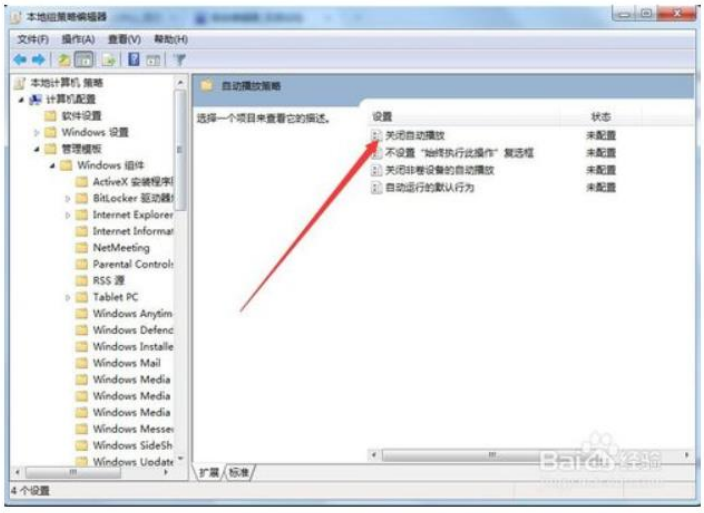
五、 通过 Windows 系统组策略禁用 U 盘、光驱自动运行功能

Windows7/10 操作系统：

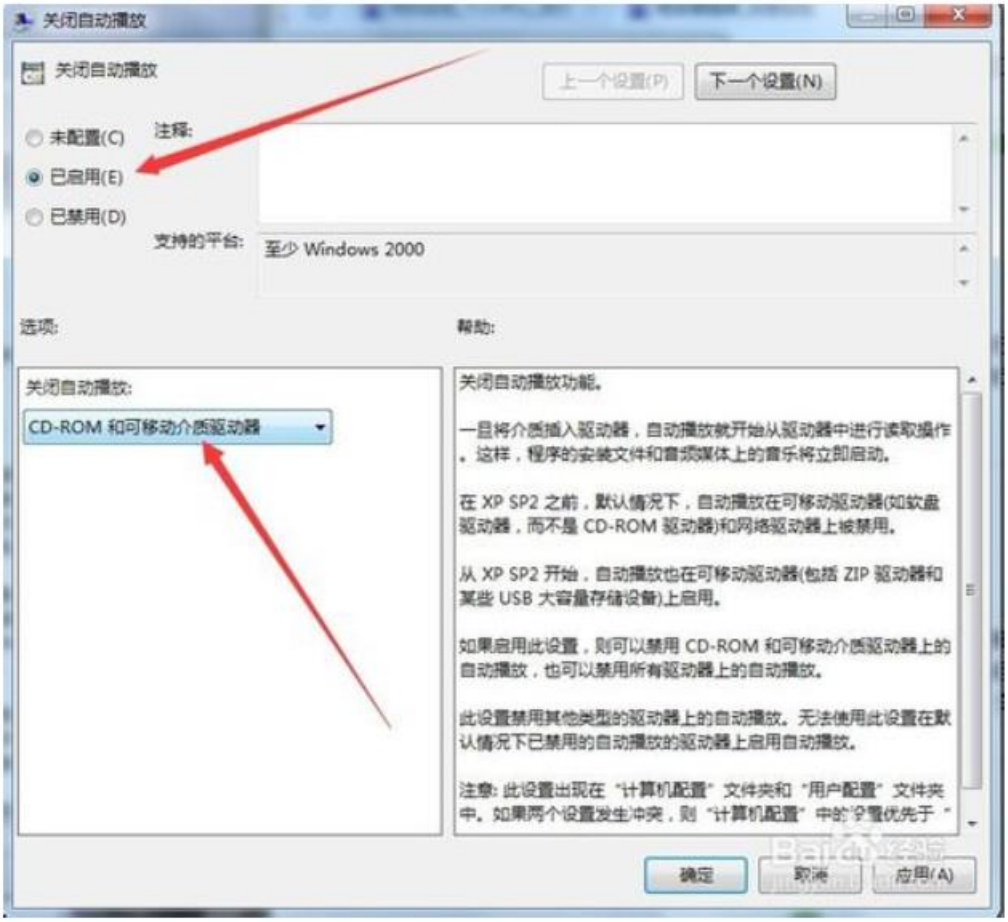
1）按下 win+R 快捷键，打开系统的运行对话框，在运行框中输入 gpedit.msc 命令，并点击确定按钮。



2）在打开的组策略编辑器窗口中，依次点击本地计算机策略/计算机配置/管理模板/Windows 组件/自动播放策略菜单，打开自动播放策略的设置窗口，双击右侧窗口中的”关闭自动播放”菜单项。



3）在打开的关闭自动播放设置窗口中，选中“已启用”项，然后在下面的选项中可以设置关闭自动播放的设备，一般选择 CD-ROM 和可移动介质驱动器就可以了，最后点击确定按钮 ，这样以后再插入 U 盘或移动硬盘，就不会再自动播放了。


关闭自动播放
关闭自动播放
上一个设置(P)
下一个设置(N)
未配置(C)
已启用(E)
已禁用(D)
注释:
支持的平台:
至少 Windows 2000
选项:
帮助:
关闭自动播放:
CD-ROM 和可移动介质驱动器
关闭自动播放功能。
一旦将介质插入驱动器，自动播放就开始从驱动器中进行读取操作。这样，程序的安装文件和音频媒体上的音乐将立即启动。
在 XP SP2 之前，默认情况下，自动播放在可移动驱动器(如软盘驱动器，而不是 CD-ROM 驱动器)和网络驱动器上被禁用。
从 XP SP2 开始，自动播放也在可移动驱动器(包括 ZIP 驱动器和某些 USB 大容量存储设备)上启用。
如果启用此设置，则可以禁用 CD-ROM 和可移动介质驱动器上的自动播放，也可以禁用所有驱动器上的自动播放。
此设置禁用其他类型的驱动器上的自动播放。无法使用此设置在默认情况下已禁用的自动播放的驱动器上启用自动播放。
注意: 此设置出现在“计算机配置”文件夹和“用户配置”文件夹中。如果两个设置发生冲突，则“计算机配置”中的设置优先于“
确定
取消
应用(A)