Windows 8/8.1 系统中的杀毒软件——Windows Defender 使用教程

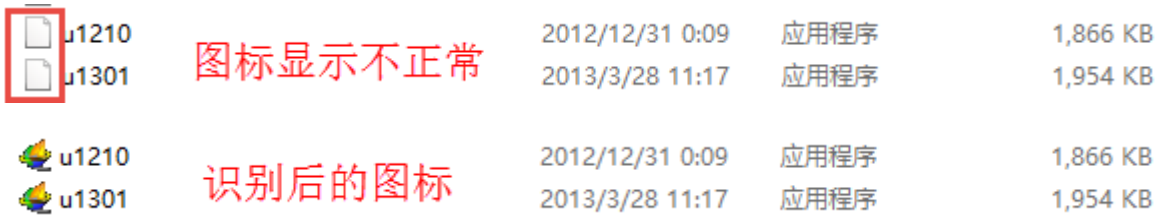
目　录

1、简介

在 Windows 8 和 Windows 8.1 系统中预安装了一个 Windows Defender 软件，其实它就是微软 MSE 杀毒软件，只是改了一个名字而已。在安装好 Windows 8/8.1 系统后，Windows Defender 就已经开始实时保护系统了，只是不显示通知栏图标，也不带有右键扫描功能。除了要检查一下 MAPS 状态外（参考“3、了解 Windows Defender 界面”），不需要额外设置。

如果在 Windows 8/8.1 系统中额外安装杀毒软件（例如小红伞、Mcafee 等），系统会自动禁用 Windows Defender，即使卸载这些杀毒软件，Windows Defender 也不会自动起作用，需要手动把 Windows Defender 调出来。具体请参考“2、启动 Windows Defender”小节。

Windows Defender 有个缺点，在打开包含许多 exe 可执行文件的文件夹时（例如自由门、无界浏览都是可执行程序），可能会出现电脑暂时停顿性能下降的情况，俗称“卡 exe”，exe 程序图标会滞后出现，遇到这种情况得耐心等待一会儿才会恢复正常，同样，在解压缩和复制包含大量 exe 文件的时候，速度也会慢一些。为了解决这个缺点，建议在经常使用的文件夹中不放置过多的 exe 可执行文件。



这个图文教程其实很简单，有的内容是为了便于理解抓图而占据了篇幅，看过一遍之后基本就不需要再看了。

使用 Windows Defender 非常简单，只需要知道：

① 如何启动 Windows Defender（参考“2、启动 Windows Defender”）

② 检查并关闭 MAPS（参考“3、了解 Windows Defender 界面”）

③ 知道如何保持病毒库的更新（参考“4、病毒库的更新”）

④ 知道发现病毒如何处理（参考“5、实时保护发现病毒的处理”）

⑤ 知道遇到误报时如何还原隔离文件（参考：6、从隔离区还原误报文件）

⑥ 知道遇到误报如何排除（参考：7、误报文件排除）

⑦ 知道如何查杀某些外来文件（参考：8、快速扫描和自定义扫描）

以上这些就是 Windows Defender 杀毒软件的全部了。

2、启动 Windows Defender

启动 Windows Defender 一般都先调出系统的控制面板，调出方法如下：

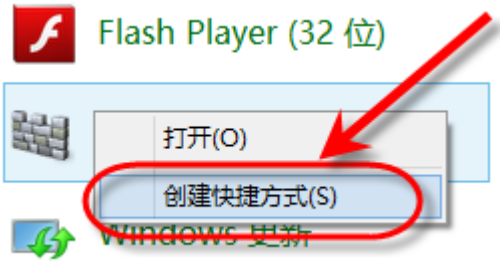
如果是 Windows 8 系统，先按下键盘的 Windows 窗口键，再按下 x 键，之后在弹出菜单选择“控制面板”。

如果是 Windows 8.1 系统，右键点桌面左下角的窗口按钮显示弹出菜单。

在弹出菜单中，选择“控制面板”

在“查看方式”处，点击选择“大图标”，就可以看到 Windows Defender 了

右键点 Windows Defender 图标，选择“创建快捷方式”，就可以为其在桌面创建一个快捷方式，方便调用 Windows Defender。

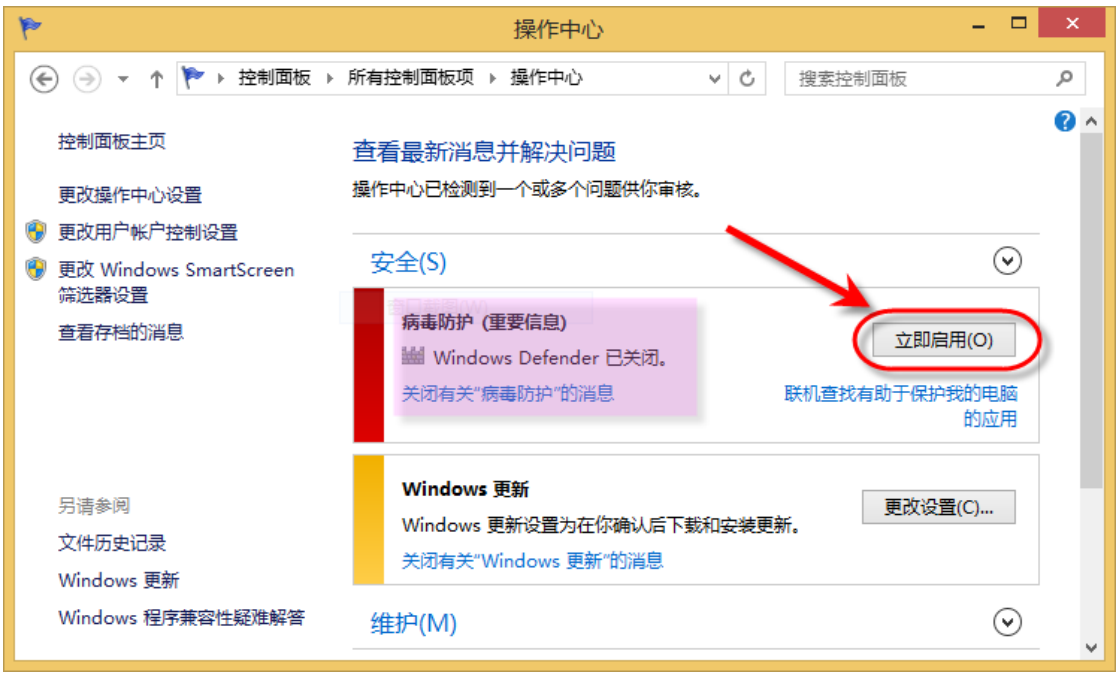


双击这个快捷方式就会显示 Windows Defender 主窗口，操作和 MSE 杀毒软件是一样的。

如果双击此快捷方式提示“**此应用已经关闭，不会监视你的计算机**”。这是因为安装其它杀毒软件时系统禁用了 Windows Defender 的原因，需要先到操作中心打开 Windows Defender。这样双击创建的快捷方式才起效。

如本小节前面的步骤调出控制面板 → “查看方式”选择“大图标”→ 找到“操作中心”

点击操作中心，点击病毒防护后面的“立即启用”按钮。就会启用并打开 Windows Defender 界面。



3、了解 Windows Defender 界面

Windows Defender 界面比较简单，分为主页、更新、历史记录、设置几个部份。

1）主页

显示实时保护是否开启、病毒库是否过期、以及手动扫描部分。如果实时防护被禁用或发现病毒等高危情况，会显示为红色警告颜色。这里需要注意病毒库不要过期，尽量不要超过一周。

在右侧有三个扫描选项

快速：迅速检查系统关键区域，包括内存中运行的程序、系统文件和注册表

完全：扫描检查计算机上的所有文件、注册表以及当前运行的所有程序。完全扫描默认不包括可移动硬盘和优盘。

自定义：仅扫描用户选择的区域，如选择扫描 C 盘或某个文件夹。

实际上，只要开启实时防护，遇到病毒会自动防护，不执行完全扫描或自定义扫描也不会降低本机安全。

2）更新

下图是离线运行病毒库更新的情况，具体注意请参考图中说明。点“更新”按钮会开始更新，会显示更新进度，也可以取消更新。这个方法任何时候都可以进行，不管 Windows Defender 是否设置为自动更新。

3）历史记录

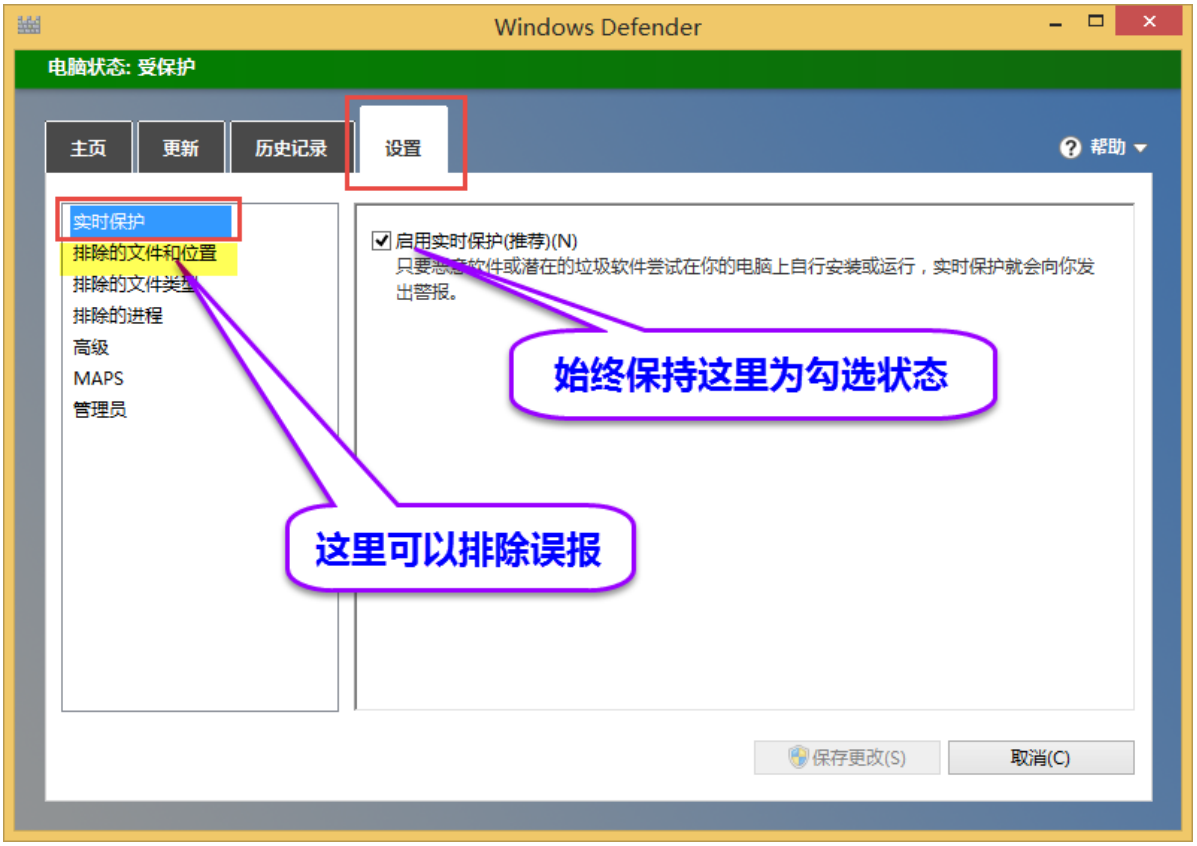
记录了已经隔离和扫描到的情况，在扫描和监控时候采取措施的病毒都可以在这里看到。恢复隔离文件可以在这里进行。

允许的项目：在发现病毒时候，如果确认是误报而允许的，这些操作设置就会在“允许的项目”中出现。

检测到的所有项目：包含所有曾经检测到的项目，可以在点“查看详细信息”后点对话框底部的“全部删除”按钮清空检测情况。

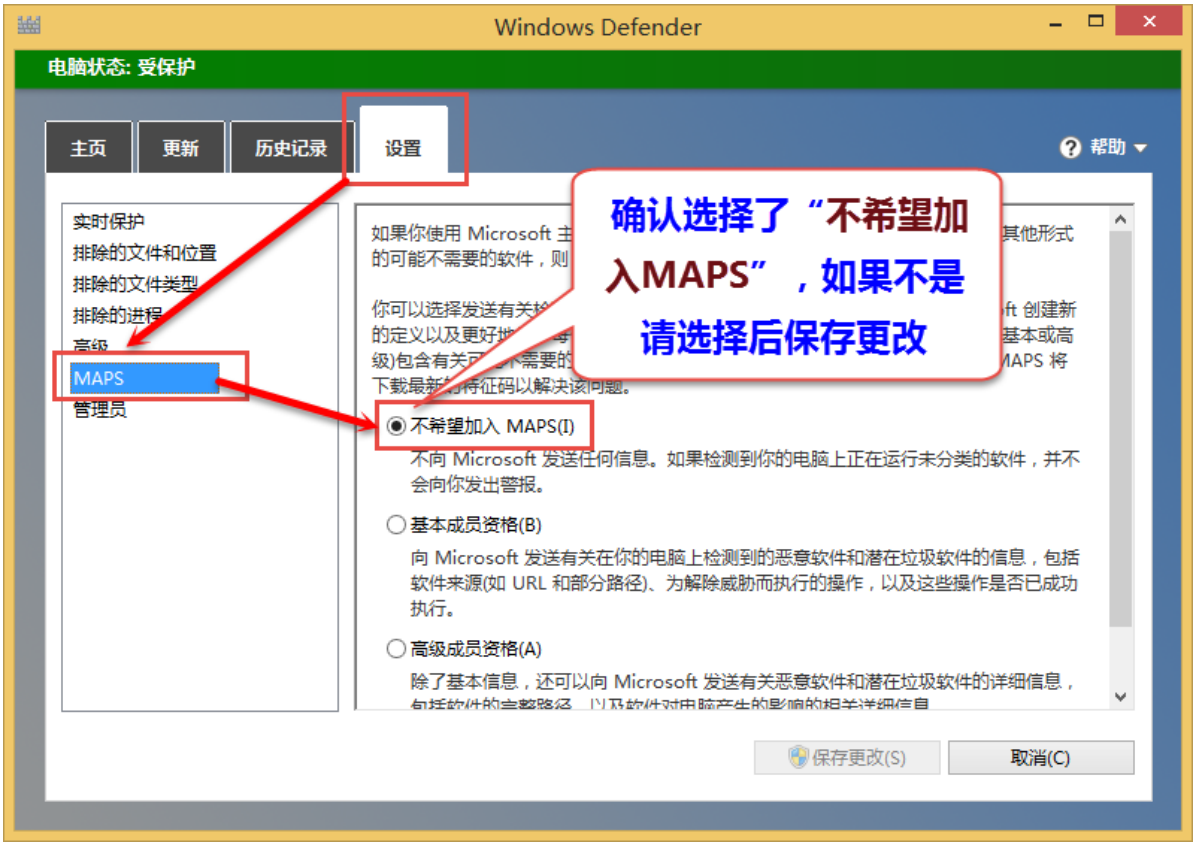
4）设置

实时防护：这里始终保持实时防护的开启状态，即使有误报文件，也可以从隔离区恢复误报文件之后再排除，不需要关闭实时防护。



MAPS：开启 MAPS 会上传用户信息，所以需要关闭，Windows 8 安装的时候默认关闭了 MAPS，Windows 8.1 安装的时候，关闭下面选项就会关闭 MAPS。

在设置页面的 MAPS 下面，确认选择的是“不希望加入 MAPS”，如果不是，请选择“不希望加入 MAPS”后点击对话框的“保存更改”按钮。



4、病毒库的更新

1）从自动更新中安装病毒库

如果电脑开启自动更新，系统会自动下载安装 Windows Defender 的定义库，然而很多情况下是设置为手动检查更新的，例如国产电脑、或者使用了国产硬件的电脑就必须设置为手动检查安装更新，以避免安装国产硬件驱动，如需相关资料，请翻墙后访问下面教程：

Windows 8 系统补丁更新方法（视频演示）（翻墙后访问）

http://tiandixing.org/viewtopic.php?f=69&t=123939

Windows Defender 在更新检查中病毒库对应重要更新中的“Windows Defender 定义更新”，如果手动更新中看到此更新，请选择安装。

2）手动在线更新

网络不太通畅时，病毒库自动更新可能无法成功，这时候可以打开 Windows Defender 窗口，点击“更新”选项页，点那个大的“更新”按钮执行手动更新检查。这个方法任何时候都可以进行，不管 Windows Defender 是否设置为自动更新。

3）手动离线更新

由于网络不通畅或其它原因导致**自动更新**和**手动在线更新**都不成功，我们可以下载离线更新包手动更新，对于无网络的电脑也可以采取这种更新方法。离线更新包下载的是完整的引擎和病毒库，把下载地址粘贴到浏览器地址栏后回车后下载，或者使用下载软件下载都可以，下载地址(无需破网)：

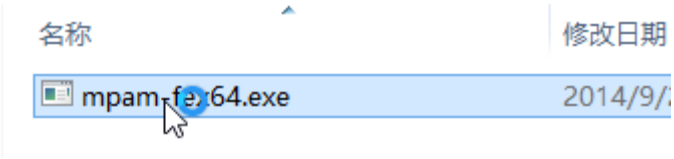
32 位系统下的离线病毒库

http://download.microsoft.com/download/DefinitionUpdates/mpam-fe.exe

64 位系统下的离线病毒库

http://download.microsoft.com/download/DefinitionUpdates/mpam-fex64.exe

离线包更新方法：以 32 位的离线更新包为例，双击 mpam-fe.exe 运行即可，安装时不会显示任何安装界面，双击后很快就安装好了，查看 Windows Defender 的主界面就会看到病毒库日期已经更新了。安装病毒库的时候，鼠标光标如果显示为忙碌状态，那么繁忙状态消失即表示安装完成。



除了上面三种更新方法外，还有一个通过计划任务自动更新病毒库的办法，相比之下更为省心，但是由于需要一定的技术能力，所以放在教程最后了，具体参考第九部份：通过计划任务自动更新病毒库(选看)。

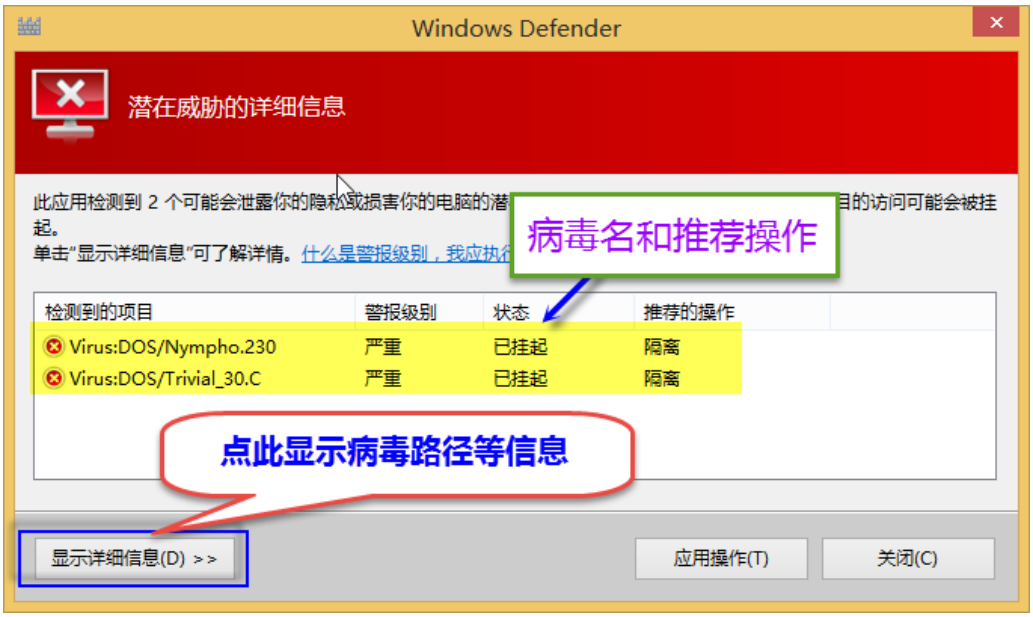
5、实时保护发现病毒的处理

当电脑上发现威胁时，例如下载到可疑文件或解压缩可疑文件，Windows Defender 会在屏幕右上角提示已检测到恶意软件（如下图）

如果 Windows Defender 确认是严重病毒，会自动对病毒文件采取隔离、删除等操作，用户无法决定如何处理。如果我们确认是绝对可靠软件被隔离了（例如核对校验值和数字签名无误的破网软件），那么需要从隔离区恢复误报文件之后添加排除（见本教程第 6、7 部份）。

还有一种情况，点击前面的灰色警告提示框会打开 Windows Defender 界面，显示威胁数目。如果点“清理电脑”，会按照程序预设的清理选项执行病毒清理操作。点“显示详细信息”可查看威胁情况，由用户选择具体处理措施。

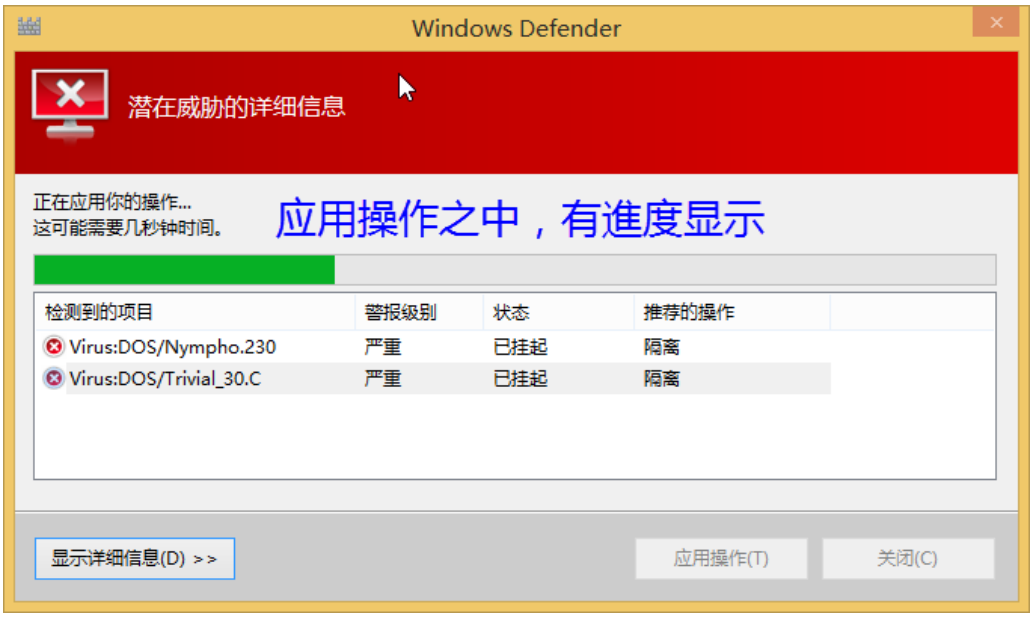
下面是点击详细信息后的对话框。



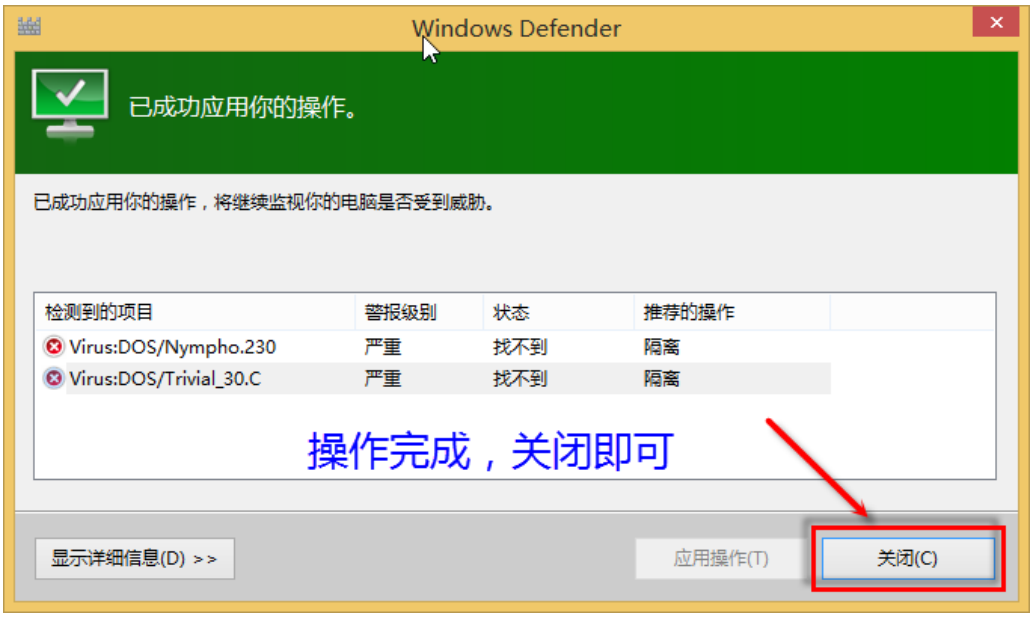
选中第一条，再点底部的“显示详细信息”。

如果这里警告的是可靠软件，例如核对校验值和数字签名无误的破网软件，我们确认是误报，那么可以在推荐的操作中选择“允许”。

依次查看所有可疑文件后，点“应用操作”按钮执行清理



清理完毕，关闭对话框即可。

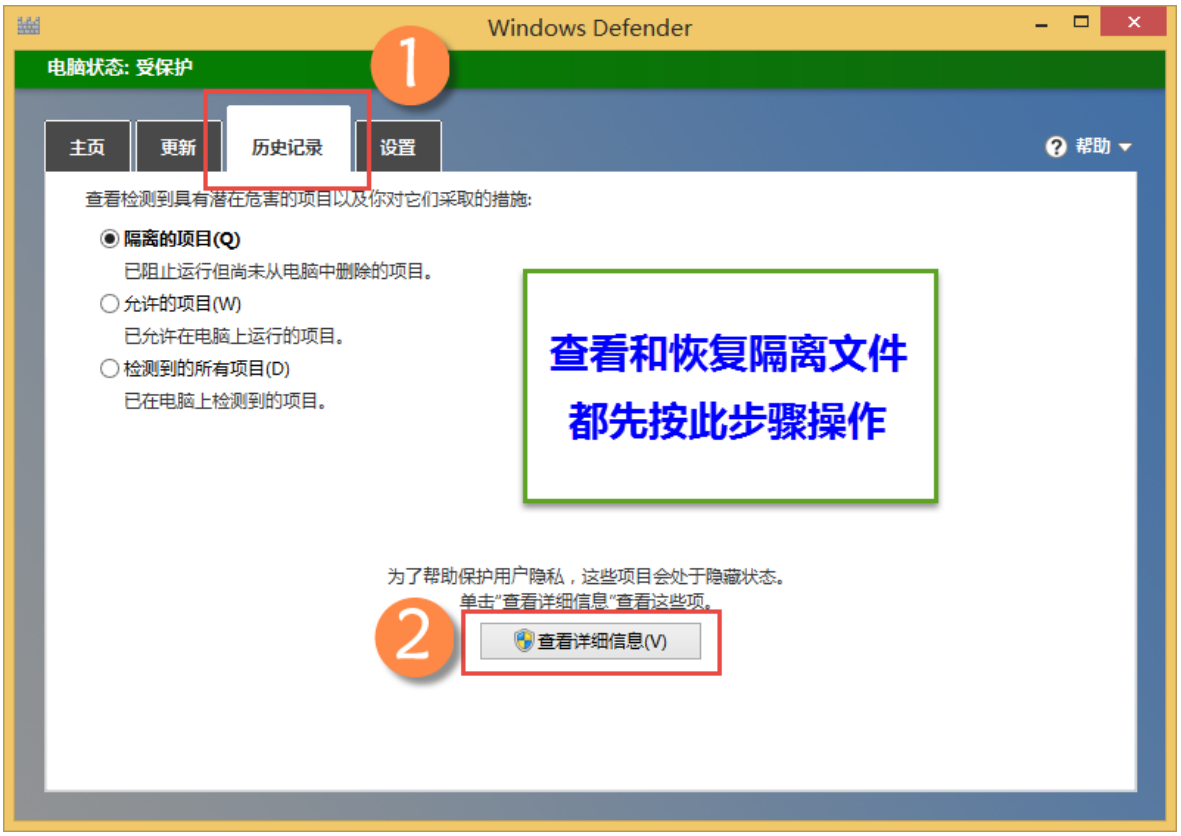


6、从隔离区还原误报文件

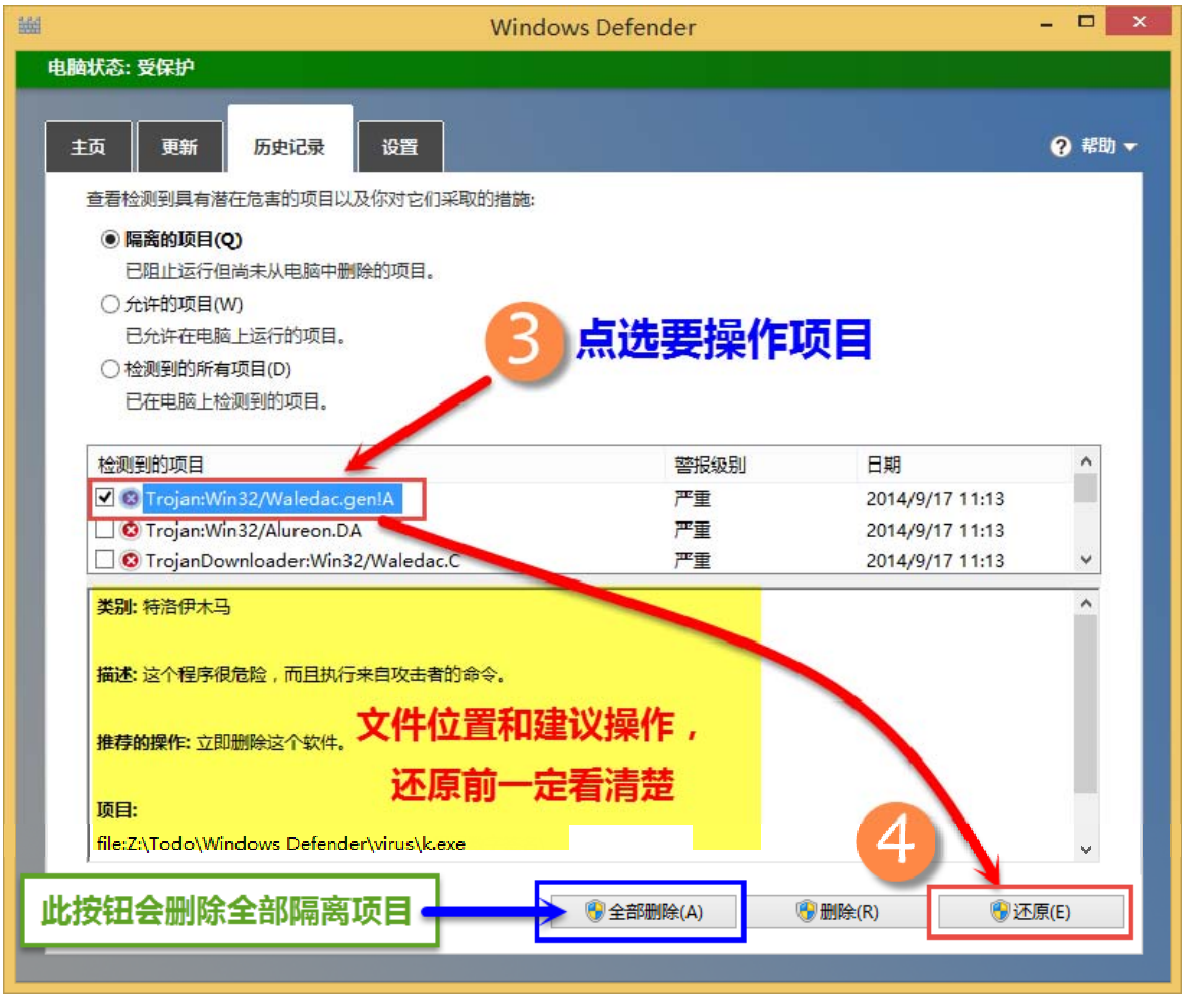
如果确认被 Windows Defender 隔离的文件是误报的，可以从隔离区恢复，并将其加入到排除列表。Windows Defender 的误报并不严重，除非你有绝对的把握知道被隔离的文件是安全的，否则请不要从隔离区中还原文件。

还原步骤如下：

点开“历史记录”，如下图，默认选择的是“隔离的项目”，点“查看详细信息信息”

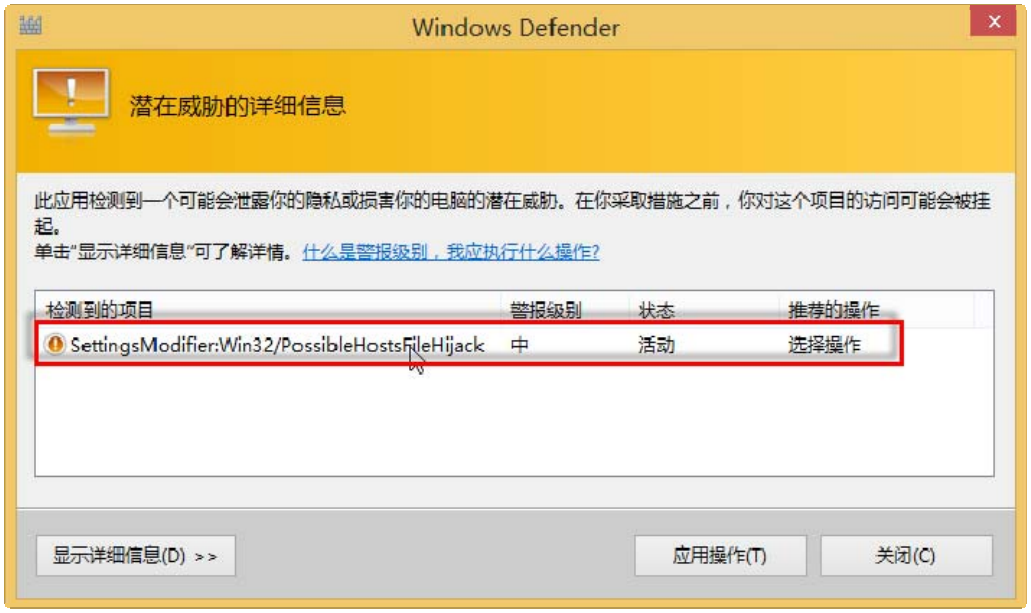


选中要还原的文件，检查文件原始位置，确认无误再点“还原”

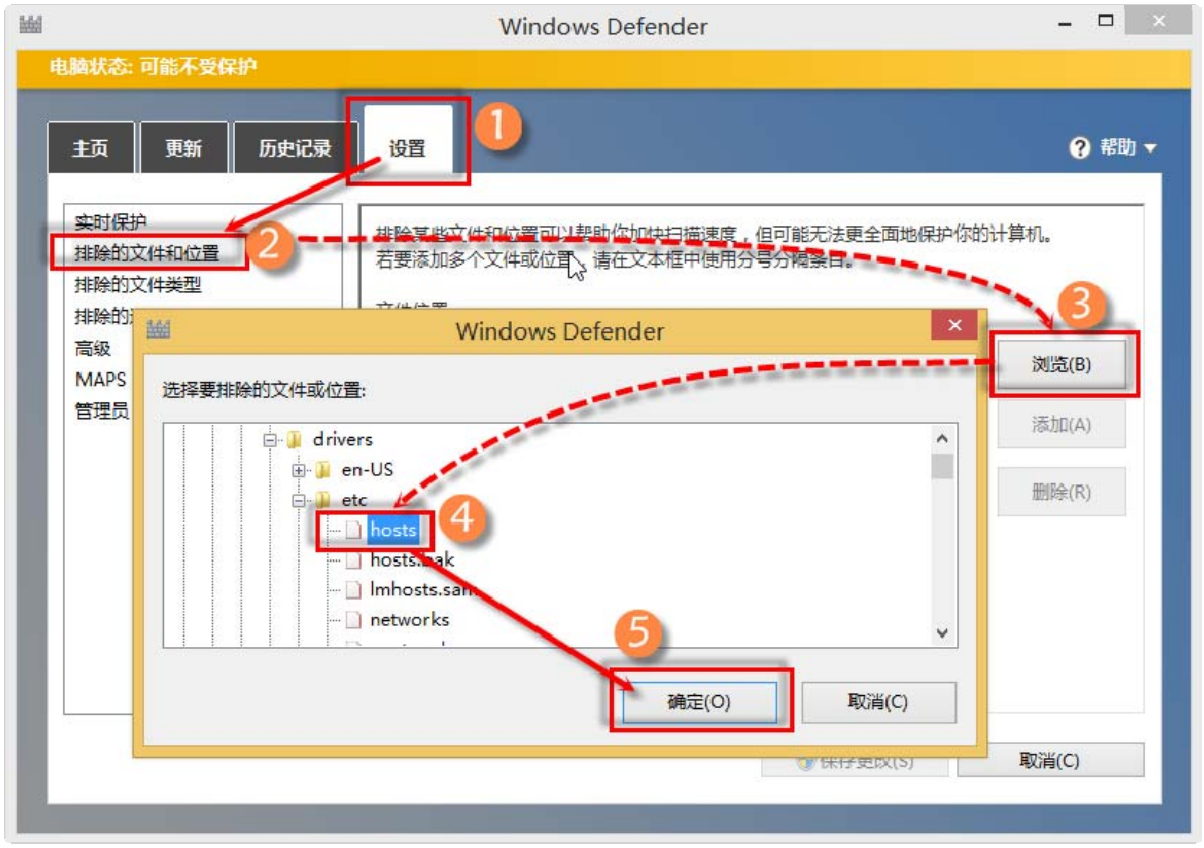


7、误报文件排除

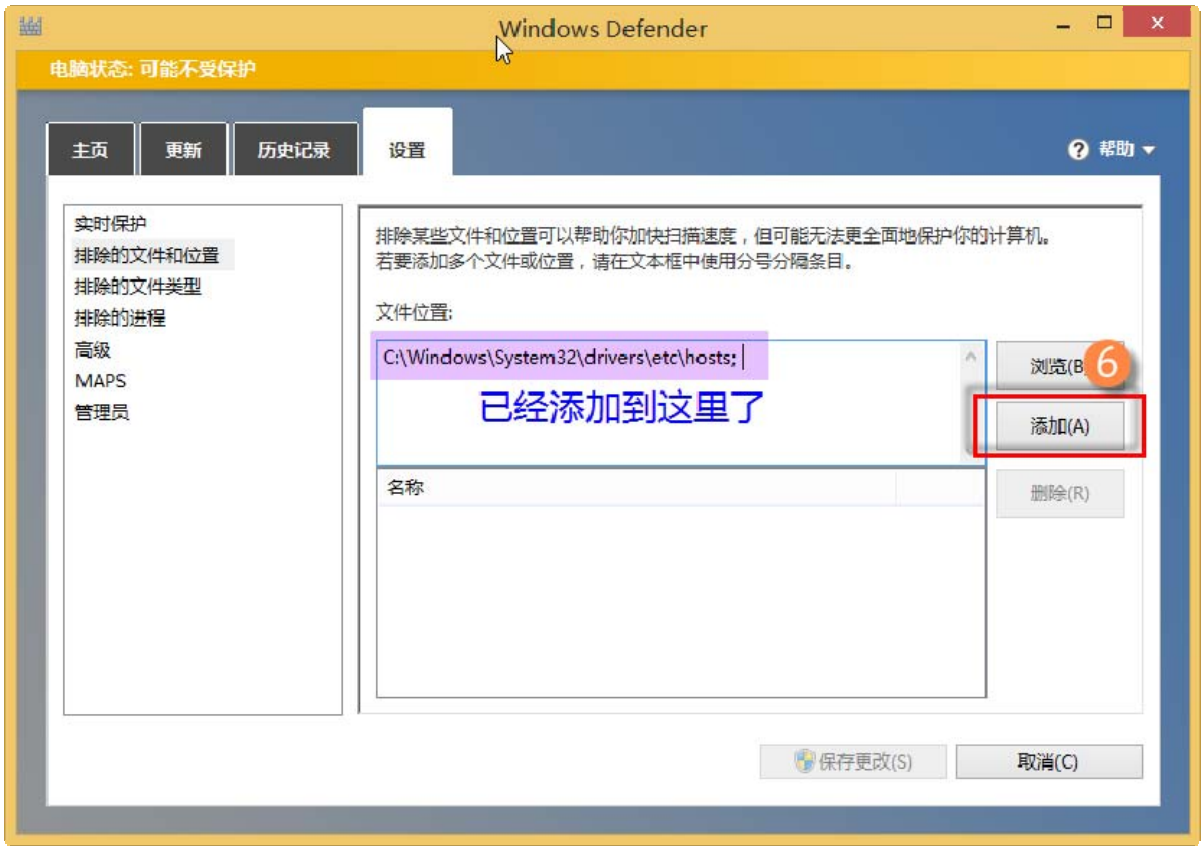
如果被警告或隔离的软件是可靠的，例如核对校验值和数字签名无误的破网软件是误报，那么可以设置排除。如果文件已被隔离，请先从隔离区恢复隔离之后再排除。这里以排除“防止直连”软件中被误报的 hosts 文件为例说明。在 Windows Defender 执行快速扫描会警告这个 hosts 文件，文件位置 C:\Windows\System32\drivers\etc\hosts。这个文件我们是为了网络安全而特别设置的，所以是误报可以排除。



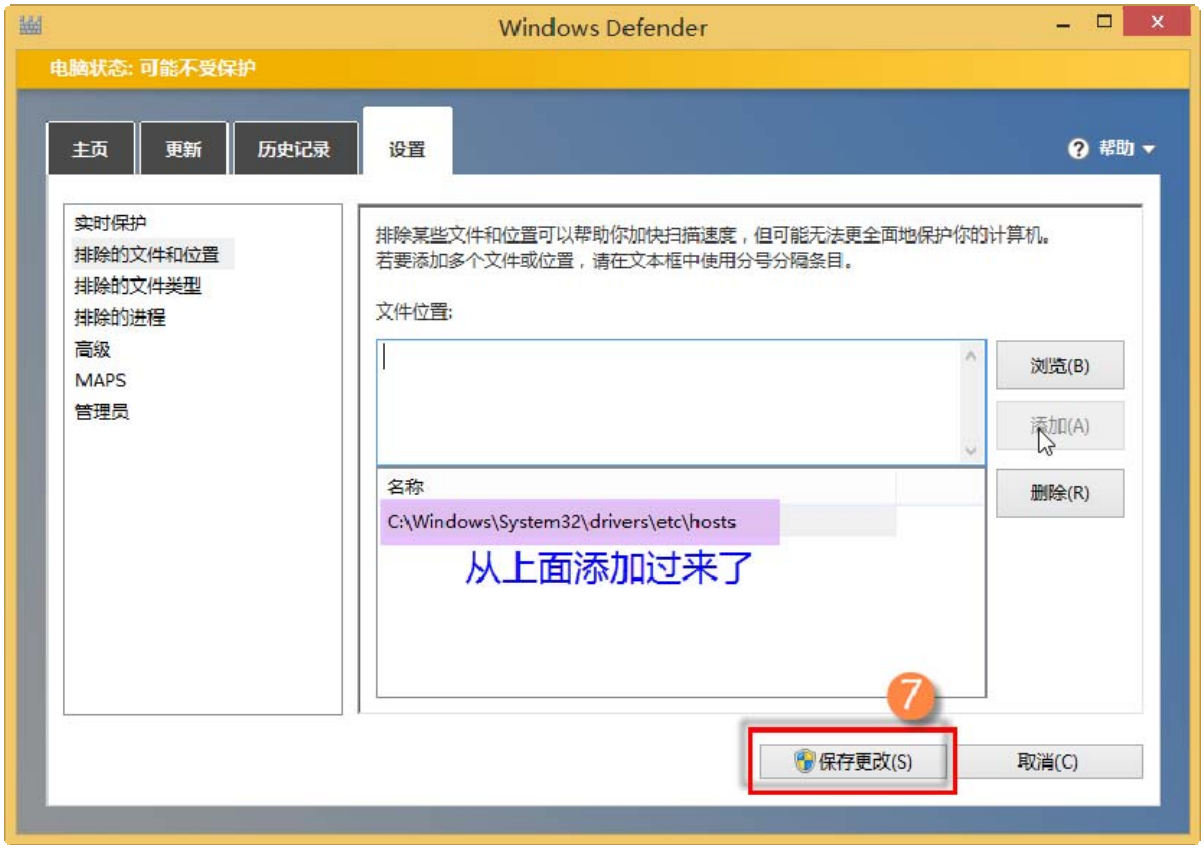
添加排除操作如下，如图步骤，浏览选择 hosts 文件，之后点“确定”（这个步骤如果选择的是一个文件夹，那么排除的就是这个文件夹下面的所有文件）。



返回后，点添加按钮



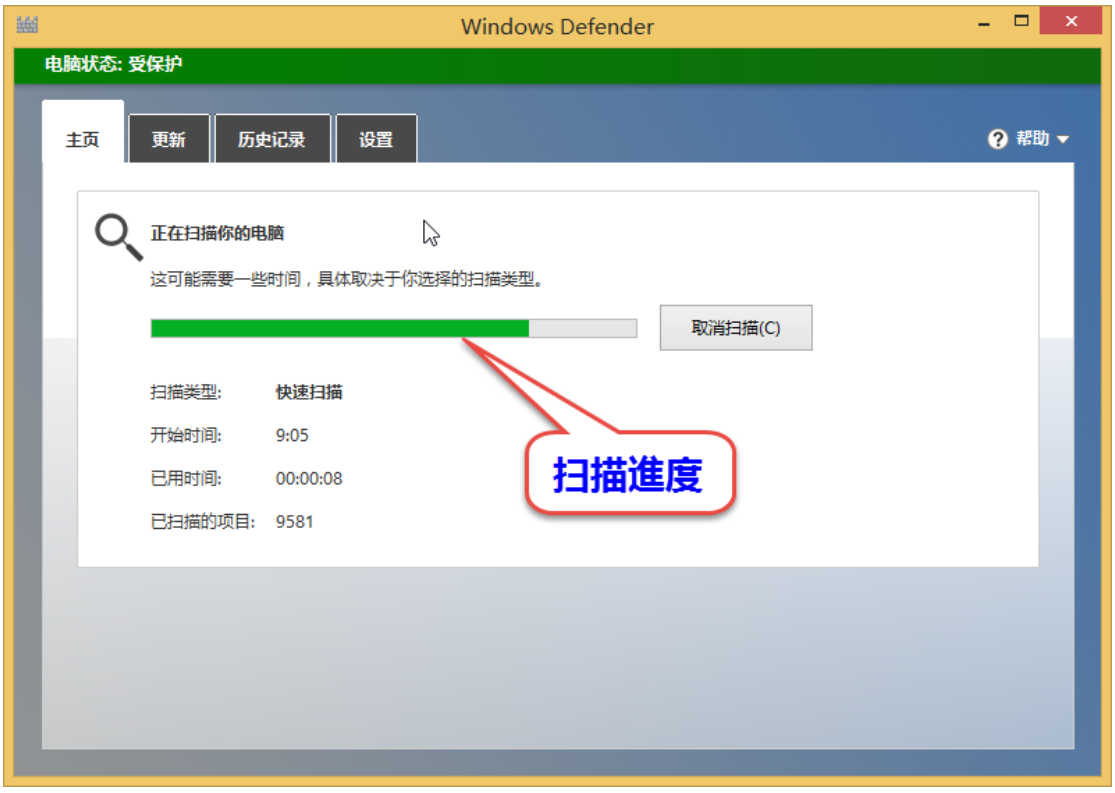
点 **保存更改** 按钮，就完成误报文件的排除了。



8、快速扫描和自定义扫描

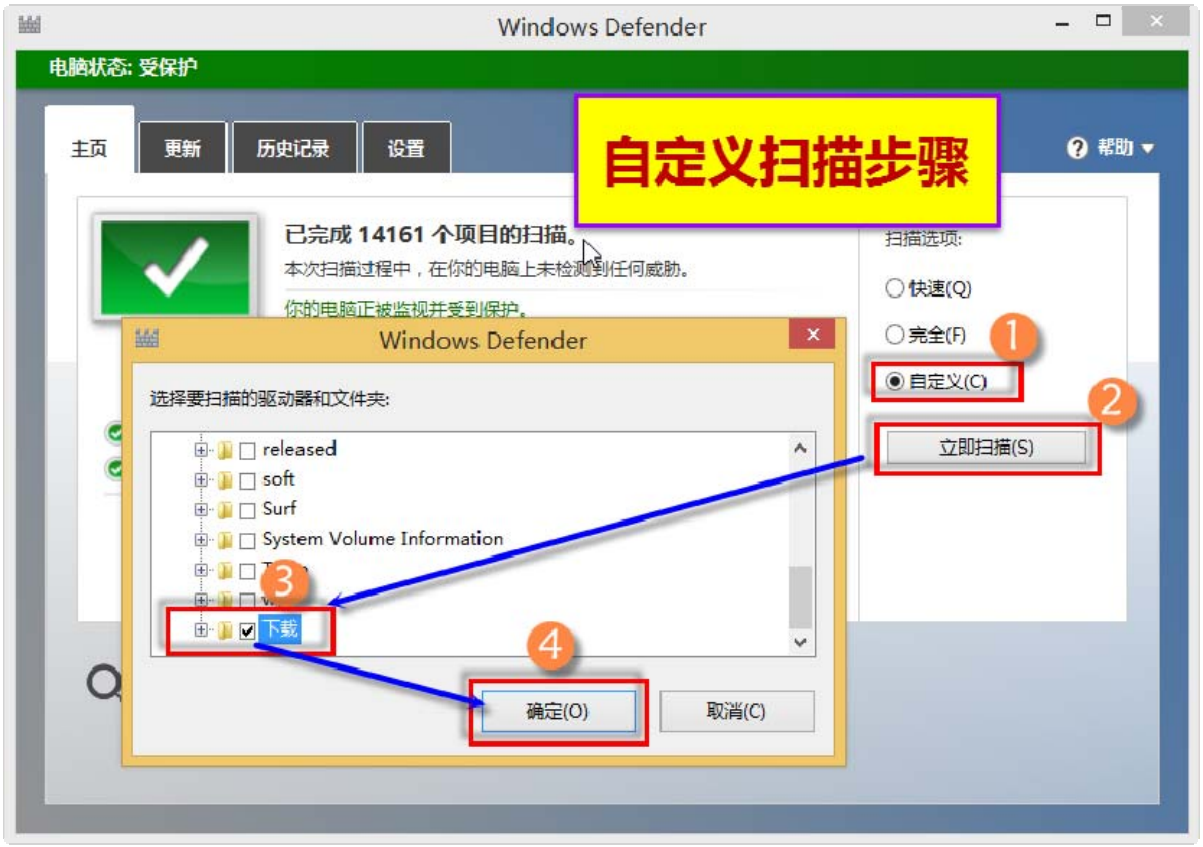
快速扫描针对系统关键区域扫描。自定义扫描可以扫描指定文件夹，以弥补 Widows Defender 没有右键扫描的缺点。实际上，只要开启实时防护，遇到病毒会自动防护，不对外来文件夹扫描也不会降低本机安全。

会显示扫描进度。



快速扫描如果发现病毒，请按照教程“5、实时保护发现病毒的处理”的原则处理。

下面是自定义扫描某个文件夹的步骤：



之后会显示扫描進度等，如果发现病毒，请按教程“5、实时保护发现病毒的处理”的原则处理。

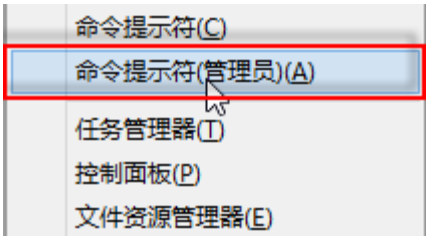
9、通过计划任务自动更新病毒库（选看）

这部分使用了一串代码，虽然这串代码实际非常简单，但是很多网友见到代码通常都会比较头疼和犯难，所以把它放在这里作为选看内容，有能力的可以参考一下。

Windows defender 的病毒库每天都会更新，每次都通过手动更新检查安装病毒库也是比较麻烦的，对于不是按照流量计费的网络，可以通过计划任务设置为开机自动更新病毒库，就不需要操心病毒库更新的事情了，步骤如下：

先按下键盘的 Windows 窗口键，再按下 x 键

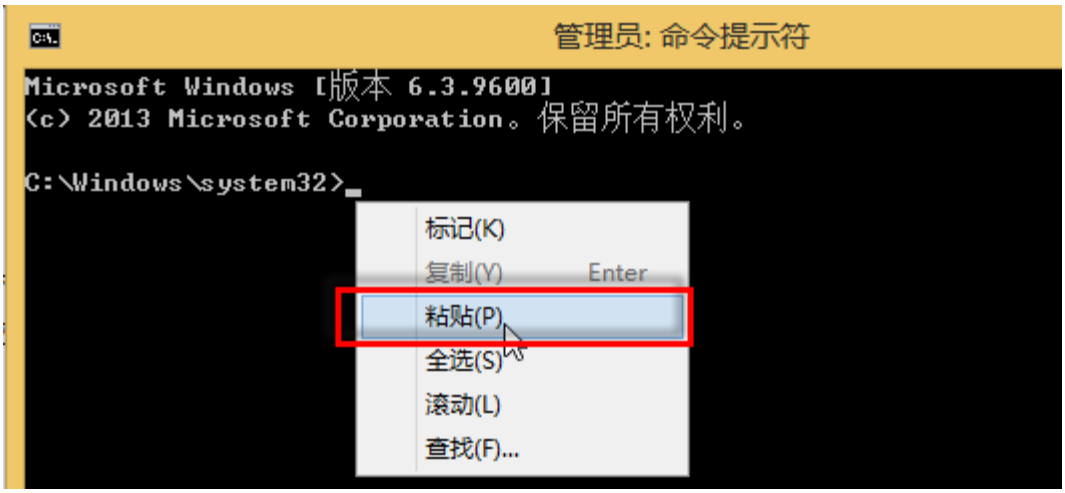
弹出菜单选择命令提示符（管理员）



先复制下面绿色文字，在命令提示符窗口点右键选择“粘贴”，把下面代码粘贴到命令提示符窗口

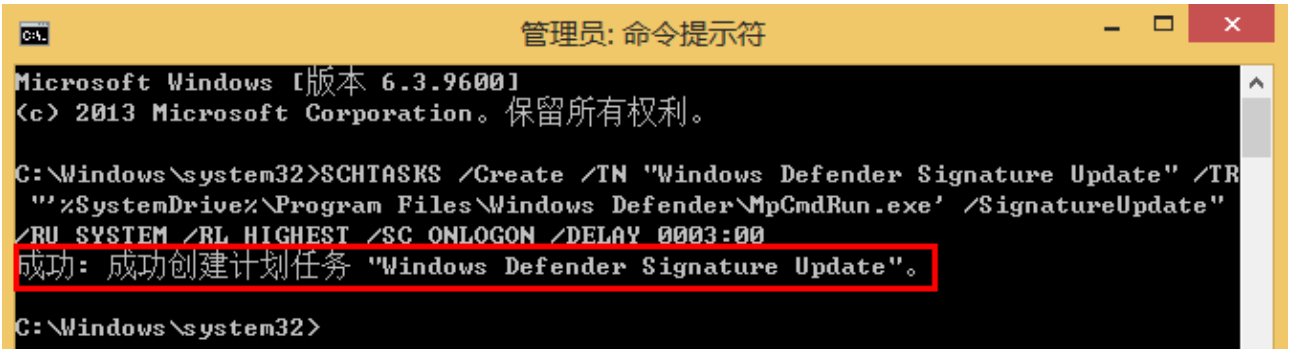
```
SCHTASKS /Create /TN "Windows Defender Signature Update" /TR
"'%SystemDrive%\Program Files\Windows Defender\MpCmdRun.exe' /SignatureUpdate"
/RU SYSTEM /RL HIGHEST /SC ONLOGON /DELAY 0003:00
```

“/DELAY 0003:00”表示延迟三分钟执行。之所以设置为三分钟，主要是考虑到启动之后加载自启动项、连接网络都需要时间，如果你需要更长的时间，可以自行修改。



粘贴效果如图，之后按键盘回车键

显示成功创建计划任务，就完成了设置。



大陆直连看禁书禁闻禁文禁网禁片禁歌禁曲

禁书网提供禁书下载阅读,禁书目录,禁书网http://www.bannedbook.org/是最大最全的禁书下载基地,中国禁书,大陆禁书应有尽有。

禁书禁闻禁片大陆直连：https://pipes.yahoo.com/pipes/pipe.run?_id=40fbfb511221f769a51746fa91a1ff4f