更多互联网新鲜资讯、工作奇淫技巧关注原创【飞鱼在浪屿】（日更新）

从7月底开始，微软开始认为，通过HOSTS文件阻止Windows 10远程服务的行为，是“严重”安全风险。

HOSTS文件是位于C:\Windows\system32\driver\etc\HOSTS的文本文件，只能由具有管理员权限的程序进行编辑。

该文件作用是无需使用域名系统（DNS），将主机名解析为IP地址。

该文件一个小技巧是，将域名主机名映射到127.0.0.1或0.0.0.0到IP地址来达到阻止计算机访问远程站点到目的。

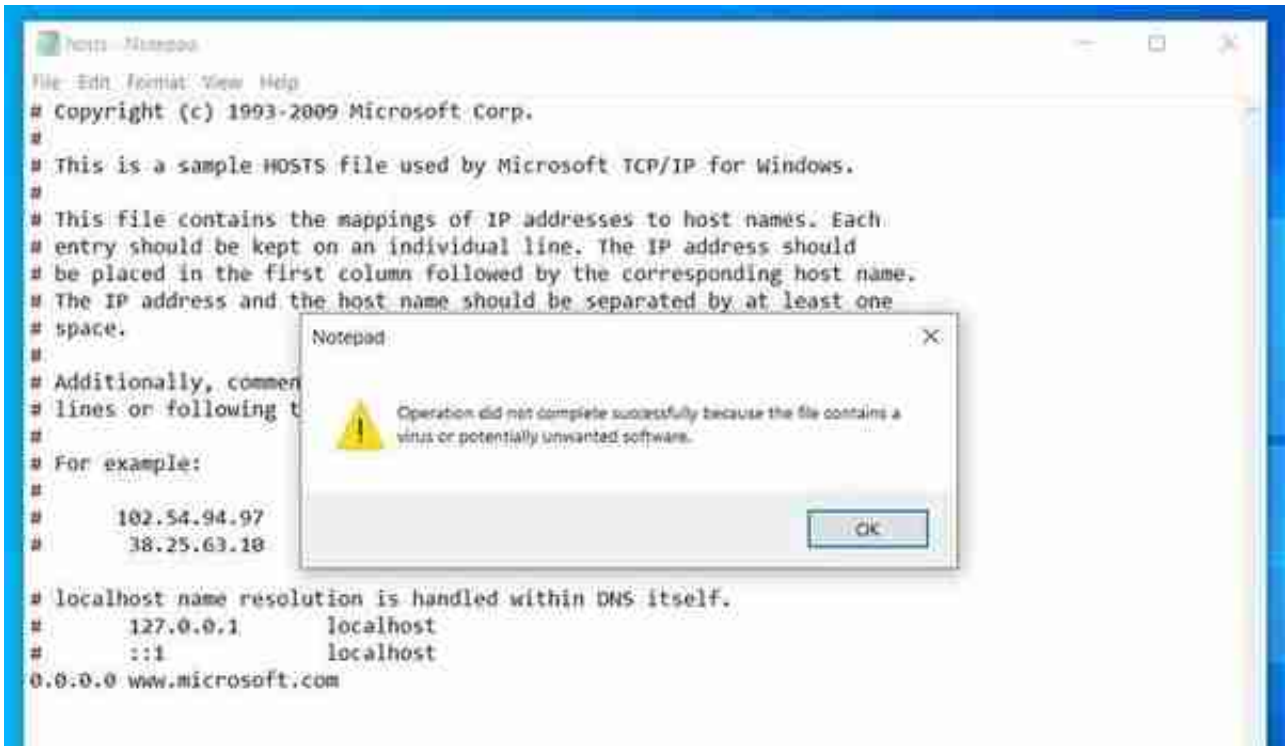
例如，如果将以下行添加到Windows HOSTS文件中，它将阻止用户访问www.google.com，因为浏览器会认为你正在尝试连接到本地计算机127.0.0.1。

```
127.0.0.1 www.google.com
```

Microsoft现在可以检测到阻止Windows远程服务的行为

自7月底以来，Windows 10用户开始报告Windows Defender已开始将HOSTS文件的windows域名修改行为“SettingsModifier：Win32 / HostsFileHijack”威胁。

一旦检测到，用户将看到以下选项，将显示他们受到“设置修改器”威胁并且具有“潜在有害行为”，如下所示。



因此，似乎Microsoft最近更新了Microsoft Defender定义，能检测微软域名服务器添加到HOSTS文件中的行为是违法的。

Windows 10 HOSTS文件中检测到告警的一些Microsoft主机包括：

```
www.microsoft.commicrosoft.comtelemetry.microsoft.comwns.notify.windows.com.akadns.netv10-win.vortex.data.microsoft.com.akadns.netus.vortex-win.data.microsoft.comus-v10.events.data.microsoft.comurs.microsoft.com.nsatc.netwatson.telemetry.microsoft.comwatson.ppe.telemetry.microsoft.comvsgallery.comwatson.live.comwatson.microsoft.comtelemetry.remoteapp.windowsazure.comtelemetry.urs.microsoft.com
```

如果决定清除此威胁，Microsoft将把HOSTS文件恢复到其默认内容。