AsiaInfo | 亚信安全

黑客预防指南

背景： 聪明的黑客不会被抓。他们闯入你的设备，偷走一切，然后毫无痕迹地完成。有时，他们会留下一条毁灭的痕迹--恶意软件，奇怪的广告，困惑的亲戚，甚至是一个耗尽的银行账户或被盗的身份。电脑、电话、路由器和无辜的网络摄像头都容易受到网络罪犯的攻击。如果他们已经闯入了，但你却不知道他们在那里呢？这里有明确的迹象表明你被黑了。

AsiaInfo | 亚信安全

常见的可疑现象

视频经常缓冲

网页需要很长时间才能加载。 当一个流媒体视频突然冻结，你的设备似乎在“思考”，这就是所谓的缓冲。这种烦恼经常发生，特别是当你播放很多视频是你的Wi-Fi连接薄弱。如果它经常发生，或者视频播放不了，你最好怀疑你的电脑已经被入侵了。

你的电脑突然慢下来

恶意软件的副作用之一是一个缓慢的小工具。软件变得迟缓，或不断冻结，甚至崩溃。如果你开始注意到其中的一些症状，你的电脑很可能被病毒，木马或蠕虫感染

程序和应用程序开始崩溃

如果您的防病毒软件和任务管理器正在崩溃或禁用，那么可能会有一个讨厌的病毒控制您的关键系统文件。

你的计算机突然重新启动

自动重新启动是正常计算机生活的一部分。软件更新和新的应用程序安装可以提示您重新启动计算机。当发生这种情况时，系统会警告您，您可以延迟或推迟它们。 然而，突然重启则是另一回事了，您可能被恶意软件控制了。

黑客觊觎你的用户名和密码

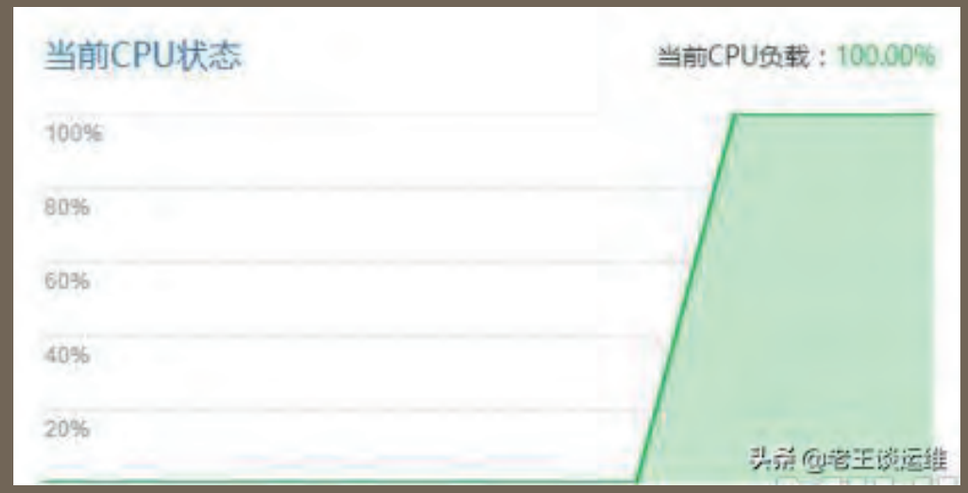
这些细节，再加上社会工程技巧，可以猜测破解您的各类帐户，如您计算机账户、社交媒体简介，以及您的在线服务。

AsiaInfo | 亚信安全

电脑自检小技巧

检查自己的任务管理器：

使用任务管理器 有几种方法可以查看计算机正在运行的进程。最简单的是打开Windows的内置任务管理器。只需使用键盘快捷方式CTRL+Shift+ESC并转到Process选项卡。 简单地说，任务管理器列出了计算机当前的所有任务，以及它们在中央处理单元(CPU)中使用的处理能力。打开任务管理器，检查每个进程的CPU和内存列。



检查自己计算机账户，在CMD中输入 net user 指令命令符，查看本台电脑上有哪些账户正在操作我们的电脑。如果你发现其中一个账户是你不认识的陌生账户，那么这个账户可能就是别人入侵你电脑的克隆账户。这个时候，你可以使用

解决方法：“net user 用户名/del”来删除掉这个账户名

AsiaInfo | 亚信安全

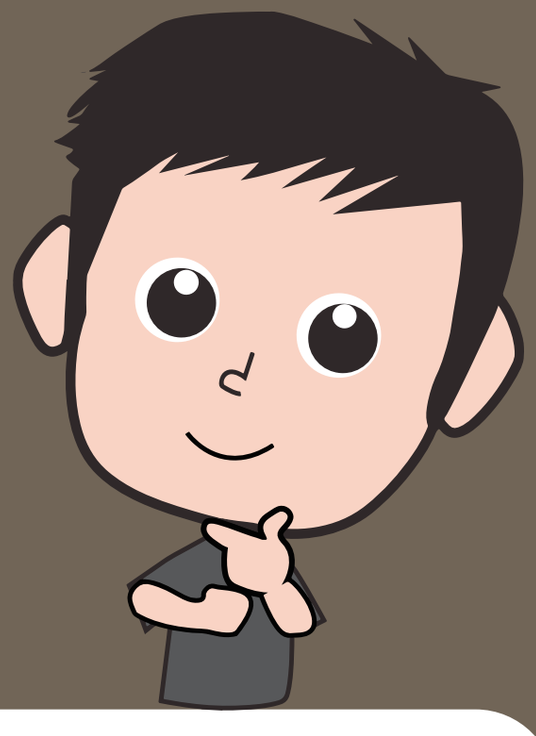
您可以通过使用Netstat命令自检：

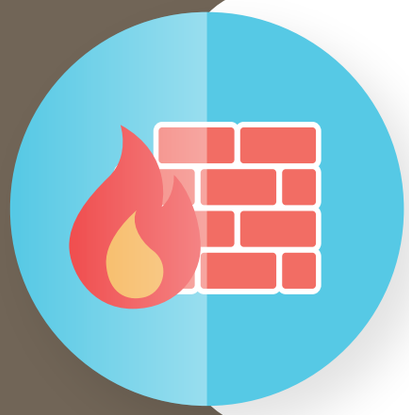
Netstat 的用法：netstat -an
查看是否存在一些恶意的IP连接，比如开放了一些不常见的端口，正常使用到的端口：

80网站端口
8888端口
21FTP端口
3306数据库的端口
443 SSL证书端口
9080 java端口
22 SSH端口
3389默认的远程管理端口
433 SQL数据库端口

AsiaInfo | 亚信安全

预防黑客的小技巧





1.安装防毒软件

切勿贪图方便让自己的计算机处于“裸奔”状态，没有防护的计算机很容易成为黑客的目标，将自己的计算机变为“肉鸡”，造成损失。现在的防毒软件也越来越厉害了。只要电脑在使用过程中没有访问乱七八糟的那些网站和软件，最新的防毒软件就可以保证的电脑的安全。

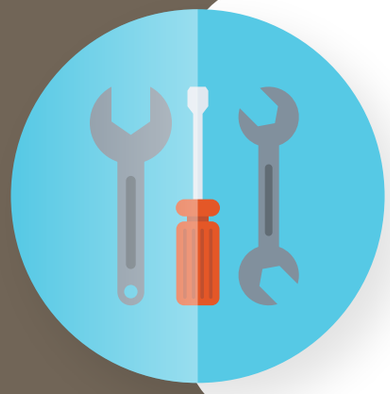
2.创建安全密码

很多人的设备一直是默认用户名和密码，或者是很简单的密码，这很容易被不法之徒破解。所以创建一个复杂安全的密码是非常有必要的，现在一个非常安全的密码使得暴力破解几乎不可能。

AsiaInfo | 亚信安全

3.定期系统清理和恢复

定期给系统做好备份。一旦电脑出现什么问题，可以直接恢复到上次安全状态，可以将那些垃圾软件包括僵尸网络软件给清理干净。



4.定期检查路由器

定期检查路由状态与设置，检查是否有未知的可疑设备连接您的网络为防止DNS劫持， 最好定期检查您的DNS设置是否已修改，并确保您的DNS服务器是安全的。建议使用复杂的密码重置路由器的默认密码。

5.定期检查自己的账户

定期检查自己的账户状态，对于一些重要账户设置复杂密码并且定期更新尽量不要使用统一的密码，尤其是和身份信息相关的密码以免被撞库破解。