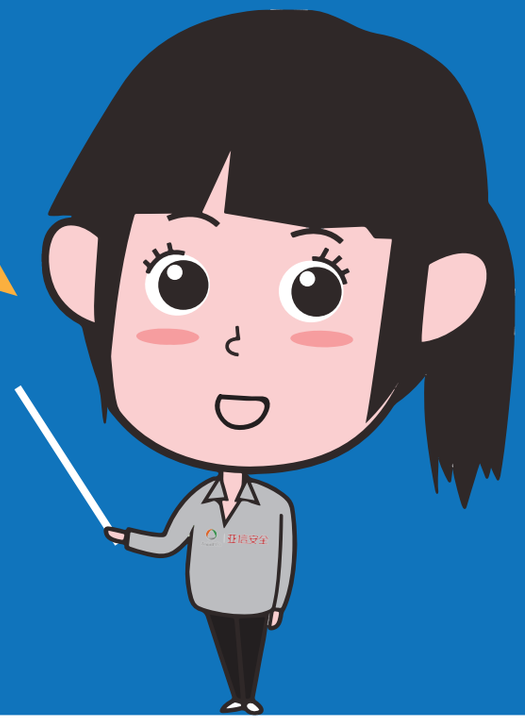
AsiaInfo | 亚信安全

游戏外挂的危害和防护建议

对于资深游戏迷来说“外挂”这个词一定不陌生。尽管面临被封号的危险，但仍有部分游戏玩家玩儿游戏喜欢到处找外挂或游戏辅助工具，而病毒传播者往往利用游戏玩家这一点传播木马病毒，专门用来游戏盗号、窃取隐私，甚至远程控制。



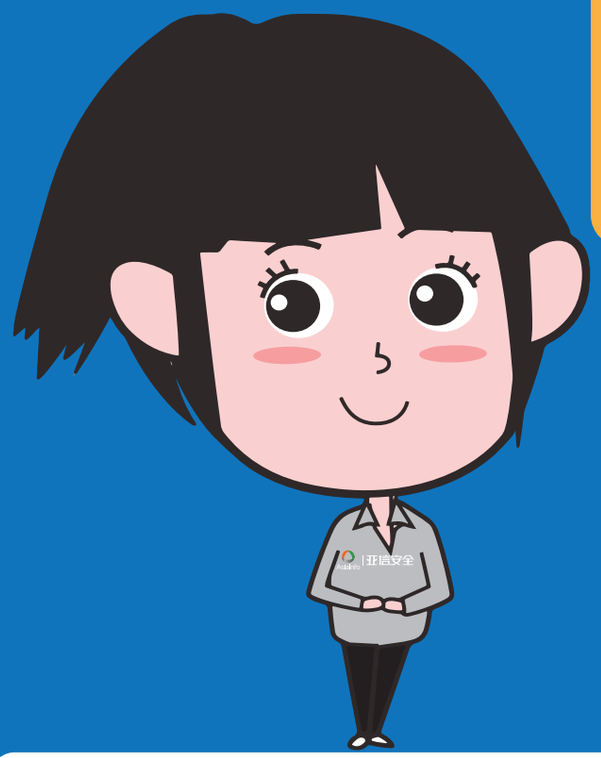
背景:

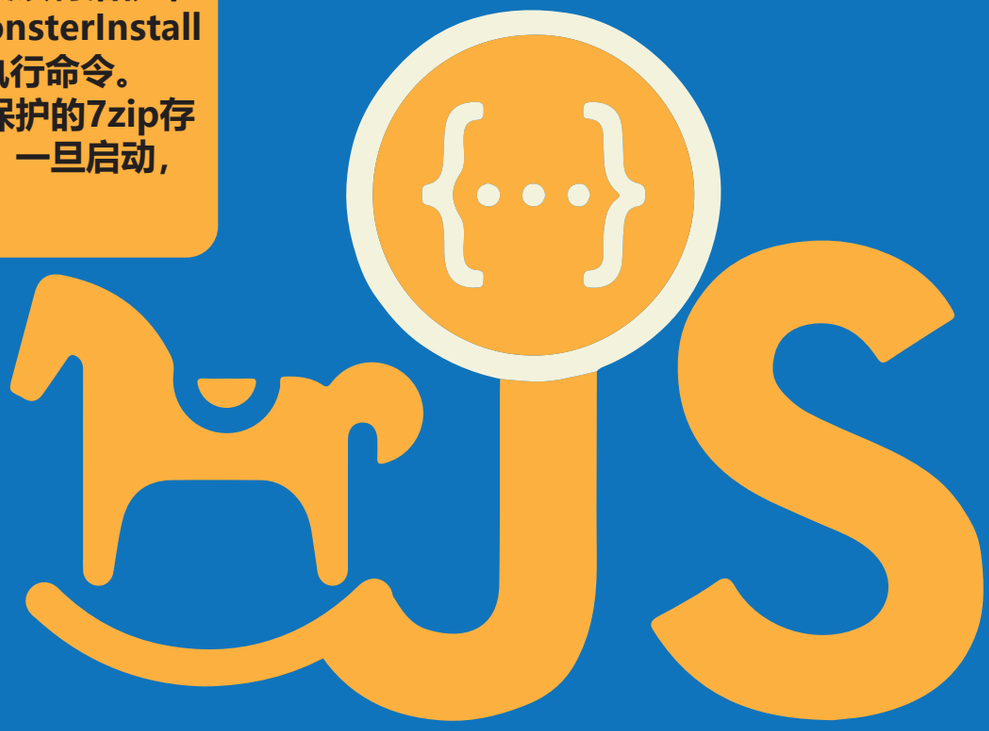
游戏外挂一般指通过修改游戏数据而为玩家谋取利益的作弊程序或软件，即利用电脑技术针对一个或多个软件进行非原设操作，篡改游戏原本正常的设定和规则，大幅增强游戏角色的技能和超越常规的能力，从而达到轻松获取胜利、奖励和快感的好处，通过改变软件的部分程序制作而成的作弊程序。主要应用原理是在游戏中用封包和抓包工具对游戏本身或游戏服务器提交假参数从而改变游戏中的人物能力。 使用外挂具有一定风险，特别是在非单机游戏中使用破坏游戏公平性的外挂，可能还会被封禁账号。

AsiaInfo | 亚信安全

外挂攻击过程简介
--基于JavaScript的木马

最近，研究人员发现了一种新的基于JavaScript的模块化下载程序特洛伊木马，并通过其开发人员拥有的网站以游戏外挂的形式分发给目标。该恶意木马是由研究人员发现，随后将其发送给研究团队进行进一步分析，并提供了有关如何分发该特洛伊木马样本的其他信息。研究人员发现，这个被称为MonsterInstall的特洛伊木马程序使用Node.js在受害者的机器上执行命令。
当用户试图下载这个外挂时，他们会将一个受密码保护的7zip存档下载到他们的计算机上，里面有一个可执行文件。一旦启动，将下载该外挂以及其他木马组件



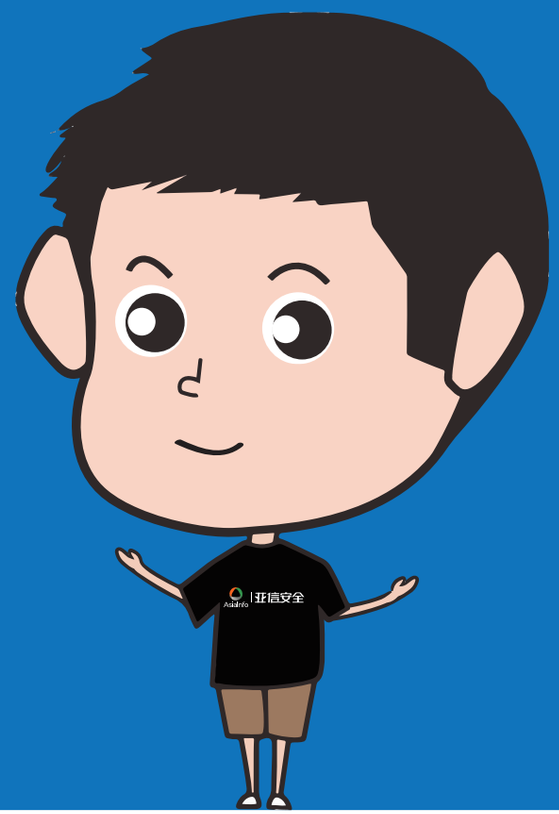


游戏外挂大多“有毒”，游戏向来是不法分子发动网络攻击的重灾地，伴随着各类游戏的火爆，不法分子也进一步精确攻击对象。其实外挂本身是通过更改游戏数据的方式实现外挂作用的，所以外挂本身就是一种病毒，自然会被识别成病毒。惟一的方法是在使用外挂的时候关闭杀毒软件。但不可否认现在外挂带病毒的现象十分普遍，关闭了杀毒软件就更容易中毒了。游戏外挂是通过修改游戏的部分程序制作而成，外挂可以对游戏数据甚至是电脑数据进行修改。外挂制作者在外挂中加入木马病毒就可以轻而易举地掌握玩家的个人信息，这些信息中可能包括支付交易的账号、密码或电脑中存放的照片，文件等。

AsiaInfo | 亚信安全

外挂攻击过程简介

--渗透系统，收集信息



启动后，MonsterInstall下载程序木马通过将自身添加到受感染计算机的自动运行来获得持久性，以便在重新启动计算机后也能自动启动。随后，MonsterInstall将开始收集系统信息并将其发送到其命令和控制(C&C)服务器。“作为回应，它接收到特洛伊木马工作程序和更新程序模块的链接，解压缩并将它们安装到系统中。”

AsiaInfo | 亚信安全

游戏外挂中毒案例

外挂引火上身了吧！
被勒索了吧！

2017年6月2日，就有消息爆料了一款冒充时下热门手游《王者荣耀》辅助工具的手机勒索病毒。该勒索病毒被安装进手机后，会对手机中照片、下载、云盘等目录下的个人文件进行加密，并索要赎金。据了解，该勒索病毒是国内第一款文件加密型勒索病毒，有爆发迹象，会威胁几乎所有安卓平台的手机。用户一旦中招，可能丢失所有个人信息。

据称，该勒索病毒伪装成当下最热门的手游《王者荣耀》辅助外挂来诱惑用户下载和安装，并通过PC端和手机端的社交平台、游戏群等渠道进行传播扩散。其在界面上高仿电脑版的“永恒之蓝”勒索病毒，功能和电脑版一致。软件运行后，用户的桌面壁纸、软件名称和图标会被篡改。如果用户三天内不解密，赎金将翻倍。一周不解密，手机中所有文件将被删除。

AsiaInfo | 亚信安全

四个必要防范措施

1 坚决不下载来历不明的exe运行程序。如果发现有来历不明的程序正在运行，**立即按Ctrl+Alt+Del三个键，立即将该程序结束任务**。检查电脑里面安装的程序，如果发现有一些陌生的程序，请直接卸载。

2 安装和使用**亚信安全终端防护产品**。如果游戏外挂程序建议你在运行前关闭杀毒软件，大概率这是安全陷阱。病毒木马传播者一贯用类似手段欺骗用户退出杀毒软件，这样病毒的破坏就能畅通无阻了。

3 不要随便打开来历不明邮件的附件

4 定期给电脑和手机系统做备份，一旦遇到问题，可直接恢复到上次安全状态，将损失降到最低程度。