警惕伪装成QVOD安装程序的释放器木马

产品名称	警惕伪装成QVOD安装程序的释放器木马
公司名称	江苏国骏信息科技有限公司
价格	1.00/台
规格参数	
公司地址	徐州市解放南路矿大科技园软件园A座
联系电话	0516-83887908-608

产品详情

江苏国骏--徐州卡巴斯基金牌供应商 资讯：近日，知名信息安全厂商卡巴斯基发布病毒播报，提醒用户注意一款恶意程序名为trojan-dropper.win32.agent.iifd的木马。

这是一个伪装成qvod安装程序的释放器木马。木马运行后首先从资源中查找“ cabinet ”的资源并将其解压至临时目录下的qvodin~1.exe和compre~1.exe并运行。其中qvodin~1.exe是qvod的安装程序，会在前端安装qvod软件，而compre~1.exe则是木马程序，会被隐蔽安装。此外，该木马还会释放驱动，关闭安全软件进程；在桌面释放广告快捷方式；修改ie主页；将mac地址等信息发送到122.207.87.***/id/count.asp?进行安装量统计；还会从61.132.227.**、186.2.165.***、186.2.165.***等地址下载安装其它恶意程序。

卡巴斯基提醒广大用户及时更新反病毒产品的病毒库，并定期为系统打补丁，不打开可疑邮件和可疑网站，不随意接收聊天工具上传送的文件以及打开发过来的网站链接，使用移动介质时最好使用鼠标右键打开使用，必要时先要进行扫描，不从不可靠的渠道下载软件，因为这些软件很可能是带有病毒的。徐州地区唯一的卡巴斯基认证服务机构--江苏国骏信息科技有限公司