警惕电脑成木马病毒“ 海洋 ”PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/475/2021_2022__E8_AD_A6_E6_83_95_E7_94_B5_E8_c67_475810.htm 11月26日，金山毒霸反病毒监测中心发布周（11.26-12.02）病毒预警，本周内广大用户需高度警惕“ 海量下载器XO号 ”（Win32.Troj.DownArpT.xo.135168）。该病毒可下载海量病毒文件至用户电脑，占用大量系统资源，造成系统严重瘫痪，致使你的电脑成为木马病毒的海洋。 金山毒霸反病毒专家戴光剑表示，该病毒运行后，会在系统盘中生成数量极大的病毒文件群，其中%windows%\目录下的upxdnd.exe病毒文件很值得注意，因为它的相关信息会被加入注册表启动项，这使得病毒在每次系统重启时都能随之启动。之后，病毒就会立即自删除源文件，使用户无法找到病毒源。 据了解，该病毒运行后就开始连接http://www.n***23***1.com/这一远程地址，下载并立即运行大量其它病毒文件，占用大量系统资源，造成系统严重瘫痪，致使你的电脑成为木马病毒的海洋。值得一提的是，这些下载的病毒文件，其文件名是由1~20的数字加上EXE后缀构成。 戴光剑分析指出，该病毒下载的其他病毒多数为盗号木马，会盗取各种网络游戏和即时聊天工具的帐号信息；还有个别病毒会下载ARP病毒，当用户中了ARP病毒后，在同一个局域网内的其它计算机都有可能遭受欺骗，造成局域网极其不稳定。 近几周，木马病毒异常活跃，本周内用户还需高度警惕“ 灰鸽子新变种333312 ”（Win32.Hack.Huigezi.hx.333312）。“ 灰鸽子 ”近日有死灰复燃的迹象，病毒运行时，在用户不知晓的情况下开启系统后

门，连接远程服务器，为让黑客远程控制用户机器提供方便。当远程控制成功后，黑客便可执行捕捉多媒体信息、文件管理、创建和关闭服务、创建和终止进程、获得用户进程与模块列表、执行命令、获取窗口标题等几乎所有他们想要的操作。将用户电脑变成一个任其摆布的“肉鸡”。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com