附件1:

# "苏拉克"木马病毒介绍

"苏拉克"木马主要传播方式是直接在ghost 镜像中植入木马，然后将ghost 镜像上传到大量网站提供给用户下载。同时该木马通过Windows8 和Windows10 的OEM 激活工具植入用户电脑中。由于该木马的主要模块名为"surak. sys" ，且通过分析得知该木马的项目名称即为"surak" ，因此将其取名"苏拉克"木马。从2015 年10 月份以来，国内反病毒机构监控到大量的传播带毒镜像的网站，此类网站一般伪装成"系统之家"网站，并通过搜索推广或者直接刷搜索引擎来使自身排名靠前。此外还在各大装机相关的论坛布满了带毒ghost 系统的推广帖，吸引大量网友上钩。

由于该木马被植入到ghost 镜像中，用户一旦安装系统就自带该木马，而此时尚未安装任何安全软件，因此木马的传播过程完全不在监控中。大量网站传播该类ghost 镜像，普通用户通过搜索引擎找到的镜像下载网站几乎均携带"苏拉克"木马。该木马进入系统时间比安全软件早，掌握了主动权，对其后安装的安全软件做了大量的功能限制，使其大量功能无法正常使用，如安全防护无法开启、信任列表被恶意操作等，导致难以检测和清除木马。木马除了锁定浏览器主页获利外，还会实时连接云端获取指令，能够下载其它木马到本地执行，给系统安全造成了极大的威胁。此外，针对64 位系统，该木马还会修改系统内核文件，使得64 位系统自带的驱动签名校验、内核防钩子等安全机制全部失效。