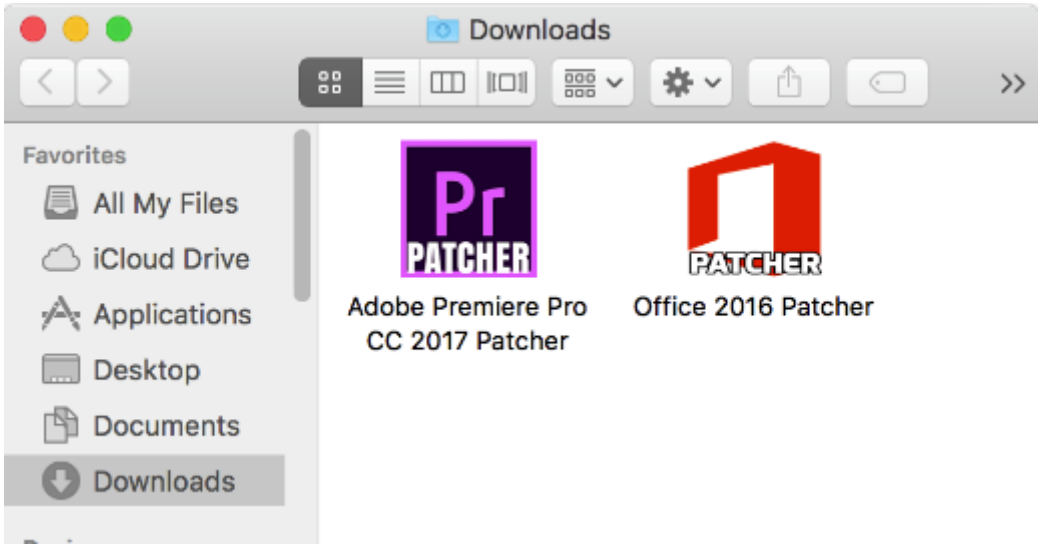
信息分享

2017 年 3 月 14 日

新型 MacOS 勒索病毒来袭

2 月初，亚信安全预测针对非 Windows 系统的勒索病毒开始崛起。如预测所言，近日亚信安全截获了针对 MacOS 的勒索病毒 Patcher，我们将其命名为：OSX_CRYPPATCHER.A。

Patcher 是通过 bittorrent 文件下载传播，其会伪装成 Microsoft Office 和 Adobe Premiere Pro 等热门软件的补丁程序，下载完成后，文件夹中会显示带有 Patcher 字样的恶意应用程序。



图一、下载到本机的勒索病毒示例

该恶意软件运行时，屏幕上会出现开始打补丁的界面，诱骗用户相信该软件是真正的补丁程序。Patcher 勒索病毒一旦被运行，其会将/Users 目录以及/Volumes 目录下外接设备中的所有文件加密。Patcher 病毒使用随机 25 个字符作为加密密钥。其也会在系统中放置勒索信息，勒索金额为 0.25 比特币（约 300 美元）。

图二、勒索病毒运行后显示开始安装界面

经过对该样本的深入研究，我们发现该勒索病毒存在严重的设计缺陷，其无法与幕后 C&C 服务器进行通讯，这也意味着即使用户交付了赎金，黑客也无法解开被加密的文件。因此我们推断 Patcher 勒索病毒作者缺乏经验，以至于出现了代码上的错误，即便如此也没有影响其危害性，由于没有解密方法，被加密的文件可能永远无法恢复。

防护方法：

亚信安全深度威胁发现设备 TDA 独特的侦测引擎加上定制化沙箱动态模拟分析，能快速发掘并分析恶意文档，恶意软件、恶意网页，C&C 通信数据以及传统防护无法侦测到的定向式攻击活动，其与亚信安全终端安全产品实时联动，有效阻止勒索病毒。

如预测所言，为获取更大利益，针对非 windows 系统的勒索病毒会越来越多，亚信安全提醒您非 windows 系统安全同样重要，用户需提高警惕，不给病毒可乘之机。