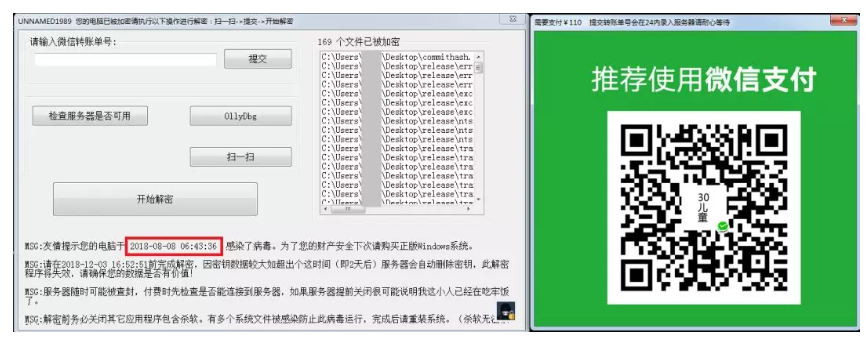
**假冒灰产工具勒索病毒“微信支付”** **安全通告**

2018年12月2日 VenusEye团队

近日，一款使用微信扫码支付作为赎金支付渠道的勒索病毒出现。该勒索病毒借助一个名为“账号操作 V3.1”的假冒灰产工具进行传播，由于使用这类灰产工具的人群经常会无视杀毒软件的拦截提示，因此，该勒索病毒针对灰产从业者的定向传播十分有效。



该勒索病毒只加密用户的桌面的txt、office等文件，并会跳过一些指定名称开头的目录文件，包括“腾讯游戏、英雄联盟、tmp、rtl、program”，而且不会感染使用gif、exe、tmp等扩展名的文件。与其他勒索病毒不同的是，没有修改原文件后缀名，并在桌面释放一个“你的电脑文件已被加密，点此解密”的快捷方式。点击后会弹出解密程序和付款二维码。



另外病毒使用白加黑的方式调用腾讯签名的程序文件加载病毒代码以逃避杀毒软件检测。

病毒使用的加密方式为简单异或加密，解密密钥相关数据被存放在%user%\AppData\Roaming\unname\_1989\dataFile\appCfg.cfg中。因此即使在不访问病毒作者服务器的情况下，即可成功完成数据解密。

**处理建议：**

目前已有厂商提供针对该勒索病毒的解密工具，可通过启明星辰VenusEye威胁情报中心勒索专题页面（lesuo.venuseye.com.cn）下载相关工具，查看病毒详情。





**参考链接：**

https://mp.weixin.qq.com/s/irFw2eXFAUeo1JRZu7hNeA

https://mp.weixin.qq.com/s/xxOIjCXtoMyyXmr0AUw\_9g