

新华社福州2月5日电(记者 颜之宏)国外网络安全机构近日截获一组名为Mind Lost的新型勒索病毒,和以往的勒索病毒最大不同在于,Mind Lost不再要求“中招”用户使用比特币等数字货币支付赎金,而是要求受害者使用信用卡或借记卡支付赎金,以此来套取银行卡信息,进而将此信息出售给不法分子牟取更大利益。

国内多家互联网安全企业也于本月初截获了该型勒索病毒。据安全研究人员介绍,该病毒目前只会对C盘下的Users文件夹中的文件进行加密,并且所有加密文件将会得到一个新的扩展名.enc(例如image.png.enc)。一旦加密结束,Mind Lost将自动下载带有勒索信息的图像,并将其设置为计算机的新桌面墙纸,该图像包含支付赎金的说明。

幸运的是,安全研究人员发现该病毒此时尚未处在“主动分发”的活跃状态。腾讯安全平台部blade团队在对该病毒样本进行研究时发现,Mind Lost的代码尚不完善,且存在大量错误,因此怀疑该病毒仍在开发阶段。但blade团队提醒,如果该病毒进入“主动分发”状态,有可能造成支付赎金的用户支付卡账户信息泄露,存在财产损失的风险。

360反病毒专家王亮告诉记者,根据目前的监测情况来看,我国尚未发现遭受此新型病毒勒索的实例,用户无需过度恐慌,只需正常安装相应杀毒软件即可。王亮同时建议,不要在非银行官网的页面下输入银行卡的口令、有效期等敏感信息,更不可在黑客提供的页面下输入上述信息,否则银行卡存在被盗刷的风险。

腾讯电脑管家安全技术专家马文瑞表示,此前发现过国产勒索病毒要求受害者通过扫描二维码支付赎金的案例,但是通过银行卡支付赎金的勒索病毒尚属首例。马文瑞认为,尽管国内尚未发现该病毒的传播迹象,但是互联网用户也应及时升级病毒查杀软件,同时不要轻易点击来路不明的下载链接,不要随意放行被杀毒软件拦截的程序。

据了解,包括360安全卫士、腾讯电脑管家、火绒安全等在内的主流杀毒软件已经具备查杀Mind Lost的能力,用户如遭遇勒索,切勿盲目使用银行卡支付赎金,应第一时间向相关网络安全企业寻求帮助。

我国第十七次计算机和移动终端病毒疫情调查启动

国家计算机病毒应急处理中心监测发现七款违法移动应用