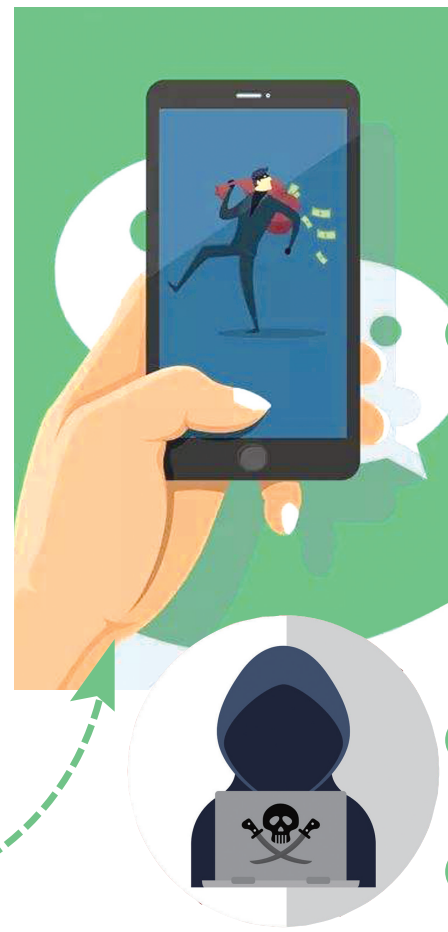
“勒索病毒”来了,这次瞄准微信

如已感染病毒 可用解密工具尝试

记者5日从国家互联网应急中心天津分中心和多家互联网安全机构获悉,12月1日前后,一种新型的勒索病毒在国内开始传播,该勒索病毒要求受害者使用“微信支付”支付赎金。病毒制作者利用github、CSDN、豆瓣、简书、QQ空间等网站页面作为下发指令的C&C服务器,加密受害者文件并勒索赎金,同时窃取支付宝等软件密码。

该勒索病毒在感染用户计算机后不会勒索比特币,而是弹出微信支付二维码,要求受感染用户使用微信支付110元,从而获得解密密钥,这也是国内首次出现要求使用微信支付的勒索病毒。目前,微信运营商判定该支付二维码存在违规行为,并表示已无法通过扫描二维码支付赎金解密。



五种措施进行防范

1. 安装并及时更新杀毒软件,目前市场主流反病毒软件都已支持针对该勒索病毒的防护与查杀。
2. 不要轻易打开来源不明的软件,该勒索病毒通过易语言编写的程序传播,减少使用来源不明的软件可有效预防。
3. 如已经感染勒索病毒,可使用相关解密工具尝试解密。目前,许多公司已经针对该勒索病毒开发了解密工具,包括火绒Bcrypt专用解密工具、腾讯电脑管家“文档守护者”、360安全卫士“360解密大师”等。
4. 已感染勒索病毒的用户,在清除病毒后,尽快修改淘宝、天猫、支付宝、QQ等敏感平台的密码。
5. 定期在不同的存储介质上备份计算机中的重要文件。

病毒还窃取QQ支付宝等密码

截至12月3日,已有超两万用户感染该病毒,被感染电脑数量还在增长。除了感染电脑中的软件,这次勒索病毒还盯上了包括路由器、智能摄像头在内的智能硬件。

网络安全专家王亮介绍,感染这种勒索病毒之后,用户第一个感觉就是突然自己的桌面背景被人换了,比如说Word文档照片打不开,文件扩展名被修改。

该病毒还窃取用户的各类账户密码,包括淘宝、天猫、阿里旺旺、支付宝、163邮箱、百度云盘、京东、QQ账号,建议被感染用户尽快修改上述平台密码。

弹出解密教程和收款二维码

“不同于其他勒索病毒,此次勒索病毒没有修改文件后缀名。”腾讯电脑管家安全专家称,一经感染,该勒索病毒对用户电脑加密txt、office文档等有价值数据,并在桌面释放一个“你的电脑文件已被加密,点此解密”的快捷方式后,弹出解密教程和收款二维码,最后强迫受害用户通过手机转账缴付解密酬金。

腾讯电脑管家安全专家表示,从多个用户机器提取和后台数据追溯看,该勒索病毒的传播源是一款叫“账号操作 V3.1”的易语言软件,可以直接登录多个QQ账号实现切换管理。

病毒作者首先攻击软件开发者的电脑,感染其用以编程的“易语言”中的一个模块,导致开发者所有使用“易语言”编程的软件均携带该“勒索病毒”。广大用户下载这些“带毒”软件后,就会感染该“勒索病毒”。

回应

微信:对涉勒索病毒账户封禁

腾讯回应称,该新型勒索病毒通过加密电脑上的doc、jpg等常用文件,然后利用微信支付二维码进行勒索赎金。

微信支付方面回应称,微信已第一时间对所涉勒索病毒作者账户进行封禁、收款二维码予以紧急冻结。微信用户财产和账户安全不受任何威胁,并表示,微信对任何形式的网络黑产犯罪“零容忍”。

微信支付提醒用户,该勒索病毒可能通过任何形式的支付方式索要转账,若遭遇勒索,不要付款,及时报警。同时,腾讯电脑管家提供解密工具和人工服务,协助用户处理相关情况。

支付宝:被盗全赔

支付宝安全团队也第一时间进行了跟进,现将了解到的相关情况同步分享给大家:

1、该勒索病毒仅出现在PC端上,被感染的电脑会记录键盘行为,获取用户在各类平台输入的密码信息。建议大家及时安装安全软件查杀病毒。

2、针对此类风险,支付宝风控系统早有针对性的防护,包括二次校验短信校验码、人脸识别等。即便密码泄露,也能最大程度地确保账户安全。

3、目前未收到支付宝账户受影响的用户反馈。

4、支付宝自2005年起便启动“被盗全赔”的用户保障计划。请放心,即便出现小概率事件的账户被盗,也会得到全额赔付。

专家解读

越高级,可能越危险

腾讯电脑管家技术专家李铁军告诉记者,“互联网领域,这几年勒索病毒的数量增长比较快,很多勒索病毒的水平不是很高,但是影响会比较大。”

上述案例中,勒索病毒采用的手法并不高级,但却是国内首款要求微信支付的勒索病毒,而且赎金仅110元,很可能打的就是网民“破财免灾”的心理战术。如果用户迫于一时麻烦缴纳了赎金,积少成多的金额也不容小觑。

“勒索者要的是这110元,感觉是个新手在恶作剧,挑战法律秩序。”李铁军表示,“目前虽然不清楚具体的总赎金金额,但因为安全厂商的解密方案是免费的,作者应该没赚到多少钱。”

总体来说,这款勒索病毒的赎金不高却给广大网民提了个醒儿:越高级,可能也越危险。

随着IoT和智能终端的普及,设备与账户支付之间的间隔路径越来越短,指纹锁、机械键盘等面临网络黑客的攻击已经很难再独善其身。面向未来的人工智能,如果安全基础没有打牢,很可能就变成了人“攻”智能。

如果你惯常使用机械键盘,那么对于一个叫做Keytap的“黑科技”就要小心了。该技术已在国外走红,可以通过监听你敲击键盘的声音,完成声波采集的任务,并还原出你输入的内容,无论是银行密码还是私密心事,都可以被“监听”。目前这款代码已经实现开源。

科技提供便利,但就像硬币的两面,在“用”与“不用”之间,未来你更是要在便利性和安全性之间做出权衡。已经有不少上市公司面向IoT时代的信息安全需求做出部署。

相关

红包短信轰炸 支付宝:没发过!

这几天,你有被“支付宝红包”短信“轰炸”吗?这些短信真的是支付宝发送的吗?记者从蚂蚁金服方面获悉,这些短信并非支付宝官方发送。“赚钱红包”是为了奖励线下商家推广移动支付而推出的一项活动。在活动规则中已明确不能采用滥发短信等过度推广的方式,否则会采取取消活动参与资格等措施。

如果收到这些短信,是不是意味着支付宝把手机号泄露给别人了?蚂蚁金服方面表示,支付宝有严格的用户信息保护措施,不会将用户手机号码等任何个人信息泄露给第三方。第三方发送红包短信的手机号码并非来自于支付宝。据了解,这样的短信主要是通过106短信营销平台等方式,直接向某个手机号段的用户集体发送,以诱导用户领取推广者的红包。

(综合新华社、北京晚报、金陵晚报)

大跌眼镜的体检:已经切除的胆囊意外“复活”!

护士冒充医生、血液丢掉不检照给正常结果……近日一家体检机构负责人对体检乱象的爆料,引发公众热议。近年来,随着人们对健康问题愈加重视,体检行业的市场需求呈爆发式增长。与此同时,误检错检频发等乱象,让人大跌眼镜。

奇葩检查结果暴露行业漏洞

海南的韩先生最近遇到了一件让他哭笑不得的事:2016年7月,韩先生在海口市人民医院做了胆囊切除手术,但2016年12月、2018年9月先后两次在海口某民营体检中心体检时,检查报告均显示“胆囊大小形态正常,壁不厚,腔内未见明显异常回声”。

对此,该体检中心回应称,这主要是因为体检系统有纰漏,磁条需要更新换代。对于这种解释,海口某三甲医院放射科医师表示,体检系统出现问题的可能性较小,很有可能是检查医师操作失误。

2018年,多家连锁体检机构和医院体检中心被曝出错检、误诊等问题。其中,今年7月底,美年大健康体检中心下属机构广州美年富海门诊部被曝存在使用“冒牌”医生等问题。

套餐分项收费明细不清

今年10月底,国家卫生健康委发文要求,“健康体检机构应当明确本机构开展的健康体检服务项目和价格并进行公示,采用套餐、打包等方式收费时应当明确分项收费明细。”

记者走访多家体检中心发现,一些体检中心并没有将套餐分项价格明细进行公示,部分机构仅在院内做了项目价格表,而套餐项目的单项价格仍让消费者摸不着头脑。记者在位于北京市西城区的一家体检中心看到,接待前台一侧的墙上张贴了各项目单价表,而在各类体检套餐的宣传册中并未看到价格明细。

价格战乱象扰乱市场

体检乱象的背后,是行业内无序竞争的价格战。

海南省一家体检机构负责人介绍,有些体检机构把价格压得很低,差不多两折、三折,根本没利润,其中有的体检机构就会为了生存下去进行造假,这种无序竞争很令人担忧,价格战把市场打乱了,最终受害的是消费者。

比如同样的检测项目,价格悬殊竟然达10倍以上。记者在北京一家体检中心走访过程中,工作人员向记者推荐了烟酒代谢基因检测6项,现价300元。而同样的检测项目在杭州军缘健康管理有限公司官网上,市场价标为3800元,现价1980元。

当问及为什么有这么大的差价时,杭州军缘健康管理有限公司一名工作人员解释说:“这个不大好解释清楚,主要是因为基因检测都是跟外面机构合作的项目,渠道不同,检测机构不一样。” **(据新华社)**