流量攻击 恶意差评 钓鱼邮件

当心网络勒索的“黑手”

2017年5月集中爆发的Wannacry(“想哭”)勒索病毒，至今让全球大量互联网用户心有余悸：该病毒利用漏洞锁定计算机数据和文件,向用户敲诈比特币。据统计,全球超过150个国家、10万家机构组织、100万台电脑遭受该病毒攻击,造成的经济损失超过80亿美元。

这种新型的勒索方式,实际上也掀开了互联网“黑产”的黑幕一角。记者调查发现,近年来随着互联网的迅猛发展,特别是移动互联网的快速普及,过去的敲诈勒索也纷纷改头换面搬到了网上,并且呈现出较过去手法更隐蔽、涉及面更广、危害更大等特点,网络勒索也逐渐发展成一条新兴的地下黑色“掘金”产业链。

黑客入侵勒索 手段不断升级

2017年7月12日,某大型房地产企业发现自己的服务器上数据库被加密，该企业的IT技术人员担心受责罚,隐瞒情况未上报。3个月后,该企业领导才发现该问题,但由于距离加密时间太久,黑客密钥已经过期,被加密的数据和文件无法恢复，给该企业造成了大量财产损失。

经安全厂商人员实际勘测发现，攻击者主要是使用带有恶意附件的邮件进行的钓鱼攻击。受害者点击附件中含病毒的脚本文件后,脚本文件就自动从网络上下载勒索软件,勒索软件会对磁盘上指定类型的文件进行加密,让受害者只能支付赎金解密。

据360互联网安全中心相关人员介绍,2017年以来该中心监测到大量针对普通网民和政企机构的勒索软件攻击，勒索软件已成为对网民直接威胁最大的一类木马病毒。目前钓鱼邮件传播依然是黑客常用的手段,此外还出现了服务器入侵、软件供应链攻击、利用挂马网页等手法，一些勒索软件还会利用系统自身的漏洞进行传播。

劫持流量、突破网站承载极限以“击溃”网站来达到勒索目的，也是一种新型的犯罪手法。2017年10月,北京法院判决了一起案件,涉案的潘某通过互联网联系境外黑客,对国内3家大型比特币交易网站进行DDoS流量攻击，导致这3家网站均出现客户端无法启动、网站交易系统瘫痪、用户不能正常访问等现象,以此要挟勒索一定数量的比特币。

“当前,黑客之间呈现团伙运作、资源整合、跨境指挥攻击等特点,使用肉鸡集群形成持续的大流量攻击。”腾讯“守卫者计划”安全专家周正介绍,其主要针对网络直播、网络游戏、网络云服务、金融教育医疗等政企网站实施攻击,继而对目标敲诈勒索钱财,威逼利诱支付保护费，已经严重危害网络空间安全稳定。

传统敲诈改头换面 网民商家容易中招

过去一些传统的敲诈勒索，如今也有不少换上了互联网的“外衣”。

今年2月，湖南省浏阳市连续发生4起受害人与陌生人聊天，被以发布不雅照片为要挟进行敲诈勒索的案件。接到报案后,湖南警方经调查发现，这些案件背后是一个福建漳州籍涉嫌犯罪团伙，主要犯罪窝点在柬埔寨，主要方式是诱骗男性用户录制不雅视频后敲诈勒索。公安部门今年7月统一收网,将该团伙77名犯罪嫌疑人成功抓获。

“不要轻信陌生人,特别是不向陌生人泄露身份和家庭等敏感信息。”腾讯“守护者计划”安全团队介绍,之所以此类犯罪能够“精准打击”,在于不法分子已提前利用非法渠道获取被敲诈对象的姓名、身份证号、家庭住址、工作单位、手机号码等个人信息。

如今，人们在网购前都会注意查看商品评价,消费者“晒单”的好坏往往能左右商家销量,但这也催生了“职业差评师”这样一个以网络勒索为生的新行当。

2017年7月底，正在机关大院办公的邱某被警方带上了警车。原来,邱某平时工作比较清闲,一天在QQ聊天群接了一份“兼职”,对方每晚给她发一些淘宝店铺的链接，让她购物后打差评。对方承诺，由其出面让商家“花钱消灾”,敲诈所得两人“对半分”。对此，受害商家在向平台投诉的同时，也选择了报警。很快,一个利用差评敲诈勒索电商卖家的团伙被警方一举破获。

部分机构疏于防范 暴露安全存在“软肋”

“2017年以来,勒索软件的攻击进一步聚焦高利润目标,其中包括高净值个人、连接设备和企业服务器，特别是针对中小企业网络服务器的攻击急剧增长。”360互联网安全中心相关负责人表示,统计显示,今年1—4月,在向360互联网安全中心求助的勒索软件受害者中,制造业是遭受攻击最多的行业,占比约为23.1%；其次是互联网企业，占比约为15.7%;外贸行业排第三,占比约为10.6%。

事实上，即使是公共服务器也可能面临网络勒索的威胁。2017年8月,某公共服务系统单位的工作人员在对服务器进行操作时，发现数据库内所有文件都无法打开，怀疑遭到勒索软件加密，因此向360安全监测与响应中心求助。幸好该勒索软件程序编写存在漏洞，安服人员直接利用解密工具恢复了数据。

调研结果显示，当前许多政企网站在安全上“裸奔”,是导致网络勒索得以乘虚而入的重要原因。例如,一些政企机构内部隔离网络中的设备不及时打补丁，这些缺乏日常维护的电脑一旦不慎与外界被感染的介质连接,反而比正常更新的电脑更无招架之力,而出现大面积陷落的情况。

腾讯“守护者计划”相关负责人表示,在线上对抗和线下配合警方打击治理中，通过综合分析案例和犯罪手法发现，当前网络勒索出现的新趋势主要表现为分工精细化、产业专业化,同时技术门槛降低,利用新技术或新模式的能力强，并有跨境公司化或团伙化运营等特点,给法律定性、调查取证、打击治理等诸多方面都带来新的挑战。

与网络勒索日益高发相对应的是，当前我国一些政企机构员工甚至IT管理者依然轻视安全问题，不能对突发安全事件作出正确的判断，甚至出现国家有关部门发布预警公告后也毫不在意的情况。360互联网安全中心发布的勒索软件威胁形势分析报告显示，政企机构面对网络安全时对病毒预警不在乎、管理规定不遵守、应急方案不执行等情况大量存在,业务优先忽视安全、内部安全监管机构级别低缺乏话语权、疏于日常的安全教育和培训等因素也影响了风险防范。

对此,业内专家表示,政府、企业和个人都必须将网络安全置于突出位置，做好日常维护,才能避开网络勒索的“黑手”。（张璁）

订单多次提交不成功 平台涉嫌价格欺诈

预订低价机票屡失败是“运气太差”?

暑期已经过半,不少“飞行达人”开始着手预订国庆出游的“早鸟票”(提前预订享受更多优惠折扣的机票)。记者近日调查发现,部分用户在一些OTA平台（线上旅行社)上反复订票不成功，错过了优惠票价甚至贻误了行程。

订单提交多次不成功,强行生成订单

“订票19天,反复尝试提交订单近百次,眼看着机票从7300元涨到11000元！”深圳市民孔先生告诉记者，原计划今年国庆和朋友去法国和西班牙旅游，但在使用携程APP订票时遭遇了网上网下机票价格不一致的现象。

孔先生表示，在每次提交订单准备支付时系统都会提示“订单提交不成功,麻烦您返回查询页重新预订”。在随后的19天内,孔先生多次尝试预订价格最便宜的直飞或仅中转一次的航班,订单均无法成功提交。

无独有偶，宁波的胡女士也遭遇了类似经历。去年12月,胡女士原计划前往悉尼旅游，当时在去哪儿网上查询到的票价单张为1752元，但每次在准备付款时票价都会在燃油费和保险费之外多出540元。更为离奇的是,当胡女士点击“重新查询”按钮后,去哪儿网强行给胡女士生成一张4000余元的订单,并反复提醒胡女士支付。在胡女士随后18天的订票经历中,上述场景一直反复出现。

记者也在携程APP上进行了订票尝试,预订9月22日至25日香港至马德里的往返航班,在随机挑选航班、选择价位最低的出票方案并填写旅客个人信息后，当记者点选下一步时,APP弹窗提示“很抱歉,您预订的价格舱位已经售完,请重新选择”。记者随即又选择了相同时间由上海往返悉尼的随机航班,在订单提交环节得到了相同的弹窗提示。

同样的问题也出现在去哪儿网APP端，在多次选择往返目的地间的低价航班，点击支付时会弹出“该价格余票已售罄,请重新搜索”的提示。

究竟是“运气太差”还是另有猫腻?

记者在社交平台搜索后发现，孔先生和胡女士的订票遭遇并非孤例，类似情况的反映从2012年起就没有间断过。

在联系携程后孔先生得到客服答复——APP端展示价格比后台机票实际价格低600余元致使机票订单无法提交,如有需要,可通过后台实际价格帮助孔先生下单。“闹了半天携程给的低价是假的，在与携程纠缠的这段时间里眼看着机票价格往上涨。”孔先生生气地说,在向携程客服投诉该问题后,他甚至还被怀疑是有意“碰瓷”。

记者就自己在订票测试中的遭遇询问携程客服，对方回复称后台并未找到记者所提供的低价航班组合，并表示可通过电话端帮记者订票,但价格会高于APP端显示价格。

业内专家表示,规模较大的OTA平台国际机票会有约5%的订单因“变价率”(机票价格实时变动的概率）造成支付失败，但类似“连订单都无法提交”且“连续多日无法购买同一往返地机票”的情况并不多见,其中不排除有“独特”的产品设计逻辑。

各方都应勇于向涉嫌价格欺诈行为“亮剑”

根据第三方大数据分析公司易观数据显示,携程和去哪儿在2018年第一季度仍占据我国在线机票预订市场的前两位，市场份额分别高达37.5%和20.8%。

记者在采访中了解到，在机票预订过程中遭遇类似情况,大多数人认为只是“运气欠佳”所致,并未向有关部门投诉。专家认为,改善行业环境需各方努力，对涉嫌价格欺诈的行为要勇于“亮剑”。

福建瀛坤律师事务所张翼腾律师表示,根据价格法和消费者权益保护法的有关规定，平台不得使用虚假或使人误解的价格手段诱导消费者进行交易。消费者在遭遇疑似价格欺诈行为时可向平台所在地的市场监管部门举报，由行政执法部门对涉事平台开展调查取证工作。

浙江大学光华法学院互联网法律研究中心主任高艳东表示，相较于互联网企业低廉的违法成本和消费者高昂的维权成本，不对等的博弈关系并不能促进消费者维权意识的养成，也不利于行业的健康发展。高艳东建议，有关部门可考虑在处理互联网企业与消费者的消费纠纷时采取举证责任倒置的思路,同时借鉴惩罚性赔偿做法,辅以信用评价体系,让失信企业在行业内寸步难行。

“用户会用脚投票的。”资深互联网观察人士尹生说，互联网行业的发展经验告诉我们，任何不诚信行为都会被放在放大镜下拷问,相关企业不应抱有任何侥幸心理。

携程方面在对记者采访回函中表示,机票预订订单提交不成功是极少数情况，并非携程的主观故意行为，并且该情况在行业内普遍存在。目前,携程机票部门已将前述问题作为重点项目,在内部开展研究改进工作。

（颜之宏）