

当前,互联网犯罪年增30%,网络“黑灰产业”亟待铲除——

# 深度联手才能拱卫网络新安全

经济日报·中国经济网记者 李万祥

## 特别关注

如今,各种利用互联网技术偷盗、诈骗、敲诈等案件时有发生,各种围绕互联网黑灰产业正以极快的速度蔓延。维护网络安全,成为全社会的共同担当。6月1日起施行的《中华人民共和国网络安全法》标志着网络安全从此有法可依,迎来了我国网络安全保障的新时代。

### 网络空间面临新安全挑战

白领点击不明链接后存款被盗、清华大学教授被骗超千万巨款、山东考生徐玉玉被电信诈骗后猝死……互联网欺诈的危害已经从财产威胁扩展到人身伤害。网络安全、信息安全已经成为这个时代的必需品。

继马云提出“新零售”、“新制造”、“新金融”、“新技术”和“新能源”等“五新”概念后,网络“新安全”议题也开始受到关注。在7月26日至27日召开的“2017网络安全生态峰会”上,来自中央网信办、工业和信息化部、公安部等相关部门和百度、阿里巴巴、腾讯等多家互联网公司的有关负责人齐聚一堂,共话网络“新安全”、推动互联网事业安全发展。

什么是“新安全”?如何应对网络环境中的“新安全”问题?

“我理解的‘新安全’,是指在互联网大数据技术即将对社会方方面面产生重大颠覆的历史阶段,如何从国家、企业、专业机构甚至全体公民形成全方面的机制,如何升级安全理念和安全体系。”阿里巴巴集团风险委员会主席邵晓锋说。

《网络安全法》明确,国家坚持网络安全与信息化发展并重,遵循积极利用、科学发展、依法管理、确保安全的方针,推进网络基础设施建设和互联互通,鼓励网络技术创新和应用,支持培养网络安全人才,建立健全网络安全保障体系,提高网络安全保护能力。

互联网复杂化趋势正使得网络安全发生着本质变化。线上线下融合安全、互联网作为新基础设施的安全和数据安全等“新安全”,正在成为网络时代新的命题和领域。对此,仅仅做到信息通信基础设施的安全已经远远不够,还需对业务层面做更多安全支撑。

“在安全领域,没有对手只有队友。”蚂蚁金服 CEO 井贤栋现场宣布,将进一步升级支付宝“你敢付,我敢赔”服务,推出“你敢扫,我敢赔”服务,把保障范围从线上延伸到线下。如果商家的收钱码被恶意替换、调包,其损失的资金将通过保险公司获得赔付。此外,如果用户扫了可疑二维码,中了病毒或木马导致支付宝账户资金被盗,也能获得赔付。

### “网络黑产”规模超千亿元

从5月份的 Wannacry 到6月份的 Petya 变种,勒索病毒今年两次大规模爆发,全球多国企事业单位、政府系统、银行系统、高校网络受到感染。勒索病毒的大规模、自动化传播,严重威胁到公共安全。

面对不断升级的黑客攻击,安全厂商应该如何提高“战斗力”?应对不断升级的公共安全威胁,软件厂商和安全厂商要注重基础安全设施建设。工业和信息化部网络安全管理局副局长张新提出,互联网企业要积极参与网络安全试点示范,深入开展针对漏洞挖掘、数据防泄露等研发,同时要在大数据、云计算、物联网等一些新领域推出更好的安全服务。

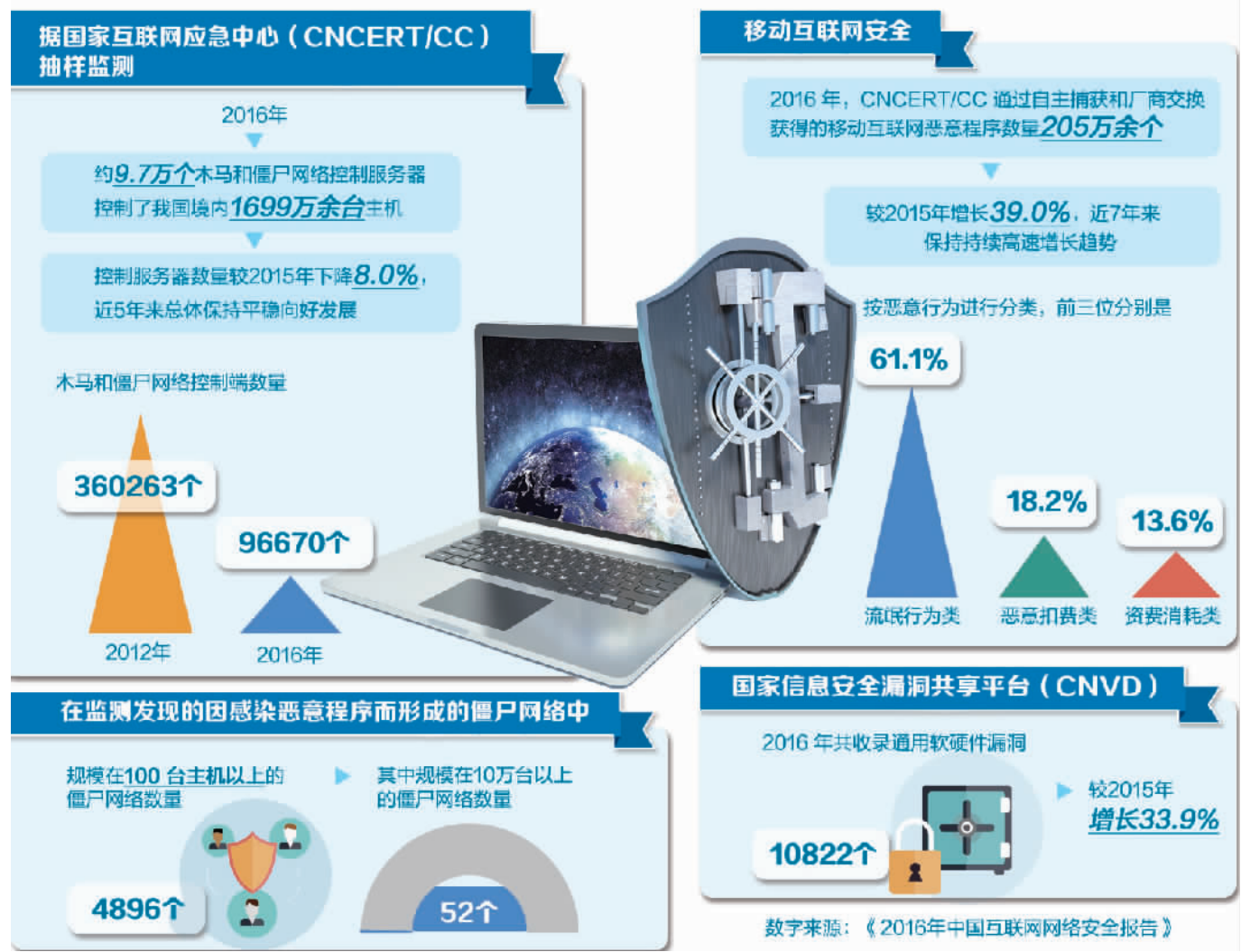
黑客攻击是典型的所谓“网络黑产”之一。国家互联网应急中心将“黑产”范围界定为3类:一是发动涉嫌拒绝服务式攻击的黑客团伙,二是盗取个人信息和财产账号的盗号团伙,三是针对金融、政府类网站的仿冒制作团伙。业内简称为“黑客攻击”、“盗取账号”、“钓鱼网站”,这些都是典型的网络违法犯罪行为。此外,网络黑产的上游产业是“恶意注册和虚假认证”,由于这种行为本身没有直接产生危害后果,又被称为“灰色产业”。

据统计,我国网络犯罪已占犯罪总数的三分之一,并以每年30%以上的速度增长。未来,绝大多数犯罪都将涉及网络。有机构测算,仅中国“网络黑产”从业人员就已超过150万人,市场规模也已高达千亿元级别。

由此,《网络安全法》强调网络运行安全,用很大篇幅突出“国家实行网络安全等级保护制度”和“关键信息基础设施的运行安全”;并以法律形式明确“网络实名制”,要求网络运营者收集使用个人信息,应当遵循合法、正当、必要的原则,“不得出售个人信息”。

据“猎网平台”统计,该平台2016年共收到全国用户提交网络诈骗举报20623例,举报金额1.95亿余元。与2015年相比,网络诈骗举报数量虽然下降了17.1%,但人均损失却增长了85.5%。这说明,网络诈骗呈现出结合个人信息精准行骗的趋势。

针对电信网络诈骗犯罪,今年的中央政法工作会议要求完善电信网络和互联网国际出入口诈骗电话防范系统,完善银行账户和支付账户异常资金交易风险防控系统,研究解决实名认证中存在的漏洞,及时查封虚假、钓鱼网站,切断不法分子实施电信诈骗的网上通道。



面对不断升级的黑客攻击,安全厂商应该如何提高“战斗力”?应对不断升级的公共安全威胁,软件厂商和安全厂商要注重基础安全设施建设。工业和信息化部网络安全管理局副局长张新提出,互联网企业要积极参与网络安全试点示范,深入开展针对漏洞挖掘、数据防泄露等研发,同时要在大数据、云计算、物联网等一些新领域推出更好的安全服务。

黑客攻击是典型的所谓“网络黑产”之一。国家互联网应急中心将“黑产”范围界定为3类:一是发动涉嫌拒绝服务式攻击的黑客团伙,二是盗取个人信息和财产账号的盗号团伙,三是针对金融、政府类网站的仿冒制作团伙。业内简称为“黑客攻击”、“盗取账号”、“钓鱼网站”,这些都是典型的网络违法犯罪行为。此外,网络黑产的上游产业是“恶意注册和虚假认证”,由于这种行为本身没有直接产生危害后果,又被称为“灰色产业”。

据统计,我国网络犯罪已占犯罪总数的三分之一,并以每年30%以上的速度增长。未来,绝大多数犯罪都将涉及网络。有机构测算,仅中国“网络黑产”从业人员就已超过150万人,市场规模也已高达千亿元级别。

由此,《网络安全法》强调网络运行安全,用很大篇幅突出“国家实行网络安全等级保护制度”和“关键信息基础设施的运行安全”;并以法律形式明确“网络实名制”,要求网络运营者收集使用个人信息,应当遵循合法、正当、必要的原则,“不得出售个人信息”。

据“猎网平台”统计,该平台2016年共收到全国用户提交网络诈骗举报20623例,举报金额1.95亿余元。与2015

年相比,网络诈骗举报数量虽然下降了17.1%,但人均损失却增长了85.5%。这说明,网络诈骗呈现出结合个人信息精准行骗的趋势。

针对电信网络诈骗犯罪,今年的中央政法工作会议要求完善电信网络和互联网国际出入口诈骗电话防范系统,完善银行账户和支付账户异常资金交易风险防控系统,研究解决实名认证中存在的漏洞,及时查封虚假、钓鱼网站,切断不法分子实施电信诈骗的网上通道。

### 联防联控将成新安全趋势

7月19日,“徐玉玉被电信诈骗案”一审宣判,山东临沂市中级人民法院以被告人陈文辉犯诈骗罪、侵犯公民个人信息罪,判处有期徒刑,剥夺政治权利终身,并处没收个人全部财产;以被告人郑金锋、黄进春、熊超、陈宝生、郑贤聪、陈福地犯诈骗罪,分别判处有期徒刑15年至3年不等,并处罚金60万元到10万元不等。

近年来,多部门联手出重拳,形成打击电信网络诈骗犯罪合力。2016年9月,最高人民法院、最高人民检察院、公安部、工业和信息化部、中国人民银行、银监会等6部门共同发布《关于防范和打击电信网络诈骗犯罪的通告》,公布了一批源头治理的措施。此后,最高法、最高检、公安部联合发布《关于办理电信网络诈骗等刑事案件案件适用法律若干问题的解释》,进一步明确法律标准,统一执法尺度。

据统计,2016年,公安机关共破获电信网络诈骗案件8.3万起,同比上升49.6%;北京、浙江、广东检察机关提前介

入侦查,及时批捕起诉张智维等116人、罗兆隆等108人,崔培明等129人特大约国电信网络诈骗案。

记者了解到,阿里巴巴集团每天都会应对垃圾注册、账号被盗、交易欺诈等10多种业务风险。基于大数据和机器学习,阿里巴巴构建了智能风控系统,其类似实践产品还包括专门反诈骗的钱盾App、团圆打拐系统、电商生态安全联盟和互联网志愿者安全联盟等。

“网络新安全不能照搬过去的方法,不能只靠个别企业,必须动员生态圈内的相关部门以及各种力量团结协作,才能解决好安全问题。”阿里巴巴集团首席风险官刘振飞说,要做到新安全保障需要有技术作为核心能力、数据作为基础保障,同时还需有创新与合作,并保持公益之心。

公安部网络安全保卫局副局长钟忠认为,网络安全新模式不同于传统的事后被动防御,而是转为事前事中主动管控,甚至具备主动进攻的能力,其核心武器在于大数据和新技术,以实现威胁的提前感知与预测。

专家提出,培育守护网络安全新能力,首先强调基于大数据人工智能和生物识别技术在网络智能防御方面的应用。具体说,人工智能和生物识别技术可利用过往沉淀的数据资源对不同的网络行为“画像”,进而识别出哪些是有威胁的网络行为并智能阻断。

“保障网络安全还需要政府、企业和社会各界联合起来构建联防联控、联治的网络安全治理局面,要把构建良好的网络生态环境当作最重要的能力提升来看待。”中央网信办网络安全协调局副局长胡啸说。

得违反《娱乐场所管理条例》、《互联网文化管理暂行规定》、《互联网上网服务营业场所管理条例》等法规对内容管理的要求。此外,《通知》还规定,迷你歌咏亭不得含有文化部公布的黑名单文化产品,平台运营企业或经营主体应当建立内容自审制度,并安排专人负责迷你歌咏亭曲库的内容审核。同时,为了保护未成年消费者的权益,《通知》强调企业要在迷你歌咏亭系统内设置累计消费时间和金额提示等措施,引导未成年消费者理性娱乐,防止沉迷。

在将其纳入监管的同时,“推动迷你歌咏亭行业健康发展也是《通知》的应有之义”。马峰说,《通知》第五条提出鼓励企业提升服务品质,并为迷你歌咏亭的推广提供了助力。例如,《通知》规定,鼓励游戏游艺场所、互联网上网服务营业场所引入迷你歌咏亭;鼓励有条件的文化馆利用迷你歌咏亭开展公共文化服务;鼓励和保护企业研发创新,不断提升迷你歌咏亭内容及设备品质,创新分享经济新模式。

“目前,迷你歌咏亭的主要功能是歌曲点播,但随着业态的进一步发展,部分迷你歌咏亭已具备朗诵等新功能,今后也不排除成为游戏、电影、上网服务等业态终端。”马峰介绍,《通知》要求迷你歌咏亭的经营不

得违反《娱乐场所管理条例》、《互联网文化管理暂行规定》、《互联网上网服务营业场所管理条例》等法规对内容管理的要求。此外,《通知》还规定,迷你歌咏亭不得含有文化部公布的黑名单文化产品,平台运营企业或经营主体应当建立内容自审制度,并安排专人负责迷你歌咏亭曲库的内容审核。同时,为了保护未成年消费者的权益,《通知》强调企业要在迷你歌咏亭系统内设置累计消费时间和金额提示等措施,引导未成年消费者理性娱乐,防止沉迷。

在将其纳入监管的同时,“推动迷你歌咏亭行业健康发展也是《通知》的应有之义”。马峰说,《通知》第五条提出鼓励企业提升服务品质,并为迷你歌咏亭的推广提供了助力。例如,《通知》规定,鼓励游戏游艺场所、互联网上网服务营业场所引入迷你歌咏亭;鼓励有条件的文化馆利用迷你歌咏亭开展公共文化服务;鼓励和保护企业研发创新,不断提升迷你歌咏亭内容及设备品质,创新分享经济新模式。

## 执法一线

就像现金结算会遭遇假钞一样,企业、银行间的票据结算同样会遭遇假票欺诈。

与假钞相比,票据的期限长、金额大,且常常是几经背书转让,查验真伪难上加难。尤其是近年来票据结算的频率和体量越来越大,各式各样的“变造票”、“克隆票”层出不穷,票据的“高仿”伎俩也花样百出。因此,堵截票据风险除需要经办人员具备丰富的经验和技能,更需绷紧制度之弦,通过科学、系统的内控机制筑牢防火墙。

本报记者

### 银行间票据

钱箐箐

#### 不放过一张假票

2017年3月24日,杭州M公司财务人员拿着一张银行承兑汇票来到浙商银行杭州分行,要求办理浙商银行“涌金票据池”的票据入池质押业务。票面显示,该银承汇票号码为30\*\*\*\*\*4648,出票金额人民币420万元整,出票人为河南H公司。

虽然粗看这张银承本身并无太多异常,但分行运营管理部业务处理中心经办这笔业务的沈佳宇、楼敏二人,注意到M公司是新近才开通的票据池业务,入池的首张票据就是这张大额银承,便多留了个心眼。

按照惯例,柜员应通过央行系统对票据实行“电查”(即对银承的票号、期限、金额、收款人、出票人、承兑行等要素信息进行核对);查复书显示的信息和票面并无二致,唯一的反常是承兑行在查复书中告知,该银承曾经被查询过10余次,其中8家银行各查询一次、2家银行各查询两次。

“票据只有经过多次背书转让才会有多次的查询记录”,楼敏事后回忆说,“但这张银承并没有黏单,背书人只有票面收款人和M公司两手,故被10余次查询不合常理”。从业多年的经验告诉两位经办人员,魔鬼往往就藏匿在这样的细节中。

鉴于近年来票据风险案件频发,有一部分特别谨慎的银行,只要有有记录的票据,一概不予办理。但浙商银行涌金票据池一直都因“不挑客、不挑票”的理念广受市场推崇,沈佳宇和楼敏觉得,“既不能冤枉一张真票,也不能放过一张假票”,故并未直接终止业务,而是向包括承兑行在内的多家银行再一次发出查询。

在与各家银行电话沟通中获知,出票人在出票日签发多张银行承兑汇票,有“小票套大票”嫌疑,现已有变造票据情况发生,当地公安部门已介入,进一步印证了这张银承疑窦重重。

#### 认清变造票据伎俩

据了解,当前伪造假汇票的伎俩一般有3种:一是“无中生有”,利用科技手段彻底伪造假票;二是“照猫画虎”,先签发真票,再根据真票伪造内容完全相同的“克隆票”;三是“改容易貌”,把金额较小的真汇票数字改大,即变造票。

这3种方式中,尤以变造票的仿真度最高、鉴别难度最大。变造银承一般通过加“0”或者改写,将银承金额由小变大;而除了被修改的极少数的关键要素,包括印章在内的其他部分都是真的,非常容易瞒天过海。

而“小票套大票”的手法,更是不法分子为躲避查验惯用的“画皮”。具体到这张变造银承,出票人在同一天内连续签发若干张连号银承,其中一张为真实的大额票据(420万元),其他均为数千元的小票。因为票号相连,在给这些小票“易容”之时,需要修改的仅有“票号末位”、“小写金额首位”及“大写金额”几处,把可能的造假漏洞降到最低。

这一点微乎其微的纰漏,则是在反复拉锯的传真查询中暴露出来的。

在常规查询后,沈佳宇向承兑行发起了传真查询请求,但承兑行提供的银承第一联(底卡联)的影像与票据实物并无明显区别。“按照人民银行对票据查询的要求,只需比照第一联底卡影像即可。但是我行始终坚持‘有疑必查、查必彻底’的内控合规要求,向承兑行再次发出传真查询,恳请其提供该银承的第二联影像。”沈佳宇说。

天网恢恢,也正是这第二联影像,将这张银承做假的嫌疑彻底坐实,第二联影像中印章盖戳和实物票据上的位置明显不同。通过这一细节可以判定,这是一张变造票。

“从技术上看,不法分子既然无中生有彻底伪造出假票来,那么在真票基础上小改几处更是不在话下。”楼敏说,“然而柜员手工盖的印戳,位置和角度都有一定的随机性,不法分子机关算尽,还是因为我们多要了一联影像,揪住了狐狸尾巴”。

事后,第三方公司专业鉴定进一步佐证了这一判断。该票据在红外光下票号和大小写金额均被涂改,表现为票号末位“8”疑似由“5”变造,大写金额“肆佰贰拾万元整”为全部刮改而成,故红线线有明显刮改、挖补痕迹,小写金额的“2”由“¥”变造,且“2”后面的所有数字均为刮改。在紫外光下票号处的团花及整版兰花图案均有明显断痕,紫外光下呈明亮色。用特殊蓝光检测,票据号码、金额处的底纹有明显断痕,说明这张银承确系变造而来。

事实确凿后,浙商银行杭州分行立即报案,目前当地警方已介入,对涉事公司进行调查。