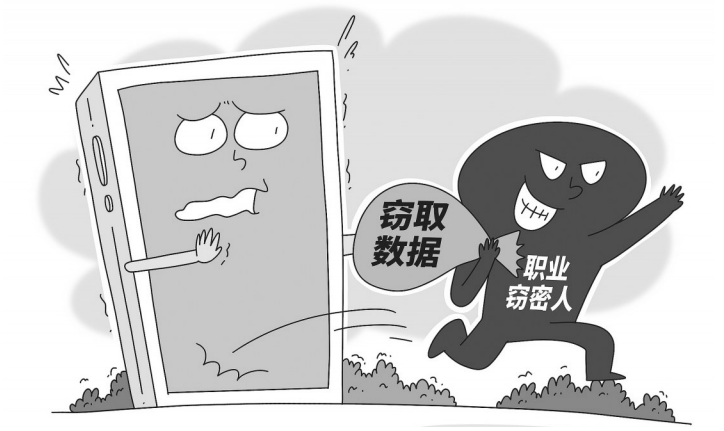
网安卫士竟“变身”木马黑客

四被告实施网络敲诈勒索均获刑

原本从事网络安全工作的工程师,竟干起黑客的勾当,利用木马病毒“黑”掉企业网络系统,索要数字加密货币作为“赎金”……近日,浙江杭州市上城区人民法院一审宣判了一起特殊的敲诈勒索案件,四名被告分别以犯敲诈勒索罪、侵犯公民个人信息罪被判处有期徒刑。

据新华社



资料图片 视觉中国供图

“老字号”遭遇黑客攻击,“赎金”是虚拟货币

2023年底的一天,杭州一家“老字号”医疗机构技术部负责人陆续接到各个科室的来电,反映系统无法正常登录。进入操作页面发现,所有的系统文件都变成了“.uncle”的后缀。经过排查,后台管理系统中一个名为readme.html的文件十分可疑。点开一看,里面赫然写着:“Important Notice! Your Files Have Been Locked!”(“注意!你们的文件已经被锁定!”)随后,技术人员陆续在文件中找到了“Payment Method”(支付方式)“Wallet Address”(钱包地址)等内容。这起系统瘫痪的始作俑者被确定为网络黑客。

经核实,公司共计89台服务器无法运行,包括电子病历、批发连锁在内的业务系统彻底陷入瘫痪。为尽快恢复线上挂号等业务,最大程度保障患者不延误诊疗,该医疗机构无奈答应了对方支付数字加密货币作为“解锁赎金”。

无独有偶,这家机构报案之后,杭州警方又发现两家被该团伙敲诈勒索的企业。经统计,三家被害企业为恢复正常经营,共计花费33万余元向第三方购买数字加密货币支付给了对方。

杭州市上城区公安分局网警大队民警介绍,嫌疑人在短时间内集中进行了大量技术操作,且反侦查意识很强,设立了多个“跳板”服务器,IP地址涉及境内外多处地点。从种种迹象看,该起案件大概率是组织严密、分工明确的团伙作案。

通过技术手段追踪侦查,公安机关逐步锁定了涉案人员的真实身份。2023年12月,以祁某某为首的四人犯罪团伙在内蒙古呼和浩特、北京等地被相继抓获归案。

一心赚“快钱”,网安卫士变勒索黑客

四人到案后,承认了利用木马病毒开展敲诈勒索的犯罪事实,案件真相逐渐浮出水面。

原来,祁某某、韩某某、李某某三人原是北京某科技有限公司负责网络安全维护的工程师,而郝某某是和祁某某、韩某某熟识的好友,也从事网络安防工作。

由于熟悉网络安全的“门道”,祁某某、郝某某、韩某某开始谋划利用技术赚点“快钱”。一开始他们盯上贩卖公民信息的生意:2023年4月至7月,祁某某等人通过服务器漏洞对系统数据进行非法爬取,共获取包含收货人、收货地址、电话等信息累计6万余条,通过非法贩卖,共获利人民币20余万元。

但这类数据在“黑市”上的价格逐渐走低,他们决定换一条“赛道”,用病毒搞敲诈勒索。

为了提升效率,祁某某、韩某某等人在呼和浩特市的出租房内开起“勒索工作室”。四名成员分工明确:祁某某、韩某某事先编写好勒索代码并进行测试,郝某某、李某某对有漏洞的企业服务器进行收集并添加漏洞“后门”,随后由祁某某、韩某某从“后门”进入网站,上传定时执行加密任务的木马病毒进行勒索。

承办检察官表示,这几人在从事网安工作的时候,就时常关注技术论坛中发布的服务器共性漏洞,在网上寻找可以攻破的堡垒机。“为了提升网络攻击效果,他们还利用人工智能技术辅助修改病毒程序代码。”

就这样,在短短一周不到的时间内,该团伙陆续作案三起,对被害企业造成损失。

扎好安全“篱笆”,应对网络勒索

2024年9月11日,上城区人民检察院分别以敲诈勒索罪和侵犯公民个人信息罪对祁某某等四人依法提起公诉。2025年3月,该案件在上城区人民法院开庭审理。近日,四名被告人被一审判处有期徒刑三年至七年六个月不等,并处罚金。目前该判决已生效。

“没耐心想要‘挣快钱’,这种心态害了自己。”面对法官的讯问,郝某某流下后悔的泪水。四名被告在一审宣判后,均表示服从判决结果不上诉。

承办检察官表示,近年来,人工智能技术的发展进一步降低了攻击门槛,导致针对企业服务器,尤其是网安能力薄弱的中小民营企业的黑客攻击勒索发案频率有所提升,加大了案件侦办难度。

网络安防专家建议,面对网络勒索,企业除了事发后要及时固定证据报警,平时要定期做好“冷备份”,即平均每7天对所有服务器数据做一次线下备份。一旦发生勒索攻击,至少可以将系统恢复到7天以内的数据,不至于陷入完全瘫痪;此外还可以选用“专用设备+安全保险”服务模式,部署一套防勒索检测设备的同时,加入一份安全保险,对因为黑客勒索造成的损失获得有效赔付。

魔高一尺,道高一丈。尽管人工智能技术和虚拟货币等的运用,让传统犯罪“花样翻新”,但调查取证手段在不断更新,相关法律法规也日益完善,建起愈加牢固的网络安全“篱笆”。同时,企业特别是中小企业要提高风险意识、完善安防措施,一旦遭遇网络敲诈勒索,及时固证维权。

小米黑公关案告破,雷军公开回应

5月19日,“@雷军”转发“@小米法务部”关于“一起有组织、有预谋的网络黑公关案件告破”博文:网络不是法外之地,对造谣、抹黑等侵权行为,小米将坚决以法律手段保护自身合法权益。

5月19日下午,“@小米法务部”发文:2025年5月15日,我司从司法机关处获悉,此前我司报案的一起有组织、有预谋的网络黑公关案件,已经告破。目前,公安机关已依法对多名犯罪嫌疑人采取刑事强制措施,案件还在进一步调查。

据了解,自2024年12月起,直至近期小米汽车相关的系列热点事件,该犯罪团伙利用文案自动生成软件捏造关于小米的虚假信息,并操纵近万个社交媒体账号,恶意造谣、散播不实言论,并采用煽动网络对立情绪、踩一捧一等方式进行恶意炒作,严重诋毁小米公司。据悉,该案反映出新型网络水军犯罪特征,团伙作案、组织严密,利用自动化软件,批量生成黑稿,分发链条复杂,犯罪金额巨大,对网络环境和企业商誉造成极其恶劣的影响。

现代快报/现代+综合小米法务部、@雷军

两名游客长城刻字,被行拘并罚款

5月19日消息,近日,工作人员在巡查中发现八达岭长城景区南六楼出现刻划行为,第一时间与八达岭派出所取得联系移交相关线索,经民警详细调查,确定刻划人张某某、孙某某已返回上海。延庆区公安分局高度重视,立即与上海警方展开沟通协作,面对跨地域难题,首次启动行政案件异地办案程序。两地警方紧密配合、高效联动,迅速推进案件办理,依法对张某某、孙某某作出行政拘留5日、罚款200元的行政处罚。

北京延庆区长城管理处郑重呼吁广大游客:游览长城时,请自觉遵守文物保护相关规定,践行文明旅游理念,拒绝任何破坏长城的行为。让我们携手同心,共筑文化遗产保护防线,为传承和弘扬中华优秀传统文化贡献力量。

据八达岭长城微信公众号

女子在贴身卫生巾里藏2003粒钻石

海关:已立案处理

图片来源:海关发布

5月19日,据海关发布:近日,深圳罗湖海关在旅检进境渠道查获旅客在身穿的卫生巾内走私藏匿钻石616.43克拉,共计2003粒,案值逾27万元人民币。

当日,罗湖海关关员在对进境旅客进行监管时,发现一名中年女性旅客进入海关监管区未向海关申报,且神色紧张、举止异常。海关关员随即对其进行拦截检查。经进一步检查,在该旅客身穿的卫生巾内查获透明包装袋2个,包装袋中各藏匿无色宝石一批。后经深圳海关工业品检测中心鉴定,该批无色宝石为合成钻石戒面。目前,海关已对当事人作立案处理。

据“海关发布”微信公众号

“木马病毒+伪造领导”,骗走会计270万

幸亏警方及时介入追回全部款项

现代快报讯(通讯员 秦公轩 记者 季雨)近日,南京市秦淮区秦虹派出所接到辖区某公司会计的紧急报警,疑似遭遇电信诈骗,已对外转账270万元。接警后,民警迅速行动,随即冻结涉案账户,并通过深入调查追回全部被骗资金。

事发当天,秦虹派出所接到某公司财务人员报警,称公司会计在微信群内接到“领导”指示,要求向两家公司分别转账90万元和180万元。会计完成转账后,察觉情况异常,怀疑遭遇诈骗,立即报警求助。民警赶到现场后,会计焦急地解释称,自己是被“公司领导”拉进一个微信群,群内还有“同事”。在群聊中,“领导”以业务往来为由,要求其尽快向指定账户汇款。由于骗子准确掌握了公司内部信息,会计未多加怀疑,便按照指示完成了转账操作。

了解情况后,民警敏锐意识到这是一起典型的冒充领导类电信诈骗,立即拨打96110反诈专线,对涉案账户进行紧急止付冻结,防止资金外流。与此同时,警方迅速展开调查,逐步揭开了诈骗分子的作案手法。经查,诈骗分子事先通过邮箱向受害人发送带入病毒的邮件,会计点击后,电脑被植入木马病毒。犯罪分子借此远程监控其电脑,窃取公司内部通讯录、财务流程等信息。随后,他们伪造微信群,冒充公司领导和同事,以“业务需求”为由,诱导会计转账。由于诈骗分子对公司的运作模式、人员关系了如指掌,受害人一时难以辨别真伪,最终落入圈套。

由于警方反应迅速,涉案账户在资金尚未被转移前就被冻结,为后续追赃挽损争取了宝贵时间。秦淮警方联合银行、反诈中心等部门,对资金流向进行追踪,最终将被骗的270万元全部追回,为企业挽回了重大经济损失。警方也借此案例提醒企业,务必加强财务管理制度,严格执行转账审批流程,避免类似案件再次发生。

未成年子女的钱,父母能随意处置吗?

孩子的钱,父母能随意处置吗?在最高人民法院发布的一起典型案例中,父亲将未成年子女的83.8万元作为首付款购买房屋,但未按照离婚协议约定登记在子女名下,人民法院依法判令父亲向子女返还财产。

赵某与丁某离婚,儿子丁小某随丁某共同生活。双方离婚协议约定赵某给付丁小某生活费70万元,同时约定该70万元及丁小某从长辈处受赠的13.8万元应作为丁小某购买某房产的产权份额,由丁某代处理买房事宜并在房产证上登记丁小某名字及份额。后赵某按离婚协议约定给付了生活费70万元。同年7月9日,丁某签订房屋买卖合同,支付首付款83.8万元,剩余房款以贷款方式支付。

同年7月12日,丁某与汪某登记结婚,并将案涉不动产登记至丁某、汪某名下,载明共同共有。丁小某向人民法院起诉,请求丁某、汪某返还人民币83.8万元及利息。

审理法院认为,根据查明的事实,案涉房屋首付款83.8万元来源于赵某给付丁小某的生活费以及丁小某受赠的财产。该83.8万元应认定为丁小某的财产。丁某作为直接抚养丁小某的监护人,在购置房产时,未按离婚协议约定登记丁小某名字及所占有的份额,侵犯了丁小某的合法财产权益。案涉房产现登记在丁某和汪某名下,双方获得相应利益,应当承担返还款项责任。

据人民日报