

涉及多地!

藏在弱电井里的电诈“黑匣子”

频繁接到显示为办公电话的陌生来电,有人因此被骗走一年收入。警方调查发现,这些涉诈电话竟是从公立医院的固定电话打出。弱电井里偷偷装上的“黑匣子”背后,是一张席卷多地的电信诈骗网络……

一场VOIP(网络电话)电信网络诈骗黑灰产业链全国集群战役就此打响。新华社记者近日采访侦办案件的内蒙古自治区鄂尔多斯市公安局东胜分局,起底一条为境外电信网络诈骗集团提供呼叫服务的黑灰产业链。



新华社发

医院来电背后的陷阱

“5月5日,我在家中接到显示归属地为鄂尔多斯的固定电话。对方说我在某直播App开通了直播带货权限,从下月开始每月自动扣取服务费800元。”一位受害人心急如焚地向警方说,“对方说可以帮我取消扣费服务,我同意了。等我反应过来,银行卡里的11万元都被骗走了,这可是我全家一年的收入!”

今年5月,东胜公安分局刑侦大队接到线索,经过对涉诈电话号码核查,三个电话号码竟然是从该市三家公立医院的办公固定电话打出。

难道是医院内部人员参与诈骗?反诈经验丰富的老刑警分析认为,三家医院同时出现“内鬼”的概率极低,侦查重点应该放在医院的电话通信设备上。

案件分析会后,民警立即联系相关医院,联合运营商对医院通信设施开展排查。当通信维修人员从弱电管道井里出来,指着手机照片上的“黑匣子”惊呼:“语音网关(VOIP固话端设备)!安在医院固话交换机上。”

反诈民警立即冲入闷热的管道井,经现场勘验,发现仅一家医院就有

16部固定电话被非法接入语音网关。

“这些‘黑匣子’相当于高级的‘号码转换器’,犯罪分子利用这些设备实现互联网与固定电话的联通。境外诈骗集团通过语音网关,将境外来电包装成了本地号码,极大降低了受害者的警惕性。”办案民警贾海军说。

顺藤摸瓜 全国收网

这些“黑匣子”如何进入医院弱电井?从哪里购买?又是谁指使安装?办案人员顺藤摸瓜,从设备安装、收售设备,再到技术支撑、组织管理等环节,逐渐摸清了该团伙的组织构架及运作情况。

今年5月8日,嫌疑人白某在鄂尔多斯市某旗安装语音网关后,准备逃离时被当场抓获。据他交代,今年4月,老乡给他介绍了一个“高工资、高风险”的工作,就是潜入单位、医院、酒店安装语音网关电话线。

根据白某的供述,一个庞大的电诈犯罪团伙浮出水面。民警在辽宁省某市将语音网关收售头目祁某某及其妻子牛某抓获,从其家中查获语音网关24个、网关合格证书340余张。随后,民警在另一城市将该团伙成员孔某抓获,铲除一处违法收售语音网关

窝点。

然而,上线团伙仍逍遥法外。祁某某出售语音网关时,均通过境外加密聊天软件与上线单线联系,案件侦办一度陷入困境。“当时,我们初步判断该团伙涉案语音网关1300余台。如果就此结案,意味着千余台语音网关很可能还安装在全国各地,继续被诈骗分子利用。”贾海军说。

从已查获语音网关上的10万余条诈骗电话入手,10名办案民警花费数月时间,将数以万计的碎片信息拼凑出犯罪团伙的完整“拼图”。经查,该团伙涉及全国21个省区市、犯罪嫌疑人80余名。

鉴于案情重大,东胜公安分局申请发起全国集群战役。2025年10月,90余名民警分赴21个省区市开展收网行动,成功抓获包括顶层管理、中层技术支持和底层设备安装在内的犯罪嫌疑人74名,扣押VOIP相关设备300余台,全链条铲除了这一为境外诈骗集团提供技术支撑的黑灰产业链。

“隐蔽角落”的安全警示

记者梳理发现,近年来相关电信网络诈骗新型犯罪案例多发,已导致不少群众被骗。

东胜公安分局刑侦大队副大队长董娜说,犯罪分子从弱电井、机房下手,便于其设备接入内部电话线路。犯罪分子多伪装成电工或通信运营商的维修人员,利用节假日或安保松懈时段,混入写字楼、医院、企业等单位,伺机潜入弱电井,在境外诈骗分子的指挥下实施安装。

网络安全等级保护制度是我国网络安全领域的基础制度,其要求网络运营者落实安全管理与防护技术措施;若落实不到位,自身要承担法律责任。

根据网络安全法,民警提醒,各单位应做好对固定电话涉诈风险的排除和防范,应联合运营商加强风险隐患排查,重点检查机房、弱电井、办公电话接口等隐蔽位置是否存在异常,如发现异常设备,立即进行拆除;对进入弱电井的人员进行身份核验登记,要求施工人员提供运营商授权文件,无文件者拒绝其进入弱电井;对机房、弱电井等重点场所加装防撬挂锁,有条件的要安装监控设备。

警方提醒,日常生活中,接到自称机关事业单位、企业的电话,应留个心眼,注意与官方公布的热线电话比对核实。新华社呼和浩特12月15日电

L3级自动驾驶车型 获附条件准入许可

释放哪些信号?

15日,工业和信息化部正式附条件许可两家汽车企业提交的搭载L3级有条件自动驾驶功能的智能网联汽车产品准入申请,受到广泛关注。这一举措释放哪些信号?记者采访了专家。

筑牢安全发展“防护栏”——

工业和信息化部装备工业发展中心主任瞿国春表示,我国始终将安全作为创新应用的前提,坚持安全为先、统筹推进,逐步形成覆盖关键技术研发、测试验证评价、政策法规制度、场景验证应用等方面的系统化推进机制。

“此次发布的搭载L3级有条件自动驾驶功能的智能网联汽车产品,在企业能力、产品安全过程保障、产品测试验证等方面均开展了系统性评估,在安全为先的前提下,限定使用主体和场景应用范围,对具备量产条件的

智能网联汽车产品给予准入许可,在推动智能网联汽车技术创新、逐步扩大可应用场景方面迈出了坚实的一步。”瞿国春说。

“安全是汽车行业永恒的主题,任何新技术的诞生与应用都应以安全为底线。”中国汽车标准化研究院总工程师孙航告诉记者,此次发布特别强调了“附条件”准入,将允许开启自动驾驶功能的路段限定在典型、低风险场景中,意在通过“小切口起步”、安全有序推进自动驾驶技术稳妥落地。

从“技术验证”迈向“量产应用”新阶段——

专家表示,伴随智能化和网联化技术稳步发展,人工智能、大模型等技术加速上车,此次发布标志着我国智能网联汽车准入和上路通行试点正式进入上路通行试点阶段。

中国汽车工业协会常务副会长兼

秘书长付炳锋认为,智能网联汽车作为跨学科、跨领域的复杂系统,其成熟度不仅依靠技术突破,更需商业闭环验证。“多部门共同构建‘产品准入+上路通行’机制,联合制定规则、并行审查,为产业划定清晰的安全基线,为创新留足空间。”

付炳锋说,对行业而言,许可自动驾驶车型产品不仅是对技术成熟度的权威认可,更是对社会各界关于未来智慧出行期待的有力回应。L3级别自动驾驶的落地,是涵盖整车、零部件、软件算法、通信、数据服务等多主体协同的系统性工程,将推动产业链上下游从“供应关系”转向“共生关系”。

推动技术迭代,健全制度体系——

据悉,下一步,两款车型将由重庆和北京两家使用主体在相关区域内开

展上路通行试点。工业和信息化部将联合有关部门及地方主管部门加强车辆运行监测和安全保障,及时总结经验,不断健全智能网联汽车准入管理和标准法规体系。

孙航认为,这实际上是对行业创新的一种双向促进,智能网联汽车准入和上路通行试点工作的推进,为我国汽车技术创新和迭代升级注入强劲动力,与此同时,也为标准制定提供宝贵的实践经验,让准入流程更顺畅、更科学。

“一方面促进汽车生产企业安全过程保障能力及产品技术进一步成熟,另一方面验证制度体系的可行性和可扩展性。”瞿国春表示,将通过试点完善技术评估流程要求,探索构建全链条安全管理模式,有序推动先进技术安全应用。

新华社北京12月15日电