

# “盐水疫苗”冲撞印度“防疫盾牌”

假疫苗已注射给了约2600名受害者,不仅无益于印度抗击疫情,而且还可能冲击疫苗接种计划

□ 陈润洋

由于担心疫情愈演愈烈,印度当局正在加紧为民众接种疫苗。近日,印度警方破获一个给民众注射“盐水疫苗”的犯罪团伙,伪造新冠疫苗接种证书,用生理盐水伪装成正规疫苗,高价出售牟利。这些假疫苗已注射给了约2600名受害者,不仅无益于印度抗击疫情,而且还可能冲击疫苗接种计划。

## 印惊现盐水疫苗

据外媒报道,7月5日,孟买警察局高级官员维沙尔·塔库尔表示,当局在印度西部马哈拉施特拉邦的金融中心孟买及附近地区,发现了至少12起假疫苗接种活动。“他们在假疫苗接种点,以盐水代替新冠疫苗为民众接种。”塔库尔说道。

据悉,此次大规模的假疫苗接种活动发生在5月下旬至6月初。一些接种假疫苗的患者对自己收到的疫苗接种证明产生怀疑并向警方报案,有关部门对此事展开了调查。

最初是接种了假疫苗的民众感到不对劲,比如发现疫苗名称的拼写有误,或者疫苗标注的名称根本不在政府公布的授权使用的疫苗清单中,而且他们也没有收到成功接种疫苗的官方短信提醒。

其中一起假疫苗接种是在一个房屋协会中进行,一位受害者称,“尽管当时我们有些怀疑,但我们所有人都没有出现任何症状,而且当时必须用现金支付”。

在印度西孟加拉邦首府加尔各答也出现了类似骗局,超过500人被注射了含有抗生素硫酸阿米卡星的假疫苗。医学专家表示,如果接种者患有肾病,这些抗生素甚至会造成生命危险。

据新德里电视台和《今日印度》日前披露的案件细节显示,印度联邦议会人民院议员、知名演员查克拉波蒂6月下旬自称是IAS官员(印度行政服务人员)的“德巴詹·德夫”的邀请,前往加尔各答南部的一个疫苗接种点作示范,鼓励民众接种疫苗。但完成接种后,他也没收到官方认证的短信通知,查克拉波蒂立刻报警。至此,“德巴詹·德夫”骗局曝光,此人被捕前已在加尔各答组织了多场假疫苗接种活动。

## 警方严打假疫苗

据报道,印度警方在过去的两个月里已逮捕14人,嫌犯以每剂10美元~17美元的价格出售假疫苗牟利,被没收2.8万美元不法所得。目前警方仍在调查其他涉案人员,逮捕人数未来可能会进一步增加。

塔库尔称,“落网者被控共谋犯罪、欺诈及伪造文书等”。其中包括一些参与这场骗局的医生,他们利用一家私人医院来生产假证书、假药瓶、假注射器从而进行诈骗。

这家私人医院此前获得印度政府许可,可以为民众接种疫苗,但并未获得许可在居民区开设疫苗接种点。私人医院在未获得授权的情况下,在居民区举行大规模疫苗接种活动。警方怀疑,该医院将用过的疫苗包装瓶重新填充,冒充新到的疫苗。而这些疫苗包装瓶本应在使用后就销毁。目前,涉事医院已被查封。

随着警方开始调查,其他人也采取了法律行动。据美国有线电视新闻网(CNN)称,6月24日,孟

买律师西达尔特·钱德拉谢卡尔提起了一项公益诉讼,当时,公诉人声称已确认了2000多名陷入骗局的受害者身份。

孟买高等法院在起诉状中写道,这些指控“非常令人震惊”,并要求孟买所在的马哈拉施特拉邦和大孟买市政公署采取行动,保证假疫苗的事件不再重演,以使无辜的民众不再受害。

## 疫苗接种任重道远

日前,印度遭遇第二波疫情的沉重打击,一度出现连续20多天单日新增确诊病例超过30万例的情况。病患死亡率的迅速增加,以及毛霉菌病等罕见疾病的大规模暴发,让印度民众接种新冠疫苗的意愿强烈。

印度直至今年6月7日,才宣布为18岁以上的成年人免费接种疫苗。此前,印度政府仅为老年人和一线医护人员免费接种疫苗,而18岁~45岁的成年人要想接种疫苗就必须自费,这给了“盐水疫苗”可乘之机。

据悉,今年6月初,印度总理莫迪宣布了疫苗集中接种计划,其中很大一部分剂量将由印度政府免费提供给各地区。根据美国约翰斯·霍普金斯大学的数据,到目前为止,该国已有超过6200万人(约占该国人口的4.5%)接种了疫苗。印度政府计划于今年年底前为全国民众完成疫苗接种,但由于接种缓慢、剂量短缺等因素,该计划进展艰难。

此外,印度生产新冠疫苗严重依赖美国的37种关键原料,但早在去年4月,时任美国总统特朗普就颁布法令禁止疫苗原材料出口,这项禁令延续至今,给印度疫苗生产造成极大阻碍。

分析认为,以当前印度的产能和进口疫苗进度计算,印度可能要到2023年才能完成全面接种疫苗的任务。

据“德国之声”报道,印度乔治国王医科大学肺部疾病专家阿斯瓦蒂说,印度至少需要13万个~14万个疫苗接种中心,超过10万名卫生保健专业人员,但现实中远远不足。“很多印度人成为疫苗欺诈的牺牲品并不奇怪,中产阶级也在恐慌。”

## 泰国新冠疫情影响严峻 政府宣布新一轮管制措施

泰国疫情管理中心副发言人阿披莎近日在例行发布会上表示,鉴于日益严峻的疫情形势,中心当天决定从7月12日起在曼谷、佛统府、暖武里府、巴吞他尼府、沙没沙空府和北榄府实施更严厉的管制措施,希望能够在2周~4周内有效控制感染人数增长。图为一名女子在泰国曼谷一处新冠疫苗接种点接种疫苗。

新华社发(拉亨摄)



# 勒索软件成网络安全主流威胁 多边协作监管迫在眉睫

□ 张莹

近日,美国软件企业卡西亚公司遭勒索软件攻击,其客户企业中有800家~1500家受波及。今年以来,全球勒索软件攻击有愈演愈烈之势,给经济和社会生活造成严重损失,已成为网络安全主流威胁之一。

勒索软件攻击自20世纪80年代末出现,其攻击模式不断发展演化,呈现新的特点和趋势,包括更多地针对高价值目标、负面影响扩大、逐渐形成网络犯罪“产业链”、越来越多地采用双重勒索策略等。

## 锁定高价目标

近几个月来,全球发生多起重大勒索软件攻击事件。这些勒索软件攻击案有一定相似性,他们都锁定高价值的目标资产并有针对性地发起攻击,索要的赎金数额巨大,造成广泛负面影响。

5月初,美国科洛尼尔管道运输公司遭勒索软件攻击,一条输油

干线被迫关停数日,导致美国多个州和地区一度面临燃油供应危机。美国联邦调查局称,一个名为“黑暗面”的网络犯罪团伙是幕后黑手。为尽快恢复系统,科洛尼尔公司以比特币方式向黑客支付价值近500万美元赎金。部分赎金后来由美国司法部追回。

5月中旬,爱尔兰卫生服务执行局网络系统遭黑客攻击,造成全国多家医院的电子信息系统无法进入。爱尔兰公共支出与改革部负责政府电子政务的国务部长奥西安·史密斯表示,对卫生服务执行局网络系统的攻击也许是该国迄今遭受的最严重网络攻击。攻击者是来自国外的网络犯罪团伙,其目的是为了钱。

5月底,世界肉类加工巨头JBS公司受到黑客攻击,其北美和澳大利亚的信息系统被“黑”,部分工厂瘫痪。一个名为“邪恶”的黑客团伙被指认为幕后黑手。该公司美国分部发布声明证实,已向黑客支付相当于1100万美元的赎金,以结束对公司业务的攻击。

最新遭到攻击的卡西亚公司是一家向IT外包公司提供软件的企业。该公司首席执行官弗雷德·沃科拉对媒体表示,最多有1500家客户企业受波及,而这些客户企业的下游用户所受影响还难以确切估计。英国牛津大学网络安全教授夏兰·马丁认为,这种“供应链袭击”以服务数千家下游企业的公司为目标,受害企业总数可能巨大。

美国媒体称,这起攻击同样与“邪恶”黑客团伙有关,该团伙在其暗网网站上提出,卡西亚公司可以用7000万美元加密货币赎金换取解除故障的通用解密器。目前,该公司拒绝透露是否打算与黑客谈判或支付赎金等事项。

对高价值目标的定向攻击是随着实体经济信息化程度不断提升而出现的。据中国安天科技集团首席技术架构师肖新光介绍,较早的勒索软件主要是非定向传播的、带有数据加密和删除功能的蠕虫病毒,依靠网络或U盘大面积感染计算机,勒索赎金数额较低。

此后,勒索攻击与高级持续性威胁攻击相结合,演化出针对高价值目标的定向勒索。

## 勒索模式进化

网络勒索高发、威胁升级的一个重要原因是网络犯罪生态系统的形成发展。美国媒体报道,勒索软件攻击如今演化为“高度分工合作的行业”,由勒索软件供应商、赎金谈判人员、攻击执行人员及话务员等组成。肖新光介绍,在网络勒索“产业链”上,一般上游团伙编写勒索软件并提供攻击设施,下游团伙负责实施攻击,上下游“分享”赎金。

据媒体报道,“邪恶”和“黑暗面”均采取名为“勒索软件即服务”的作案模式。他们向其附属团伙提供勒索软件和相关设施,并从附属团伙所获的赎金中抽成。加密追踪企业英国埃利普蒂克公司联合创始人汤姆·鲁宾逊说,从美国政府缴获的比特币可以看出“黑暗面”与其合作伙伴的分赃比例。

在攻击模式上,上述两个黑客

团伙都使用渐成主流趋势的“双重勒索”策略:黑客首先窃取存储在受害者系统内的敏感信息,然后对这些敏感数据加密,并要求以赎金换取密钥;勒索者还会发出额外威胁:如果勒索目标拒绝支付赎金,他们就在网上公布窃取的数据。这意味着无论受害者是否预先备份了数据,都可能被迫支付赎金。

中国瑞星公司6月发布的《瑞星勒索指南》认为,这种“复合勒索”使受害企业既面临隐私数据泄露,还面临相关法规、财务和声誉受损等多重风险。

由于网络勒索多为跨国、跨境作案并具有在网络空间难以追踪等特性,取证和执法面临诸多挑战。欧洲刑警组织去年10月发布报告建议,为了更有效应对网络犯罪挑战,应通过公共部门和私人伙伴之间的协调与合作加强信息共享,增强防范意识和防御能力建设,同时让多边协作机制继续在打击网络犯罪领域发挥关键作用。

海外传真

## 俄美总统通电话 讨论打击网络犯罪等问题

本报讯 俄罗斯总统普京7月9日与美国总统拜登通电话,讨论打击网络犯罪等问题。

据克里姆林宫网站发表的声明,两国领导人在通话中就双方上月在瑞士日内瓦会晤期间谈及的信息安全与打击网络犯罪问题继续对话。双方强调在网络安全领域进行实质性、建设性合作的必要性。就近期有关一系列针对美方的网络攻击或源自俄罗斯境内的报道,普京表示,近一个月来美方相关部门并没有就这些问题与俄方进行沟通。俄方愿与美方共同开展行动,打击网络犯罪行为。

普京表示,俄美双方应在信息安全领域展开长期、专业的协作,不搞政治操演,相关协作应在双边法律机制框架内进行,并符合国际法相关条款。

另据美国白宫发表的声明,拜登在通话中要求俄方采取行动打击在其境内活动的勒索软件犯罪团伙,并表示他将致力于与俄方就此保持沟通,美方将采取一切必要行动来保护美国民众和关键基础设施的安全。美国白宫新闻秘书普萨基7月6日说,美俄高级别官员下周将就勒索软件攻击问题举行会晤。

据新华社报道,近几个月来,发生了多起针对美国企业的勒索软件攻击事件。美国软件企业卡西亚公司近日遭勒索软件攻击,其客户企业中有800家至1500家受波及。有美国媒体报道称,这起攻击与俄境内的“邪恶”黑客团伙有关。(李奥)

## 伊朗交通部门连续遭到网络攻击

本报讯 继伊朗铁路系统7月9日遭到黑客袭击后,伊朗道路和城市发展部计算机系统10日又受到网络攻击,导致多个官方网站一度瘫痪。

据伊朗国家电视台报道,伊朗道路和城市发展部的内部计算机系统7月10日遭到网络攻击,使得该部网站和旗下其他网站中断服务。报道没说怀疑对象和黑客是否索要赎金。据悉,7月9日,伊朗全国多地火车站的电子告示牌上出现列车晚点或取消的“假信息”。伊朗铁路部门说,铁路电子追踪系统遭到黑客袭击,告示牌系统被侵入,但列车运行未受影响。

伊朗通讯与信息技术部长穆罕默德·贾瓦德·阿扎里-贾赫鲁米提醒相关部门修补计算机系统漏洞,以免遭到勒索软件攻击。

伊朗去年底就有两个政府机构遭到大规模网络攻击,但没有指明幕后操纵者。伊朗过去曾指认美国和以色列对其发动网络攻击。(王宏彬)

## 德国消费者组织对戴姆勒提起诉讼

本报讯 据法新社报道,日前,德国消费者保护组织VZBV联合会表示,他们已经就“柴油门”排放作弊丑闻对汽车巨头戴姆勒提起诉讼,此前他们也对大众公司进行了类似的诉讼。

VZBV联合会表示,在德国斯图加特高级地方法院的诉讼将帮助梅赛德斯奔驰GLC和GLK车主获得与排放测试作弊软件相关的损失赔偿。此次德国消费者针对戴姆勒的诉讼具体涉及装有OM 651发动机的奔驰GLC和GLK车型。

据VZBV联合会估计,受到影响的汽车可能多达5万辆。德国法律不允许许多人共同提起集体诉讼,因此VZBV联合会代表受害车主们发起了集体诉讼。

VZBV联合会负责人克劳斯·穆勒在一份声明中说:“可能受到影响的人将确定戴姆勒是否故意在数千款车型上使用了减效装置。尽管戴姆勒公司进行了官方的召回,但仍然否认故意操纵车辆的排放数据。”穆勒表示,最高地方法院现在应该就此项诉讼做出最终判决,这样众多消费者才会获得法律上的确定性依据。

据悉,去年9月,戴姆勒已与美国政府达成和解,为其柴油车排放超标支付赔偿金。美国监管部门对戴姆勒的相关调查已持续近5年。美国法院文件显示,戴姆勒将为此支付22亿美元。戴姆勒表示,与美国监管部门的和解费用预计将达15亿美元,与车主的和解费用预计为7亿美元。

法院文件显示,戴姆勒同意向每名车主支付最高3290美元的赔偿,并承担高达8340万美元的律师费。戴姆勒将召回并修理排放超标的机动车,但无须回购车辆,除非其未能在规定期限内解决排放超标问题。(秦天弘)