新民晚报社
上海市国防教育协会
联合主办

军界瞭望

20
看不见就打
打完了也没看见

本报时政新闻中心主编 | 第641期 | 2021年5月17日 星期一 本版编辑:吴 健 视觉设计:竹建英 编辑邮箱:wujian@xmwb.com.cn


■ 科洛尼尔管道公司的储油区

危机降临！
黑暗面 绑架美国能源大动脉

■ “你被黑了”


■ 科洛尼尔管道公司的管网受到黑客威胁

5月上旬，美国科洛尼尔管道公司管理的横贯北美大陆的燃油管线突然关闭，导致东海岸经济精华区出现“能源恐慌”，拜登政府宣布17个州和华盛顿特区进入紧急状态。美国联邦调查局、国土安全部等认定这是蓄意的网络攻击，始作俑者是绰号“黑暗面”的黑客组织，“他们要为科洛尼尔管道公司网络中枢瘫痪负责”。

专盯“大客户”

波士顿网络安全公司总裁莱奥·迪夫介绍，“黑暗面”是2020年8月份才出道的，以勒索软件侵入专用网络，通过锁闭关键文件、盗取重要数据等敲诈受害者。美国政府确认此次攻击的元凶是“黑暗面”，就因为网络特工识别出侵入管道公司专用网的勒索软件出自“黑暗面”。

尽管“黑暗面”并非老牌黑客组织，但在网络攻击领域却显得“够狠够专业”。“黑暗面”也在网上留言自夸：“我们是黑客行业的新来者，但不意味着我们没有根基或经验。”美国“突破防务”网站称，“黑暗面”正凭借高度的组织性和专业技能在黑客界崛起，“他们由资深黑客组成，拥有高超的网攻技巧、丰富的经验和多样的工具……除专业黑客，还有人负责外联、调查乃至谈判……为方便与受害者联络和谈判，他们甚至会在网页留下电话号码以及‘帮助’按钮”。

与别的网络勒索团伙不同，“黑暗面”通常在入侵前仔细调查目标。“内容不局限于技术层面，还包括目标一般信息，比如公司性质、规模大小、收益情况等等，”迪夫说，“目的是确定目标是否值得攻击。”“黑暗面”分子认为，值得攻击的应该是规模较大、收益较高的公司。该组织的首个受害者，就是一家资产高达57亿美元的土地开发商，而此次遭殃的科洛尼尔管道公司同样在美国乃至西方能源运输领域位居榜首。

欲立“侠盗”人设

尽管网络入侵及勒索属于犯罪行为，尤其燃油管道关乎民生和国家安全，但“黑暗面”却辩称自己是当代“侠盗”，入侵网络时“有所为，有所不为”——只有那些规模庞大、收益丰厚的公司才是攻击目标，而医院、养老院、学校、非盈利组织或政府机构等是“绝对禁止攻击目标”，入侵前调查时一旦发现目标在“绝对禁止”名单里，攻击会立即叫停。“黑暗面”强调自己的存在是为了“世界更美好”，手段是从“为富不仁”的大公司兜里把钱掏出来，分给更需要的人们。他们乐意以“劫富济贫”自居，在黑客论坛内发帖称，“（被入侵的）公司缴纳的赎金，将有一部分捐给慈善机构……不管我们在你们的意识里留下的印象有多坏，我们都会因能够帮助别人摆脱困苦而高兴”。

2020年，“黑暗面”曾向“儿童国际”以及“水项目”两家慈善机构各捐赠0.88个比特币（约合1万美元），并将税务收据张贴在暗网上，但两家并不领情，干脆拒绝捐赠，称“不会接受脏钱”。尽管“黑暗面”洗白的努力未获成功，却仍得到其他黑客效仿，像擅用“黑兹”勒索软件打劫商业公司的黑客组织就宣布只对年收入超过10亿美元的目标下手，让富得流油的资本家“受到应有惩罚”。

不会“杀鸡取卵”

美国国土安全部已把“黑暗面”列为重大国家安全威胁，因为它的具体入侵技巧还不清楚，而且不断变异，造成防御和反击的无力。“‘黑暗面’的攻击套路叫‘双重勒索’，”迪夫说，“先要求受害者支付一定的赎金，换取解锁文件的专用工具包；若被拒，他们就把公司机密数据放到专门的‘展览台’上公开，造成公司股价动荡，他们趁机在股市上大捞一笔。”所谓“展览台”就是“黑暗面”设置的“网上新闻中心”，新闻记者和受害公司可在此直接联系“黑暗面”——记者们可以获得爆炸性新闻素材，受害者则可借助平台与黑客讨价还价。

尽管尚不知晓“黑暗面”要求科洛尼尔管道公司支付多少赎金，但按惯例，该组织勒索的赎金数额通常在20万至200万美元之间。“根据‘黑暗面’网上消息，迄今他们勒索过的公司超过40家，”迪夫说，“这意味着数千万美元的赎金。”不过“黑暗面”不希望受害对象因勒索而破产，他们声称行动前会花费大量时间“仔细分析目标往来账目，并根据公司净收入情况确定需要支付的赎金数额”。他们还声称，“我们只攻击能满足我们要求的公司，我们不会杀鸡取卵”。

老巢疑在东欧

美国网络安全部门分析，“黑暗面”老巢很可能在东欧，且他们动用的软件只针对英语国家，遇到与原苏联有关的国家会自动绕开。“我们对‘黑暗面’软件进行反向破解，发现它会自动检测目标的语言设置，避免攻击使用俄语的公司。”匿名的美国国土安全部官员称，这让他们疑心大起，在管道遭袭后的第一反应是“俄罗斯人干的”。但随着调查深入，他们并未发现俄罗斯参与的证据，“尚无证据表明莫斯科卷入这起事件，连间接证据都没有。”“黑暗面”也于5月10日公开声明，否认与俄政府有关，其行为也没有政治目的，“我们不关心政治，也不参与地缘政治竞争，我们不想给社会制造麻烦，我们只为了挣钱”。

尽管俄政府没有回应美国管道遇袭事件，但俄官方之前已多次抱怨美国网络安全问题多半是“贼喊捉贼”。俄联邦安全会议副秘书奥列格·克拉莫夫称，2016–2019年，全球40%至75%的黑客攻击是从美国本土发起的，“这清楚表明，以美国为首的西方国家一直集体炮制网络安全谎言，他们把俄罗斯描绘成‘网络安全威胁’是毫无根据的”。于晓晶

热点聚焦


■ SK–64救生钟内部操作空间

俄海军潜艇救援“动真格”

4月21日，印尼海军潜艇“南伽拉”号训练时沉没，全体艇员丧生，再次表明潜艇一旦出事，应急救援极为关键。不久前，俄罗斯红星电视报播放黑海舰队潜艇“阿尔罗萨”号坐底救援的画面，让外界一窥相关训练的细节。

按照想定，“阿尔罗萨”号在指定海域模拟“失事坐底”，俄黑海舰队立即出动救生船、AS–5救生艇、飞机等施救。

找到“阿尔罗萨”号后，“艾普朗”号救生船先用自带的遥控潜水器与之建立通信，并获得“失事”潜艇的现场图片，方便救援人员判断态势。救援开始后，俄海军大尉列文、日梅特科夫和谢夫留金驾驶的SK–64救生钟被“艾普朗”号吊放入水，三人配合默契，逐渐接近潜艇救生口并与之对接，让艇员挨个进入救生钟。要注意的是，潜艇出事后，未必所有人能撤到救生口所在舱段，因此救援中，除了安排已集合的艇员转移到救生钟里，还要维持艇内别的隔舱受困艇员的生命。值得称道的是，俄制潜艇所有隔舱围壁上都有接头，救援人员设法将缆绳和软管接上去，向有人的舱室输送通风用气，并把污浊空气置换出来，这才是稳妥的方法。为验证不同救援装备的性能，继SK–64救生钟后，俄海军又动用“公社”号救生船上的AS–5救生艇与潜艇对接，在实战背景下锤炼了官兵的救援技能。

潜艇既可能在水下失事，也可能在水面浮航时因舱内失火、丧失浮力等原因而不得不弃艇，这就涉及集体救生内容了。演习第二阶段，“阿尔罗萨”号模拟因舱内火灾紧急上浮，艇员通力协作把PSNL–20M救生筏搬到潜艇甲板上，但筏子得先入水并充气撑开后才能收容艇员，人们只能先跳到水里，再自行爬上筏子。于是，“阿尔罗萨”号艇员们全都穿上ARO/V40救生服，一个个从艇艏和水平舵上纵身跳入水中，这种救生服既防寒防水（穿着者能在10℃的水里漂浮四五个小时），又因醒目的橙黄色而容易被发现。

与此同时，扮演“营救天使”的“雨燕”救生艇离开“艾普朗”号救生船，正快速向PSNL–20M救生筏驶来。由于现场风浪较大，一部分潜艇艇员无法登上救生筏，他们必须在水面上手挽手连在一起，抵挡风浪冲击，坚持到救援人员到来。好在“雨燕”行动迅速，只用十几分钟就把所有艇员从水中捞起，然后把缆绳抛给救生筏，一路牵引着回到“艾普朗”号救生船。

常立军


■ “阿尔罗萨”号潜艇与AS–5救生艇对接

外军掠影