■ 有消息称，在要求赎金之前，黑客从科洛尼尔管道公司窃取了近 100GB 的数据 本版图片 CJ

■ 输油管道关闭引发恐慌性抢购

让美国能源『大动脉』瘫痪，还把『手』伸向世界各国 『黑暗面』到底什么来头？

当地时间5月9日，美国总统拜登宣布，美国17个州和哥伦比亚特区进入国家紧急状态，原因是美国最大输油管线运营商科洛尼尔管道公司7日遭到一个名为“黑暗面”的黑客组织的网络攻击，为此不得不关闭整个能源供应网络。

时隔四天，当这家管道公司宣布全线恢复运营，“黑暗面”再次出手。13日，其在暗网发表声明称，已窃取日本东芝公司法国分公司740GB机密信息和个人资料。

连续几个“大动作”，让这个去年8月才“出道”的黑客组织一时间“名声大噪”。

既能让美国能源“大动脉”陷入瘫痪，还能把“手”伸向世界各地，“黑暗面”究竟是个怎样的黑客组织？

并非资深组织 成员都是老手

科洛尼尔是美国炼制油品输油管线的巨头。每天，来自墨西哥湾沿岸炼油厂的至少250万桶汽油、柴油、飞机燃油通过这家公司旗下主线管道，被运输至人口稠密的纽约、华盛顿等地。该条管道总长约8850英里，运输量占美国东海岸供应量的45%。

5月7日，科洛尼尔管道公司称其部分主线网络遭遇网络攻击。黑客窃取了100GB的数据，不仅对其加密，还限制访问，并企图借此索要上百万美元的赎金。

5月8日，科洛尼尔管道公司发表声明称，此事件与勒索软件有关。但从当日声明来看，“真凶”还未浮出水面，但该公司已决定主动关闭一些系统，停止部分管道运作。

9日，科洛尼尔管道公司线路“罢工”的影响显现，输油管道关闭引发美国民众的恐慌性抢购。从佛罗里达州到弗吉尼亚州的加油站汽油供不应求，美国汽油期货涨幅超过3%，创下三年以来的新高。

同一天，拜登宣布美国17个州和华盛顿特区进入紧急状态，旨在放宽这些地区石油产品公路运输的限制，以防燃油短缺。

“‘黑暗面’要为科洛尼尔管道公司网络中枢瘫痪负责。”10日，美国联邦调查局（FBI）发声确认了此次事件的背后主谋，“黑暗面”由此进入大众视野。

“黑暗面”也是“敢作敢当”。11日，它们发表声明承认实施了此番操作，但原因只是“为了钱，而非为社会制造麻烦”。

13日，科洛尼尔管道公司称，该公司受网络攻击而被迫关闭的燃油运输管道全线恢复运营。但此次攻击对美国社会产生的负面影响仍在延续。直到16日，不少加油站仍处于汽油短缺状态，华盛顿特区近81%的加油站无油可加。

美国能源界人士对此担忧不已，称“这是迄今为止发生在美国的、对能源基础设施破坏性最严重的一次攻击”。

入侵美国能源“大动脉”，让17个州进入紧急状态，还惊动了总统和FBI亲自出马……“黑暗面”究竟是什么来头？

“黑暗面”并不是老牌黑客组织，成立时间还不足一年。但这并不代表其“道行不够深”。“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。”该组织曾在网络上这样介绍自己。

网络安全专家指出，该组织虽然“年纪尚轻”，但成员却都是“黑客老手”。美国一网络安全公司情报部门负责人称，曾在2013年左右发现“黑暗面”背后一些“资深黑客”的踪迹。当时，这些黑客服务于一个名叫“碳蜘蛛”的组织。他们曾攻击过俄罗斯的金融组织，随后几年又将“矛头”转向了中东和欧美。

“黑暗面”还是一个有组织、有纪律的团体，还有着一套独有的商业模式。

通常，“黑暗面”开发推出勒索软件，再将其出售给犯罪分子，网络攻击由后者实施。窃取、加密后进行勒索是其常用手段，获取大额赎金是其最终目的。“黑暗面”还建立了一个网站，专门用来公开受害者的隐私数据。网站上留有联系电话，受害者可自行与该公司联系，进而商讨“解决方案”。赎金通常以比特币或门罗币支付，金额在20万到2000万美元不等。

对于“黑暗面”如何获得个人信息，“数码阴影”联合创始人查佩尔认为其极有可能购买了一些远程桌面软件的账户登录信息。

“黑暗面”总部所在地也引起了人们的猜测。

10日，美国总统拜登宣布美国将起诉“黑暗面”，并称该组织有可能位于俄罗斯。“虽然没有证据表明俄政府参与其中，但我计划很快将与普京总统会面，莫斯科应该为此承担一些责任。”

一家网络安全公司的分析报告称，“黑暗面”的“受害者”大多是美国公司，偶有欧洲、南非和巴西的公司。“要求分支机构不攻击俄罗斯和独联体国家，这或许能表明‘黑暗面’的总部所在地。”报告指出。

引发犯罪狂潮 称只为了搞钱

据美国《企业家》杂志介绍，自“出道”以来，“黑暗面”的创始人及其旗下分支机构引发了全球性的犯罪狂潮，目前已波及超过15个国家及多个垂直领域。

从去年下半年至今，该组织已成功勒索了10家企业、机构，其中不仅有油田服务公司，还有银行和律师事务所等。

“黑暗面”网站发布的内容显示，美国地毯生产商迪克西集团、美国农产品供应商卡罗莱纳东部公司、密歇根州的汽车焊接企业帕斯林都曾是该组织的攻击对象。

但直到科洛尼尔管道公司遭遇攻击后，“黑暗面”才吸引了全球的目光。

然而，“黑暗面”在声明中表示其起初并不想掀起轩然大波。

“我们对政治不感兴趣，我们不参与地缘政治竞争，不需要把我们与特定的政府捆绑在一起，也不用寻找我们的其他动机。我们的目标是搞钱，而不是为社会制造问题。从今天开始，我们将对每个目标进行审核，以避免一些社会影响。”该组织这样解释其动机。

■ 美国多地加油站贴出汽油短缺告示

■ 科洛尼尔管道公司

值得提高警惕 不必过度恐慌

科洛尼尔管道公司的危机，让美国社会和美国媒体担忧不已。

10日，美国土安全顾问伊丽莎白·舍伍德·兰德尔在新闻发布会上表示，这一事件将美国关键能源基础设施主要由私营部门所有并运营而导致的脆弱性暴露无遗。

“网络保险和加密货币的兴起助长了勒索软件案件的‘爆炸式’增长：网络保险使公司和政府部门成为犯罪团伙的目标，加密货币使赎金支付变得更难被追踪。”《纽约时报》发文称，这次攻击会使黑客对电网、管道、医院等关键基础设施的攻击变得愈发肆无忌惮。

“这对美国关键基础设施来说是个不祥的征兆。”美国《连线》杂志称，这是迄今为止，网络攻击中对美国能源系统冲击最大的一次。

但在美国消费者新闻与商业频道（CNBC）发表的一篇题为《科洛尼尔管道公司所以遭遇的网络攻击不会引起恐慌》的文章却持相对乐观的看法。

“这并不意味着我们突然面临新风险。因为，像这样的勒索软件攻击其实十分常见。”文章写道，“它们的目标并不是要让国家基础设施‘罢工’，很多黑客的动机都是谋求经济利益。”

网络安全公司红金丝雀情报总监凯蒂·尼克尔斯说：“这起网络攻击事件之所以引发全世界的高度关注，完全是由于它影响到了输油管道网络。但对我和其他网络安全专业人士来说，类似的攻击已经持续了很多年，但因为这次涉及美国关键基础设施，才会触动一根特别的神经。”

正当人们开始关注“黑暗面”之时，14日，美国《华盛顿邮报》报道称，“黑暗面”在向其合作伙伴发送的一封邮件中称其团队目前已经解散。

但专家认为，团队解散的消息可能只是个把戏，黑客可能只是想借此隐藏行踪，不排除他们会以另一个名字重启的可能。

值得玩味的是，在解散传闻流出之时，“黑暗面”的受害者还在不断扩大，而日本东芝公司的法国分公司就是其中之一……

弦子

●国内邮发代号3-5/国外发行代号D694/全国各地邮局均可订阅/广告经营许可证号：3100020050030/社址：上海市威海路755号/邮编：200041/总机：021-22899999转各部
●本报印刷：上海报业集团印务中心等，在国内外7个印点同时开印/上海灵石、上海龙吴、上海金桥、上海界龙/北京、香港、美国洛杉矶
●本报在23个国家地区发行海外版/美国、澳大利亚、加拿大、俄罗斯、西班牙、泰国、菲律宾、日本、法国、巴拿马、意大利、荷兰、南非、匈牙利、新西兰、罗马尼亚、尼日利亚、印度尼西亚、阿联酋、英国、德国、希腊等
24小时读者服务热线 962555
本报零售价 每份1.00元