

# 研究报告

2021 年第 30 期

2020.06.01

本期执笔：余德克

邮箱：

yudeke.xdjr@icbc.com.cn

## 从科洛尼尔事件看网络信息安全

- **摘要：**近期，美国最大成品油管道运营商科洛尼尔因黑客攻击被迫关闭美国东海岸的关键燃油网络，美国因此宣布进入国家紧急状态。科洛尼尔事件造成美国社会紧张和政府关注。本报告从网络信息安全的角度解读该事件，并提出相关建议。
- **关键词：**网络安全、输油管道、加密货币

重要声明：本报告中的原始数据来源于官方统计机构和市场研究机构已公开的资料，但不保证所载信息的准确性和完整性。本报告不代表研究人员所在机构的观点和意见，不构成对阅读者的任何投资建议。本报告（含标识和宣传语）的版权为中国工商银行现代金融研究院所有，仅供内部参阅，未经作者书面许可，任何机构和个人不得以任何形式翻版、复制、刊登、上网、引用或向其他人分发。

当地时间 5 月 7 日，美国最大成品油管道运营商科洛尼尔管道公司（Colonial Pipeline，简称“科洛尼尔”）<sup>1</sup>称其工业控制系统遭受网络威胁和攻击，黑客通过非法软件入侵并控制其 IT 系统和数据，公司已被迫关闭为美国东海岸各州供油的关键燃油网络以控制风险。5 月 13 日消息称，科洛尼尔在被攻击当天已通过加密货币向“黑暗面（DarkSide）”勒索软件团队支付近 500 万美元赎金。

表 1 科洛尼尔事件梳理

当地时间	事件
5 月 7 日	科洛尼尔遭黑客攻击，被迫关闭输油管道系统。
5 月 8 日	美国白宫表示总统拜登已经听取相关事件简报，政府将努力帮助科洛尼尔恢复运营。
5 月 9 日	美国宣布进入国家紧急状态，解除公路运输燃料的各种限制，以帮助燃料运输尽快恢复正常，降低科洛尼尔输油管道持续关闭的影响。
5 月 10 日	拜登表示政府非常重视科洛尼尔遭黑客攻击事件及其影响，联邦调查局（FBI）、国土安全部、国防部均在对此次黑客袭击进行调查，政府也在加紧改善网络安全问题，加强对跨国犯罪的防御。
5 月 10 日晚间	FBI 发布声明确认“黑暗面（DarkSide）”勒索软件对此次科洛尼尔事件负有责任。
5 月 11 日	DarkSide 在其官网发布声明称“我们的目的是要钱，而不是为社会制造麻烦”，但并未提及科洛尼尔及具体金额。此后美国方面表示尽管调查仍处于初期阶段，但已有证据将 DarkSide 与俄罗斯或东欧联系起来。
5 月 12 日下午	科洛尼尔宣布重启所有输油管道系统，但供应链仍然需要数天时间才能恢复正常。
5 月 13 日消息	科洛尼尔在被攻击当天已通过加密货币向 DarkSide 支付近 500 万美元赎金。赎金支付后，DarkSide 提供解密工具帮助科洛尼尔恢复网络，但因恢复速度过慢，科洛尼尔最终还是使用自己的备份数据来恢复系统。

<sup>1</sup> 科洛尼尔是美国炼制油品输油管线的龙头，其输油管道每天从美国墨西哥湾沿岸的炼油厂运输约 250 万桶汽油、柴油、航空燃油和家庭取暖用油到人口稠密的美东地区，如纽约、华盛顿、亚特兰大等地，管线总长约 8851 公里，是美东地区油气输送的主要动脉，美东地区 45% 的燃料供应依赖科洛尼尔。科洛尼尔还为美国军方提供相关服务。



## 一、事件分析

### （一）关键基础设施成为近年来网络安全主战场

关键基础设施<sup>2</sup>（Critical Infrastructure, CI）关系国计民生，是经济社会运行的神经中枢。随着近年来经济社会对网络依赖程度的加深及CI数字化程度提高，针对CI的威胁不断增加。一旦CI受到网络攻击陷入瘫痪，引发的连锁反应可能会对一个国家或地区造成巨大损失，因此CI的安全防护成为网络信息安全的重中之重。此次科洛尼尔事件就是网络攻击给现实世界基础架构造成巨大影响的案例。

根据绿盟科技<sup>3</sup>今年3月发布的《2020年度安全事件响应观察报告》（简称《报告》），在2020年度记录的安全事件中，交通、卫生、教育、能源、运营商、金融这些涉及CI的领域是黑客热衷攻击的主要对象，所占比例高达80%，而勒索软件攻击是排名前三<sup>4</sup>的安全事件类型。

2020/02	2020/02	2020/04	2020/05	2020/06	2021/02	2021/02	2021/04
<ul style="list-style-type: none"> <li>美国某天然气管道运营商遭勒索软件攻击，导致天然气压缩设备关闭。</li> </ul>	<ul style="list-style-type: none"> <li>克罗地亚最大石油公司INA Group后端服务器被加密，造成业务瘫痪。</li> </ul>	<ul style="list-style-type: none"> <li>葡萄牙跨国能源公司EDP被要求赎金1090万美元。</li> </ul>	<ul style="list-style-type: none"> <li>中国台湾炼油厂CPC遭勒索软件攻击，无法访问用于管理收入记录的数字平台。</li> </ul>	<ul style="list-style-type: none"> <li>巴西电力公司Light S.A所有windows系统被加密，黑客要求赎金1400万美元。</li> </ul>	<ul style="list-style-type: none"> <li>巴西两家主要电力公司Eletrobras和Copel遭受勒索软件攻击。</li> </ul>	<ul style="list-style-type: none"> <li>厄瓜多尔财政部和Banco Pichincha银行遭勒索软件攻击。</li> </ul>	<ul style="list-style-type: none"> <li>荷兰最大物流服务提供商之一的Bakker Logistiek遭勒索软件攻击。</li> </ul>

图1 近两年关键基础设施勒索攻击事件

### （二）定向勒索事件比例上升、危害大

勒索软件攻击分定向勒索和非定向勒索。根据《报告》，勒索软件团队为了追求利益最大化，开始关注攻击成本和效率，攻击方式从最初广撒网的非定向勒索逐渐演变为对有价值的攻击目标进行定向勒索，定向勒索事件比例近年来

<sup>2</sup> 关键基础设施是指对社会顺利运作至关重要的基本资产。该术语主要被用来描述某个国家和地区的基础设施框架，包括交通系统、电力和其他能源需求以及卫生系统等，还可能包括财政、电信和供水等。

<sup>3</sup> 创业板上市公司，我国网络安全解决方案供应商，我行在网络安全方面使用该公司产品。

<sup>4</sup> 安全事件类型前三名分别为入侵事件、虚拟挖矿和勒索软件。

持续上升。2020 年以来，越来越多的勒索软件团队开始有计划地瞄准大型企业（图 2），虽然攻击成本高，但一旦成功，回报远高于广撒网式勒索。DarkSide 是去年新出现的勒索软件团队，已知攻击过 40 多个受害者，一般要求赎金 20 万-200 万美元，此次科洛尼尔向 DarkSide 支付了近 500 万美元赎金。

勒索软件攻击使得数据窃取和泄露事件增加。勒索软件团队不再局限于对受害者数据进行加密，还会窃取受害者数据，并威胁如果不支付赎金就将数据外泄，对受害者财务和品牌形象造成双重打击。

2020/11	2021/03	2021/04	2021/04
<ul style="list-style-type: none"> <li>• 富士康受到勒索攻击，其文件在 DoppelPaymer 勒索软件泄露数据网站上被发布，攻击者索要 3400 万美元赎金。</li> </ul>	<ul style="list-style-type: none"> <li>• 宏碁 Acer 受到 Revil 勒索软件攻击，攻击者索要迄今为止已知的最大勒索金额，5000 万美元。</li> </ul>	<ul style="list-style-type: none"> <li>• 勒索软件团伙入侵英国铁路网 Merseyrail 电子邮件系统，并使用该电子邮件系统向员工和记者披露此次攻击。</li> </ul>	<ul style="list-style-type: none"> <li>• 意大利最大的合作信贷银行之一 BCC 受到勒索软件攻击，导致 188 个分支机构业务瘫痪，给客户造成严重影响。</li> </ul>

图 2 近一年定向勒索攻击事件

### （三）美国关键基础设施陈旧老化、易被攻击

美国网络安全与基础设施安全局专家指出，2019 年已有证据表明黑客可获得目标公司 IT 和 OT<sup>5</sup> 系统访问权限，包括负责控制物理设备的工控计算机。科洛尼尔事件表明该公司并未从历史事件中吸取教训，其管道控制系统存在重要安全漏洞，同时也说明美国 CI 能轻易被网络攻击已成现实。

美国类似事件已有多次。据统计，近年来针对美国企业工控系统和 CI 的勒索软件事件显著上升。过去一年，勒索软件不仅袭击了各大企业，还侵袭了美国多个州的医院、警察局、学校和政府机构，仅 2020 年支付的赎金就达

<sup>5</sup> Operational Technology, 运行技术、操作技术、运营技术。



到 3.5 亿美元，比上一年增加了三倍，平均每笔赎金超 30 万美元。

## 二、影响分析

### （一）短期影响

科洛尼尔事件对美国社会和资本市场已经造成一定短期影响。不仅美国宣布进入国家紧急状态，而且美国油罐车运输费率跃升 26%，不少消费者担心燃油短缺还出现恐慌性抢购。5 月 10 日美国汽油期货一度涨超 4% 至 2.2170 美元/加仑，创 2018 年 5 月以来最高；美国取暖油期货一度涨超 3% 至 2.0776 美元/加仑，创 2020 年 1 月以来最高水平。

### （二）远期展望

科洛尼尔事件或将引起美国政府及业界对其关键基础设施保护体系（CIP）的反思，进而更加重视加强网络安全防御。拜登 5 月 13 日的演讲号召要重新认识 CIP 对美国的重要性，并指出“我和我的政府将加大力度，致力于不断加强推动美国关键基础设施现代化与安全保护力度，因为美国不可能仅仅依靠 20 世纪陈旧的基础设施，去经济地赢得与中国及其他国家之间的 21 世纪竞争。”

此前，白宫已于今年 4 月推出一项“网络安全 100 天”行动计划，旨在采取新的措施来帮助电力、供水和其他 CI 行业领域防范潜在的破坏性网络攻击。本次事件或将助力该计划实施。5 月 12 日拜登又签署了一份名为《改善国家网络安全》的行政令，为加固网络安全制定了新的路线图。

## 三、政策建议

一是加快适应国家顶层设计需要。近年来我国先后设立中央国家安全委员会、中央网络安全和信息化委员会，发布《中华人民共和国国家安全法》、《中华人民共和国网络安全法》及相应的配套法规，制定《国家网络空间安全战略》、“等保 2.0 标准”<sup>6</sup>等政策标准，标志着我国对于整个国家网络安全的投入和建

<sup>6</sup> 即网络安全等级保护制度 2.0 标准。中国国家标准化管理委员会、国家市场监督管理总局 2019 年 5 月发布，2019 年 12 月 1 日正式实施。网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法。

设进入了一个新的历史阶段。企业应尽快建设满足国家新要求的网络安全防御体系。

**二是加强员工安全意识。**当网络攻击者难以通过传统技术对企业进行攻击时，因员工安全意识不足、安全管理薄弱等问题导致的弱口令、钓鱼邮件、配置不当等漏洞往往更容易成为攻击者的突破口。

**三是做好“防患于未然”工作。**要加强网络规划，做好漏洞补丁修复升级和配置加固，改善安全边界，增强安全运维监控，保持终端安全防御软件实时更新，提升有效防护水平。推动安全演练常态化，尤其是对黑客真实网络攻击的场景模拟，提升应急保障处置能力和团队协作能力。加强数据备份和容灾能力建设，增强业务的连续性。

**四是做好网络隔离，建立防御纵深。**根据内外网、IT 和 OT 间安全要求和对抗需求，将防火墙、入侵检测、深包检测等手段有机结合建立安全屏障，依托网络纵深控制攻击路径，通过态势感知和积极防御手段在攻击者达到攻击目的前及时响应和快速处置。

**五是加强网络信息安全合作与人才培养。**加强同高校、科研机构、企业在网络信息安全方面的沟通与合作，加强人才联合培养，助力网络信息安全教育投资，提升我行在网络信息安全领域的影响力。