勒索病毒再次对能源行业数据安全保护敲响警钟

5月8日，据外媒纽约时报报道，美国最大成品油管道公司Colonial Pipeline被勒索软件攻击，据了解，实施网络攻击的黑客很可能是专业的网络犯罪团伙。为避免造成更大影响，该公司已主动切断部分系统网络，暂停所有管道运营。

国家的关键基础设施面向公众直接或间接提供支撑性服务，它们的中断或破坏将对重要的社会功能产生严重影响。这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、社会、国防、环境以及人民的生命财产造成严重损失，后果不可估量。

勒索病毒如何防范

目前大部分勒索病毒加密后的文件都无法解密，主要安全防范手段有：

1、及时升级系统和应用，修复常见高危漏洞；

2、对重要的数据文件定期进行异地多介质备份；

3、不要点击来源不明的邮件附件，不从不明网站下载软件；

4、尽量关闭不必要的文件共享权限；

5、更改账户密码，设置强密码，避免使用统一的密码，因为统一的密码会导致一台被攻破，多台遭殃；

6、如果业务上无需使用RDP的，建议关闭RDP，尽量避免直接对外网映射RDP服务。

如何应对能源行业安全问题？深信服提出三大能力

实施勒索病毒攻击成本低、收益高，用户难以防范。针对日渐严重的勒索病毒威胁增长趋势，深信服进行大量长期的行业经验积累，并首次提出基于多维智能一体化的数据安全解决方案，从能源行业专用威胁情报库、能源数据安全大脑和能源定制化自主可控云终端三个维度，解决能源行业数据全生命周期安全问题。

在能源行业专用威胁情报库方面，利用AI技术和大数据分析技术，从勒索病毒攻击源头上对勒索病毒相关的攻击者进行攻击者组织画像和攻击行为分析，对攻击者武器进行特征提取，将勒索病毒威胁拦截在“墙（新一代防火墙）、门（零信任安全网关）”之外。

在数据安全大脑方面，对能源行业关键敏感业务数据进行实时的全生命周期安全监控，在数据存储、数据传输、数据使用和数据共享等方面，全方位保障数据的“生命”安全。

在能源定制化自主可控云终端方面，对数据产生的源头进行安全防护，保障终端数据在不幸遭遇勒索病毒时，能够进行实时的数据恢复和镜像回滚，保证业务的正常运转。

安全防护非一朝之事，需要时刻保持警惕，防患于未然。

原文地址：http://www.china-nengyuan.com/news/169171.html