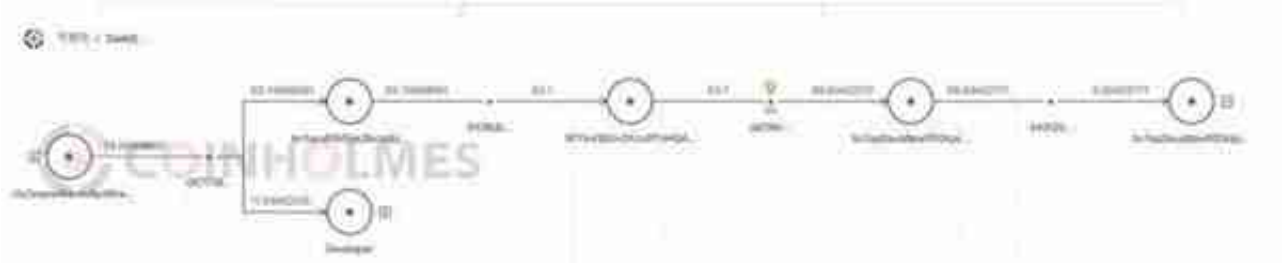
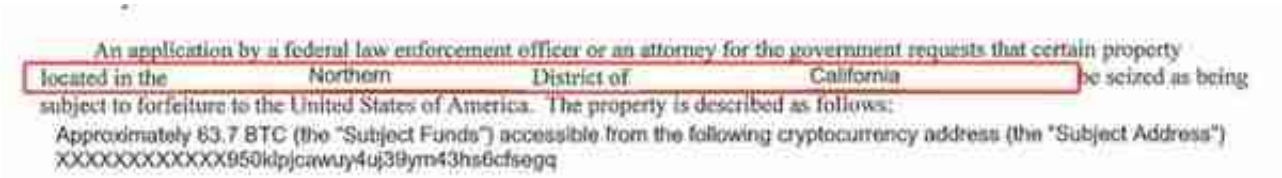
美国司法部宣布已追回此前 Colonial Pipeline 支付给勒索软件 DarkSide 的部分加密货币赎金。

据悉，此前美国最大的燃油管道 Colonial Pipeline 遭到勒索软件 DarkSide 攻击，DarkSide 提出价值 500 万美元的比特币赎金要求。Colonial Pipeline 于北京时间 5 月 9 日交付赎金 75 BTC



PeckShield「派盾」此前分析过 DarkSide 这个勒索组织已经形成完整的「勒索即服务（RaaS）」产业链，开发者向下家提供作案工具和方法，然后抽成获利。从资金流转图可以看出，这一次被 FBI 冻结的是勒索下游的资金（开头为 bc1qxu，63.7 BTC），开发者的资金自收到后就没有动过（开头为 bc1qu5，11.2 BTC）。

属于勒索下游的开头为 bc1qxu 的 63.7 BTC 先是转到了开头为 3EYkxQ 的地址，随后转入开头为 bc1qq2 的地址，再分两笔分别转入开头为 bc1qpx 的目标地址（FBI 掌握私钥的地址，63.7 BTC）和另一地址（5.9 BTC）。


An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Northern District of California be seized as being subject to forfeiture to the United States of America. The property is described as follows:
Approximately 63.7 BTC (the "Subject Funds") accessible from the following cryptocurrency address (the "Subject Address")
XXXXXXXXXXXX950kdpjcawuy4uj39ym43hs6cfsegq

PeckShield「派盾」 反洗钱专家表示：“FBI 很可能追踪到了勒索软件在美国的服务器代理，然后被端了，私钥可能存在服务器上面。”

早前 DarkSide 的网站被封，他们发文宣布解散，并将支付服务器上的资金转移到了一个未知的地址。