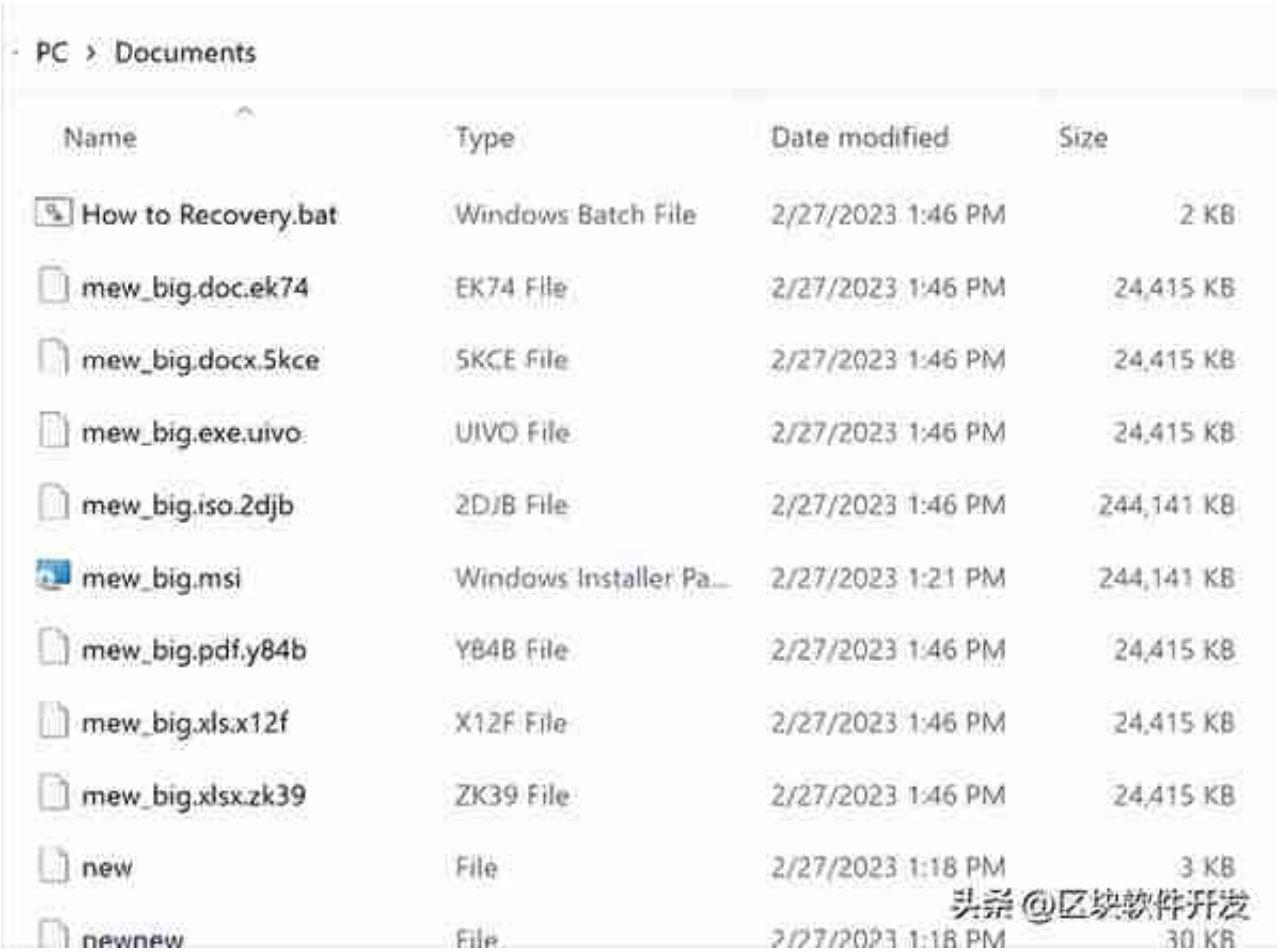
Sirattacker 勒索软件

Sirattacker 勒索软件是 Chaos 勒索软件的变种之一。Chaos 在 2023 年 2 月中旬被首次发现，地下论坛中提供了多个版本的 Chaos 勒索软件构建工具，任何人都可以使用自定义的配置生成 Chaos 勒索软件。

感染载体

Sirattacker 勒索软件很可能是冒充以太坊挖矿应用程序进行分发，因为所有样本文件都包含一个以太坊的图标。

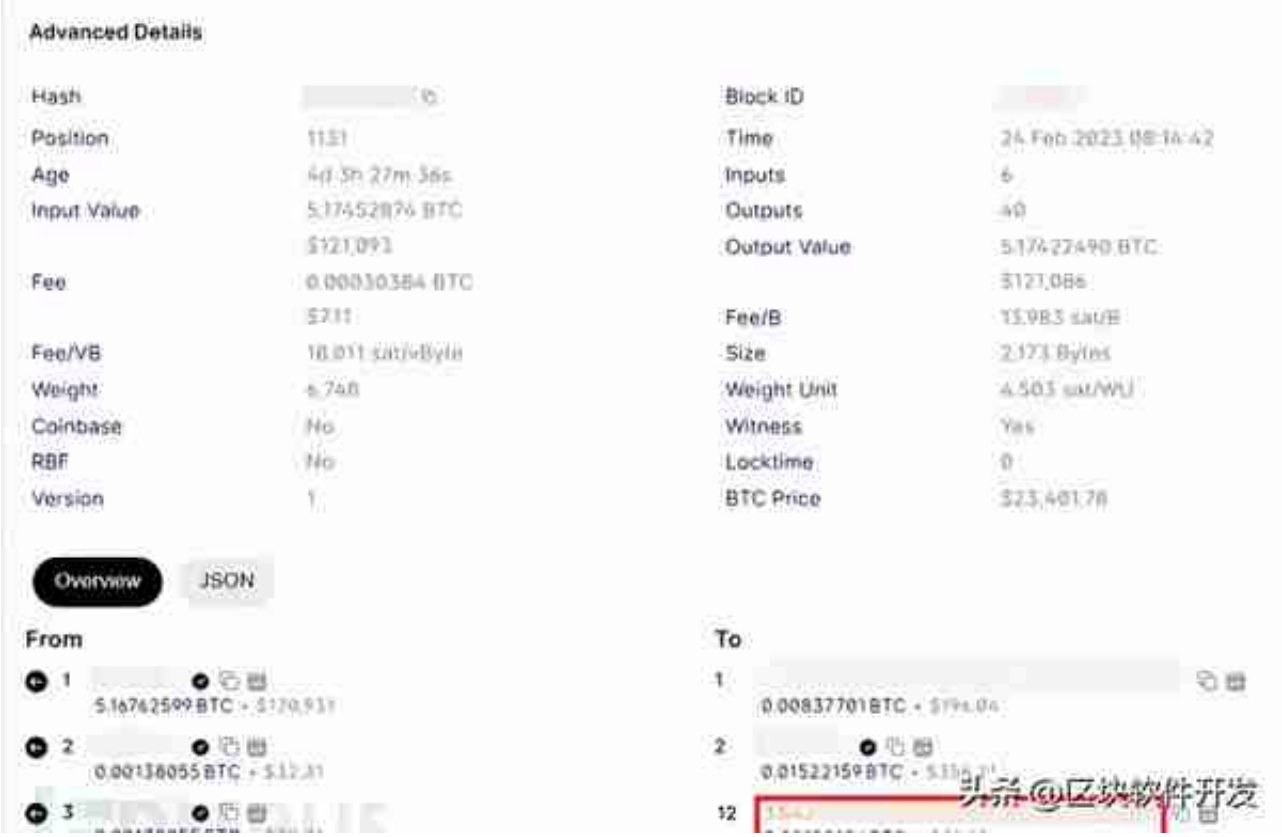


加密的文件

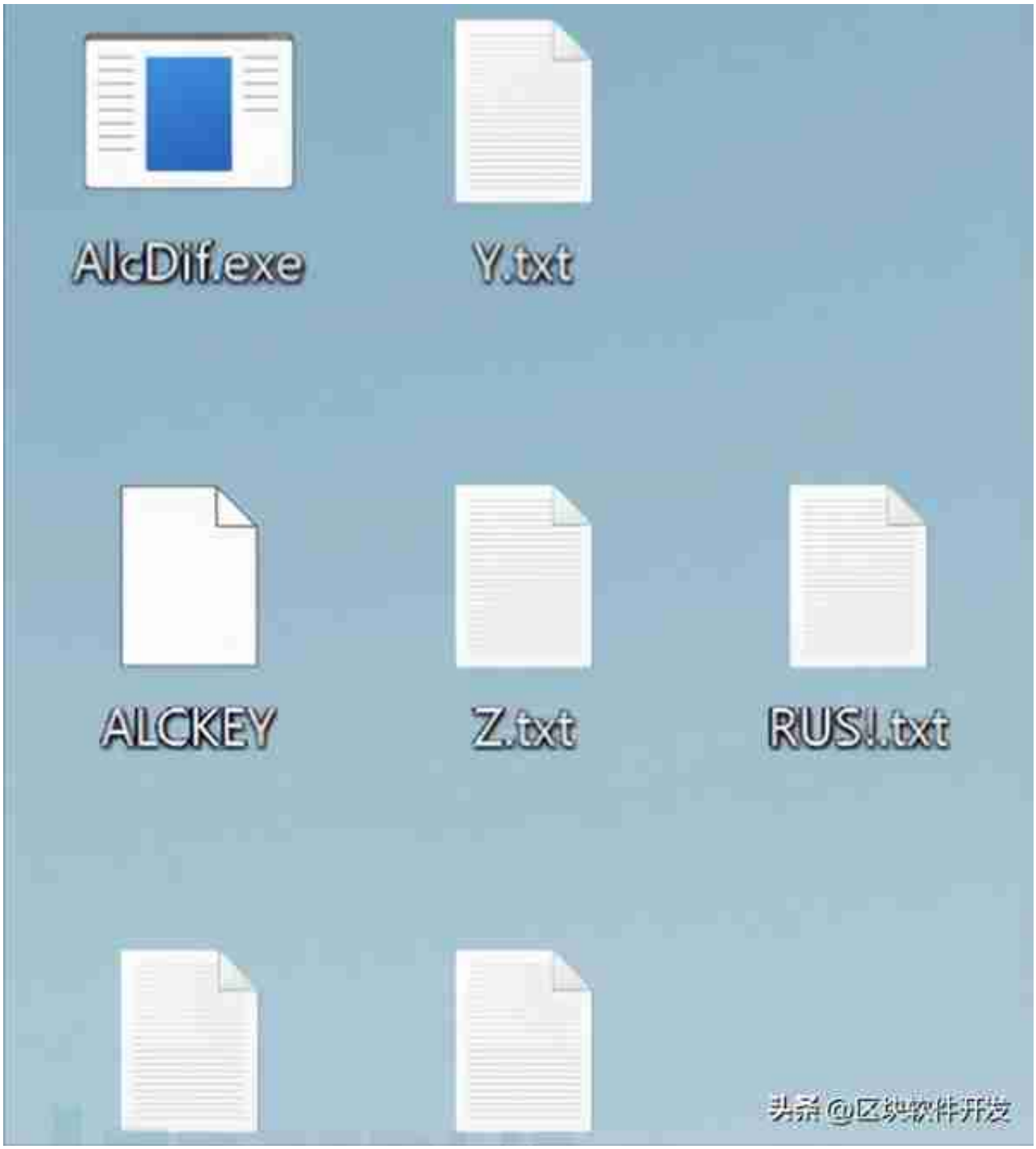
文件加密后，Sirattacker 会显示勒索信息：

壁纸替换

Sirattacker 勒索软件攻击者使用的比特币钱包里目前没有余额，2023 年 2 月 24 日还对外进行转账。但该钱包地址曾经持有高达 538.57 比特币，价值超过 1200 万美元。

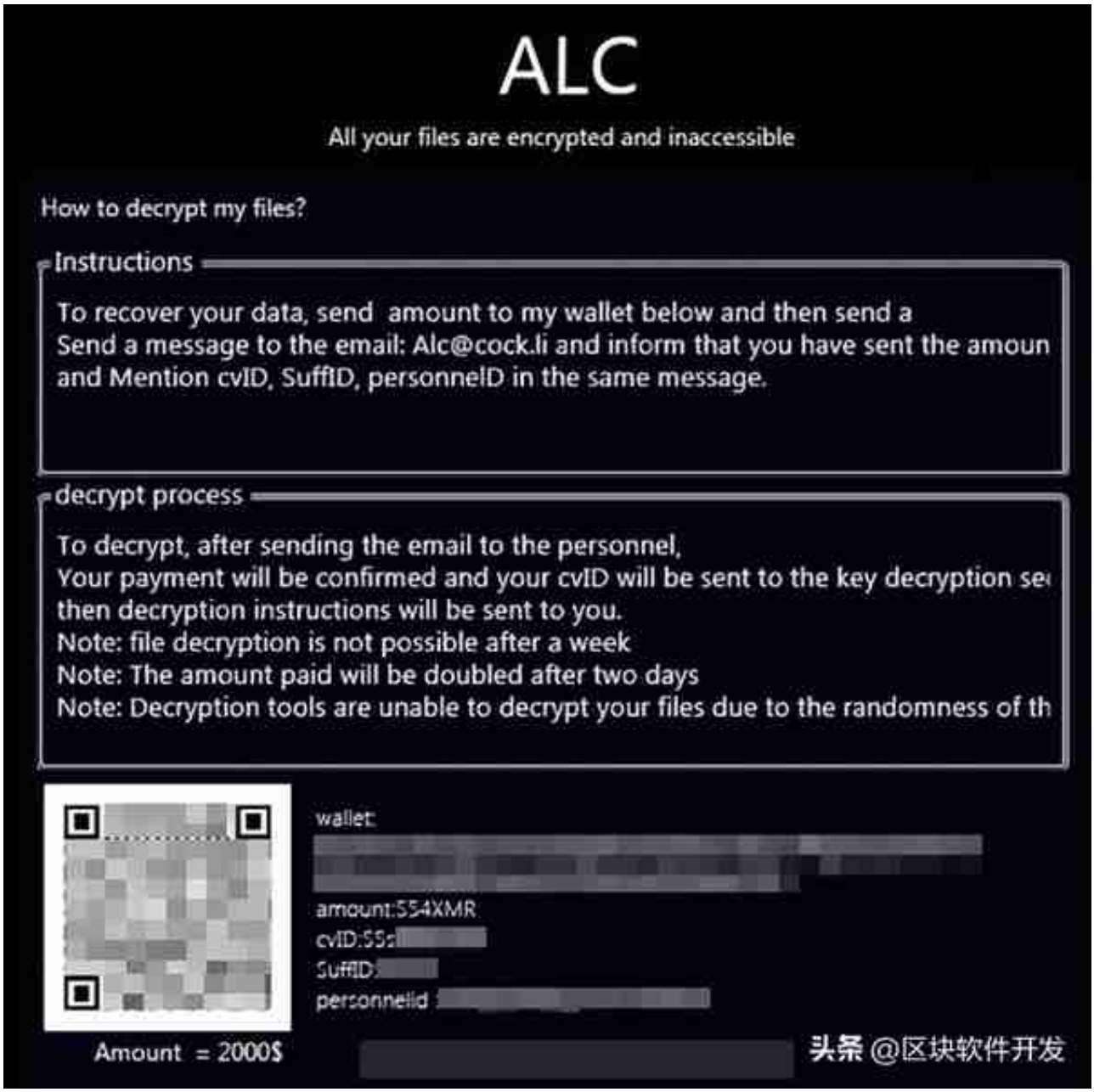

Advanced Details
Hash
Position
Age
Input Value
Fee
Fee/VB
Weight
Coinbase
RBF
Version
Block ID
Time
Inputs
Outputs
Output Value
Fee/B
Size
Weight Unit
Witness
Locktime
BTC Price
Overview
JSON
From
To
头条@区块软件开发

转入交易记录



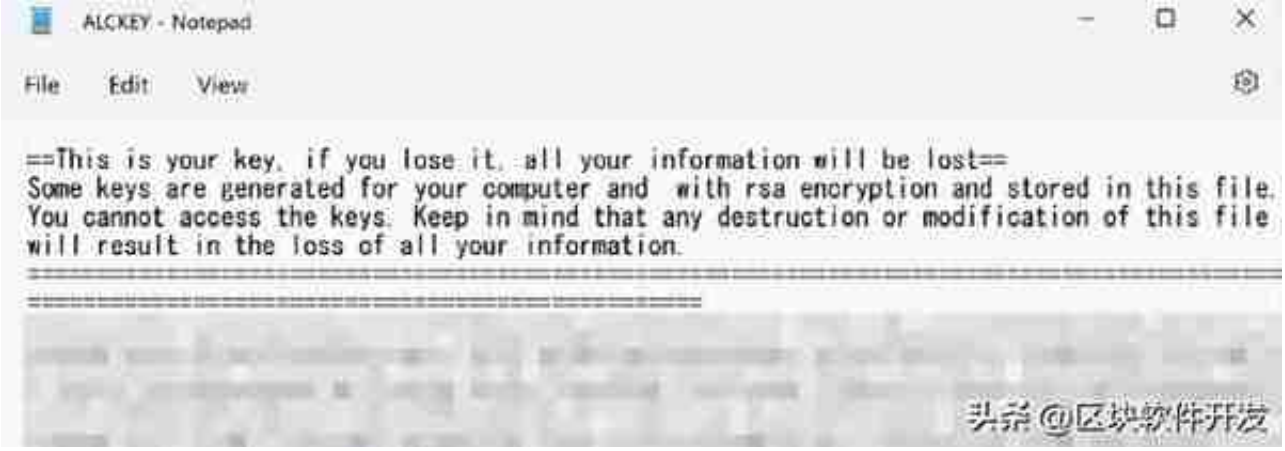
桌面截图

RUS!.txt 是勒索信息，根据拼写猜测作者并不是以英语为母语的人。勒索信息中提到，攻击者主要针对“俄罗斯与其同伙”。攻击者要求受害者通过 Telegram 与攻击者联系，但并没有指出赎金价格。



勒索信息

与文本文件中的勒索信息不同，这次的勒索信息十分详细，提供了联系攻击者的地址、钱包地址、赎金价格与受害者
ID。尽管二维码下方指出赎金两千美元，但实际上攻击者勒索 554
门罗币（价值约为 8 万美元）。



包含 AES 密钥的的 ALCKEY 文件

翻译自：https://www.fortinet.com/blog/threat-research/ransomware-roundup-sirattacker-acl