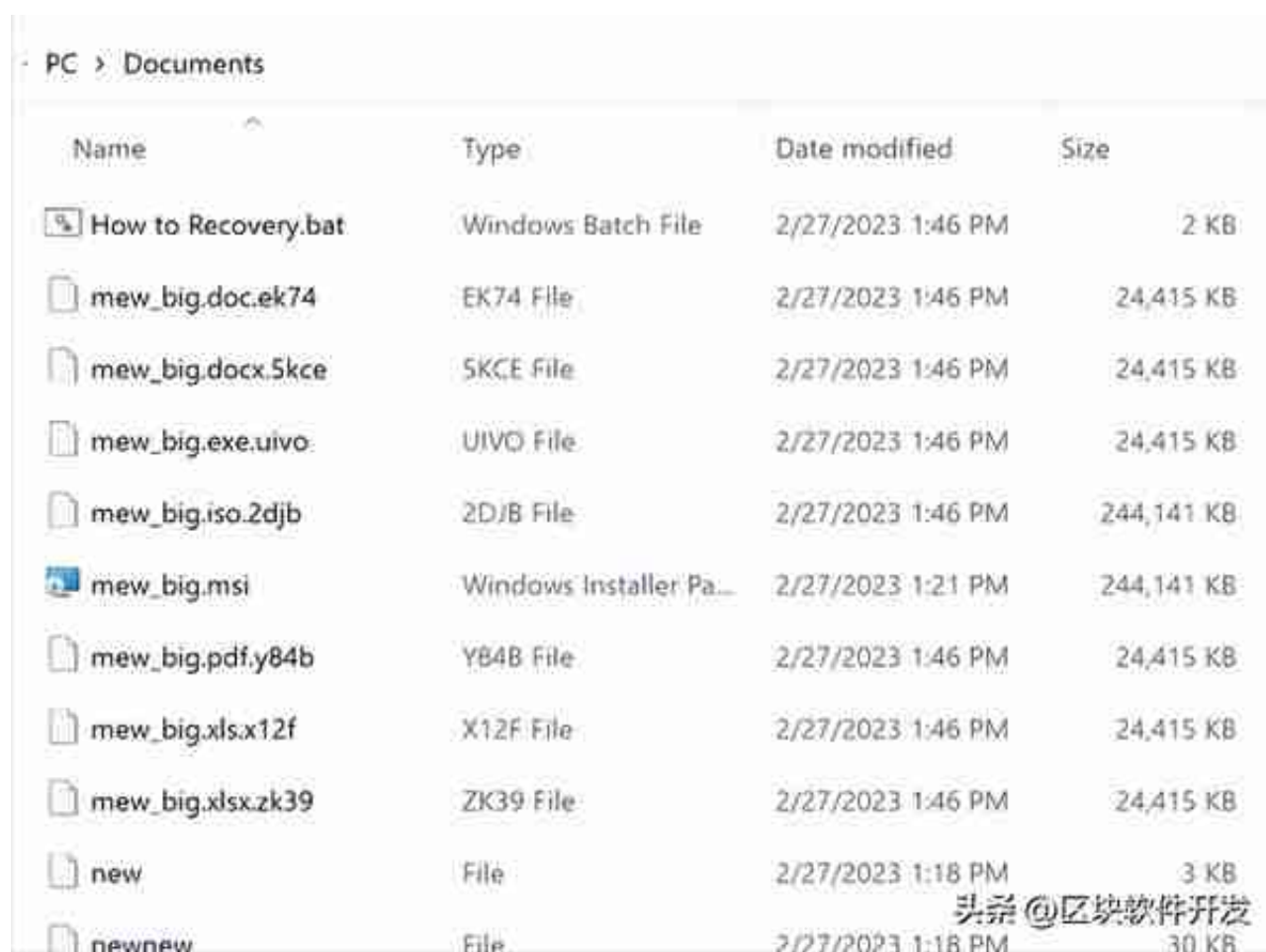


## Sirattacker 勒索软件

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。



Name	Type	Date modified	Size
How to Recovery.bat	Windows Batch File	2/27/2023 1:46 PM	2 KB
mew_big.doc.ek74	EK74 File	2/27/2023 1:46 PM	24,415 KB
mew_big.docx.5kce	5KCE File	2/27/2023 1:46 PM	24,415 KB
mew_big.exe.uivo	UIVO File	2/27/2023 1:46 PM	24,415 KB
mew_big.iso.2djb	2DJB File	2/27/2023 1:46 PM	244,141 KB
mew_big.msi	Windows Installer Pa...	2/27/2023 1:21 PM	244,141 KB
mew_big.pdf.y84b	Y84B File	2/27/2023 1:46 PM	24,415 KB
mew_big.xls.x12f	X12F File	2/27/2023 1:46 PM	24,415 KB
mew_big.xlsx.zk39	ZK39 File	2/27/2023 1:46 PM	24,415 KB
new	File	2/27/2023 1:18 PM	3 KB
newnew	File	2/27/2023 1:18 PM	30 KB

## 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	[Redacted]	Block ID	[Redacted]
Position	1131	Time	24 Feb 2023 08:14:42
Age	4d 5h 27m 36s	Inputs	6
Input Value	5.17452876 BTC \$121,093	Outputs	40
Fee	0.00030384 BTC \$7.11	Output Value	5.17422490 BTC \$121,086
Fee/VB	18.011 sat/vByte	Fee/B	13.983 sat/B
Weight	6,740	Size	2,173 Bytes
Coinbase	No	Weight Unit	4.503 sat/WU
RBF	No	Witness	Yes
Version	1	Locktime	0
		BTC Price	\$23,401.78

Overview JSON

**From**

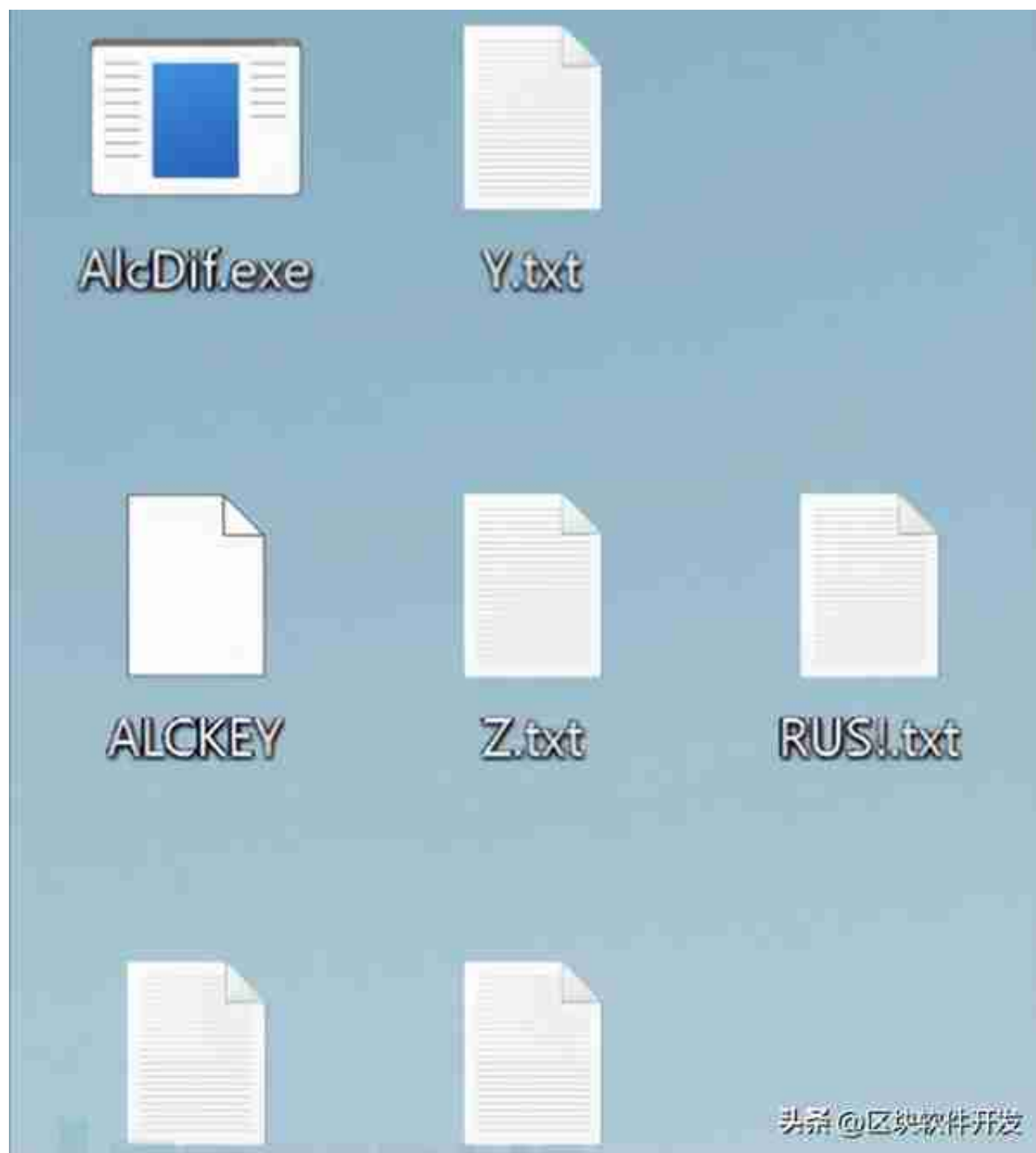
- 1 [Redacted] 5.16762599 BTC - \$120,937
- 2 [Redacted] 0.00138055 BTC - \$32.31
- 3 [Redacted]

**To**

- 1 [Redacted] 0.00837701 BTC - \$194.04
- 2 [Redacted] 0.01522159 BTC - \$356.71
- 12 [Redacted]

来源@区块链软件开发

### 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）。

