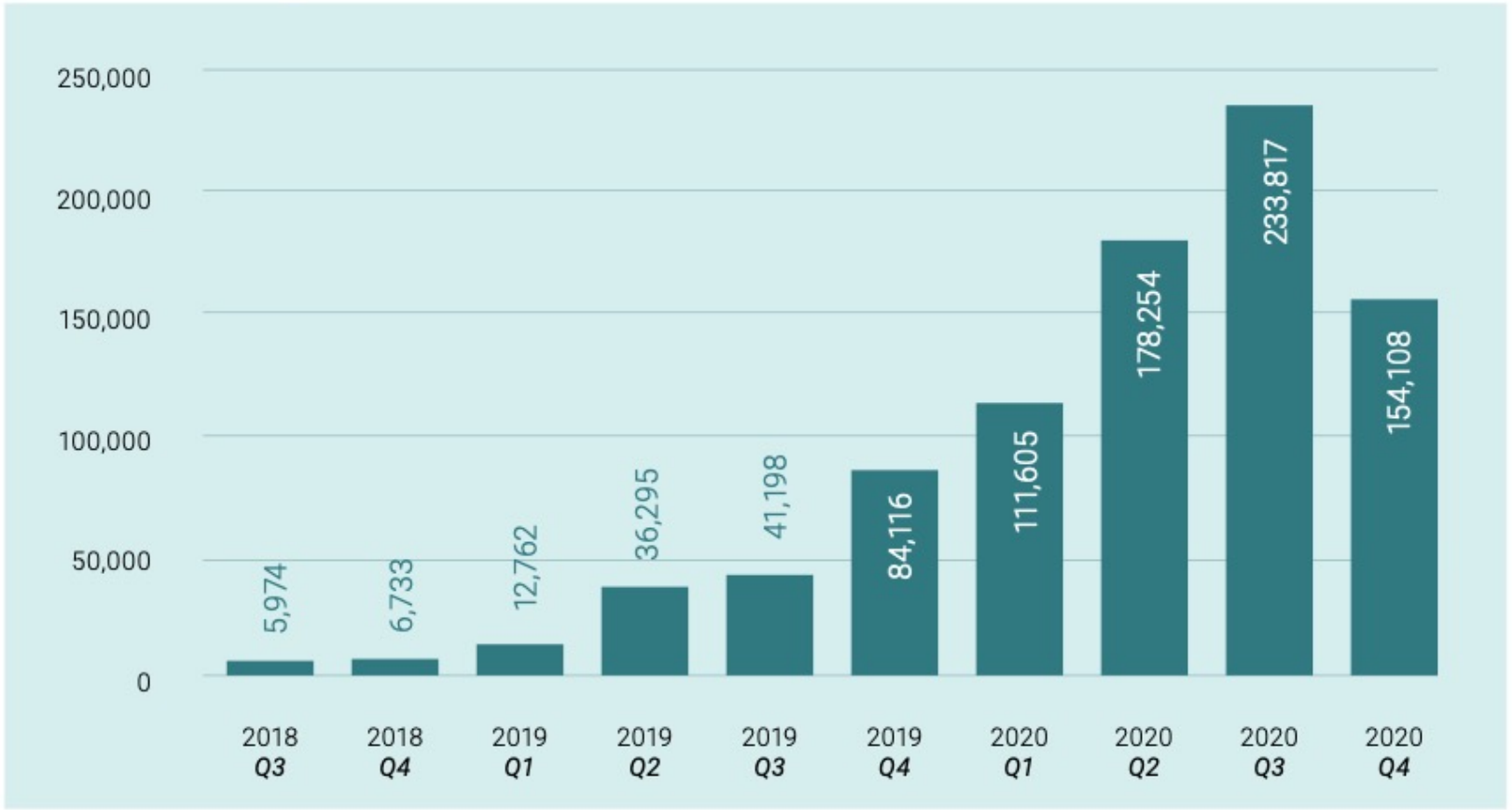
CIPHERTRACE

Ransomware and Actionable Intelligence

Pamela A. Clegg

VP of Financial Investigations - CipherTrace

FIGURE 1 Average ransom in USD



From The Coveware Quarterly Ransomware Report

2021: average payment up 82% at a record $570,000

- Palo Alto Networks' Unit 42

Ransomware Targets:

- ➔ Hospitals
- ➔ Schools
- ➔ Local police
- ➔ Local governments
- ➔ Small businesses
- ➔ Large corporations

In the News: DarkSide

The New York Times

F.B.I. confirms group behind the hack of a top U.S. pipeline.

s in Woodbridge, N.J. Ted Shaffrey/Associated Press

NBC NEWS

Colonial pipeline hack claimed by Russian group Darkside spurs emergency order from…

Nicole Perlroth
@nicoleperlroth

The assumption is that Darkside is not nation state affiliated, but like oh-so-many ransomware groups it uses tools like "GetUserDefaultLangID" to perform language checks. If the victim uses any languages below, DarkSide moves on.

- Russian
- Ukrainian
- Belarusian
- Tajik
- Armenian - Armenia
- Azeri (Latin)
- Georgian
- Kazakh
- Kyrgyz (Cyrillic)
- Turkmen
- Uzbek (Latin)
- Tatar
- Romanian - Moldava
- Russian - Moldava
- Azeri (Cyrillic)
- Uzbek (Cyrillic)
- Arabi - Syria

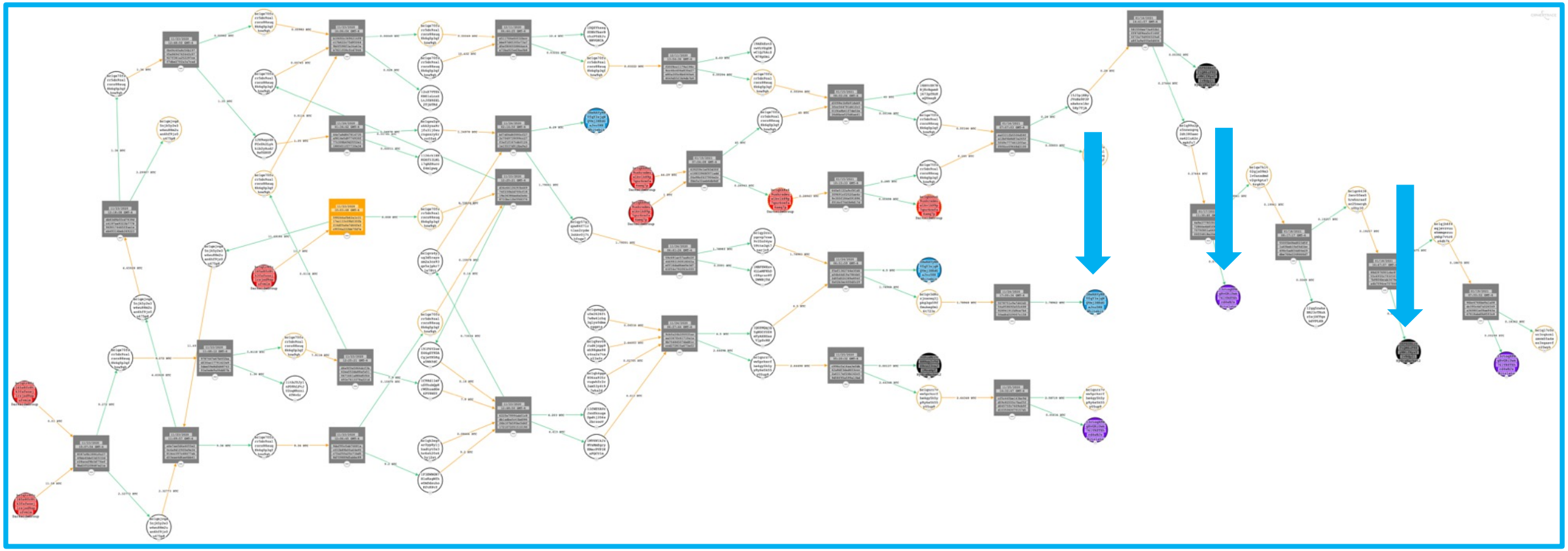
THE WALL STREET JOURNAL.

Colonial Pipeline Seeks to Restore Service After Cyberattack by Weekend

CNBC

Here's the hacking group responsible for the Colonial Pipeline shutdown

DarkSide: Analysis of Previous Funds Movements



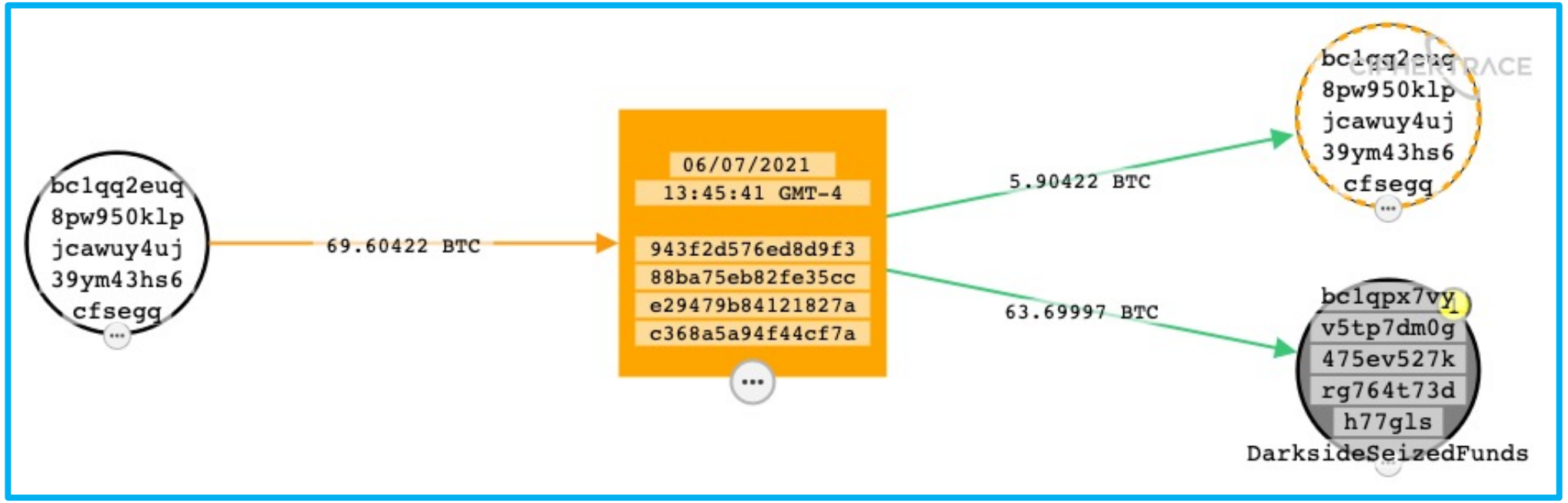
Colonial Pipeline Seizure: 63.69 BTC

INTRODUCTION

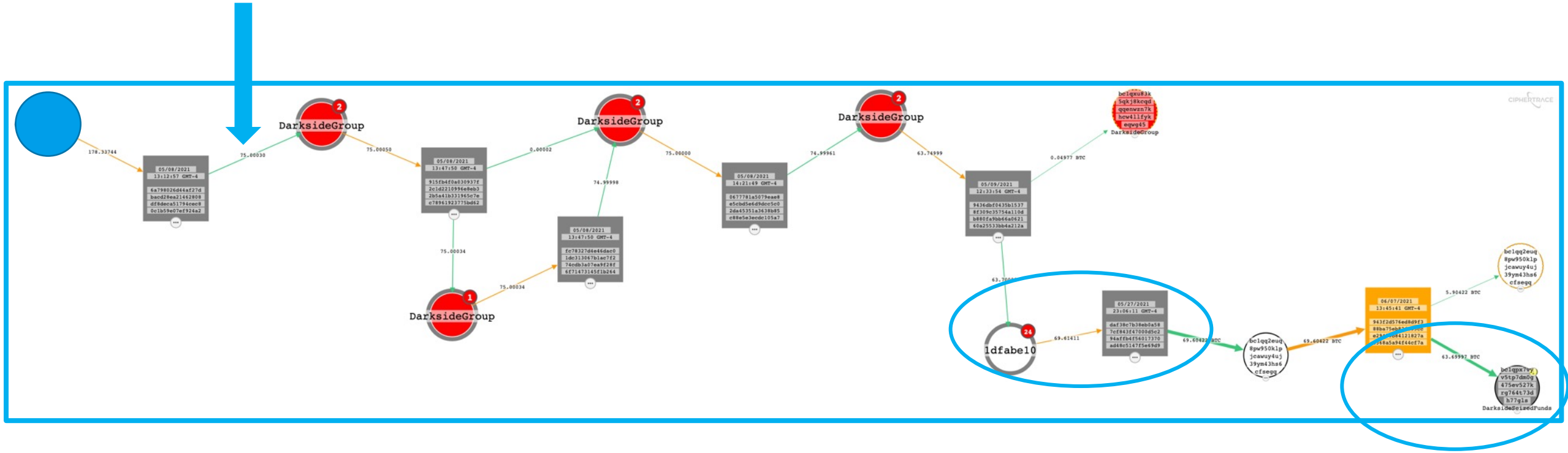
1. This affidavit is in support of a seizure warrant for approximately 63.7 bitcoins (the "Subject Funds") accessible from the following cryptocurrency address (the "Subject Address"): XXXXXXXXXXXXX950klpjcawuy4uj39ym43hs6cfsegq.

https://www.justice.gov/opa/press-release/file/1402056/download

Colonial Pipeline Seizure: 63.69 BTC



Colonial Pipeline Seizure: 63.69 BTC



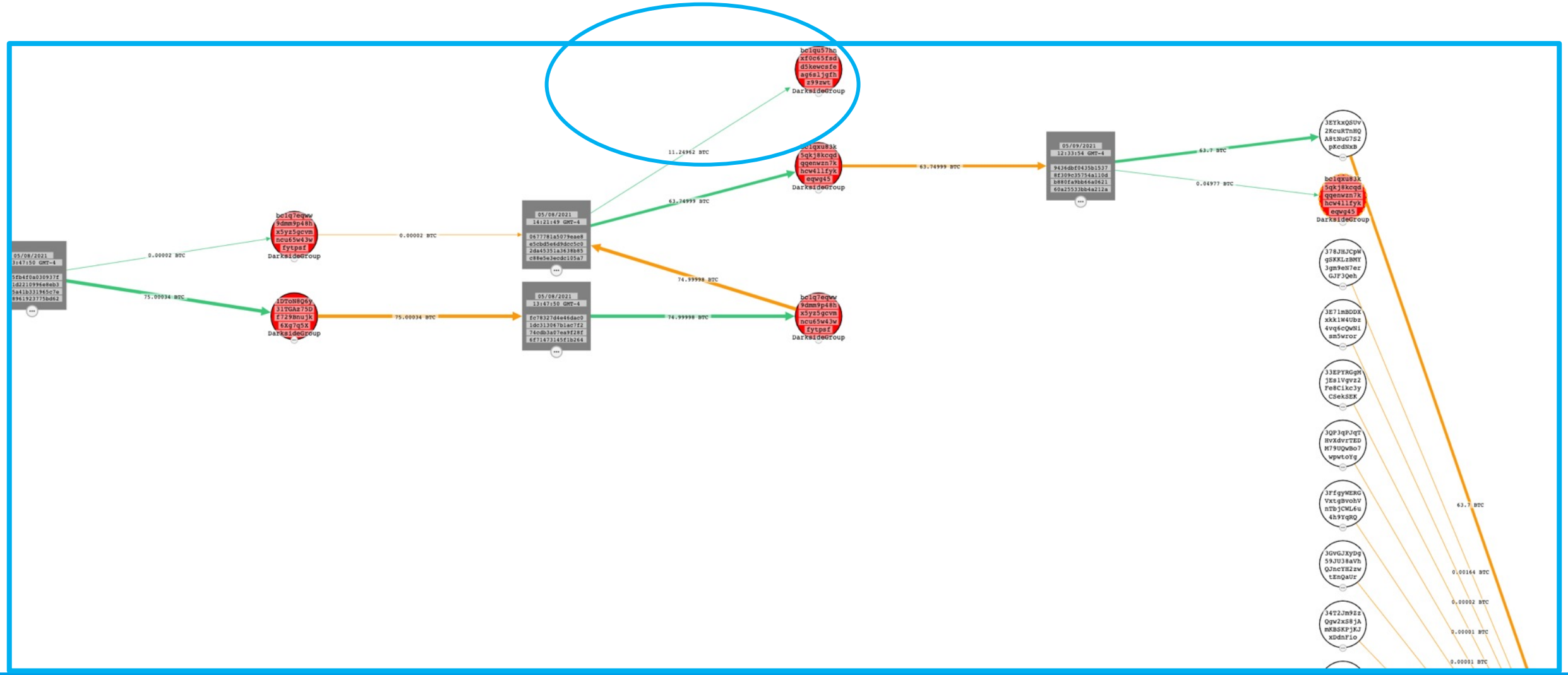
Colonial Pipeline Seizure: 63.69 BTC

33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNxB in one wallet. [redacted] on May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNxB was transferred to address XXXXXXXXXXXX950klpjcawuy4uj39ym43hs6cfsegq (the "Subject Address"), and it has not moved since.

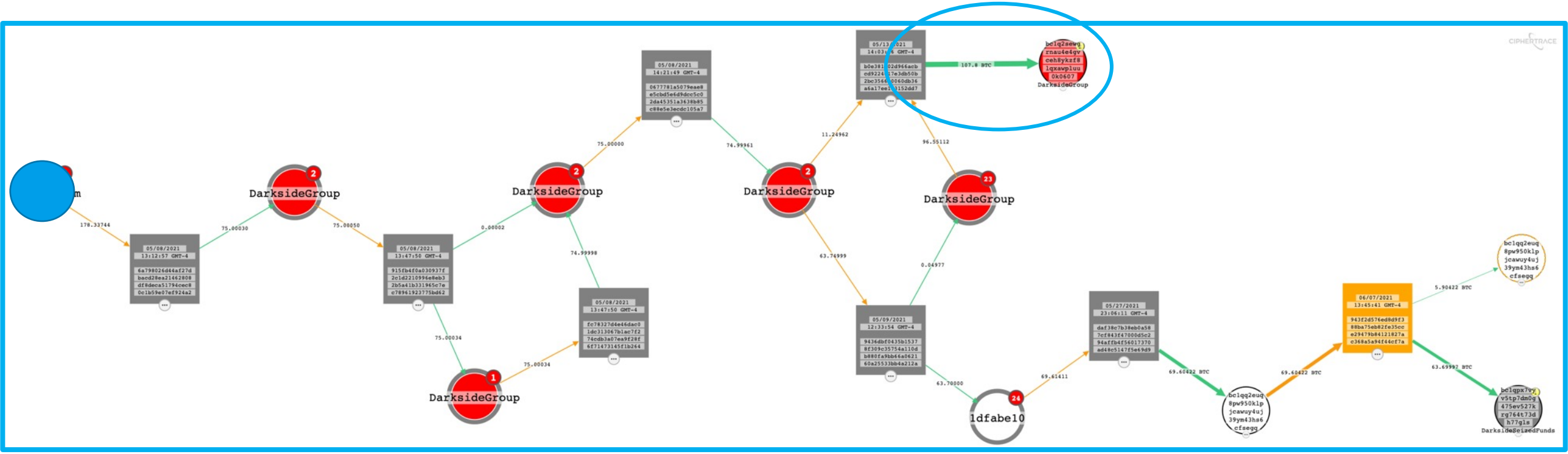
34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.

https://www.justice.gov/opa/press-release/file/1402056/download

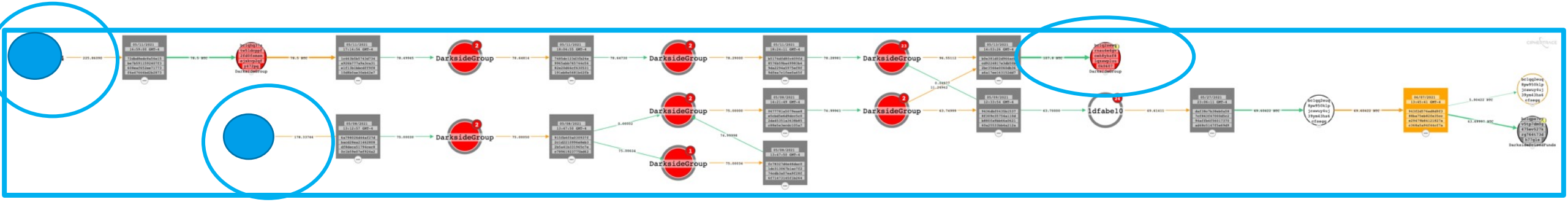
Colonial Pipeline Seizure: 63.69 BTC



Colonial Pipeline Seizure: 63.69 BTC



Colonial Pipeline Seizure: 63.69 BTC



FinCEN, OFAC Warn of Potential Sanctions Violations for Allowing Customers to Pay Ransomware

- If a ransomware victim uses a VASP to send cryptocurrency to a sanctioned actor, that VASP could be in violation of sanctions. Blockchain analysis is vital to determine the entities associated with counterparty addresses.
- Even if a specific crypto address isn't designated, if it is associated with a sanctioned entity, transacting with said address is a potential sanctions violation.

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

OFAC Sanctions SUEX OTC, S.R.O.

Sep 21, 2021 - In response to the growing ransomware threat, OFAC imposed financial sanctions on a cryptocurrency exchange platform, SUEX.

OFAC claimed that SUEX facilitated the laundering of cryptocurrency from eight ransomware strains, and that approximately 40% of its overall trading — more than $370 million — was illicit.

SUEX was incorporated in the Czech Republic and advertised its services to Russian users.

OFAC included a total of 25 bitcoin, ethereum, and tether addresses known to be controlled by SUEX on its sanctions list, which have received more than $930 million in total in various cryptocurrency.

https://home.treasury.gov/news/press-releases/jy0364

OFAC Sanctions SUEX OTC, S.R.O.

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following entity has been added to OFAC's SDN List:

SUEX OTC, S.R.O. (a.k.a. "SUCCESSFUL EXCHANGE"), Presnenskaya Embankment, 12, Federation East Tower, Floor 31, Suite Q, Moscow 123317, Russia; Skorepka 1058/8 Stare Mesto, Prague 110 00, Czech Republic (Latin: Skořepka 1058/8 Staré Město, Praha 110 00, Czech Republic); Website suex.io; Digital Currency Address - XBT 12HQDsicffSBaYdJ6BhnE22sfjTESmmzKx; alt. Digital Currency Address - XBT 1L4ncif9hh9TnUveqWq77HfWWt6CJWtrnb; alt. Digital Currency Address - XBT 1LrxsRd7zNuxPJcL5rttnoeJFy1y4AffYY; alt. Digital Currency Address - XBT 1KUUJPkyDhamZXgpsyXqNGc3x1QPXtdhgz; alt. Digital Currency Address - XBT bc1qdt3gml5z5n50y5hm04u2yjdphefkm0fl2zdj68; alt. Digital Currency Address - XBT 1B64QRxfaa35MVkf7sDjuGUYAP5izQt7Qi; Digital Currency Address - ETH 0x2f389ce8bd8ff92de3402ffce4691d17fc4f6535; alt. Digital Currency Address - ETH 0x19aa5fe80d33a56d56c78e82ea5e50e5d80b4dff; alt. Digital Currency Address - ETH 0xe7aa314c77f4233c18c6cc84384a9247c0cf367b; alt. Digital Currency Address - ETH

https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921

CIPHERTRACE

Questions

pamela@ciphertrace.com

Questions and answers from the conference participants (1)

Q: You mentioned US has introduced legislation/regulation which makes those who pay Ransomware 'accountable' can you advise what this legislation is.
A: It isn't new legislation. It is an advisory from OFAC (of the Department of Treasury) stating that those ransom payments can violate sanctions.

Q: What are the main reason the ransomware victim be sanctioned when they make a payment?
A: They are sending money (the ransom payment) to a criminal organization and if that criminal organization is a sanctioned organization, which for a US company would include hackers based in North Korea or Iran, then that payment is a sanctioned payment.

Q: If the victim is based overseas are they able to be sanctioned by the US?
A: They could possibly be sanctioned even outside the US if they any US connection, like US branch or subsidiary, or if they use any US financial instruments (banks, credit cards, etc).

Q: So criminals invest (time/effort) in specific ways so that they get crypto specific criminal know how? If their method works, then why change it?
A: If we can trace their funds, then their methods do not work well enough.

Questions and answers from the conference participants (2)

Q: You mention UTXOs, could you give a brief overview of what those are?
A: Unspent Transaction Outputs (UTXOs) are the building blocks of transactions (Txns) on some blockchains, with Bitcoin being the most well-known use case. A bitcoin transaction is made up of both inputs and outputs. Inputs can either contain a single address or multiple addresses, from which the UTXOs are being spent. The output address and/or addresses that are receiving the spent funds from the inputs and are now UTXOs themselves— until they are eventually spent.

Q: What happens to the funds seized? Are they returned to the victims?
A: In most cases, there is reparation to the victim if the funds can be directly traced to a specific victim.

Q: Do you know how the private key was obtained?
A: I understand that in this case a server was seized and the private key was on that server

Q: Are any traditional fiat tracing methodologies accepted in the tracing of cryptocurrencies from a law enforcement/legal standpoint? (LIFO, FIFO, LIBR).
A: For an account-based crypto, like ETH, generally LIFO is the methodology used for tracing. There have been a few times where FIFO was used but it was justified by the type of case we were investigating.

Questions and answers from the conference participants (3)

Q: What is the value of bitcoin paid by Colonial Pipeline as r-ware and what is the value of bitcoin when it was recovered by authority? You can pull the historical pricing.
A: The payment on 8 May, 2021 was for 75 BTC and the recovery was 63.69 BTC on 7 June, 2021.