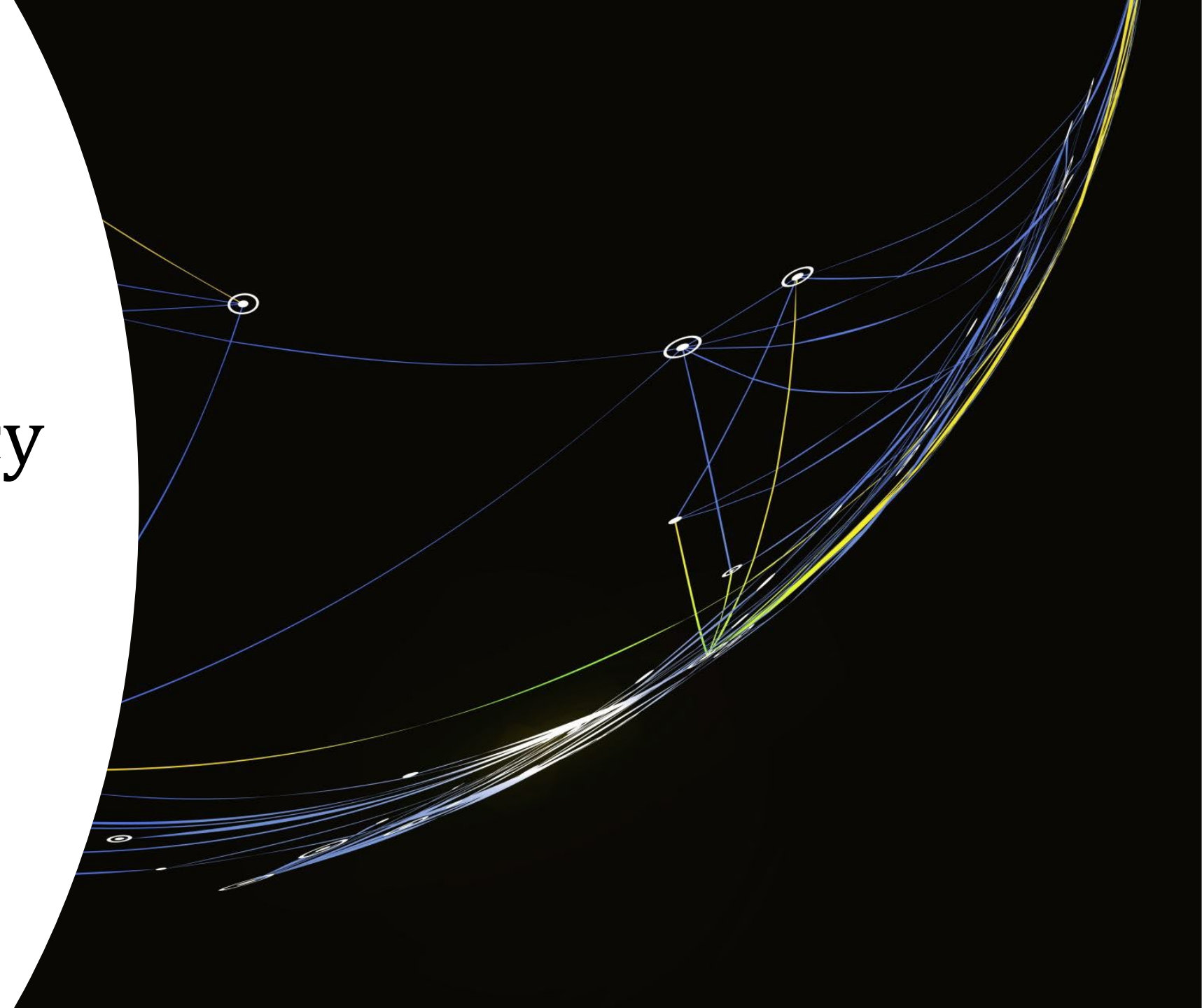
Cryptocurrency Investigation

Bo Ra Jung, BS

Boston University



Review: Understanding Cryptocurrency as a Tool for Cybercrime

Cryptocurrency and Its Attraction to Cybercriminals:

- Pseudonymity and Anonymity
- Borderless Transactions
- Ransomware Payments:

Darknet Marketplaces and Illegal Activities:

- Role of Cryptocurrencies in Darknet Marketplaces
- Money Laundering (Crypto Mixer, Crypto Laundry)

Investigative Techniques

Digital Forensics:

- Specialized tools to analyze blockchain transactions
- Tracing cryptocurrency flow and identifying transaction patterns

Collaboration:

- Cooperation with international agencies and law enforcement
- Partnerships with private sector organizations and cryptocurrency exchanges for information sharing

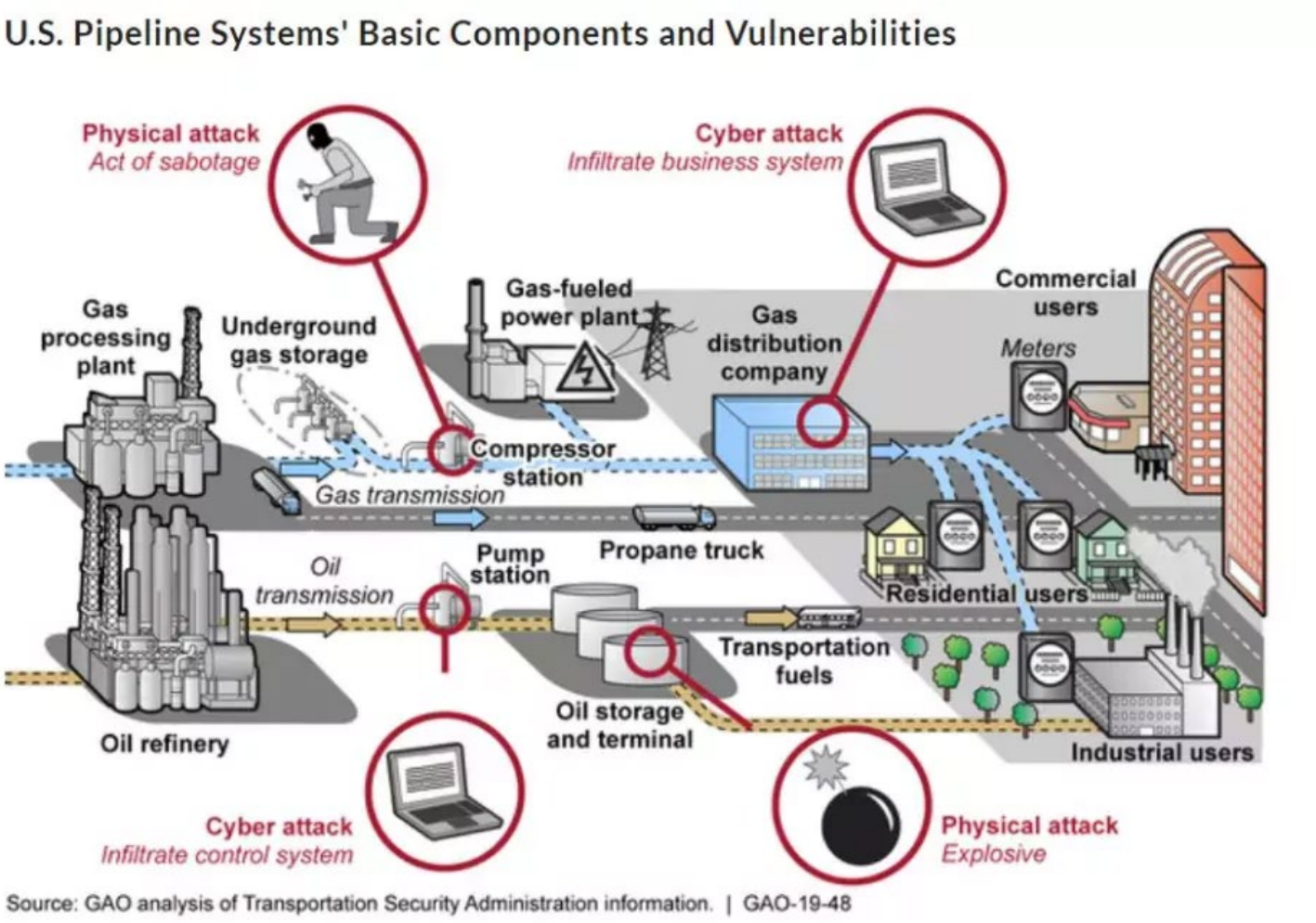
Infiltration:

- Undercover operations to infiltrate darknet marketplaces
- Monitoring illicit activities and gathering crucial evidence

Financial Analysis:

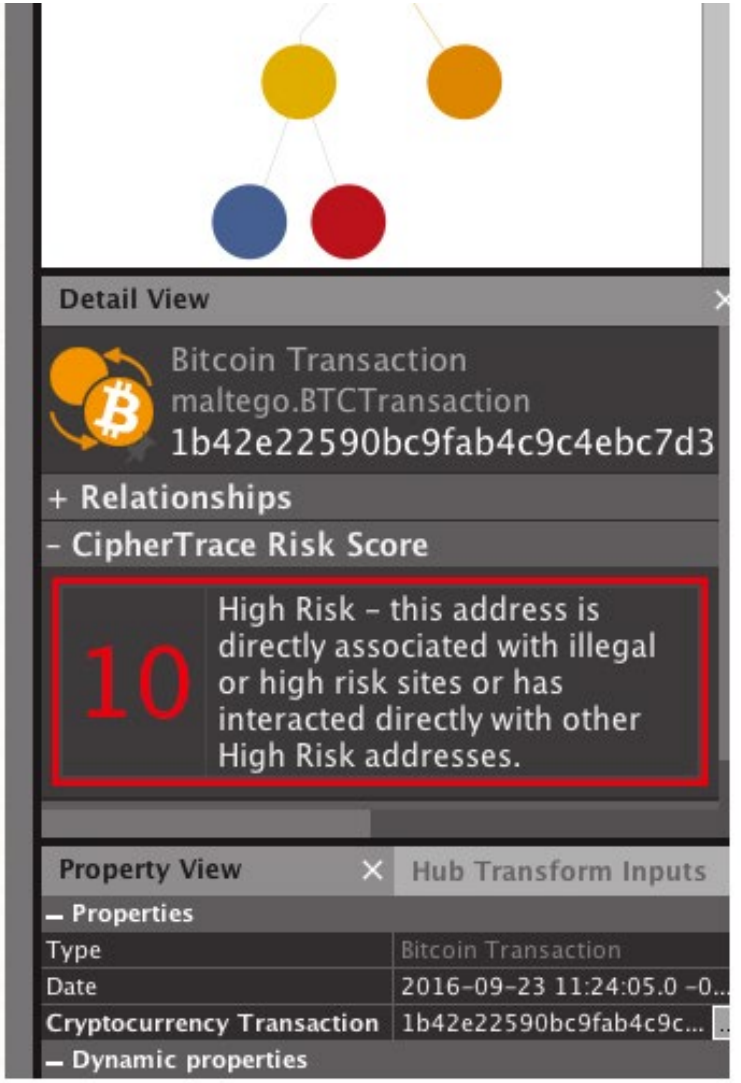
- Tracking cryptocurrency wallets and exchanges
- Following the money trail to identify cybercriminals

Case Study: Colonial Pipeline Ransomware Attack



CRYPTOCURRENCY ANALYSIS

CRYPTOCURRENCY ANALYSIS: ADVANCED



Hands-On Activity

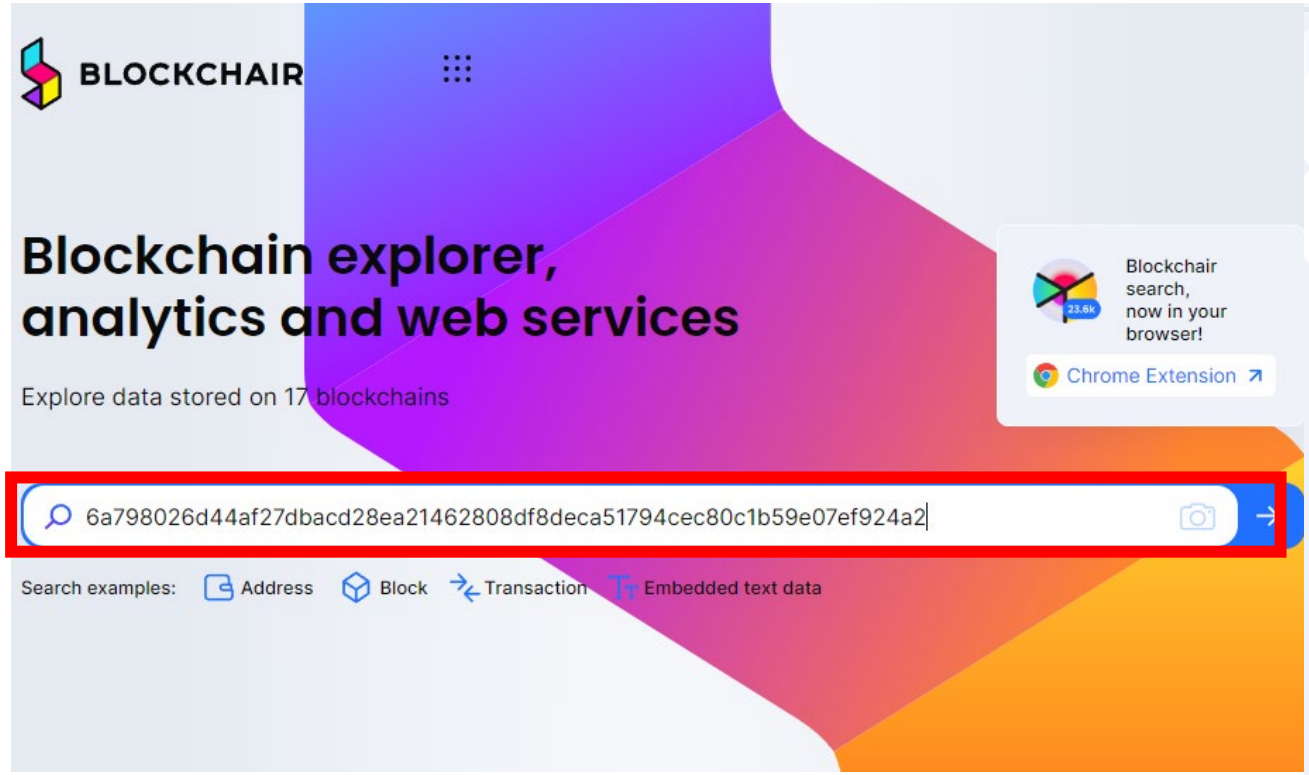
- DarkSide's ransom payment address
- Intermediate addresses where DarkSide transferred the ransom payment
- The DarkSide collection address from which the FBI seized the partial ransom payment

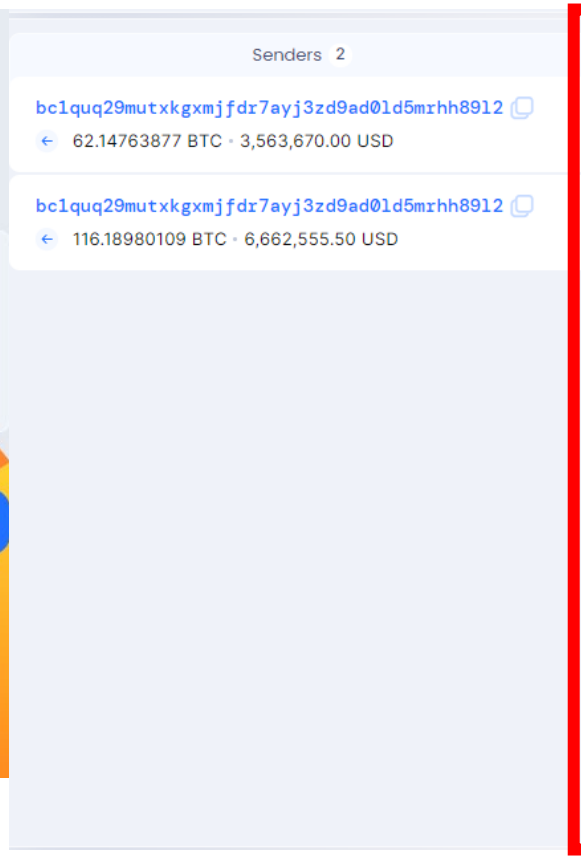
FBI’s Seizure Warrant

- **On 7 May, 2021, Colonial Pipeline**, a US oil pipeline system, that mainly carries gasoline and jet fuel to the southeastern United States **suffered a ransomware cyberattack** that impacted the computerized equipment that managed the pipeline. The company learned of the attack shortly before 5 a.m. when an employee discovered a ransom note on a system in the IT network. The company believes that the attack was orchestrated by DarkSide, a cybercriminal group believed to operate, at least in part, out of Russia. **Colonial Pipeline made the payment on 8 May 2021.**
- On 13 May, the general public learned that Colonial Pipeline paid approximately 75 Bitcoins, or around US$5M, in ransom. Criminal organizations such as DarkSide prefer the use of Bitcoin as ransom payment because it provides a degree of anonymity, allows for the transfer from one person to another without the use of a bank, and lastly, can be converted back into fiat via multiple methods, some of which do not require the use of a legal name or address.
- **On 7 June, the US Federal Bureau of Investigation (FBI) announced that it recovered nearly $2.3M of the stolen funds using money flow analysis and other investigative techniques**. Coinciding with the China crackdown on Bitcoin mining, the news of the FBI’s “hack” of Bitcoin sent the broader market for cryptocurrencies tumbling. While the FBI did not provide specific details of the recovery process in order to safeguard their methods for future investigations, the seizure warrant filed with the US District Court, Northern District of California, did provide some insights.

Transaction Hash	Description
6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2	Ransom payment (Item #1)
915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62	Intermediate #1
fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264	Intermediate #2
0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7	Intermediate #3
9436dbf0435b15378f309c35754a110db880fa9bb66a062160a25533bb4a212a	Intermediate #4
daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9	Sent to Subject Address (Item #3)
943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a	Sent to FBI ‘s Holding Address (Item #4)

- Go to https://blockchair.com/
- In the search engine, type 6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2





Transaction history

Show inputs and outputs

Sent	75.0005 BTC	May 8, 2021, 5:47 PM UTC
	Confirmed	

Transaction hash: 915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62

Senders: 2 Recipients: 2

Received	75.0003 BTC	May 8, 2021, 5:12 PM UTC
	Confirmed	

Transaction hash: 6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2

Senders: 2 Recipients: 8

Received	0.0002 BTC	May 8, 2021, 4:35 PM UTC
	Confirmed	

Transaction hash: 61689f0cc5960fea23e707e73cb6c8be033a11f851911a4455a390064c7b0915

Senders: 2 Recipients: 3

Senders 2	Recipients 2
15JFh88FcE4WL6qeMLgX5VEAFCbRXjc9fr ← 0.00020000 BTC · 11.47 USD	bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf 0.00001693 BTC · 0.97 USD →
15JFh88FcE4WL6qeMLgX5VEAFCbRXjc9fr ← 75.00030000 BTC · 4,300,667.00 USD	1DToN8Q6y31TGAz75Df729Bnujk6Xg7q5X Change 75.00034246 BTC · 4,300,669.50 USD →

Privacy

45 Low ?

Issues: 2

⚠ Matched addresses identified

Privacy-o-meter shows the level of traceability of a transaction via various tracking tools

Transaction history

Show inputs and outputs

Sent	75.00034246 BTC	
	Confirmed	May 8, 2021, 5:47 PM UTC

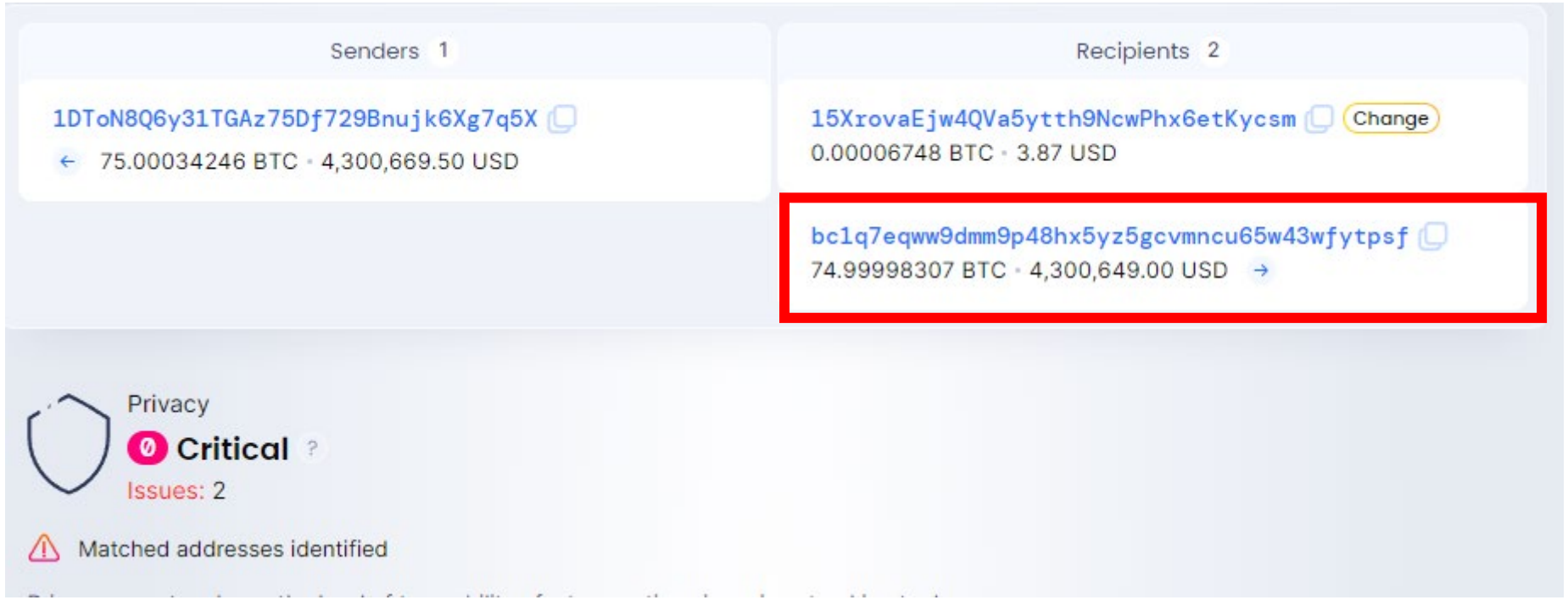
Transaction hash: fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264

Senders: 1 Recipients: 2

Received	75.00034246 BTC	
	Confirmed	May 8, 2021, 5:47 PM UTC

Transaction hash: 915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62

Senders: 2 Recipients: 2


Senders 1
1DToN8Q6y31TGAz75Df729Bnujk6Xg7q5X
75.00034246 BTC · 4,300,669.50 USD
Recipients 2
15XrovaEjw4QVa5ytth9NcwPhx6etKycsm
Change
0.00006748 BTC · 3.87 USD
bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf
74.99998307 BTC · 4,300,649.00 USD
Privacy
0 Critical
Issues: 2
Matched addresses identified

Transaction history

Show inputs and outputs

Sent — 75 BTC — Confirmed — May 8, 2021, 6:21 PM UTC

Transaction hash: 0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7

Senders: 2 Recipients: 2

Received — 74.99998307 BTC — Confirmed — May 8, 2021, 5:47 PM UTC

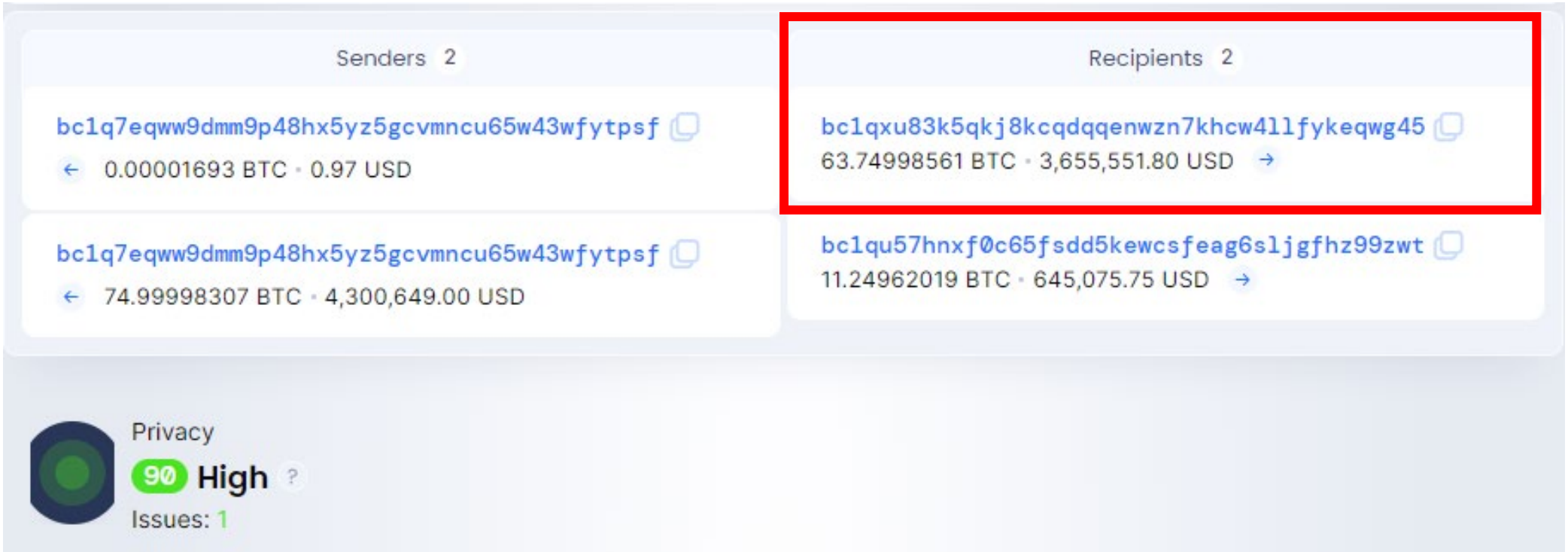
Transaction hash: fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264

Senders: 1 Recipients: 2

Received — 0.00001693 BTC — Confirmed — May 8, 2021, 5:47 PM UTC

Transaction hash: 915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62

Senders: 2 Recipients: 2


Senders 2
bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf
0.00001693 BTC · 0.97 USD
bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf
74.99998307 BTC · 4,300,649.00 USD
Recipients 2
bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45
63.74998561 BTC · 3,655,551.80 USD
bc1qu57hnxf0c65fsdd5kewcsfeag6sljgfhz99zwt
11.24962019 BTC · 645,075.75 USD
Privacy
90 High
Issues: 1

Sent

66.59626631 BTC

Confirmed

May 13, 2021, 6:03 PM UTC

Transaction hash: b0e381d02d966acbcd9224817e3db50b2bc3566e0060db36a6a17ee163152dd7

Senders: 24 Recipients: 1

Received

66.5465 BTC

Confirmed

May 11, 2021, 10:24 PM UTC

Transaction hash: b5174dfd8fc409fd8576b59ba49983b49da2294a5975ef8f9dfea7c1fee0a65f

Senders: 1 Recipients: 2

Sent

63.7002193 BTC

Confirmed

May 9, 2021, 4:33 PM UTC

Transaction hash: 9436dbf0435b15378f309c35754a110db880fa9bb66a062160a25533bb4a212a

Senders: 1 Recipients: 2

Received

63.74998561 BTC

Confirmed

May 8, 2021, 6:21 PM UTC

Transaction hash: 0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7

Senders: 2 Recipients: 2

Transaction status

Confirmed · 116,707 confirmations ? SegWit

Block id 682,787

▸ Additional info

.PDF Transaction receipt

Senders 1	Recipients 2
bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45	3EYkxQSUv2KcuRTnHQA8tNuG7S2pKcdNxB Multisig 2/3
← 63.74998561 BTC · 3,655,551.80 USD	63.70000000 BTC · 3,748,745.00 USD →
	bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45 Change
	0.04976631 BTC · 2,928.75 USD →

Transaction history

Show inputs and outputs

Sent

63.7 BTC

Confirmed

May 28, 2021, 3:06 AM UTC

Transaction hash: daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9

Senders: 24 Recipients: 1

Received

63.7 BTC

Confirmed

May 9, 2021, 4:33 PM UTC

Transaction hash: 9436dbf0435b15378f309c35754a110db880fa9bb66a062160a25533bb4a212a

Senders: 1 Recipients: 2

Senders 24	Recipients 1
378JHJCpWgSKKLzBMY3gm9eN7erGJF3Qeh Multisig 2/3 0.00164331 BTC · 92.86 USD	bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq 69.60422177 BTC · 2,679,136.00 USD
3E71mBDDXxkk1W4Ubz4vq6cQwNism5wror Multisig 2/3 0.00002104 BTC · 0.14 USD	
33EPYRGgMjEs1Vgvz2Fe8Cikc3yCSekSEK Multisig 2/3 0.00000547 BTC · 0.33 USD	
3QP3qPJqTHvXdvrTEDM79UQwBo7wpwtoYg Multisig 2/3 0.00000547 BTC · 0.33 USD	
3FfgyWERGVxtgBvohVnTbjCWL6u4h9YqRQ Multisig 2/3 0.00055095 BTC · 26.12 USD	
3GvGJXyDg59JU38aVhQJncYH2zwtEnQaUr Multisig 2/3 0.00001200 BTC · 0.11 USD	
34T2Jm9ZzQgw2xS8jAmKBSKPjKJxDdnFio Multisig 2/3 0.00002138 BTC · 0.22 USD	

Transaction Hash	Description
6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2	Ransom payment (Item #1)
915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62	Intermediate #1
fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264	Intermediate #2
0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7	Intermediate #3
9436dbf0435b15378f309c35754a110db880fa9bb66a062160a25533bb4a212a	Intermediate #4
daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9	Sent to Subject Address (Item #3)
943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a	Sent to FBI ‘s Holding Address (Item #4)

Received

0.00099099 BTC

Confirmed

Apr 18, 2023, 2:56 PM UTC

Transaction hash: 4a064218c7e699e34c2d4cdf29823d7dc85b756aa0792555771be8d9d1266028

Senders: 31 Recipients: 159

Sent

5.90422177 BTC

Confirmed

Jun 7, 2021, 5:53 PM UTC

Transaction hash: 280c5f96397b9502b99703842712b78fda84f1a0faabf826f683448082f46369

Senders: 1 Recipients: 1

Sent

63.7 BTC

Confirmed

Jun 7, 2021, 5:45 PM UTC

Transaction hash: 943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a

Senders: 1 Recipients: 2

Received

69.60422177 BTC

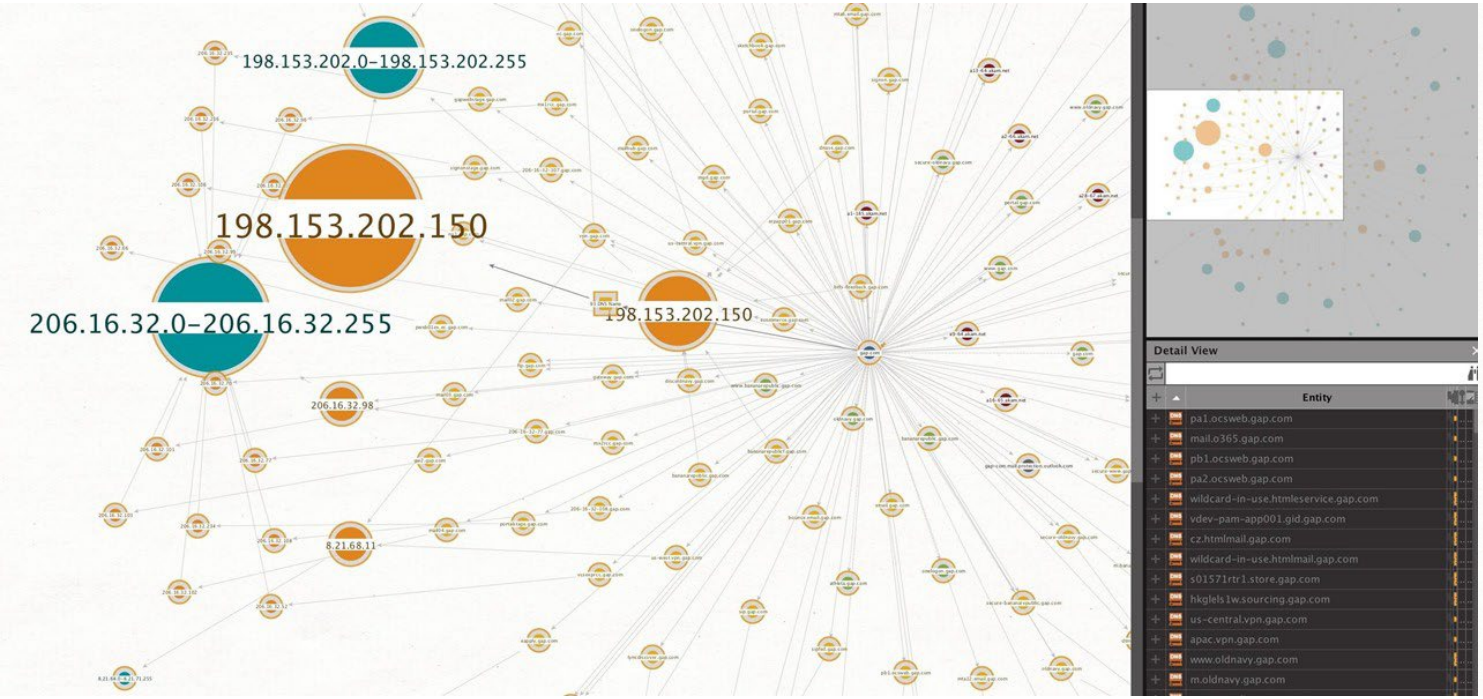
Confirmed

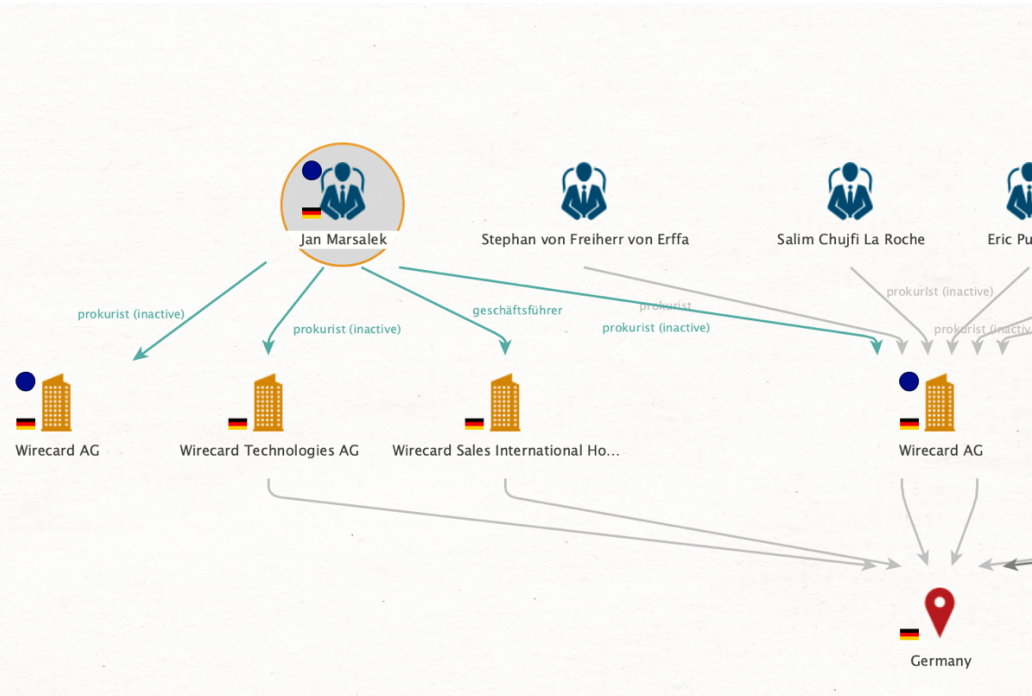
May 28, 2021, 3:06 AM UTC

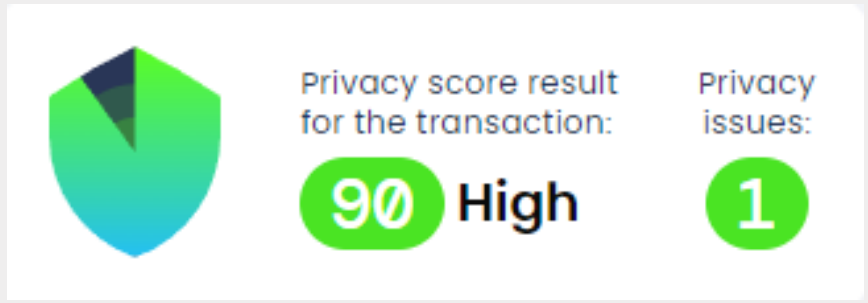
Transaction hash: daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9

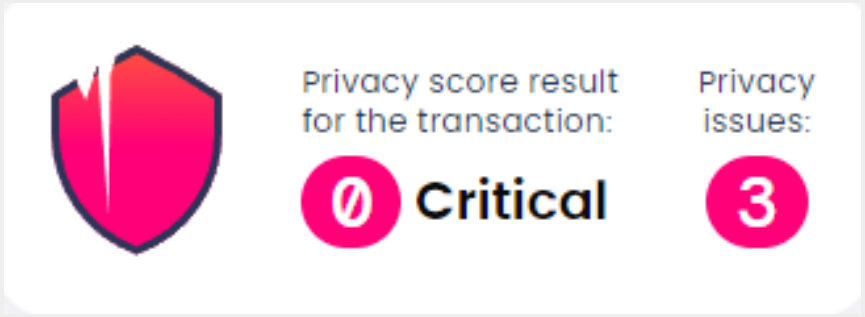
Senders: 24 Recipients: 1

Senders 1	Recipients 2
bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq ← 69.60422177 BTC · 2,679,136.00 USD	bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq Change 5.90422177 BTC · 211,453.80 USD →
	bc1qpx7vyv5tp7dm0g475ev527krg764t73dh77gls 63.69996546 BTC · 2,281,350.50 USD →


198.153.202.0–198.153.202.255
198.153.202.150
206.16.32.0–206.16.32.255
198.153.202.150
206.16.32.98
8.21.68.11
Detail View
Entity
pa1.ocsweb.gap.com
mail.o365.gap.com
pb1.ocsweb.gap.com
pa2.ocsweb.gap.com
wildcard-in-use.htmlservice.gap.com
vdev-pam-app001.gid.gap.com
cz.htmlmail.gap.com
wildcard-in-use.htmlmail.gap.com
s01571rtr1.store.gap.com
hkglels1w.sourcing.gap.com
us-central.vpn.gap.com
apac.vpn.gap.com
www.oldnavy.gap.com
m.oldnavy.gap.com


Jan Marsalek
Stephan von Freiherr von Erffa
Salim Chujfi La Roche
prokurist (inactive)
prokurist (inactive)
geschäftsführer
prokurist (inactive)
prokurist (inactive)
Wirecard AG
Wirecard Technologies AG
Wirecard Sales International Ho...
Wirecard AG
Germany


Privacy score result
for the transaction:
90 High
Privacy
issues:
1


Privacy score result
for the transaction:
0 Critical
Privacy
issues:
3