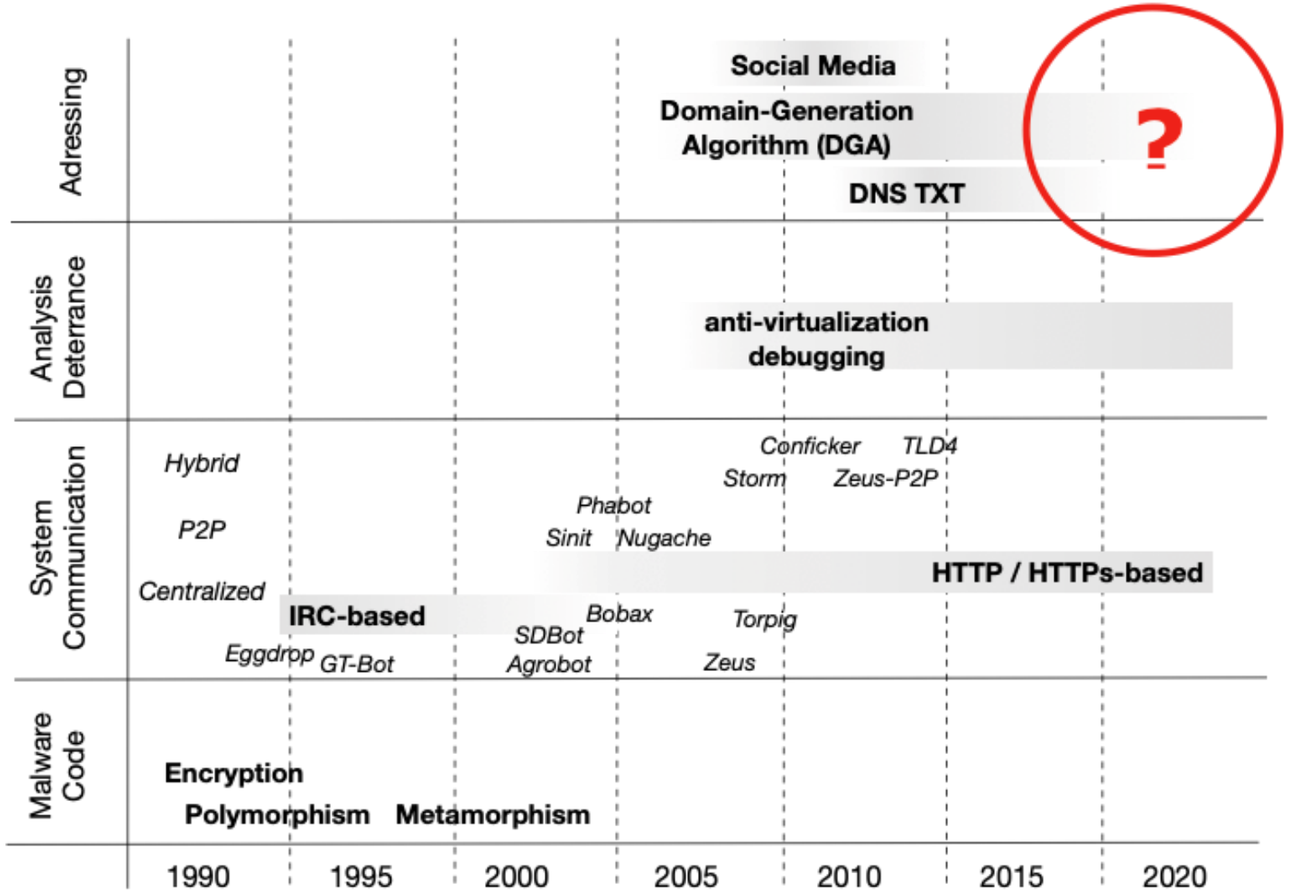
black hat ASIA 2021
May 6-7, 2021
BRIEFINGS

# How Did the Adversaries Abusing Bitcoin Blockchain Evade Our Takeover

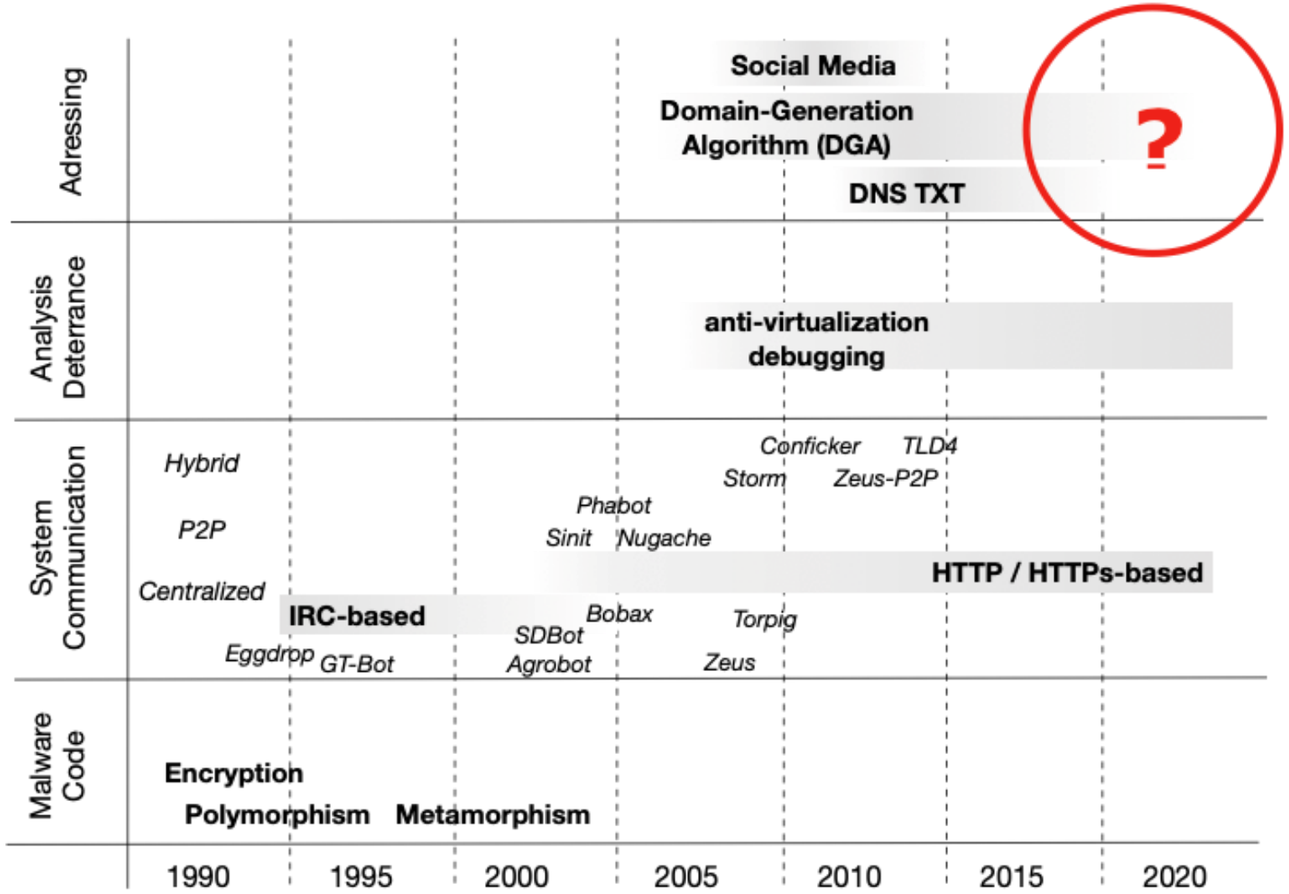
Tsuyoshi Taniguchi

Christian Doerr

# A Game Of Cat And Mouse: Malware Evolves When Detection Is Good Enough



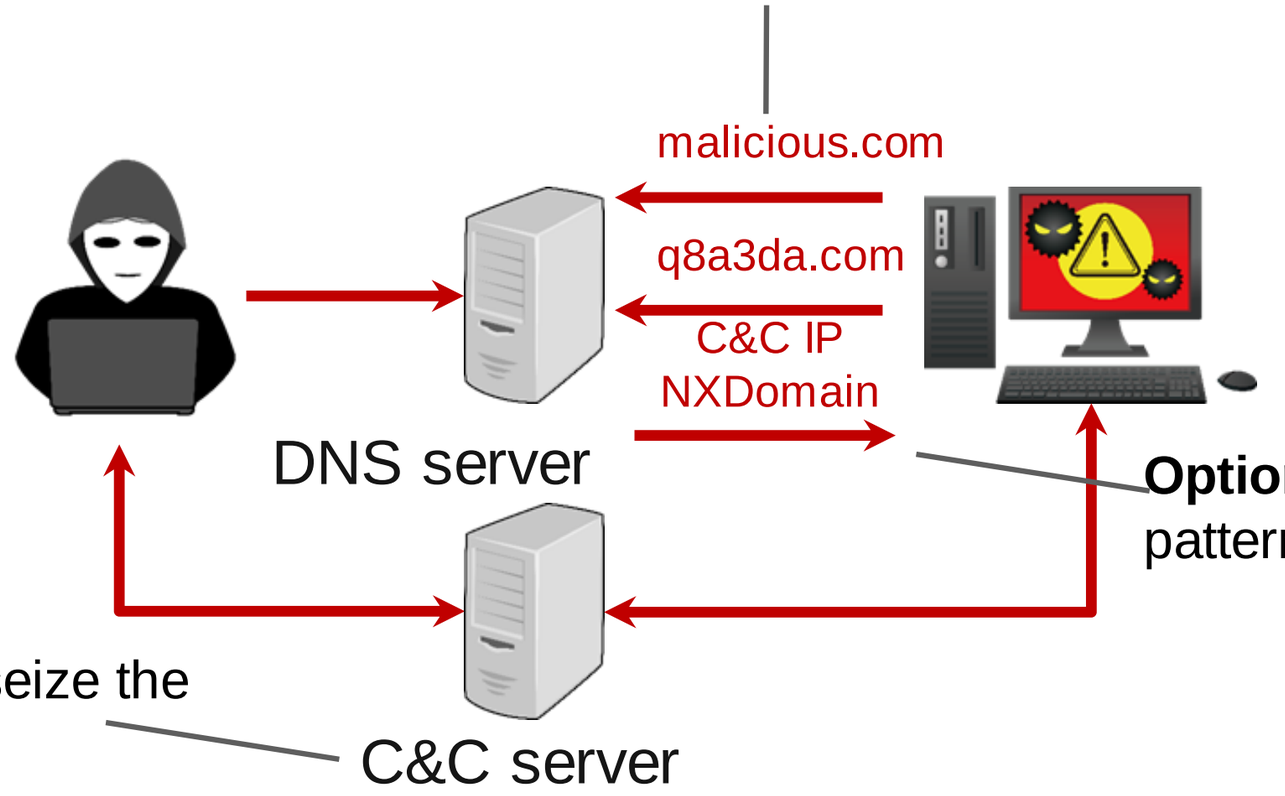
# A Game Of Cat And Mouse: Malware Evolves When Detection Is Good Enough




More on Cerber: Pletinckx, Trap and Doerr, Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware, IEEE Conference on Communications and Network Security 2018, https://www.cyber-threat-intelligence.com/publications/CNS2018-Cerber.pdf

# Three Main Angles for Today's Mitigation

**Option 1:** Predict the domain names and stop them




**Option 2:** Detect lookup patterns, especially NXDomains

**Option 3:** Locate and seize the physical infrastructure

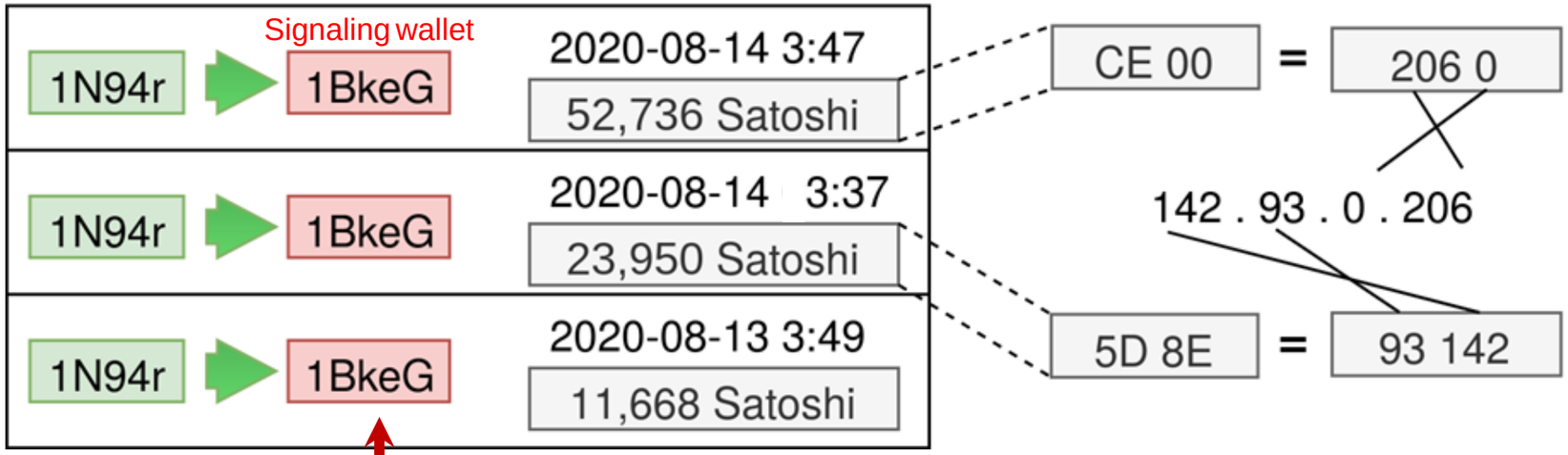
# Who Are We

Tsuyoshi Taniguchi, Ph.D.
Researcher
Fujitsu System Integration Laboratories

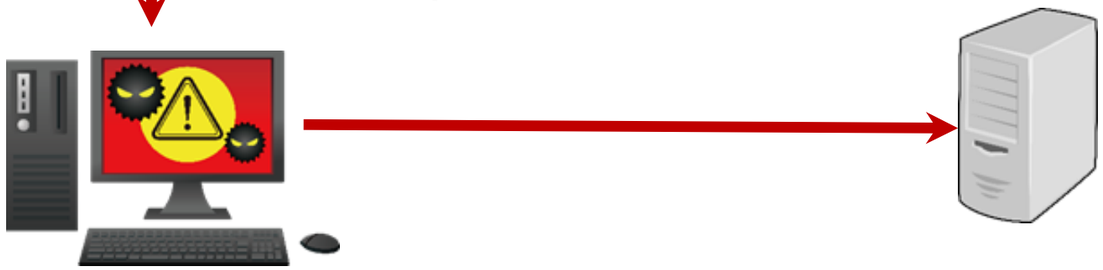
Harm Griffioen
PhD Candidate
Hasso Plattner Institute for Digital Engineering

Christian Doerr, Ph.D.
Professor Cybersecurity + Enterprise Security
Hasso Plattner Institute for Digital Engineering

# Advertising C&C Information via the Blockchain




Fetch the last two payments
from a specific bitcoin wallet



C&C server
142.93.0.206

# Three Main Angles for *Yesterday's* Mitigation

This latest criminal evolution is a significant problem for cyber defense.

X **Option 1:** Predict the domain names and stop them

*There is nothing to predict anymore.*
*Nobody can remove transactions from the blockchain.*


X **Option 2:** Detect lookup patterns, especially NXDomains

*No DNS lookups to unusual sites.*
*Never any NXDomains*

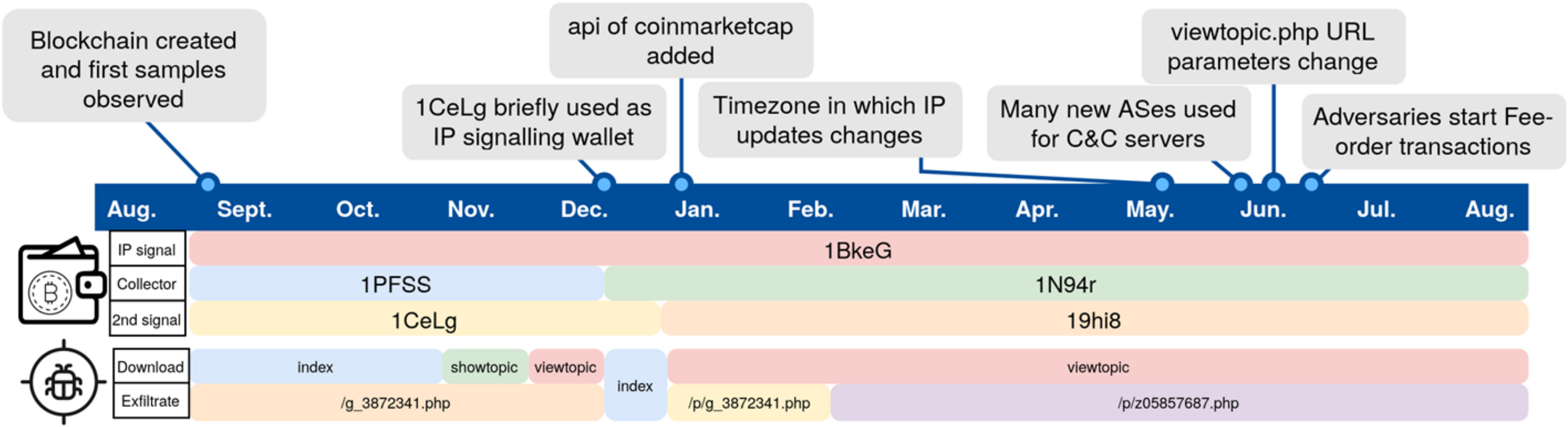
*Some hide behind TOR gateway.*

X **Option 3:** Locate and seize the physical infrastructure

C&C server

# Criminals Continuously Experimented & Improved

During our 12 month observation, the attackers went through many rounds of redesign and continuous improvement. Let's look at two, for a full discussion refer to our report.




Paper reference: Taniguchi, Griffioen and Doerr, Analysis and Takeover of the Bitcoin-Coordinated Pony Malware, AsiaCCS 2021
download: https://www.cyber-threat-intelligence.com/publications/AsiaCCS2021-pony.pdf

# Why? The Blockchain is not Predictable

| | | |
|---|---|---|
| 1N94r → 1BkeG | 2020-08-14 3:47 | 52,736 Satoshi |
| 1N94r → 1BkeG | 2020-08-14 3:37 | 23,950 Satoshi |

Attacker signals new IP
142.93 + 0.206

Previous transaction on the blockchain:
67.205 + 148.45

| | | |
|---|---|---|
| 1N94r → 1BkeG | 2020-08-13 3:49 | 11,668 Satoshi |
| 1N94r → 1BkeG | 2020-08-13 3:42 | 52,547 Satoshi |

Client queries blockchain:
C&C @ 0.206 + 142.93

Incorrect order!

Transaction 2 is confirmed by the network

Transaction 1 is confirmed by the network

time

# Why? The Blockchain is not Predictable

| | | |
|---|---|---|
| 1N94r → 1BkeG | 2020-08-14 3:47 | 52,736 Satoshi |
| 1N94r → 1BkeG | 2020-08-14 3:37 | 23,950 Satoshi |

Attacker signals new IP
142.93 + 0.206

How do you get payments to be confirmed as quickly as possible and in the right order?

Previous transaction on the blockchain:
67.205 + 148.45

| | | |
|---|---|---|
| 1N94r → 1BkeG | 2020-08-13 3:49 | 11,668 Satoshi |
| 1N94r → 1BkeG | 2020-08-13 3:42 | 52,547 Satoshi |

Client queries blockchain:
C&C @ 0.206 + 142.93

Incorrect order!

Transaction 2 is confirmed by the network

Transaction 1 is confirmed by the network

time

# Higher Fees, More Incentive for Miners = Better Control over Your Transactions


Source: bitcoinwiki.org

# Avoiding High Transaction Fees


Bitcoin halving
-> Fees soared

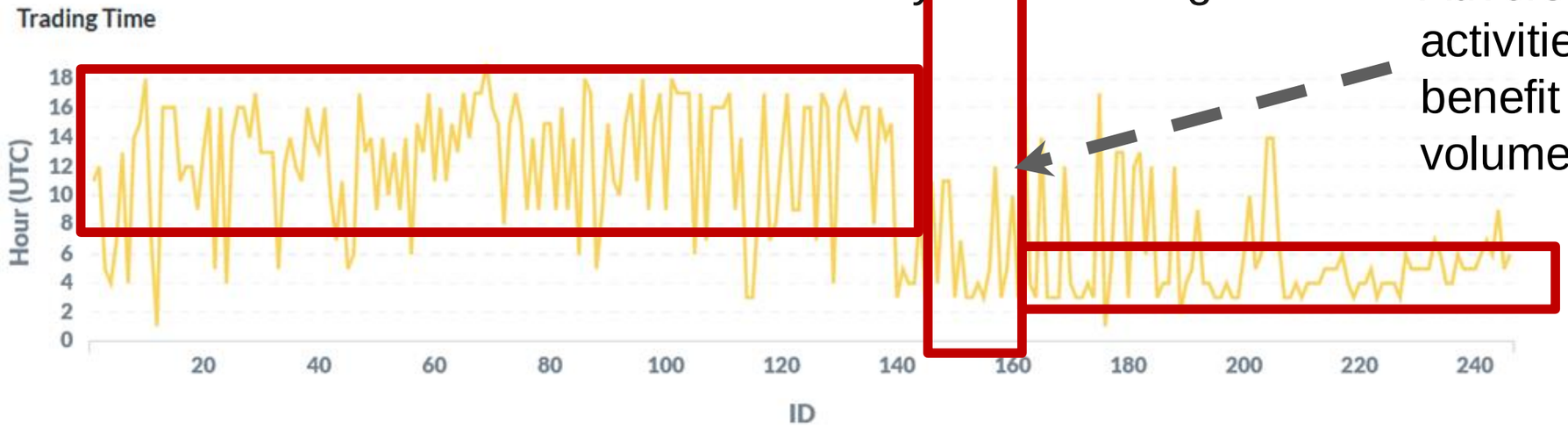
Aug. 2019

Mar. 2020

May 2020

Aug. 2020

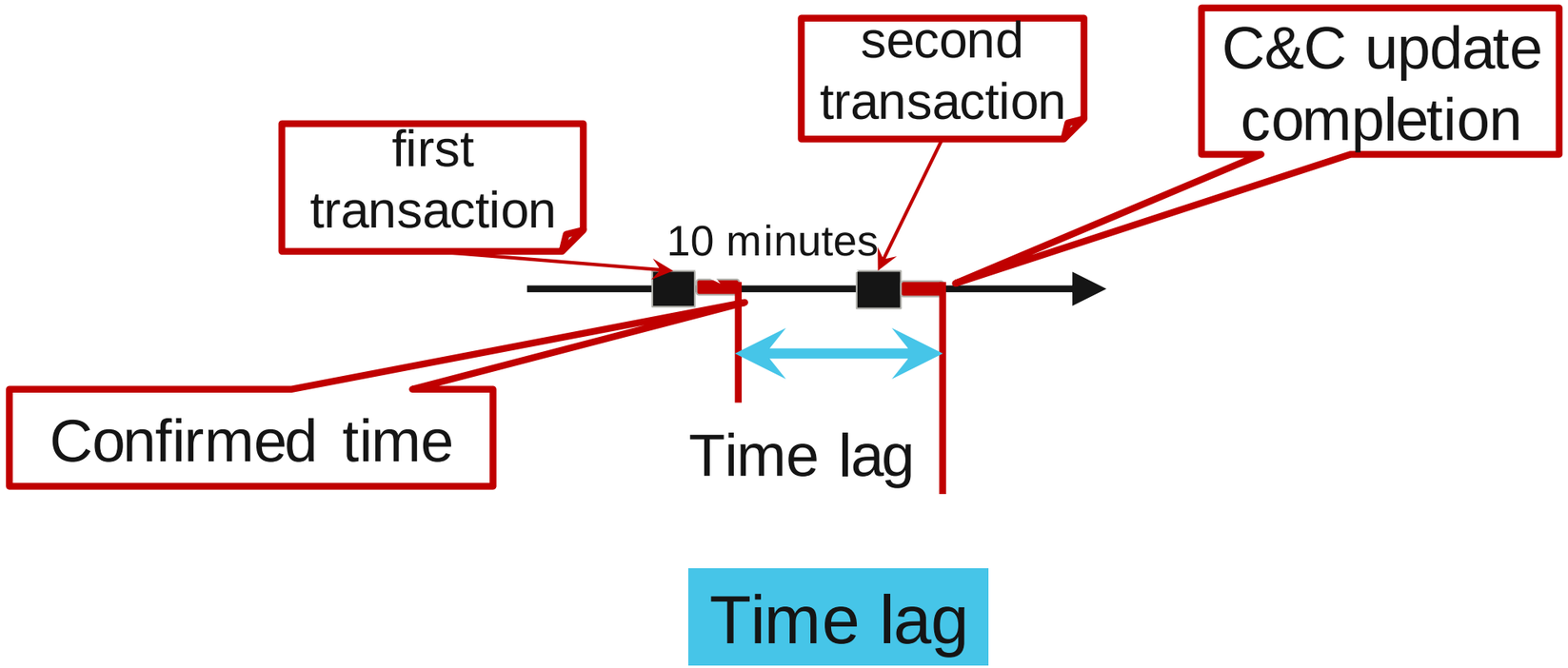
Jan. 2021




Adversaries shifted their activities into the night to benefit from lower transaction volume and cheaper fees

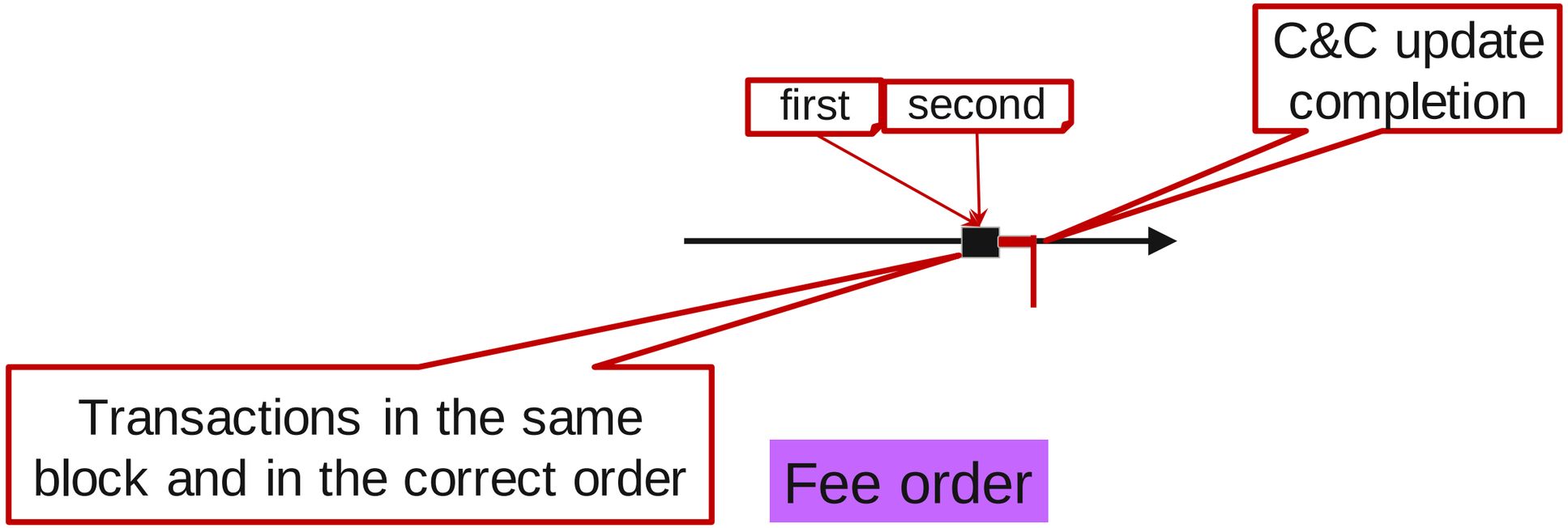
# Experimenting with Transactions

- Time lag: the first and second transactions in **different** blocks
- Fee order: the first and second transactions in **the same** block

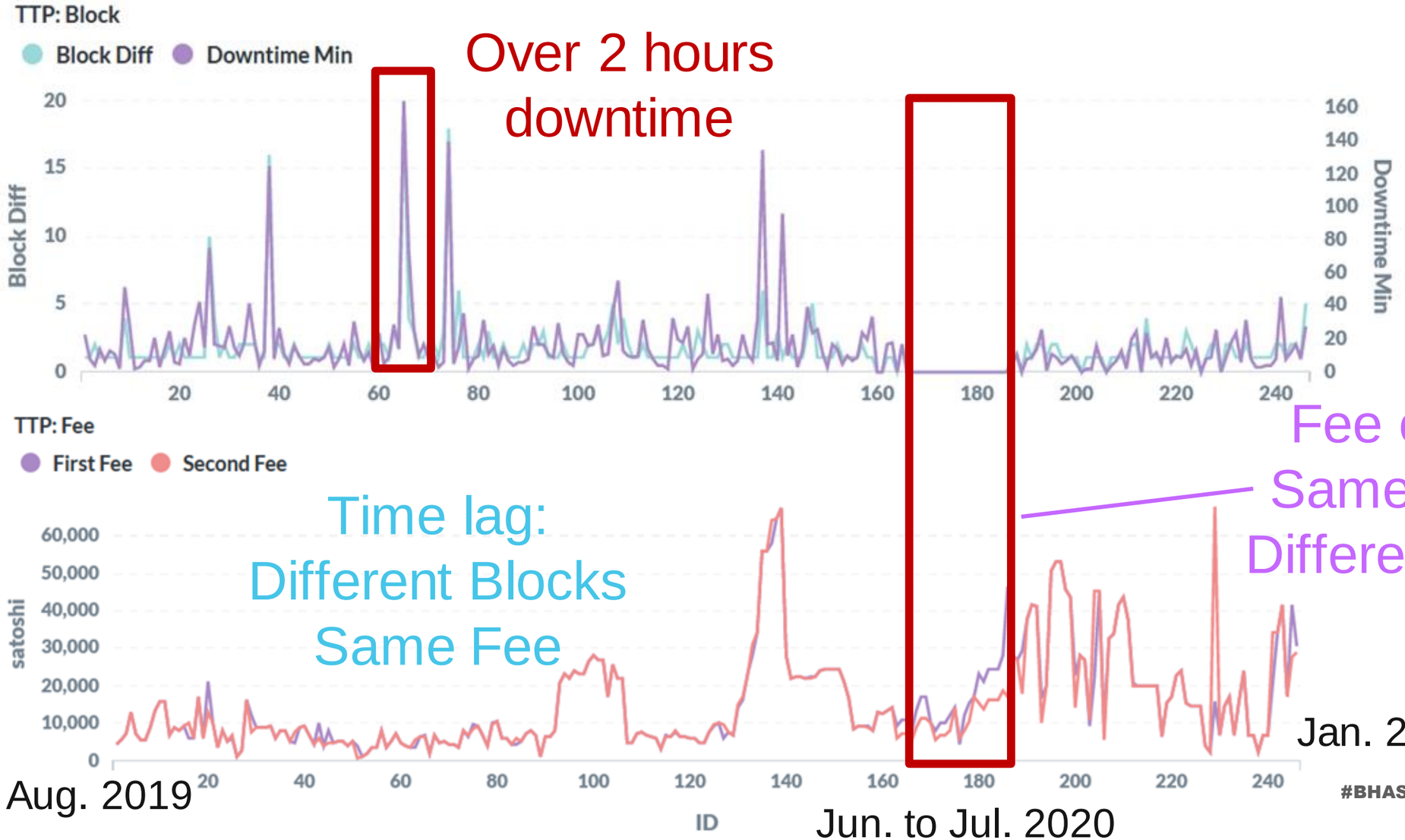


# Experimenting with Transactions

- Time lag: the first and second transactions in **different** blocks
- Fee order: the first and second transactions in **the same** block

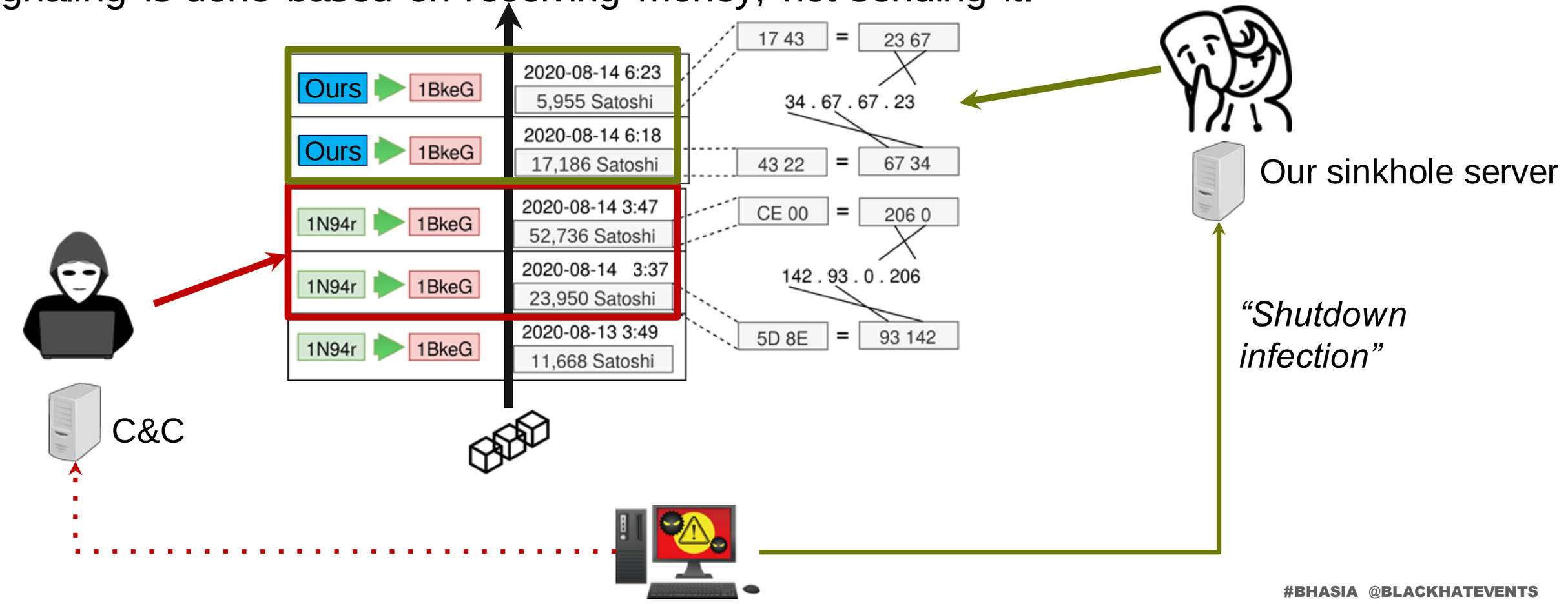


# Experimenting with Transactions



# Malware Takeover by Sending BTC to the Wallet

Although ingenious, the blockchain C&C contained a mistake:
Signaling is done based on receiving money, not sending it.



# Takeover and Adversarial Evasion

| | | |
|---|---|---|
| Aug. 14 | 3:37, 3:47: | 142.93.0[.]206 |
| Aug. 14 | 6:18, 6:23: | 34.67.67.23 |
| Aug. 16 | 10:12, 10:12: | 142.93.0[.]206 |
| Aug. 17 | 5:46, 5:48: | 142.93.0[.]206 |
| Aug. 17 | 6:45, 6:47: | 34.67.67.23 |
| Aug. 17 | 13:54, 14:10: | 142.93.0[.]206 |
| Aug. 17 | 14:20, 14:26: | 142.93.0[.]206 |
| Aug. 19 | 7:02, 7:02: | 34.67.67.23 |

**Takeover 1:**
Downtime 2 days

**Takeover 2:**
Adversaries noticed and reset C&C

**Takeover 3:**
Adversaries stopped their malicious activity

# Takeover and Adversarial Evasion

| | | |
|---|---|---|
| Aug. 14 | 3:37, 3:47: | 142.93.0[.]206 |
| Aug. 14 | 6:18, 6:23: | 34.67.67.23 |
| Aug. 16 | 10:12, 10:12: | 142.93.0[.]206 |
| Aug. 17 | 5:46, 5:48: | 142.93.0[.]206 |
| Aug. 17 | 6:45, 6:47: | 34.67.67.23 |
| Aug. 17 | 13:54, 14:10: | 142.93.0[.]206 |
| Aug. 17 | 14:20, 14:26: | 142.93.0[.]206 |
| Aug. 19 | 7:02, 7:02: | 34.67.67.23 |

**Takeover 1:**
Downtime 2 days

**Takeover 2:**
Adversaries noticed and reset C&C

**Takeover 3:**
Adversaries stopped their malicious activity

But this was only a suspension...

| | | |
|---|---|---|
| Sep. 1 | 3:41, 3:47: | 45.61.138[.]66 |

Adversaries redesigned their C&C mechanism so that it could no longer be taken over

# Takeover and Adversarial Evasion

| | | |
|---|---|---|
| Aug. 14 | 3:37, 3:47: | 142.93.0[.]206 |
| Aug. 14 | 6:18, 6:23: | 34.67.67.23 |
| Aug. 16 | 10:12, 10:12: | 142.93.0[.]206 |
| Aug. 17 | 5:46, 5:48: | 142.93.0[.]206 |
| Aug. 17 | 6:45, 6:47: | 34.67.67.23 |
| Aug. 17 | 13:54, 14:10: | 142.93.0[.]206 |
| Aug. 17 | 14:20, 14:26: | 142.93.0[.]206 |
| Aug. 19 | 7:02, 7:02: | 34.67.67.23 |

But this was only a suspension...

| | | |
|---|---|---|
| Sep. 1 | 3:41, 3:47: | 45.61.138[.]66 |

**Takeover 1:**
Downtime 2 days

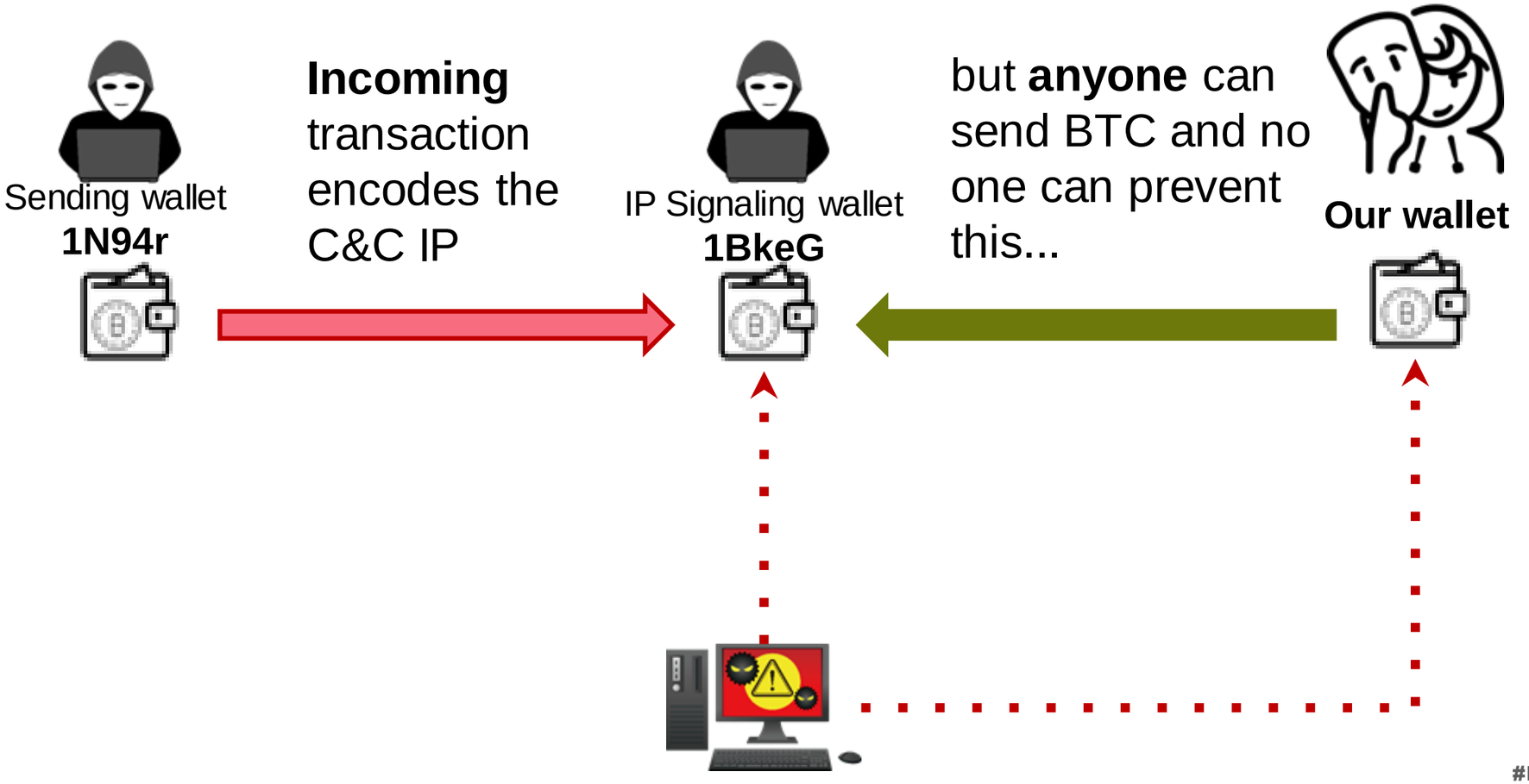
**Takeover 2:**
Adversaries noticed and reset C&C

**Takeover 3:**
Adversaries stopped their malicious activity

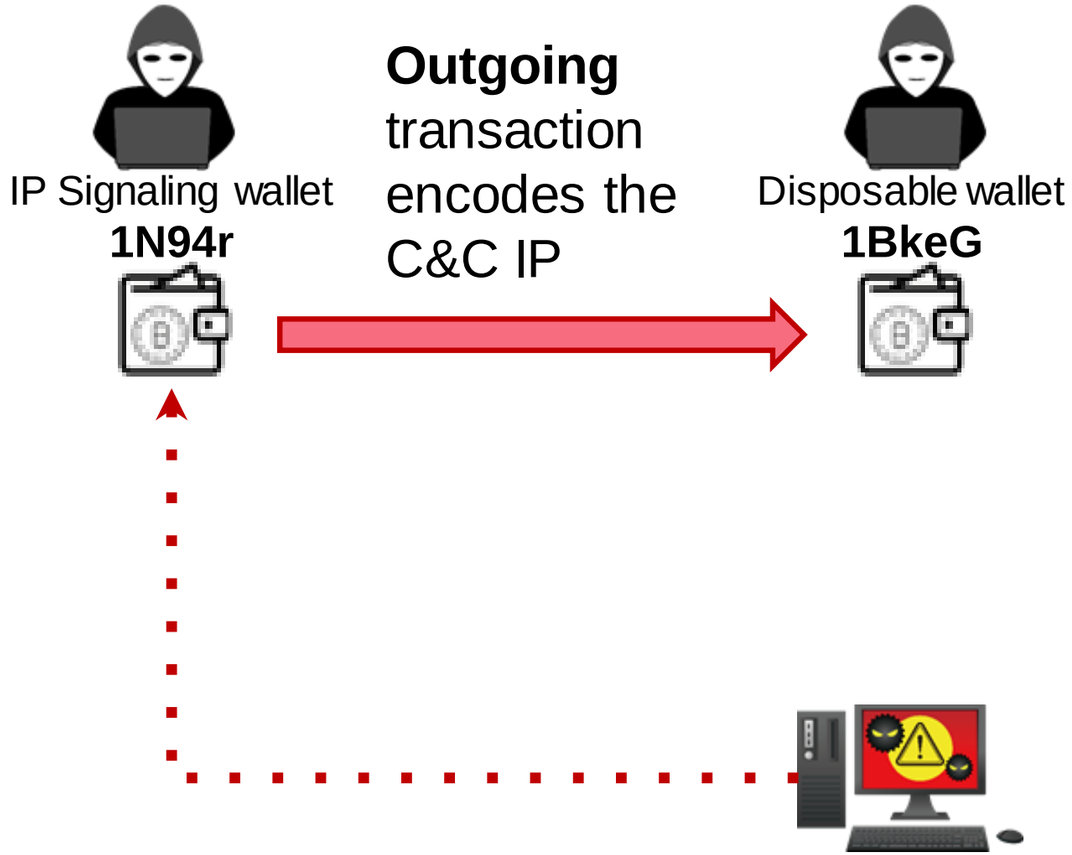
**What did we accomplish?**
3 takeovers
malware offline for 17 days
prevented 2 million USD in damages

Adversaries redesigned their C&C mechanism so that it could no longer be taken over

# How Did the Adversaries Evade our Takeover?



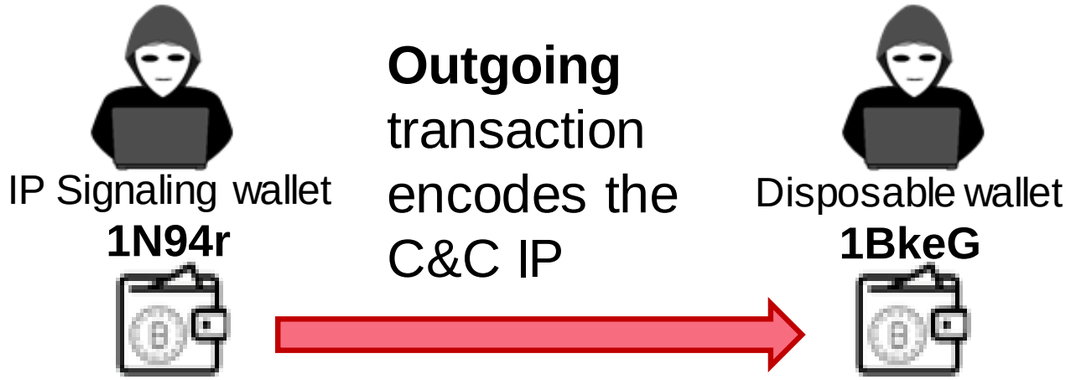
# How Did the Adversaries Evade our Takeover?




The simple fix was rolled out in malware samples from September 1 onwards

Clients are programmed to watch a bitcoin wallet for **outgoing** transactions

# How Did the Adversaries Evade our Takeover?




The simple fix was rolled out in malware samples from September 1 onwards

but they eventually gave up.

# Concluding Remarks and Takeaways

- Blockchain-based C&C is the next step in a long evaluation of criminal TTPs, but it will be very difficult to mitigate this technique in the future
- We could study how the adversaries experimented, learned and improved their TTPs over time, and traded off performance with how much they had to pay for it
- A simple design mistake allowed us to takeover their operation until they redesigned, but eventually they dropped their use of the Bitcoin blockchain for C&C coordination
- This mechanism was ingenious, however, vulnerable to Bitcoin (fees) surge which cut their profit, as the result, they gave up when the cost was not worth it
- After evading our takeover, we could track their malicious activity by monitoring Bitcoin behavior

# Citation


1. Pletinckx, Trap and Doerr, Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware, IEEE Conference on Communications and Network Security 2018, https://www.cyber-threat-intelligence.com/publications/CNS2018-Cerber.pdf
2. Taniguchi, Griffioen and Doerr, Analysis and Takeover of the Bitcoin-Coordinated Pony Malware, AsiaCCS 2021, download: https://www.cyber-threat-intelligence.com/publications/AsiaCCS2021-pony.pdf
3. Pony's C&C servers hidden inside the Bitcoin blockchain, https://research.checkpoint.com/2019/ponys-cc-servers-hidden-inside-the-bitcoin-blockchain/
4. Metabase, https://www.metabase.com/
5. Inside look at lifecycle of stolen credentials and extent of data breach damage, https://www.helpnetsecurity.com/2018/07/19/credential-spill-report/