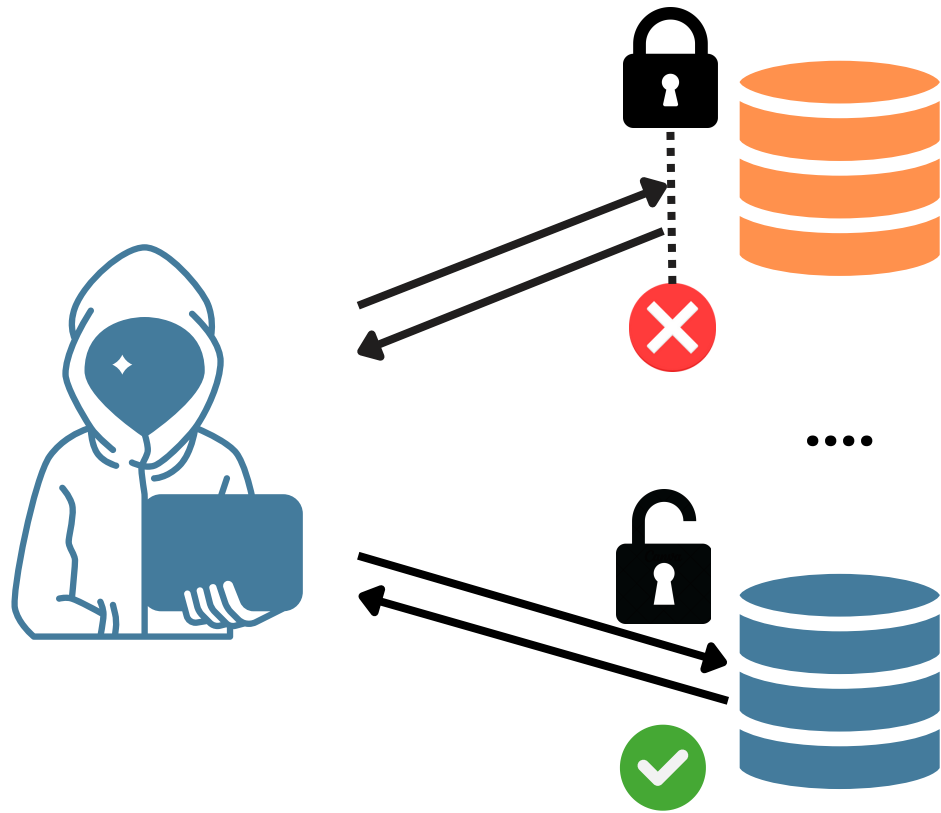


(Work in Progress): Clustering-Based Characterization of Database Server Ransom Scams

Kevin van Liebergen, Gibrán Gómez,
Srdjan Matic, and Juan Caballero

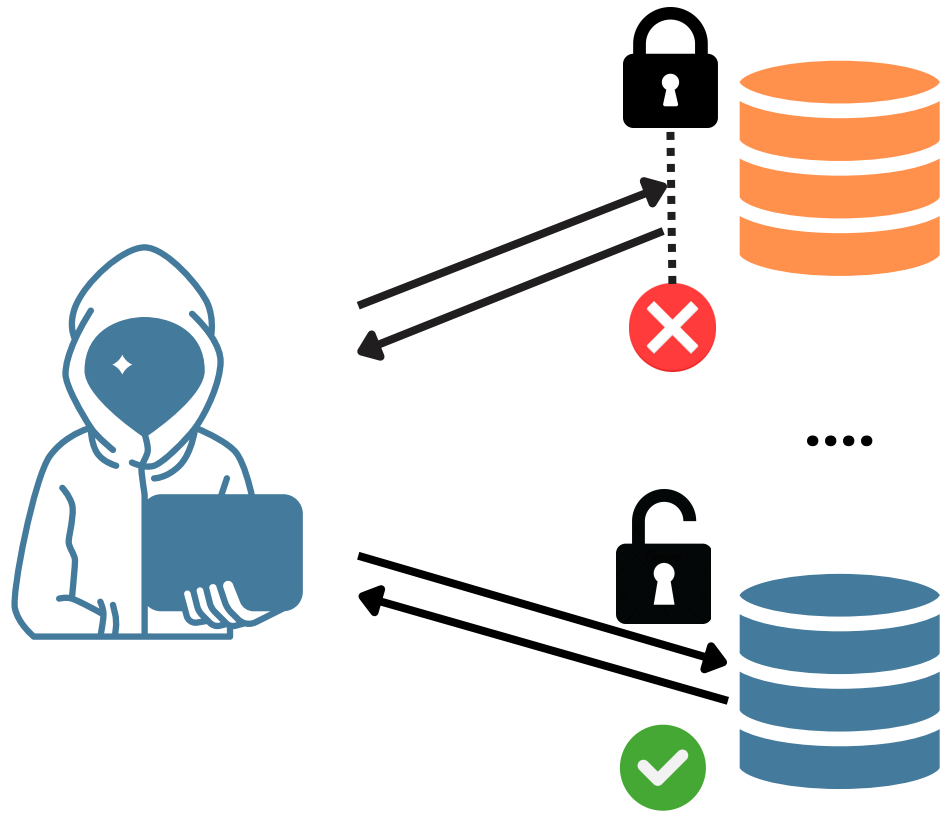


Database Server Ransom Scams



1. Attackers search for unauthenticated servers

Database Server Ransom Scams

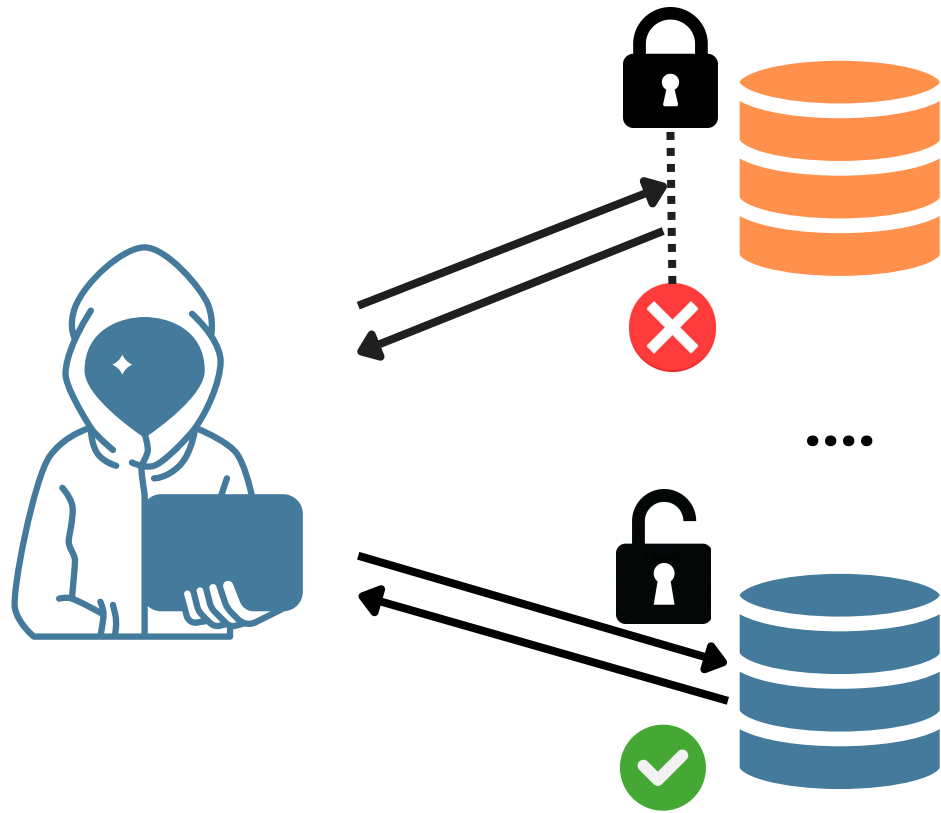


1. Attackers search for unauthenticated servers



2. Drop database content

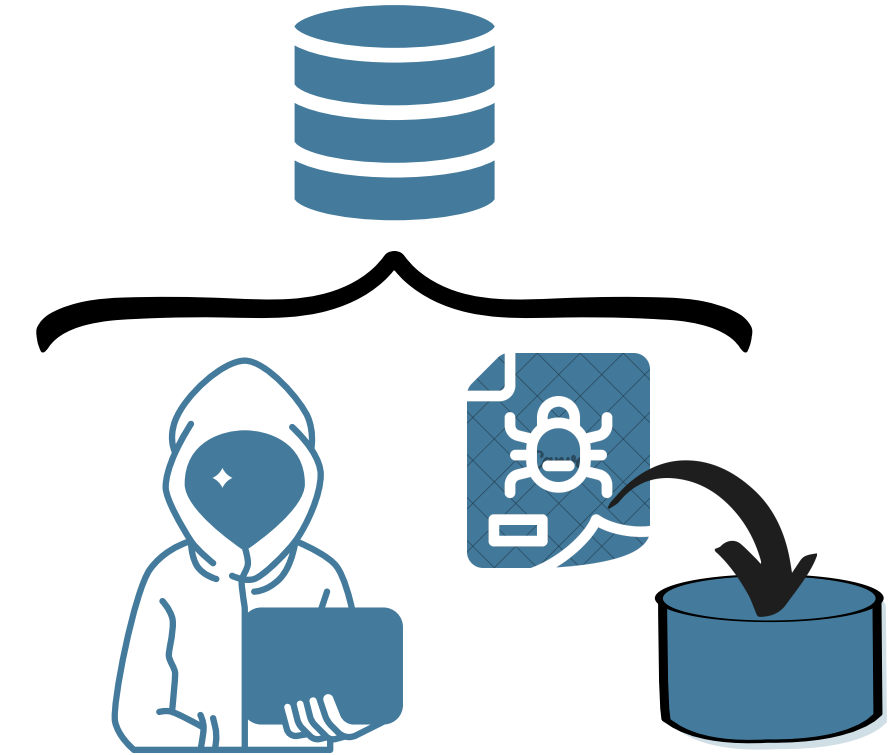
Database Server Ransom Scams



1. Attackers search for unauthenticated servers



2. Drop database content



3. Leave a ransom note:

- “Pay 0.7 BTC to bc1qzx”
- “You need to email us at rambler+2z1ed@onionmail.org”

Scams VS Ransomware

- Why scams?
 - People not get data back
- No proof data was exfiltrated

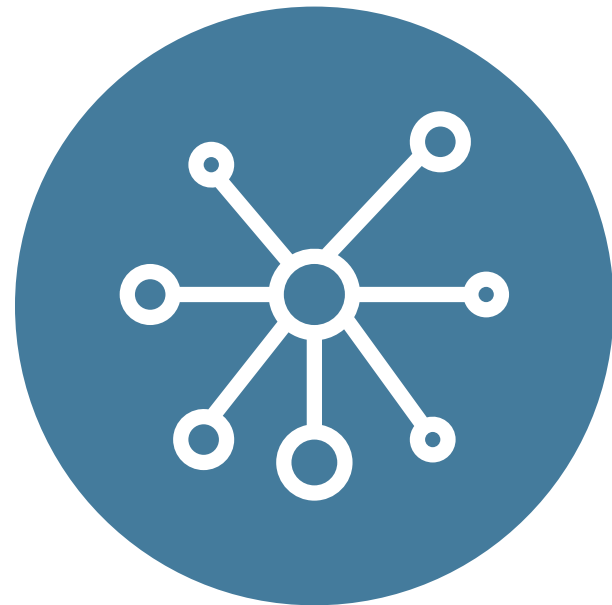


↓
Don't pay: Data can not be recovered



BTC abuse report:
"Stole data. Requested ransom.
Paid ransom, didnt return data."

Attribution



Who is behind these attacks?

- A single infection has little information
- Multiple infections provides more information
- Identifying campaigns*
- BTC tracing

* Campaign: Notes generated with the same template

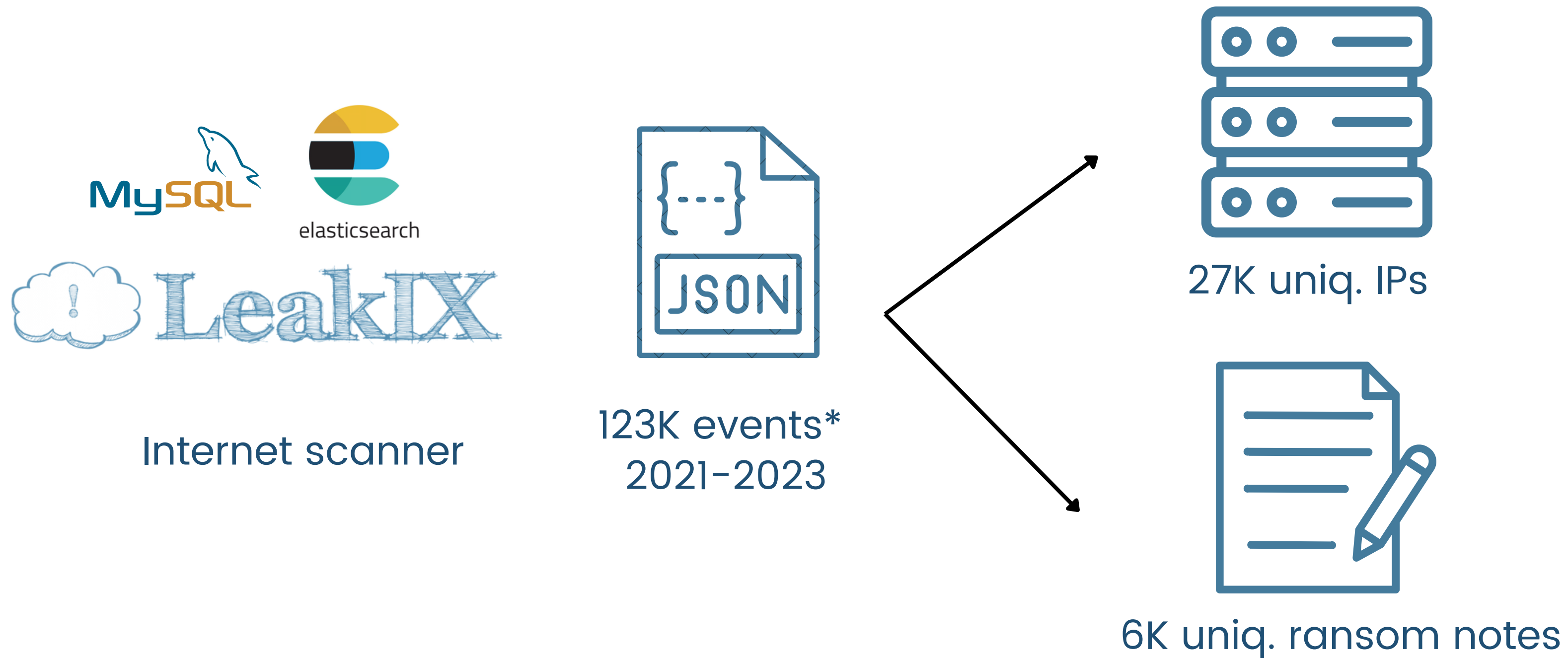
Attribution



**How can we identify
different campaigns that
belong to the same group?**

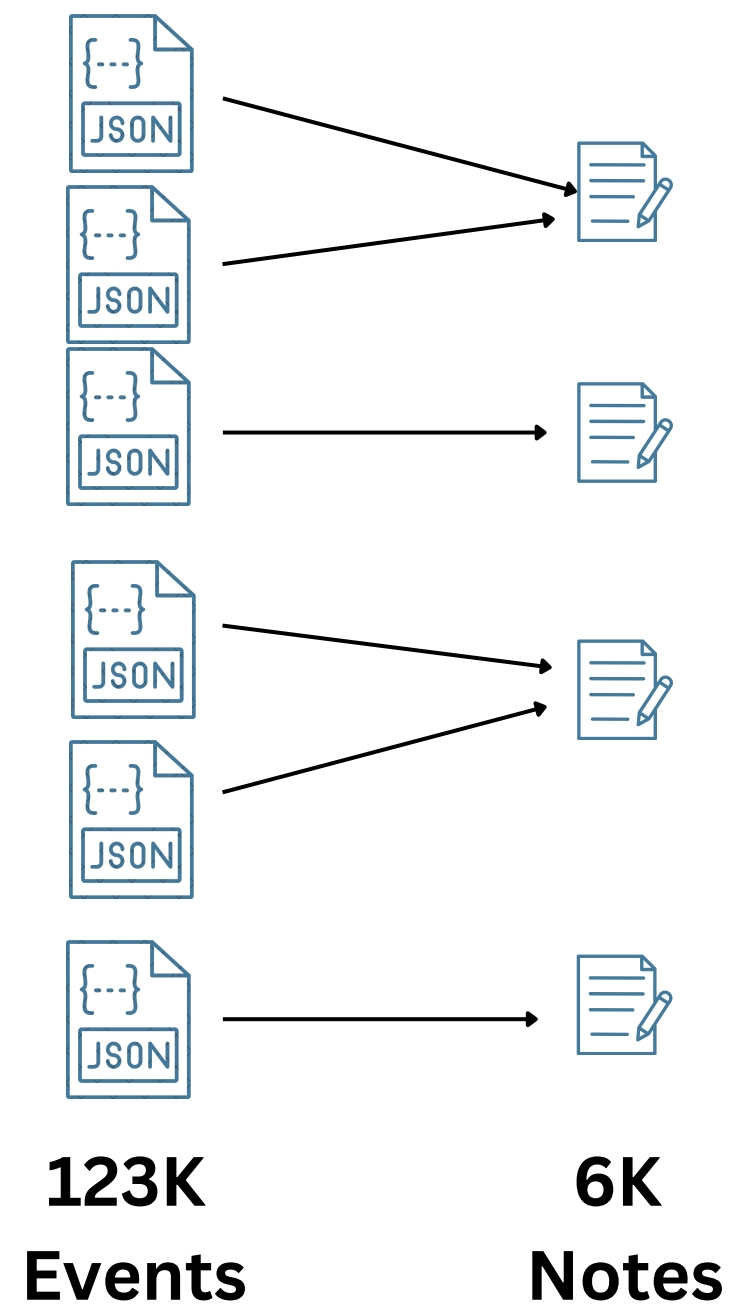
- Group related infections
 - Same campaign
 - Same responsible threat group
- Campaigns with different text
- Notes in different languages

Dataset

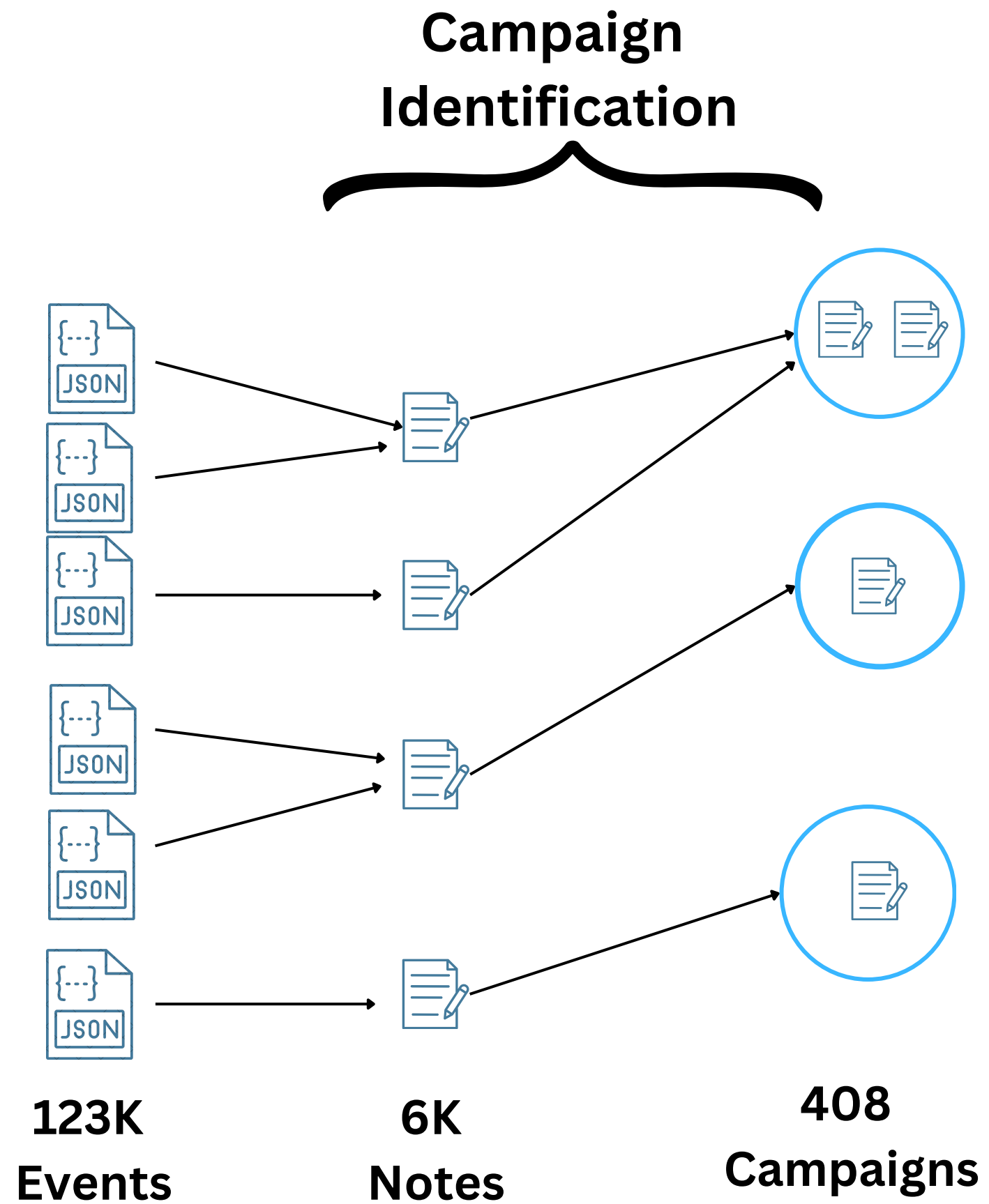


* Event: IP scan at specific time with ransom note

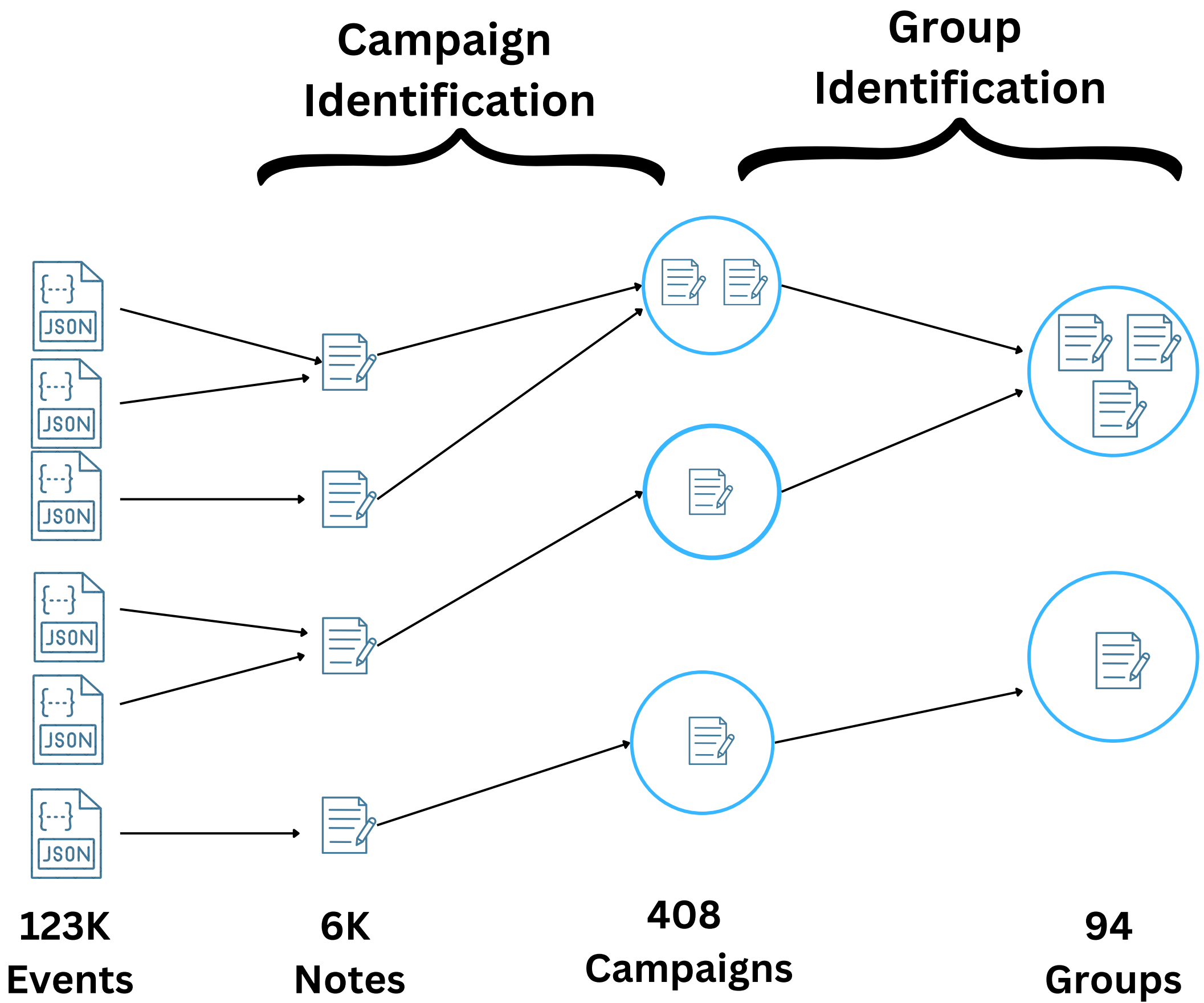
Clustering Approach



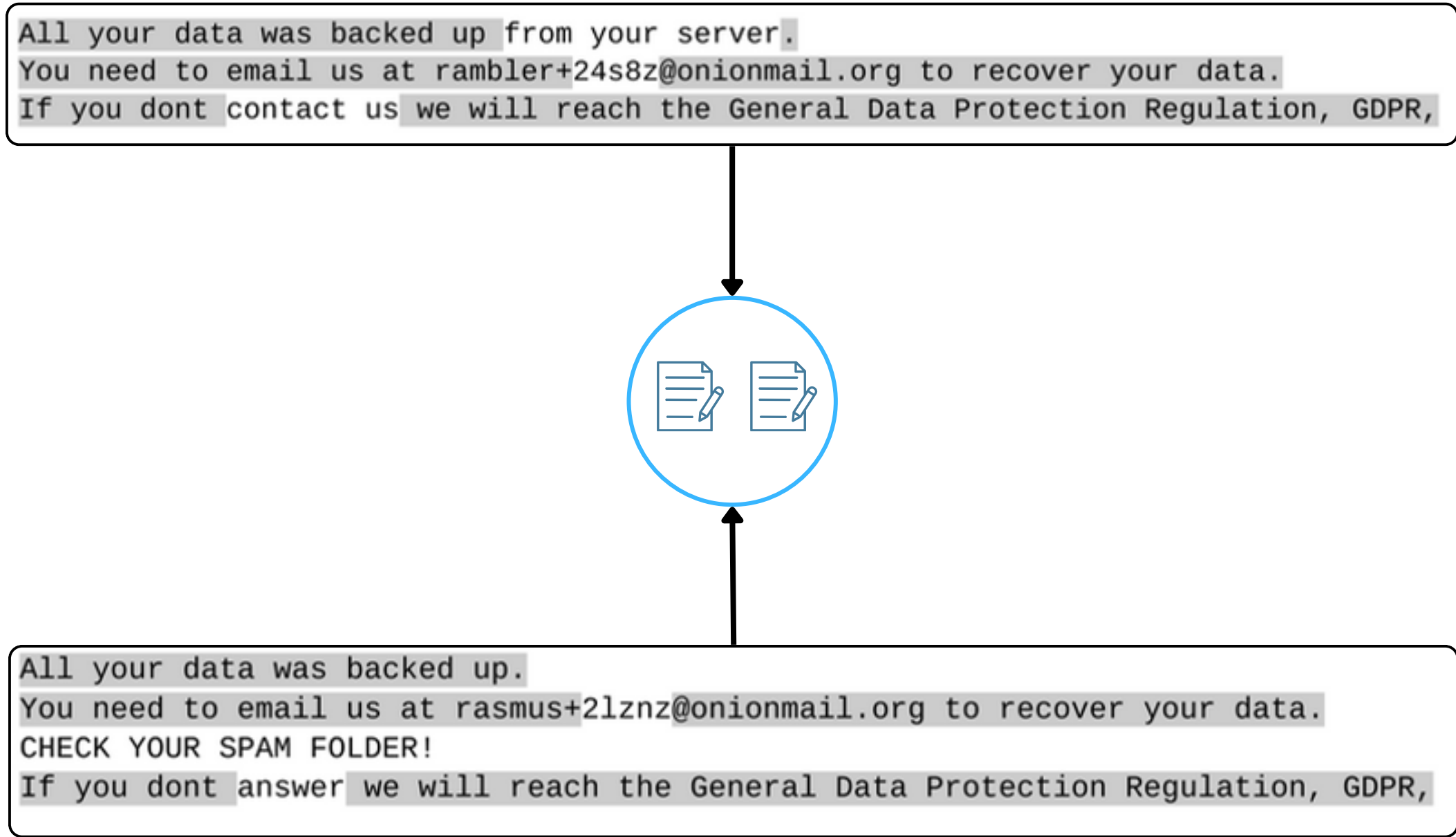
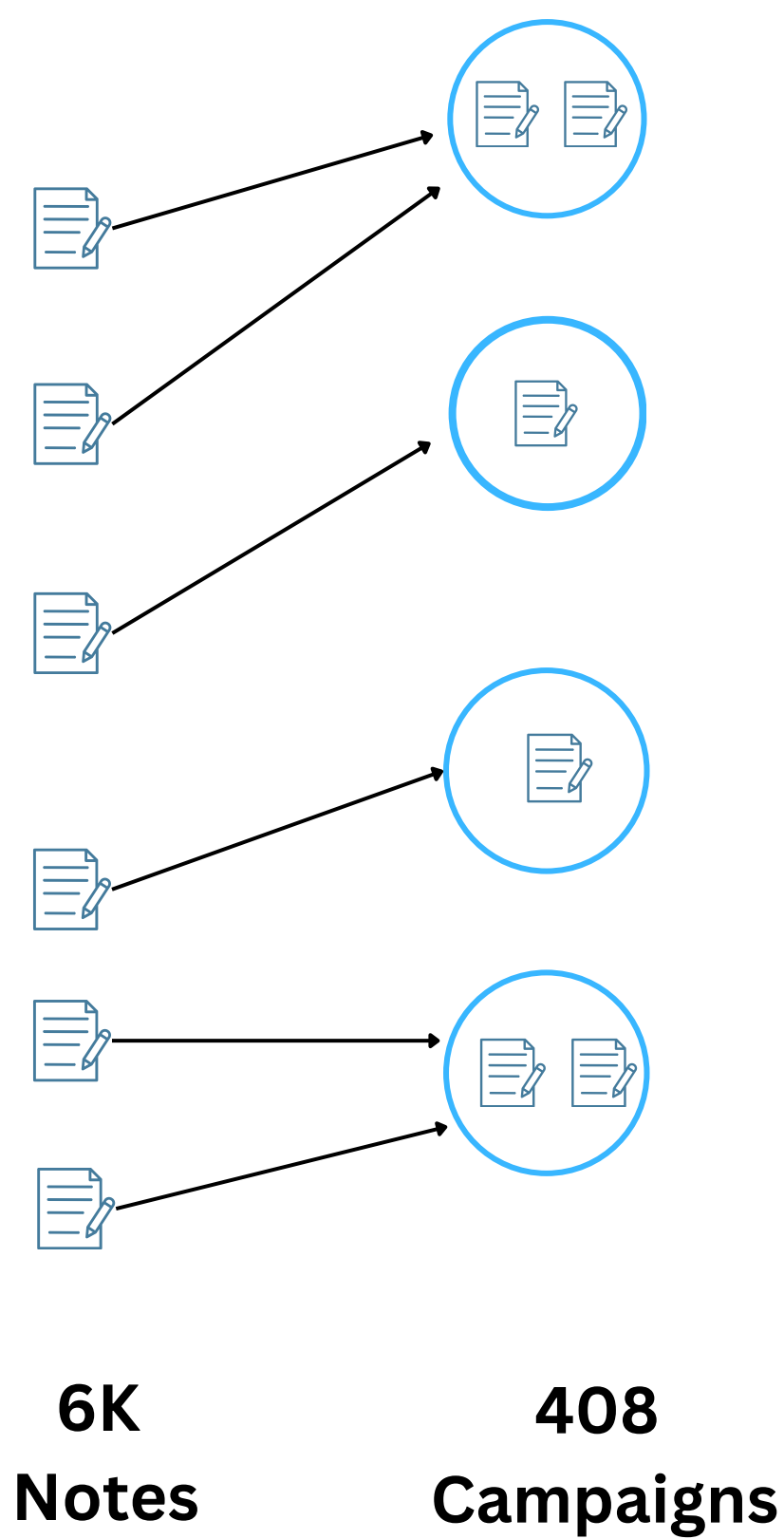
Clustering Approach



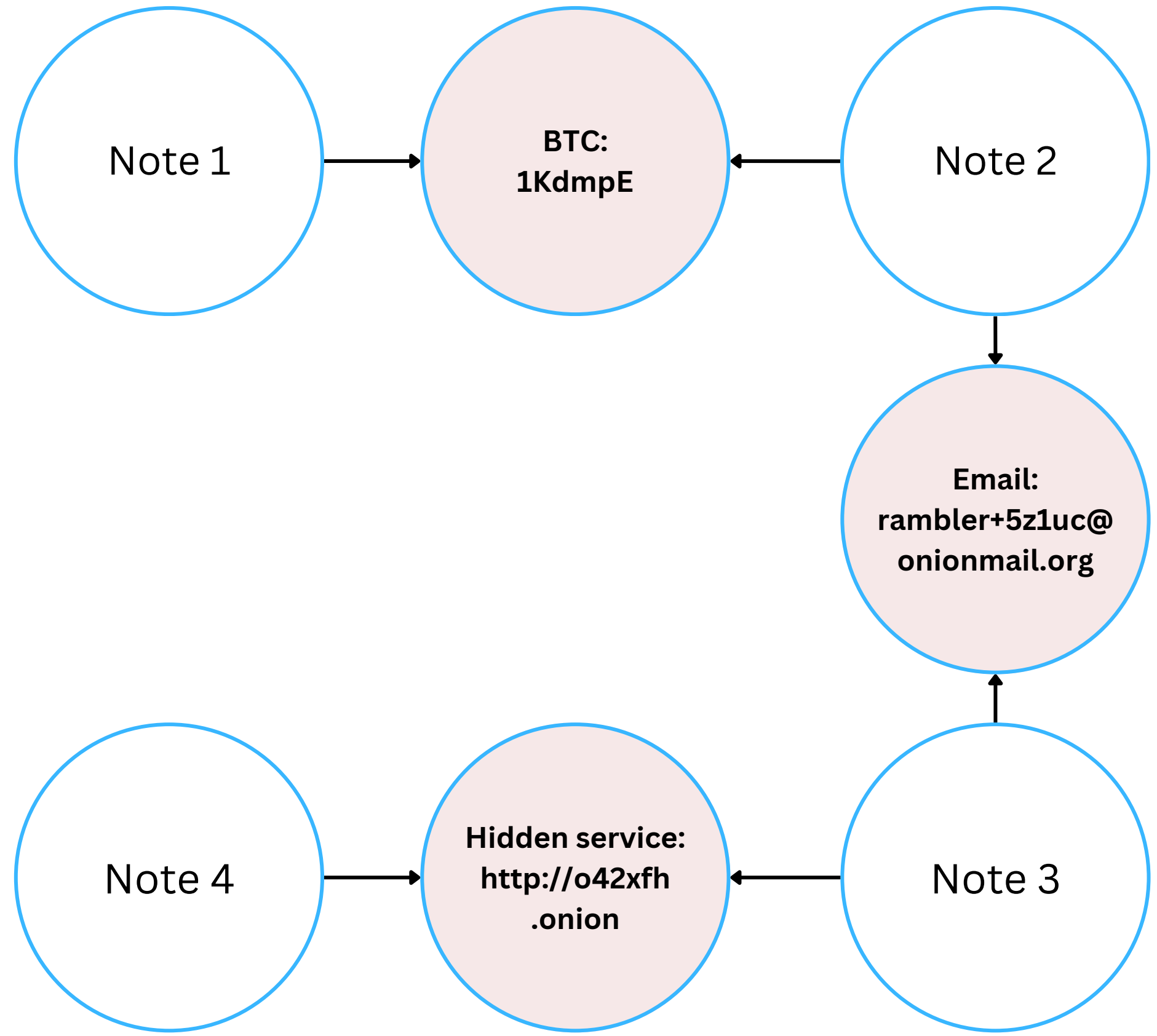
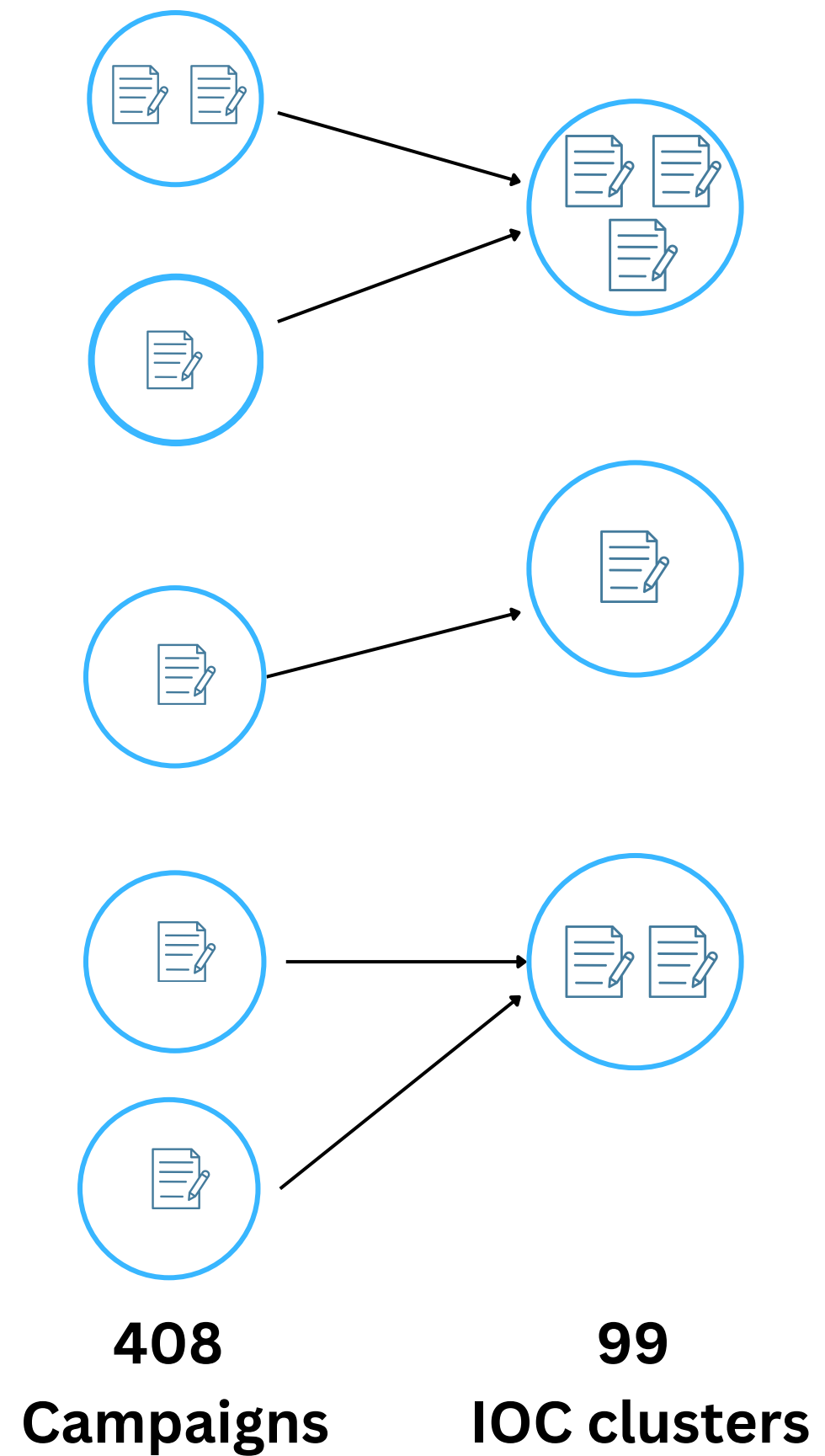
Clustering Approach



Campaign Identification: Note Similarity Clustering

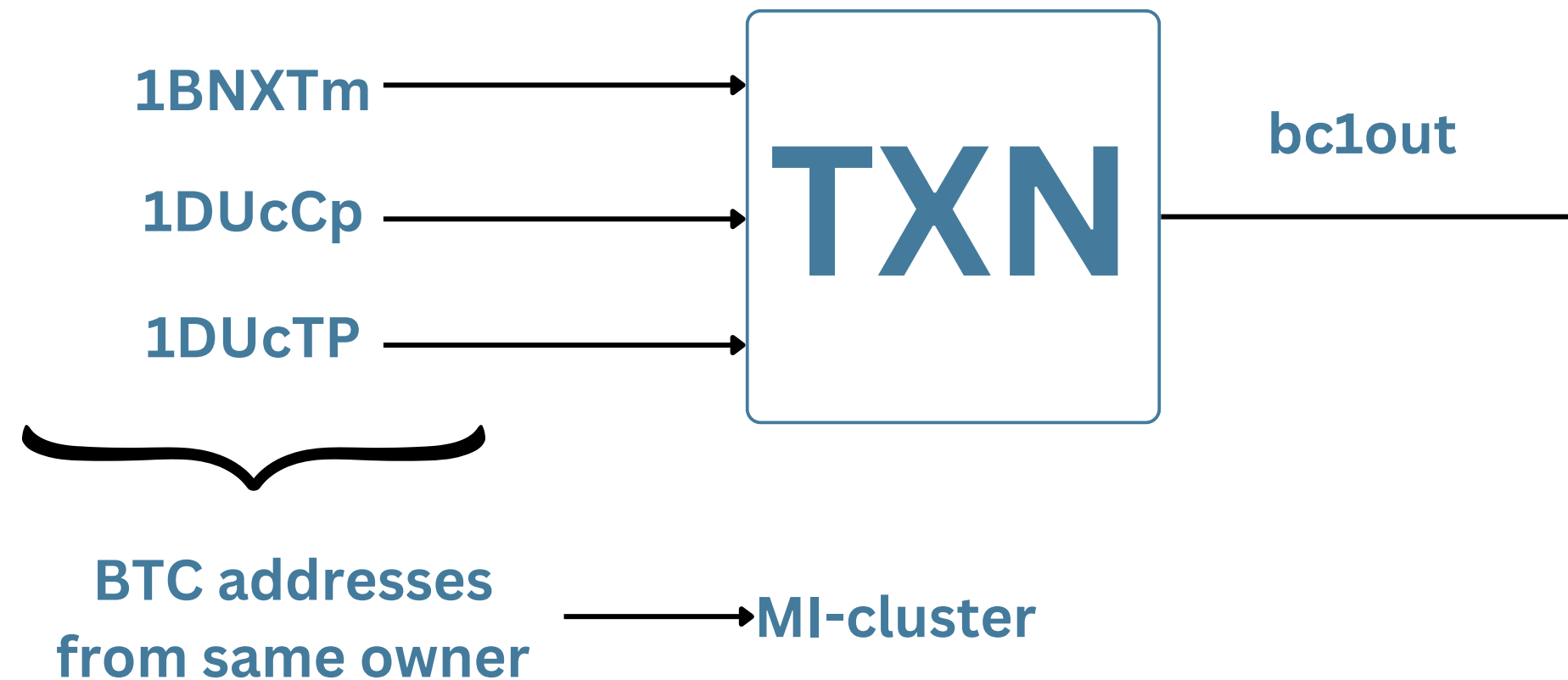


Group Identification: Indicator Of Compromise Reuse



Group Identification: Bitcoin Multi-Input (MI) Clustering

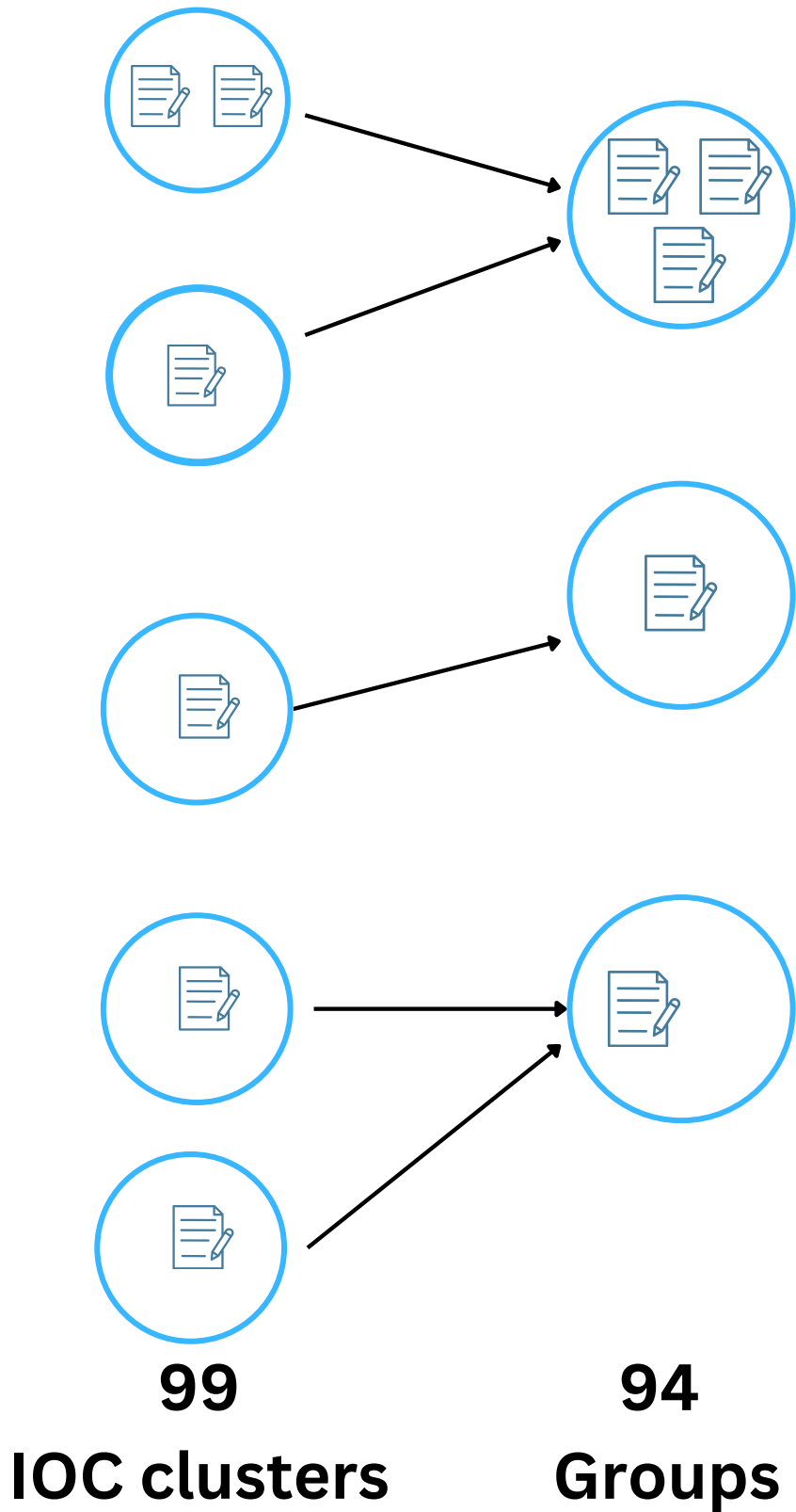
- BTC transaction (TXN) example



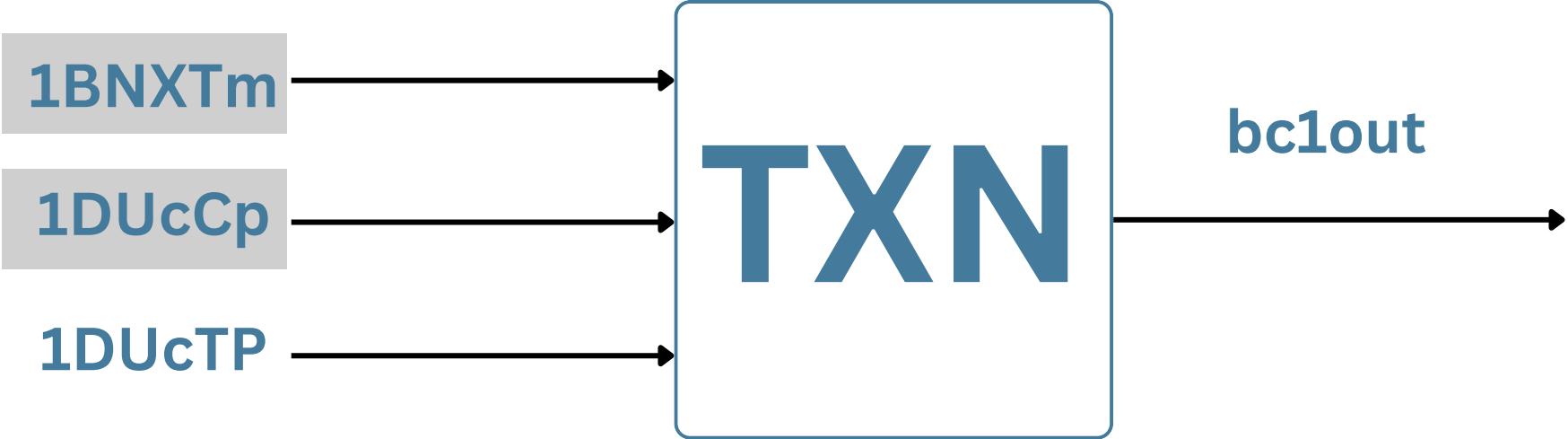
- Analyze all BTC TXNs using WYB* to extract MI-clusters
 - BTC transaction tracing and revenue estimation

*G. Gomez, K. van Liebergen, and J. Caballero, "Cybercrime Bitcoin Revenue Estimations: Quantifying the Impact of Methodology and Coverage", ACM CCS '23, URL: <https://github.com/cybersec-code/watchyourback>

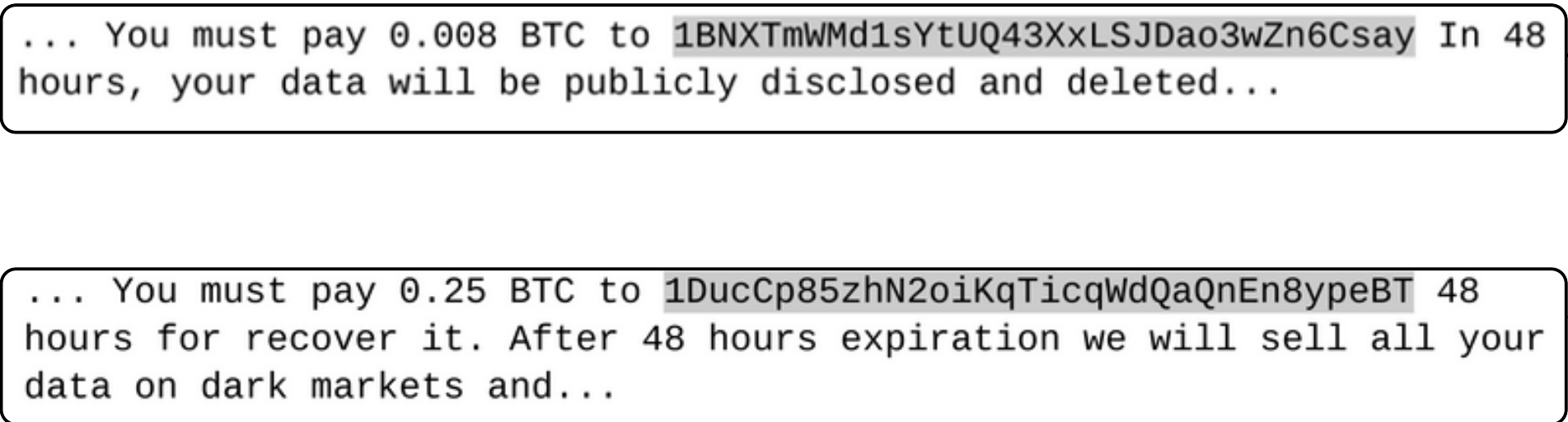
Group Identification: Bitcoin Multi-Input (MI) Clustering



1. Identify MI-clusters



2. Merge IOC clusters that belong to same MI-cluster



Cluster Analysis

- 🔒 How prevalent are database server ransom scams?
 - 27K infected MySQL and ElasticSearch servers with no authentication
- 🔒 How many groups are responsible for the infections?
 - 94 groups



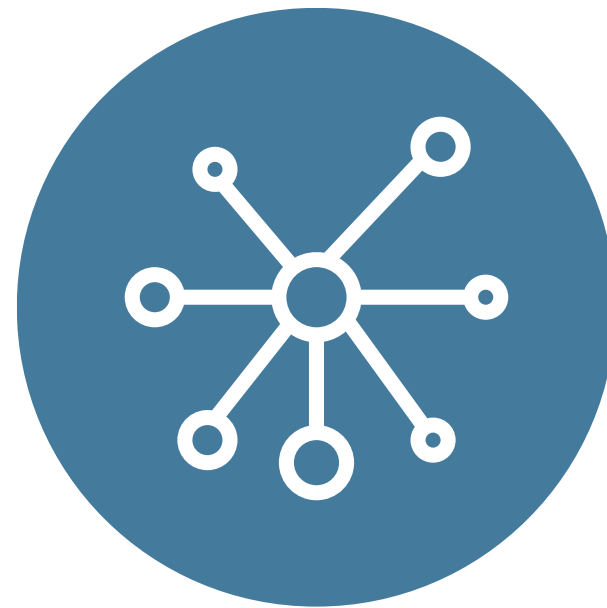
Largest group

- 49% server infections
- Run 109 campaigns (\$165k revenue)
- Different locations (English and Chinese notes)
- 149 BTC addresses, 3.5K emails

Contributions



**First study of DB server
ransom scams**



Novel Clustering
Campaign identification
+
Group identification



**Dominant group
responsible for most
attacks**

Clustering-Based Characterization of Database Server Ransom Scams

Kevin van Liebergen, Gibrán Gómez,
Srdjan Matic, and Juan Caballero



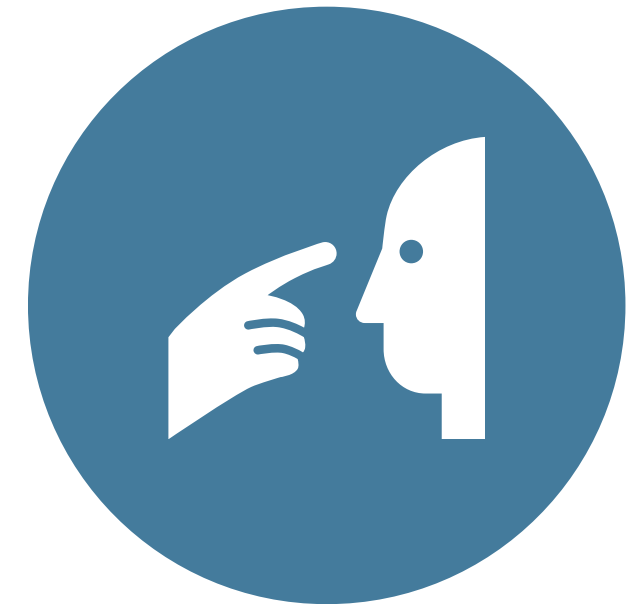
Future Work



**Improve Note
Similarity**

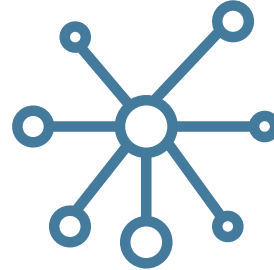



Attribution Target Selection



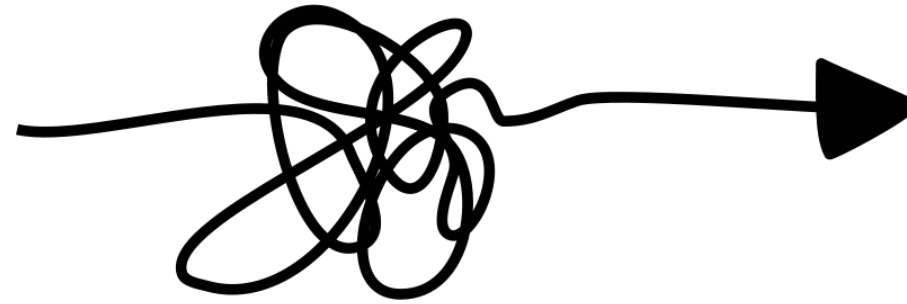
**Attribution Case
Studies**

Related Work

-  Clustering scam websites, emails, malware samples
 - Cluster campaigns that belong to the same attacker
-  Ransomware targeting servers and encrypting data
 - Database server ransom scams delete data, not encrypt it
-  Support scams, sextortion, romance scams
 - First work investigating database server ransom scams

Discussion 1/2

Evasion techniques



- Not provide ransom payment details

To recover your databases, visit
`http://godransm3nnlofdwounmfdfaaivjzlnkeslxmo6siw45gn2gjy7av2qd.onion`
and type in this token: `01GC9YP9A892D51RCMZ8YB4RRF`

- Hamper IOC extraction

..... If we dont receive your payment in the next 10 Days, we will delete or leak your sensitive
information.
`bc1qvt6d7gjzdvmf3ns8nlq56g6pzjmg74exwyu6tf8datarecover@protonmail.com`

Discussion 2/2

Ethics



- LeakIX collects data from servers
 - No authentication
- Only database tables name
- Download content whose table name matches with regex