

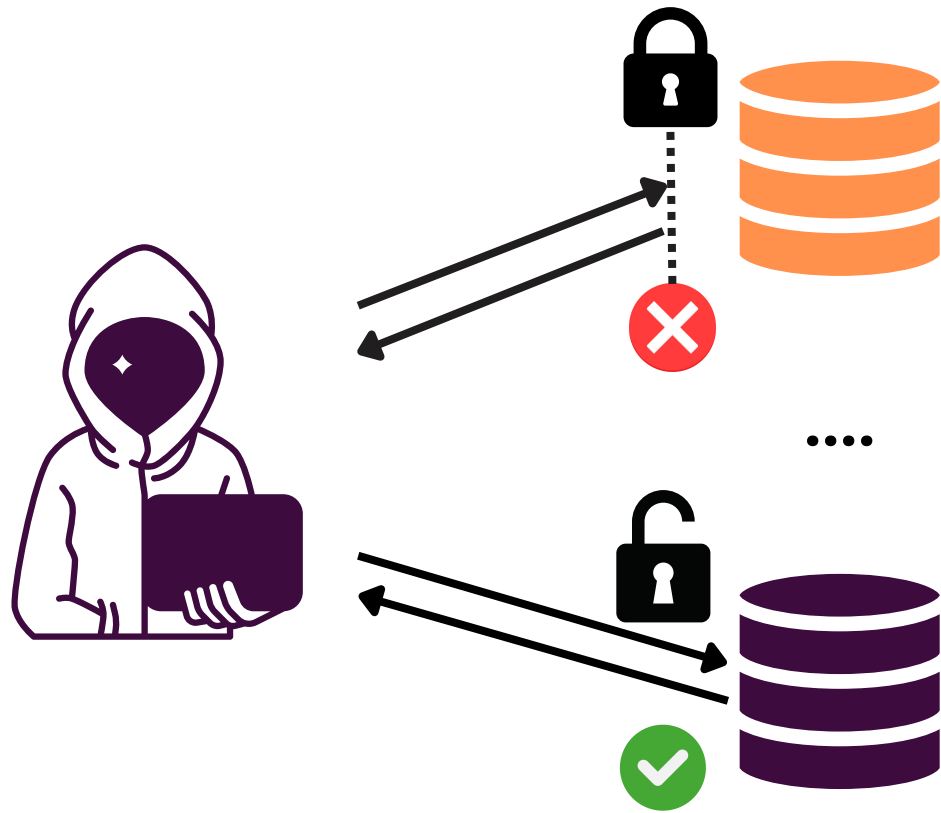


All your (data)base are belong to us:

Characterizing Database Ransom(ware) Attacks

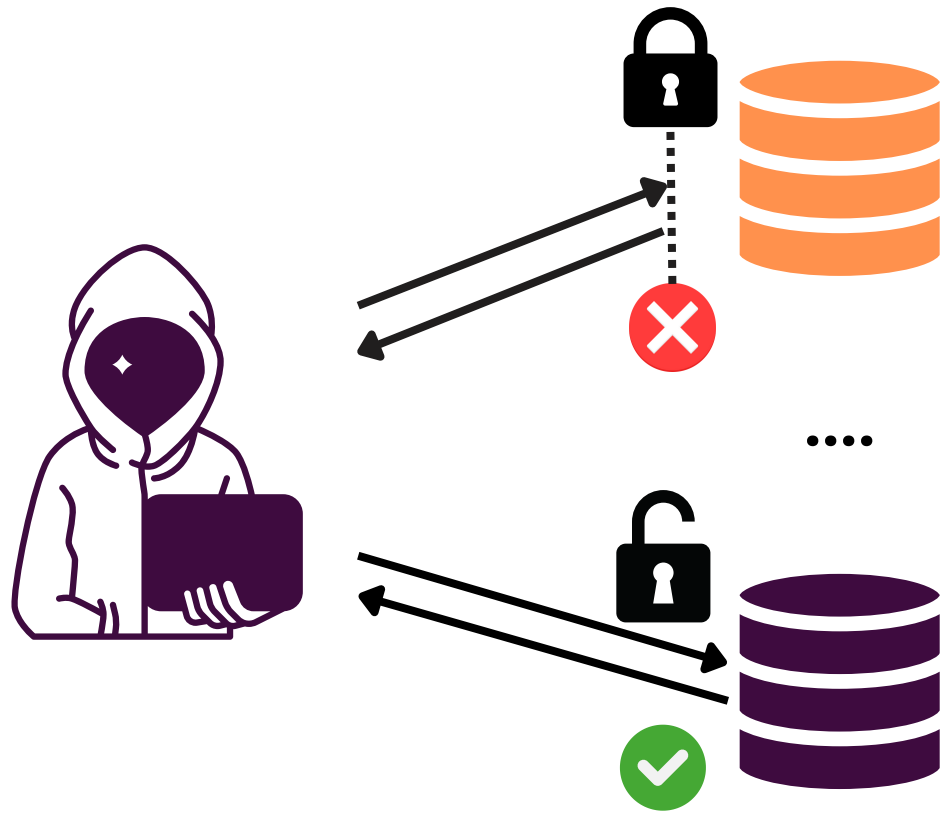
Kevin van Liebergen, Gibrán Gómez, Srdjan Matic, and Juan Caballero

Database Ransom(ware) Attacks

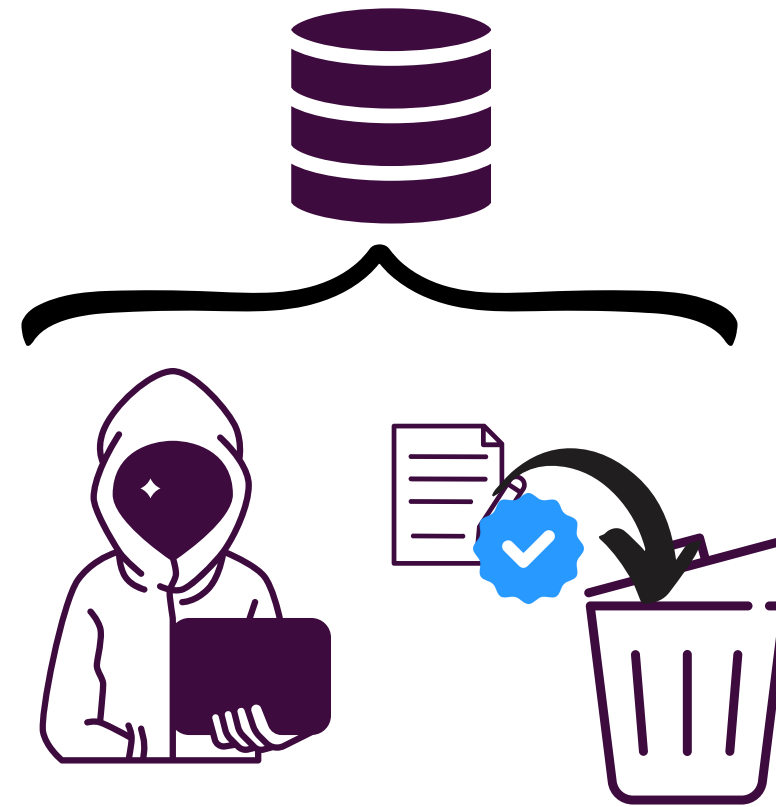


1. Attackers search for unauthenticated servers

Database Ransom(ware) Attacks

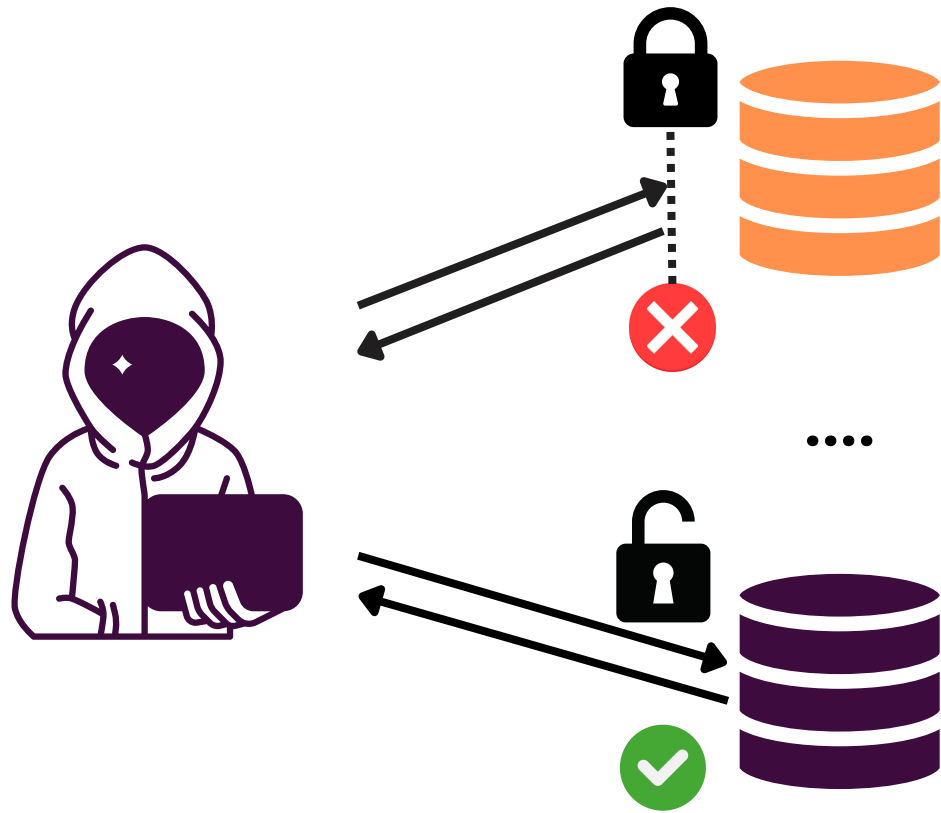


1. Attackers search for unauthenticated servers



2. Delete database content

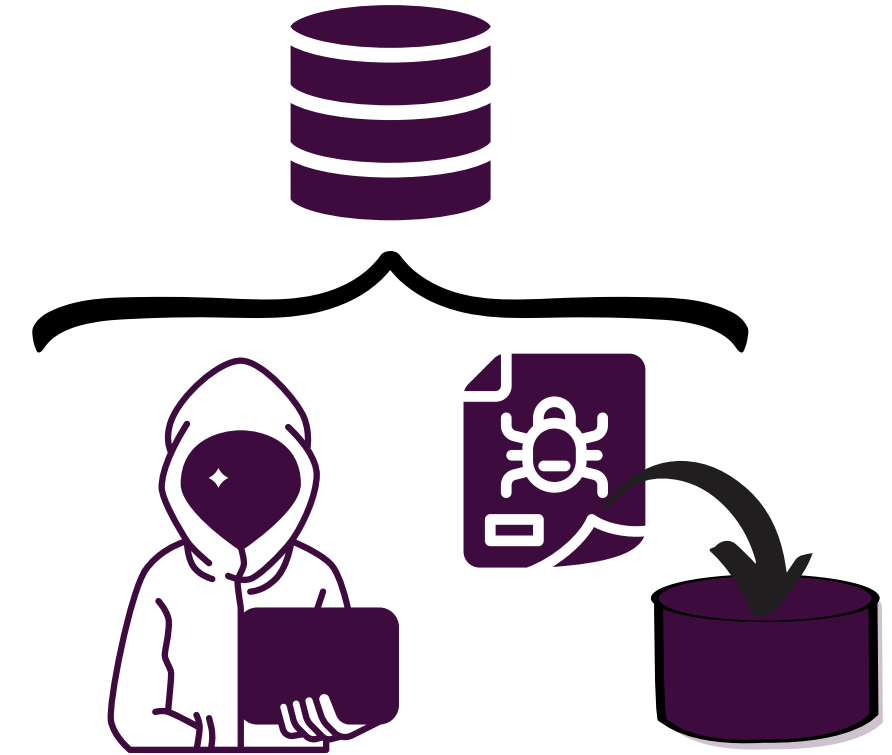
Database Ransom(ware) Attacks



1. Attackers search for unauthenticated servers



2. Delete database content



3. Leave ransom note:

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

Datasets



LeakIX Internet Scanner

- Longitudinal: 2021–2024
- 302K infections
- 60K IPs
- 23K ransom notes



Honeypots

- Gather first-hand 2024 information
- 5 VMs in different countries
- Cloud hosting providers
- Empty password for root user

RQ1: How Do These Attacks Work?

- 131 honeypot infections
- Infection sequence
 - Brute-force login
 - List databases
 - Delete data
 - Leave ransom note
 - Lock DB (opt.)



RQ1: How Do These Attacks Work?

- 131 honeypot infections
- Infection sequence
 - Brute-force login
 - List databases
 - Delete data
 - Leave ransom note
 - Lock DB (opt.)

- **Automated infections**
- **First infection in 14h**
- **No malware**
- **No data exfiltration**
- **Scams!**

RQ2: How Many Groups and Campaigns? (Honeypots)

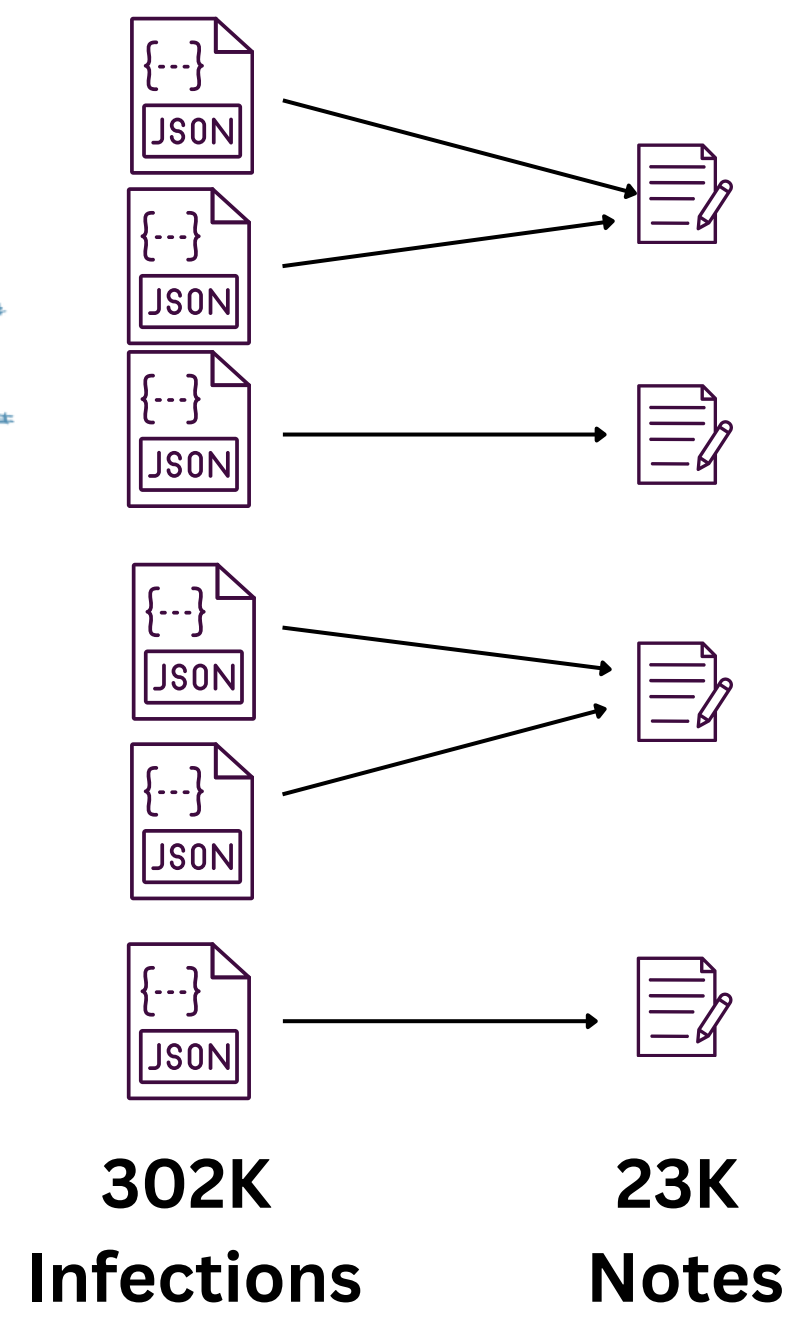
- Sequence of commands identifies 2 groups

		Notes	Campaigns
Group A		123	1
Group B		8	2

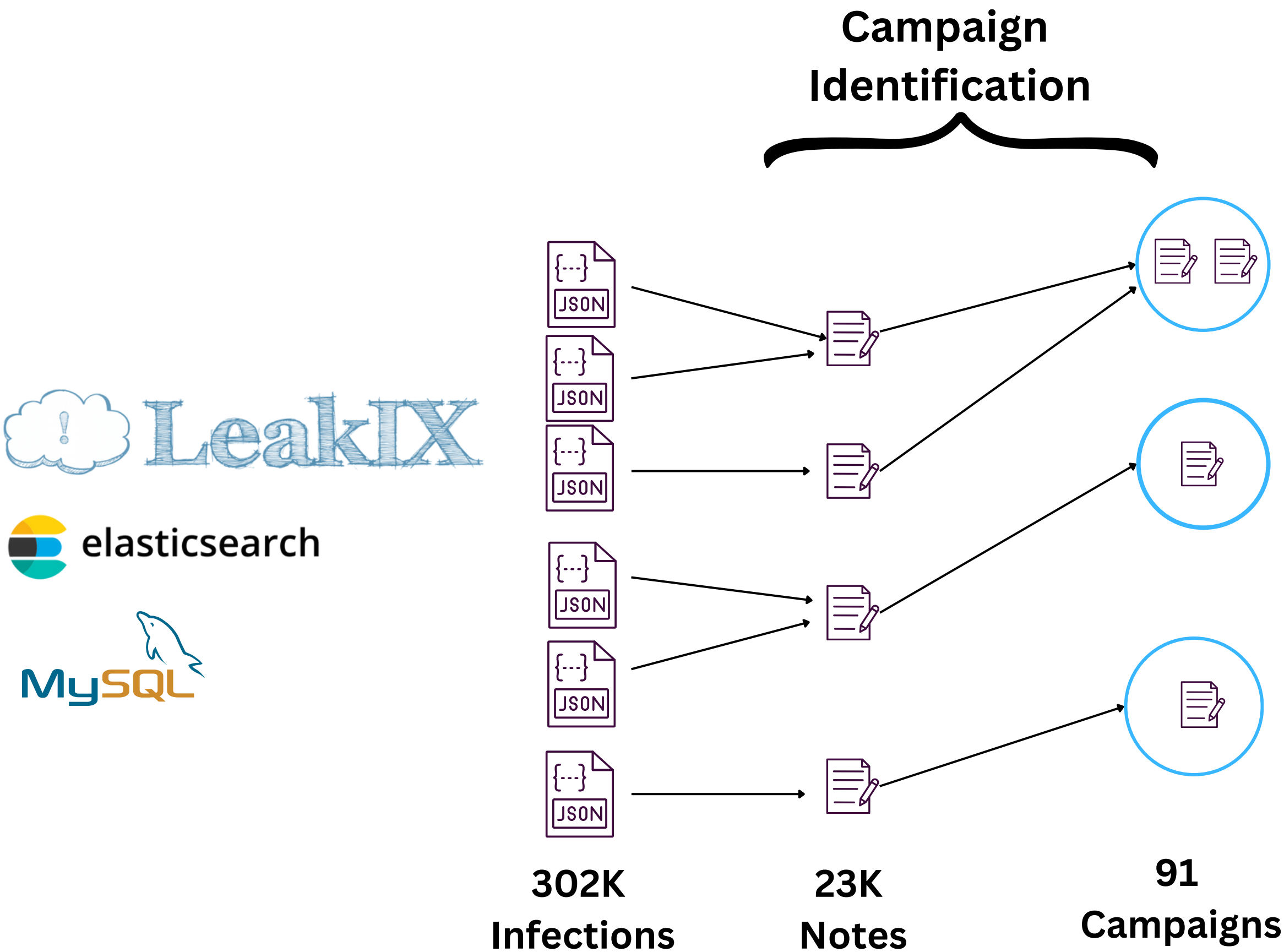
“To recover your lost databases pay <AMOUNT> BTC to this address: <BITCOIN>...”

“I have backed up all your databases. To recover them you must pay <AMOUNT> BTC to ...”

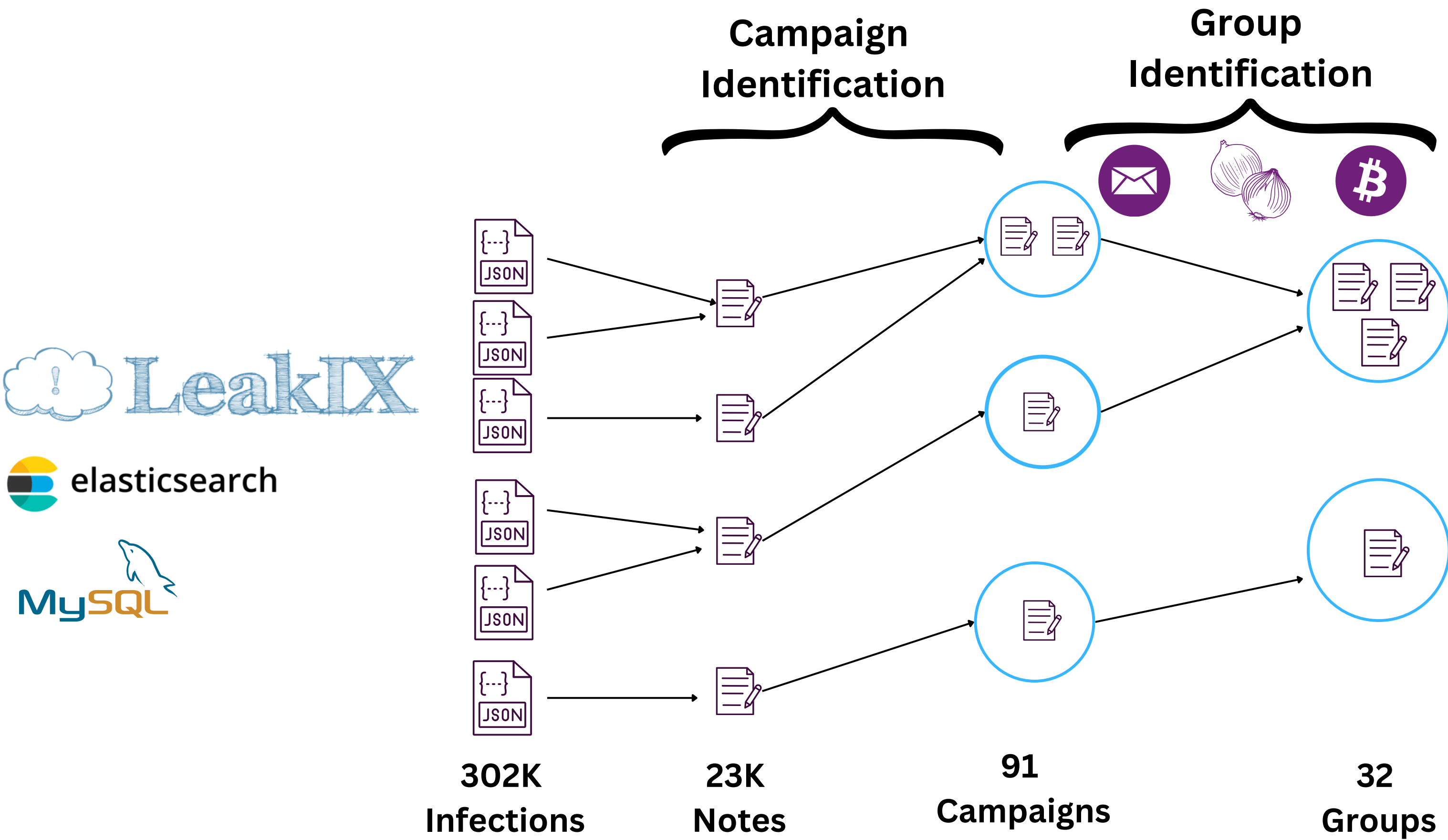
RQ2: How Many Groups and Campaigns? (LeakIX)



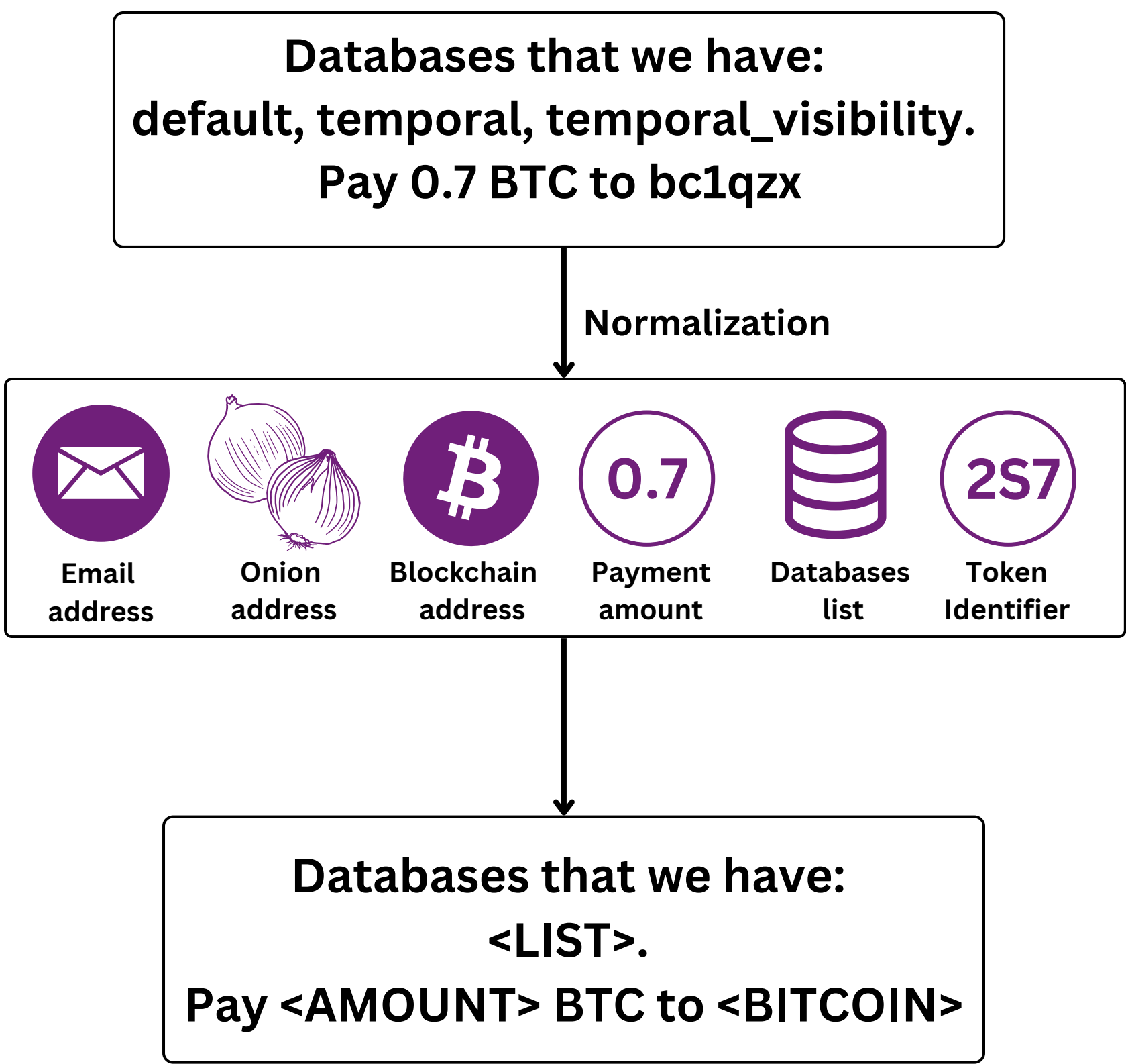
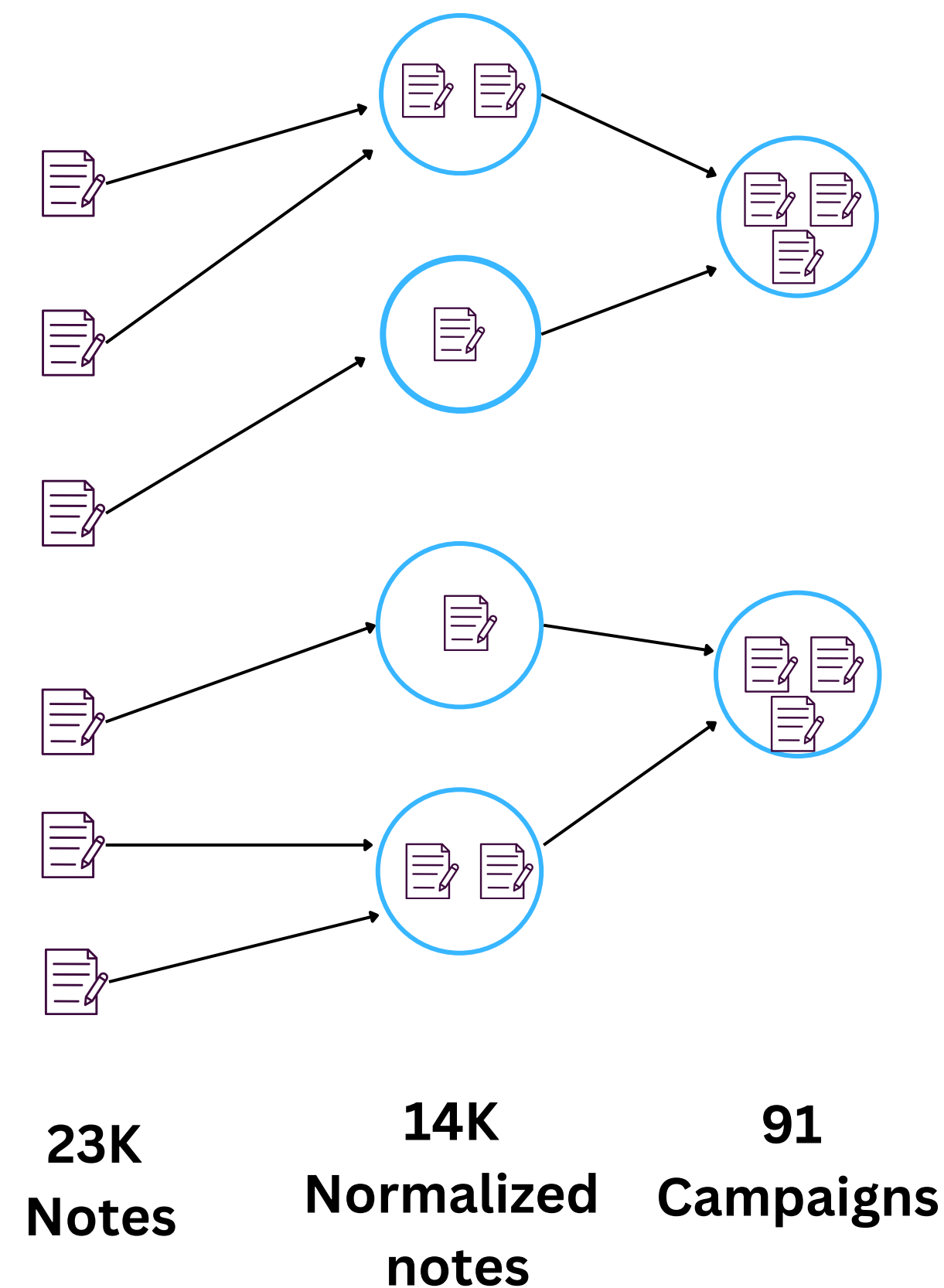
RQ2: How Many Groups and Campaigns? (LeakIX)



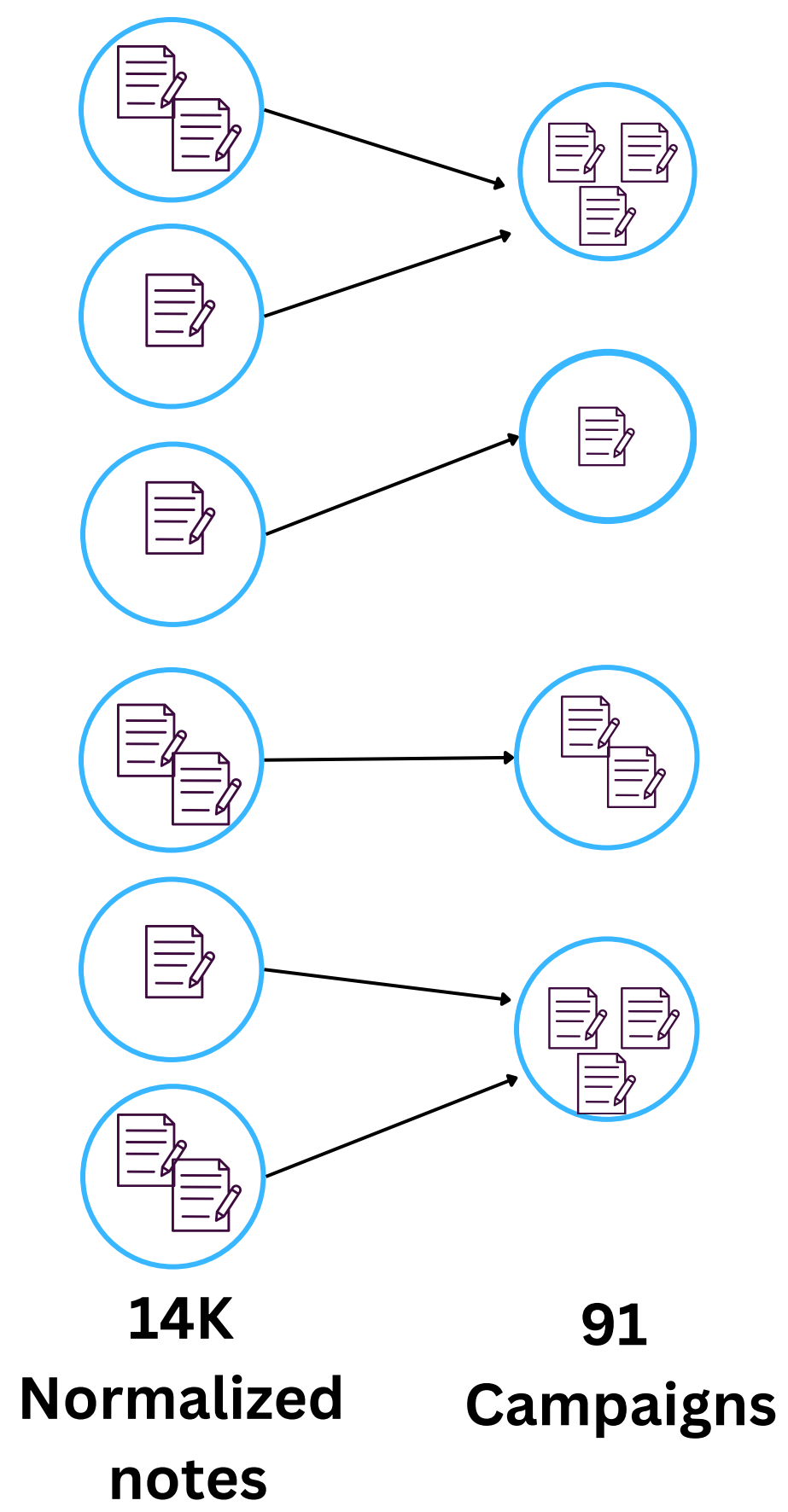
RQ2: How Many Groups and Campaigns? (LeakIX)



Campaign Identification: Normalization



Campaign Identification: Note Similarity Clustering

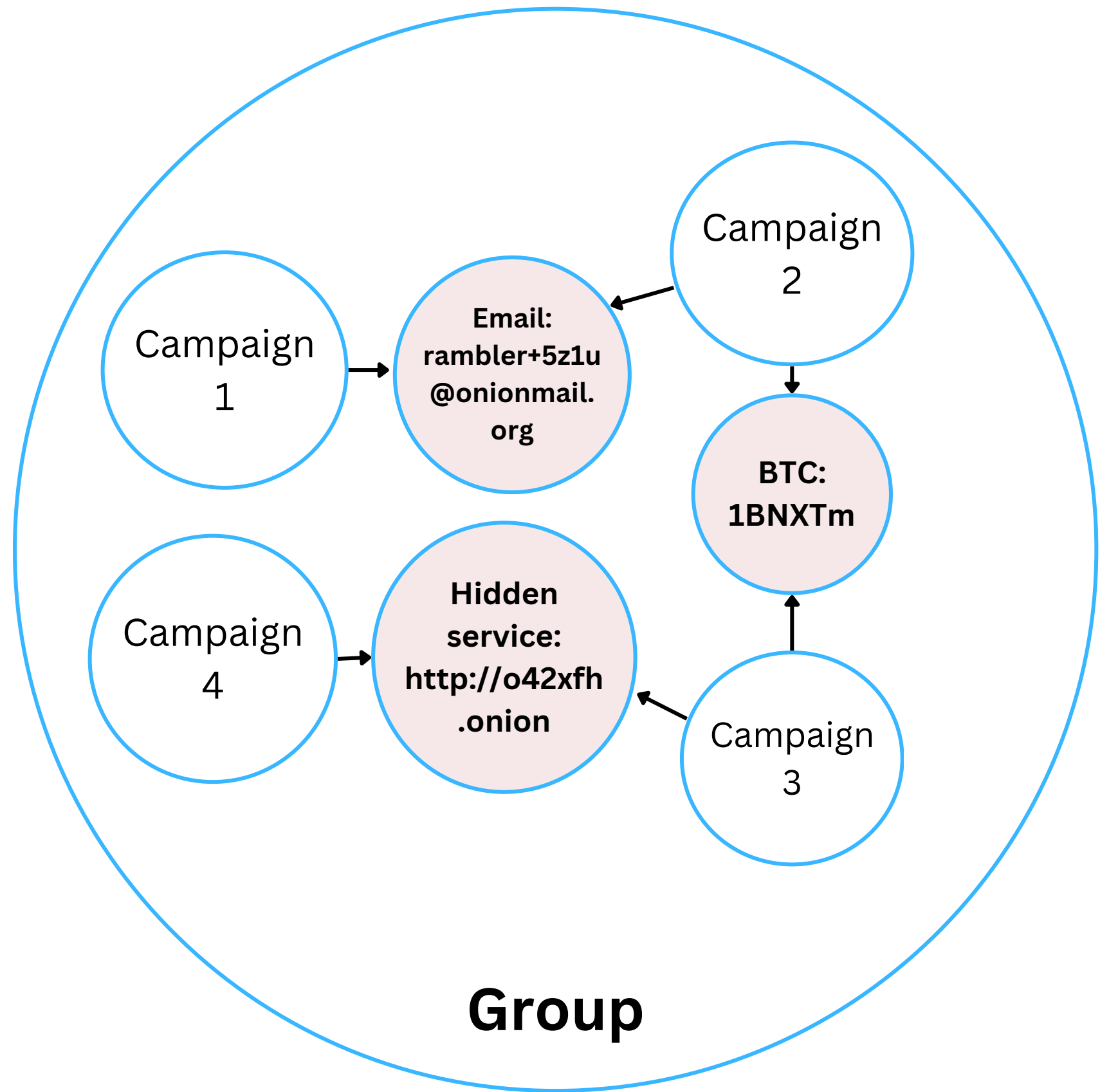
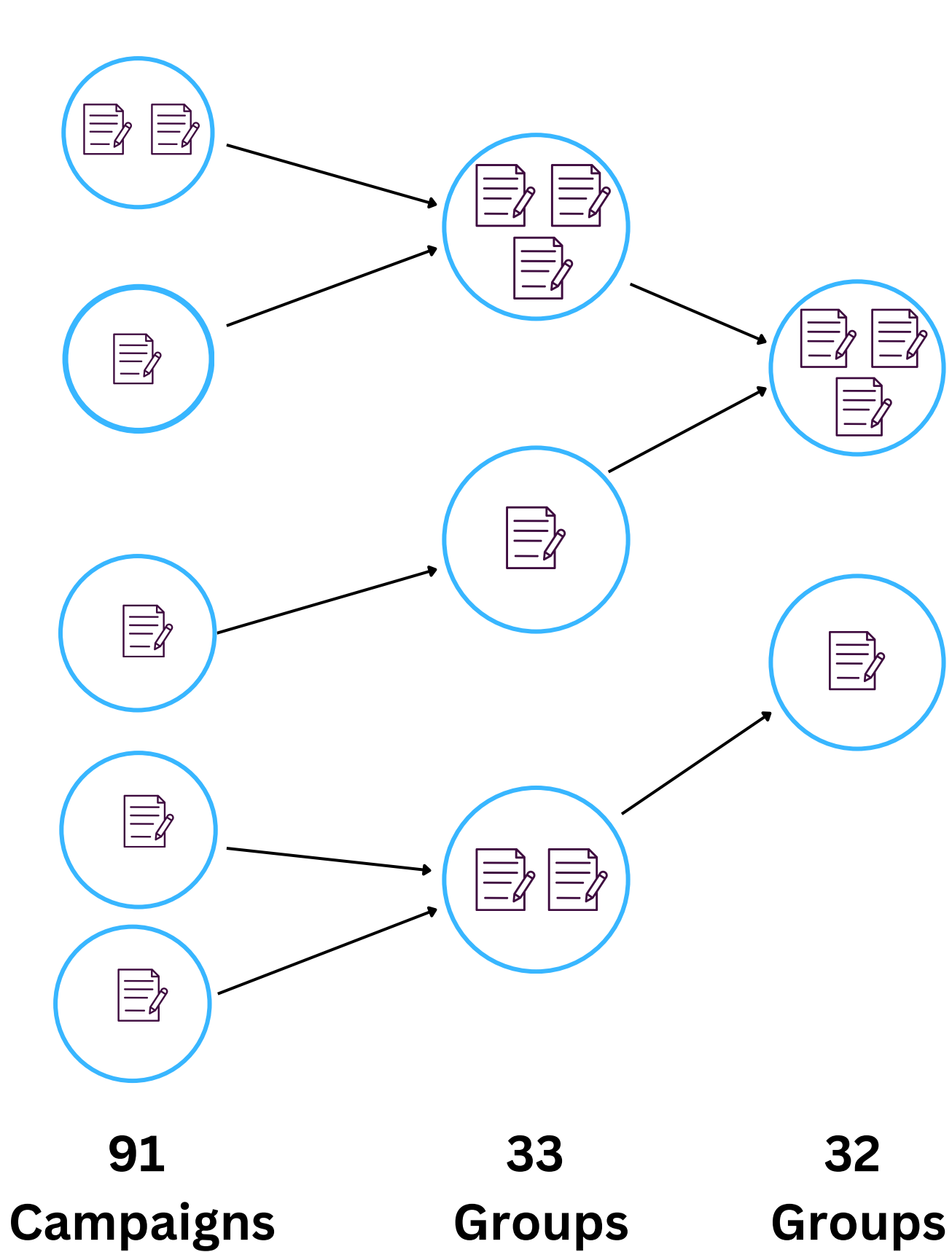


All your data was backed up .
You need to email us at <EMAIL> to recover your data.
If you dont contact us we will reach the General Data Protection Regulation, GDPR,

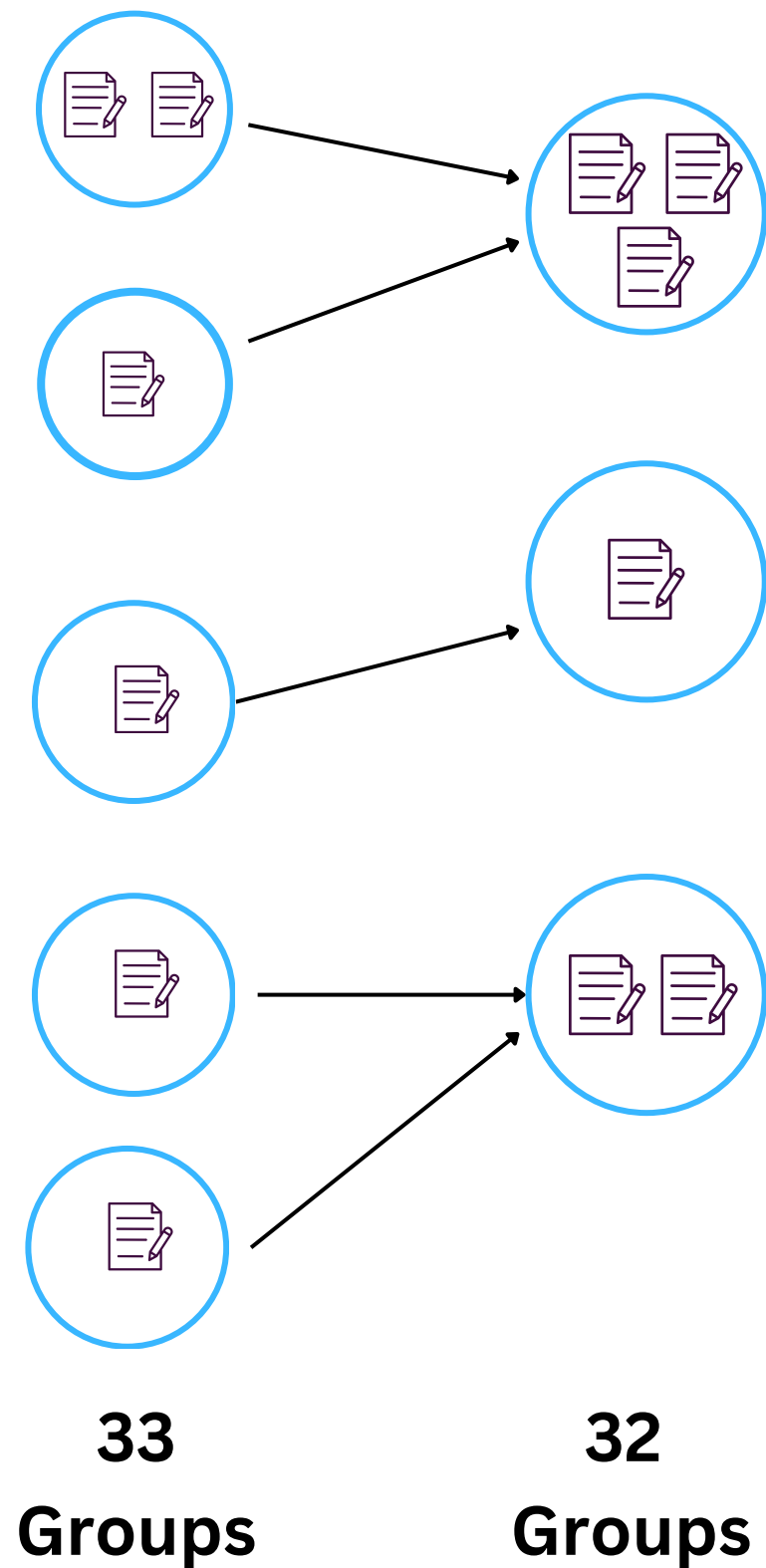


All your data was backed up.
You need to email us at <EMAIL> to recover your data.
If you dont answer we will reach the General Data Protection Regulation, GDPR,

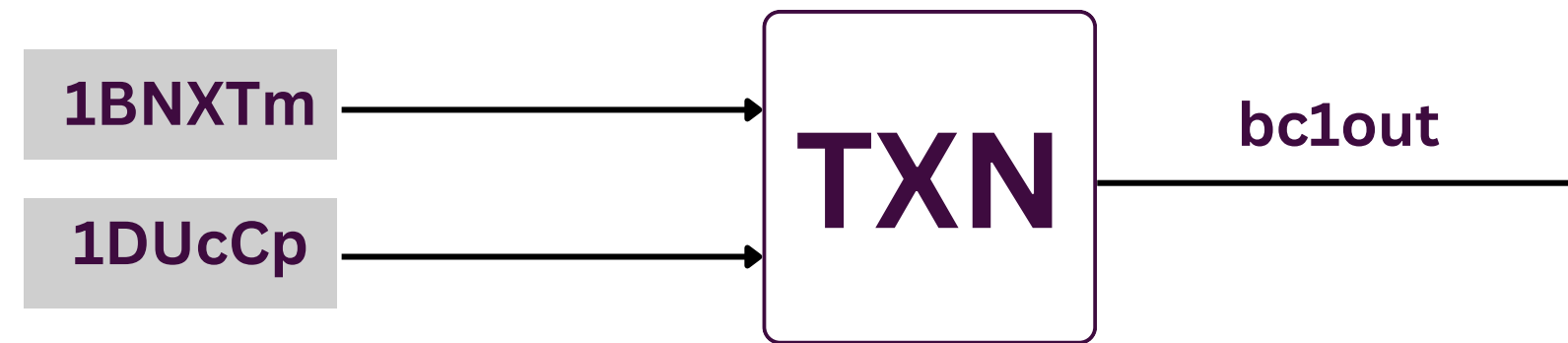
Group Identification: Indicator of Compromise Reuse



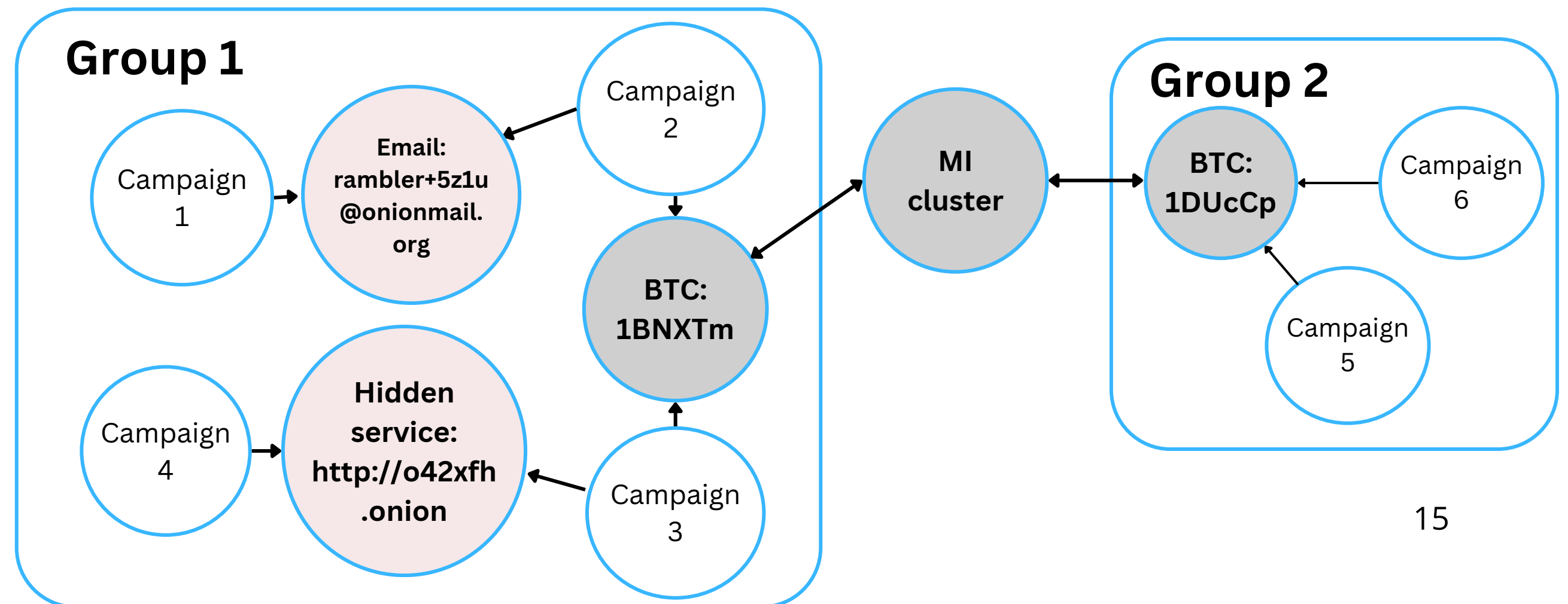
Group Identification: Bitcoin Multi-Input (MI) Clustering



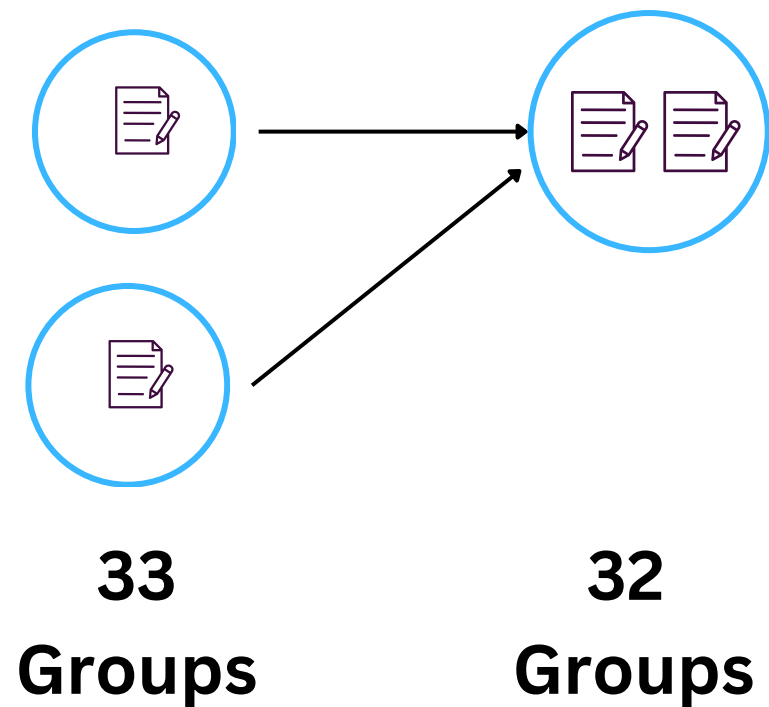
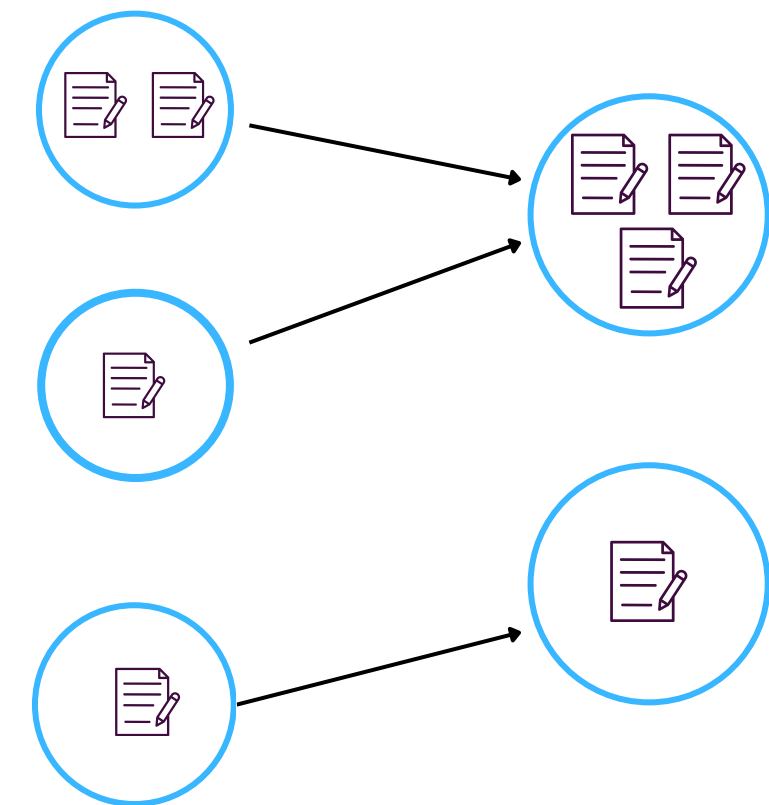
1. Identify MI-clusters using WatchYourBack



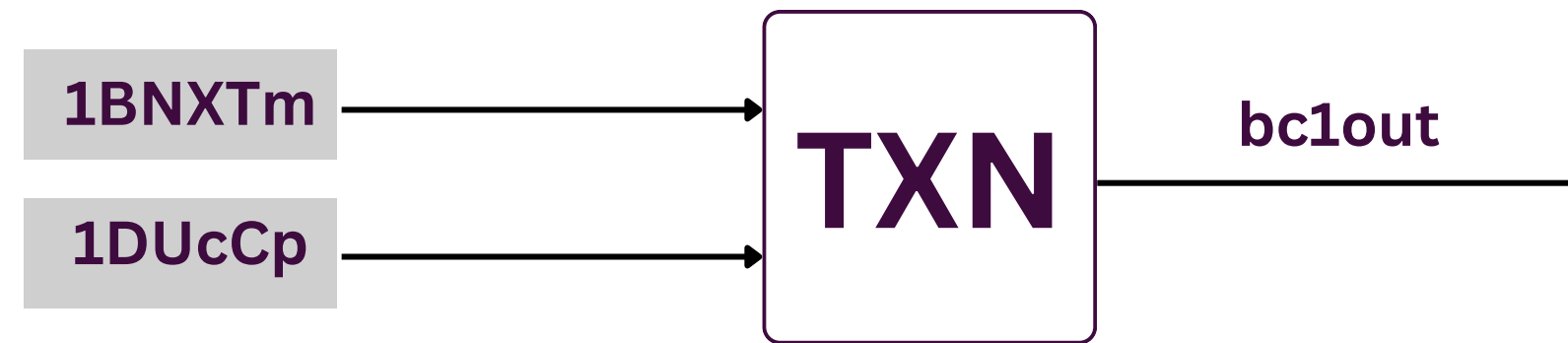
2. Merge groups that belong to same MI-cluster



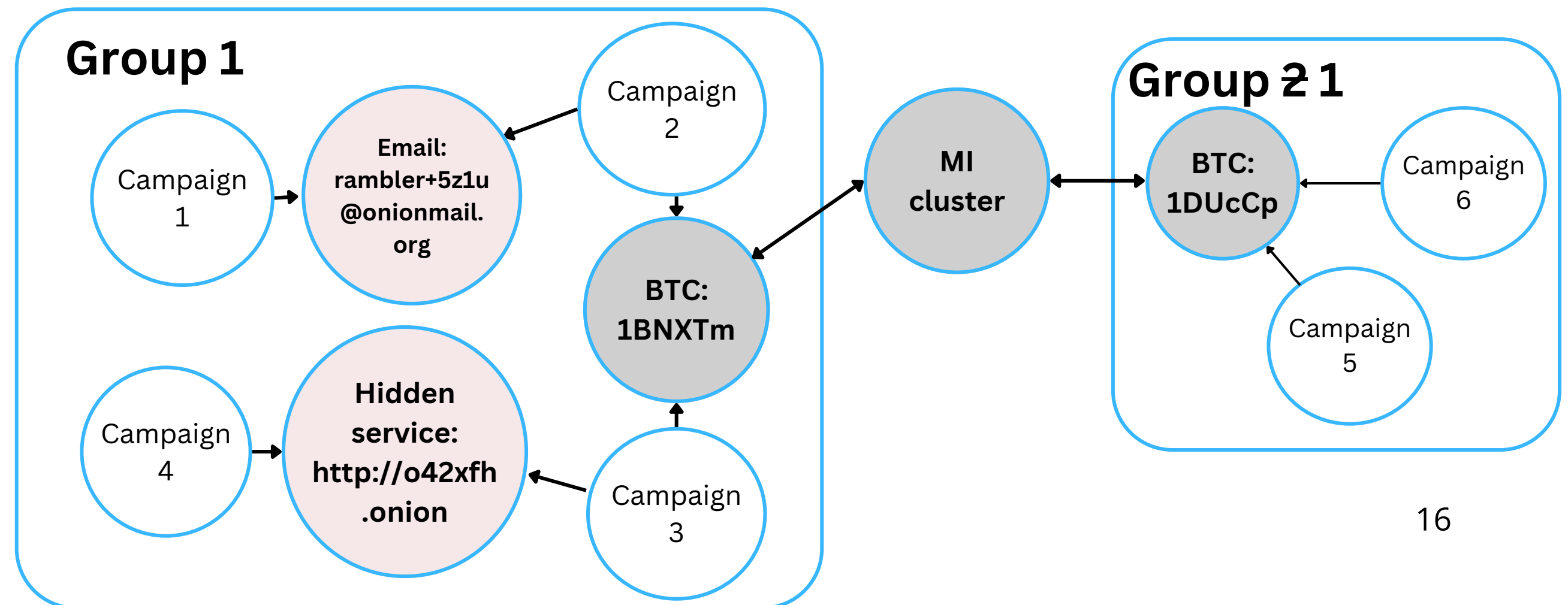
Group Identification: Bitcoin Multi-Input (MI) Clustering



1. Identify MI-clusters using WatchYourBack



2. Merge groups that belong to same MI-cluster



RQ3: Group Comparison



32 groups
\$498K



Specialization



**Geographical
targeting**



Long lifetime

Dominant Group



Active since



Server infections



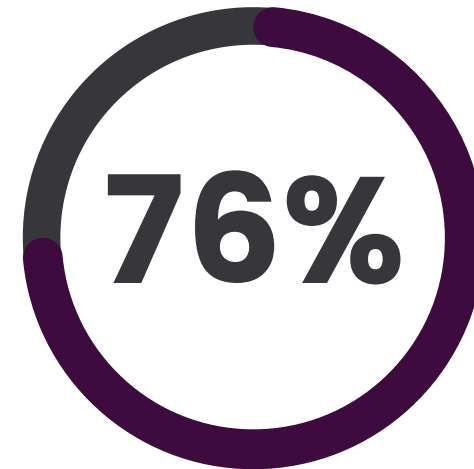
Total revenue

35 campaigns

Dominant Group



Active since



Server infections



Total revenue

35 campaigns



Honeypot group A



Professional group

Dominant Group Links



**2019 Git repositories
attack**



**North Korea
attributed address**

RQ4: Why Do Attacks Keep Happening?



Weak authentication



67% infections



Secure installation

MySQL: 2010 (98%)
ElasticSearch: 2022 (11%)

RQ4: Why Do Attacks Keep Happening?



Weak authentication



67% infections



Secure installation

MySQL: 2010 (98%)
ElasticSearch: 2022 (11%)

Questions?

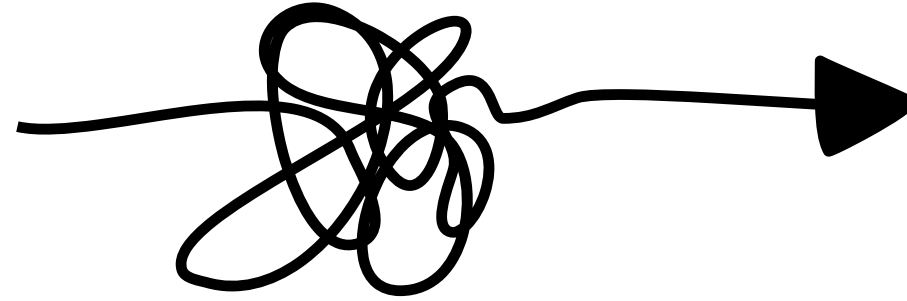
kevin.liebergen@imdea.org

<https://github.com/KevinLiebergen/dbransom>

Backup slides

Discussion 1/3

Evasion techniques



- Not provide ransom payment details

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

- Complicate IOC extraction

..... If we dont receive your payment in the next 10 Days, we will delete or leak your sensitive
information.bc1qvt6d7gjzdvf3ns8nlq56g6pzjmg74exwyu6tf8datarecover@protonmail.com

Discussion 2/3

Lack of ground truth

- Manual analysis
- Perfect precision
- Different campaigns can be grouped -> Fewer campaigns



- Searches Elasticsearch, MySQL, and MariaDB
- Limited by Regex -> May miss infected databases
- Only access unauthenticated DBs

Discussion 3/3

Ethics

- LeakIX collects data from servers
 - Without authentication
- Downloads content from infected tables matching a regex

