IC00AI83 Privacy and Social Engineering

Harsha Gunasekara

Study Right No. 2401908

Week 4: Open-source Intelligence

Task 1: Have I been Pwned

1 A) Looking for leaks

In how many data breaches and pastes can this email be found?

Data breaches - 267 and pastes - 96

What are the compromised data types in the following services?

Bell

- Potential compromised data types in a breach might include
- Customer names and addresses
- Phone numbers and Addresses
- Billing information (credit card nons in some cases, depending on how they are stored)
- Account details (e.g., service plans, call history)
- Login credentials (usernames and passwords)

Drizly

- Potential compromised data types in a breach might include:
- Customer names and addresses
- Email addresses and Phone numbers
- Billing info. (credit card numbers in some cases, depending on how they are stored)
- Payment history
- Order details (e.g., past purchases, delivery locations)
- Login credentials (usernames and passwords)
-

Robinhood

- Potential compromised data types in a breach might include:
- Customer names and addresses (depending on verification requirements)
- Social Security numbers (depending on verification requirements)
- Email addresses and Phone numbers
- Account details (e.g., investment holdings, transaction history)
- Banking information (linked bank accounts for funding)
- Login credentials (usernames and passwords)

1 B) Breach data content

Find at least three of these paid services and list them.

LeakBase - Paid service that provided access to breached data, including email addresses, passwords, and other information. It was shut down in 2017 after facing legal pressure.

WeLeakInfo - Paid service providing access to a vast database of breached data, was shut down by law enforcement in 2020.

DeHashed - Paid service that claimed to provide access to billions of breached records, is now unavailable and its status remains unclear.

Write a short answer (150-200 words) of your thoughts. There might not be a correct or incorrect answer, but you need to make arguments.

Making all breach data publicly searchable creates significant risks. While transparency is valuable, freely available information can be misused for identity theft, social engineering scams, or even blackmail. Verifying accuracy of such a huge amount of data would be difficult. Removing all breach data entirely might be unrealistic. Even with takedown requests, copies might linger online. This leaves users with limited options for verifying the scope of a breach or taking action. A potential solution could be a permissioned system. Users could verify their identity to access a platform shows confirmed breaches involving their data. This empowers users with knowledge while limiting access to malicious actors.

Public awareness of breaches can definitely change user behavior. Transparency can encourage stronger passwords, multi-factor authentication, and a more cautious approach to online services. Multifaceted approach might be best. Can strive for a balance between user awareness, data security, and responsible breach notification by companies. Focusing on removing the most damaging breaches while offering verified breach information to affected users could be a productive starting point.

Task 2: Hardcoded Passwords

Hex-Rays

8.4.0.240320

```
49  __int64 (__fastcall *_frame_dummy_init_array_entry)() = &frame_dummy; // weak
50  __int64 (__fastcall *_do_global_dtors_aux_fini_array_entry)() = &_do_global_dtors_aux; // weak
51  void *_dso_handle = &_dso_handle; // idb
52  char *secret = "aQLpavpKQcCVpfcg"; // idb
53  _UNKNOWN _bss_start; // weak
54  FILE *stdout; // idb
```

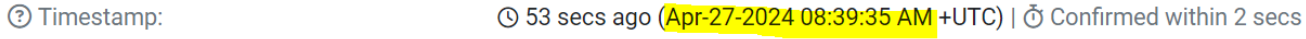
Task 3: OSINT exploitation

Task 4: Blockchain

Provide the following information:

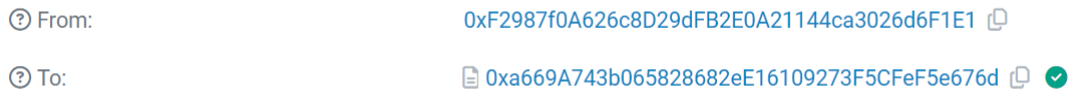
Transaction:

- Date and Time of the transaction -



- of the transaction -

- Address of sender and Address of receiver -



- Transaction fee amount in bitcoin -

Receiver Address:

- Who was the owner of this address? Use OXT.me and Google to figure out the real name of the user

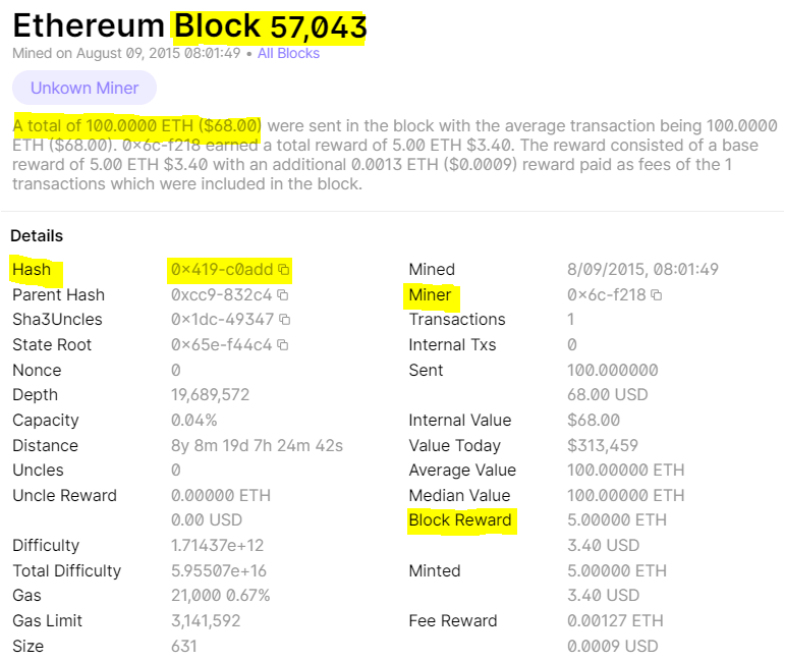
https://coinmetrics.io/

Nic Carter and Aleksei Nokhrin

- The owner instantly divided and forwarded the 10,000 to (how many?) other addresses
- Addresses that received the 10,000 bitcoin and the corresponding sums to each address
  Unable to access/ not working, https://oxt.me/

Block

- Hash of the block 57043
- Amount of transactions in the block
- Block reward amount



Ethereum Block 57,043

Mined on August 09, 2015 08:01:49 • All Blocks

Unkown Miner

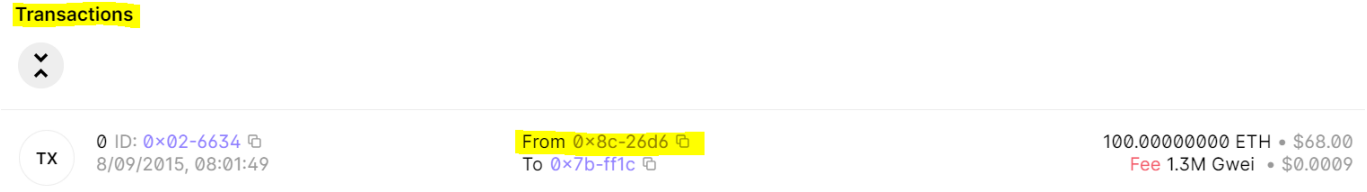
A total of 100.0000 ETH ($68.00) were sent in the block with the average transaction being 100.0000 ETH ($68.00). 0×6c-f218 earned a total reward of 5.00 ETH $3.40. The reward consisted of a base reward of 5.00 ETH $3.40 with an additional 0.0013 ETH ($0.0009) reward paid as fees of the 1 transactions which were included in the block.

Details

Hash	0×419-c0add	Mined	8/09/2015, 08:01:49
Parent Hash	0xcc9-832c4	Miner	0×6c-f218
Sha3Uncles	0×1dc-49347	Transactions	1
State Root	0×65e-f44c4	Internal Txs	0
Nonce	0	Sent	100.000000
Depth	19,689,572		68.00 USD
Capacity	0.04%	Internal Value	$68.00
Distance	8y 8m 19d 7h 24m 42s	Value Today	$313,459
Uncles	0	Average Value	100.00000 ETH
Uncle Reward	0.00000 ETH	Median Value	100.00000 ETH
	0.00 USD	Block Reward	5.00000 ETH
Difficulty	1.71437e+12		3.40 USD
Total Difficulty	5.95507e+16	Minted	5.00000 ETH
Gas	21,000 0.67%		3.40 USD
Gas Limit	3,141,592	Fee Reward	0.00127 ETH
Size	631		0.0009 USD

Miner

- Address of the miner for block 57043
- Has this address spent the block reward they received? Yes



Transactions

TX

0 ID: 0×02-6634
8/09/2015, 08:01:49

From 0×8c-26d6
To 0×7b-ff1c

100.00000000 ETH • $68.00
Fee 1.3M Gwei • $0.0009