Anatomy of a High-Profile Data Breach

Dissecting the Aftermath of a Crypto-Wallet Case

Svetlana Abramova, Rainer Böhme

32nd USENIX Security Symposium · Anaheim, CA · 9 August 2023

Why Study High-Profile Data Breaches ?

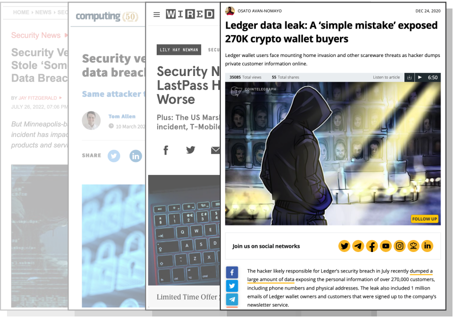
Measure harm

Examine consumer sentiments

Understand response behavior

"High-profile" breaches affect security vendors.

- Stepping stones for future attacks
- Barely covered in breach research



HOME › NEWS › SEC

Security News ▸

Security Ve
Stole 'Som
Data Breac

BY JAY FITZGERALD ▸
JULY 26, 2022, 07:06 PM

But Minneapolis-b
incident has impac
products and servi

computing (50)

Security ve
data breacl

Same attacker t

Tom Allen
10 March 202

SHARE

WIRED

LILY HAY NEWMAN SECU

Security N
LastPass H
Worse

Plus: The US Marsl
incident, T-Mobile

Limited Time Offer

OSATO AVAN-NOMAYO DEC 24, 2020

Ledger data leak: A 'simple mistake' exposed 270K crypto wallet buyers

Ledger wallet users face mounting home invasion and other scareware threats as hacker dumps private customer information online.

35085 Total views 55 Total shares Listen to article 6:50

Join us on social networks

The hacker likely responsible for Ledger's security breach in July recently dumped a large amount of data exposing the personal information of over 270,000 customers, including phone numbers and physical addresses. The leak also included 1 million emails of Ledger wallet owners and customers that were signed up to the company's newsletter service.

Case in a Nutshell

Customer data leaked in the second half of 2020

First and last names, postal and e-mail addresses as well as phone numbers were exposed.

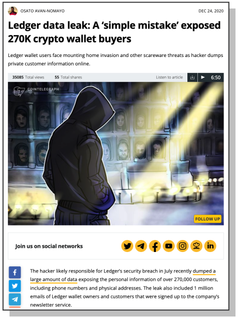
Most victims are **crypto-asset owners**.

- Attractive targets for fraudsters
- Affluent, tech-savvy and mistrustful at times

  [Abramova et al., 2021; Lindqvist et al., 2021]
- Hard-to-reach community for behavioral research

  [Abramova et al., 2021]

Nano S crypto-wallet



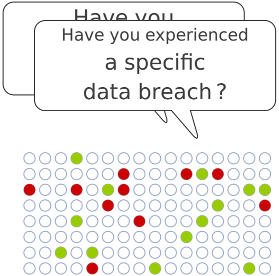
OSATO AVAN-NOMAYO DEC 24, 2020

Ledger data leak: A ‘simple mistake’ exposed 270K crypto wallet buyers

Ledger wallet users face mounting home invasion and other scareware threats as hacker dumps private customer information online.

The hacker likely responsible for Ledger’s security breach in July recently dumped a large amount of data exposing the personal information of over 270,000 customers, including phone numbers and physical addresses. The leak also included 1 million emails of Ledger wallet owners and customers that were signed up to the company’s newsletter service.

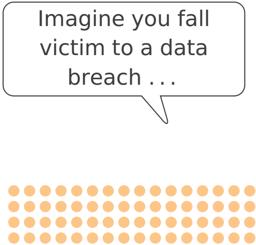
Sampling Victims of a Data Breach



Have you

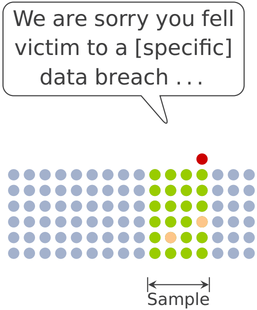
Have you experienced a specific data breach ?

Population



Imagine you fall victim to a data breach . . .

Convenience sample



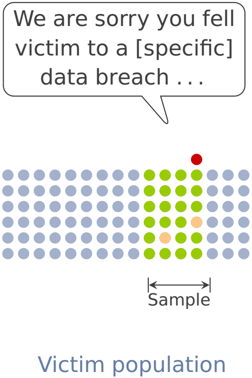
We are sorry you fell victim to a [specific] data breach . . .

Victim population

Legend: ● high validity, ● medium validity, ● low validity (noise)

Sampling from Leaked Datasets

Many legal and ethical questions, but little guidance . . .



We are sorry you fell victim to a [specific] data breach . . .

Sample

Victim population

Recruiting with Leaked E-Mail Addresses

Legal aspects

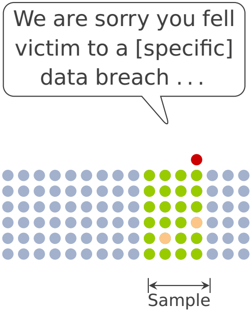
Jurisdiction: EU with GDPR [Article 6, p. 1(e) GDPR]

- **Solicitation:** legitimate interest if *“processing is necessary for the performance of a task carried out in the public interest”*, such as academic research.
- **Survey:** explicit consent

Ethical aspects

We compared benefits and risks. [The Menlo report, 2012]

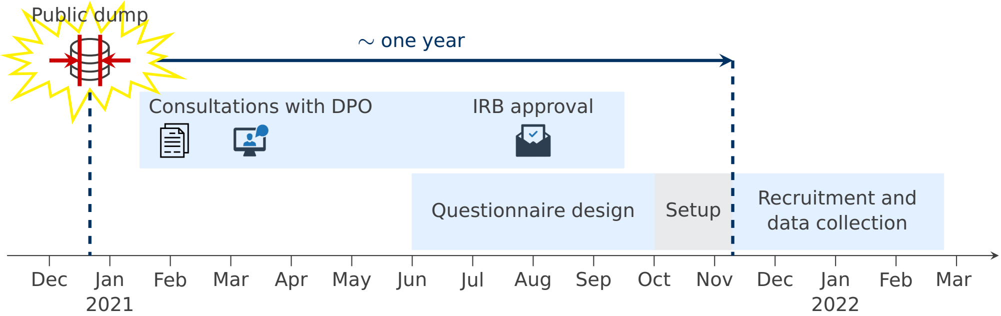
- Necessity (sample size !) and absence of other means.
- Risks and mitigation strategies for the stakeholders


We are sorry you fell victim to a [specific] data breach . . .
Sample

Victim population

Many details in the paper !

Timing of Research



- ∼ 32k non-personalized, one-off e-mails (11.7% of the leaked records)
- No reminders & no compensation
- 104 responses after data cleaning (0.34% response rate)

Why Study High-Profile Data Breaches ?

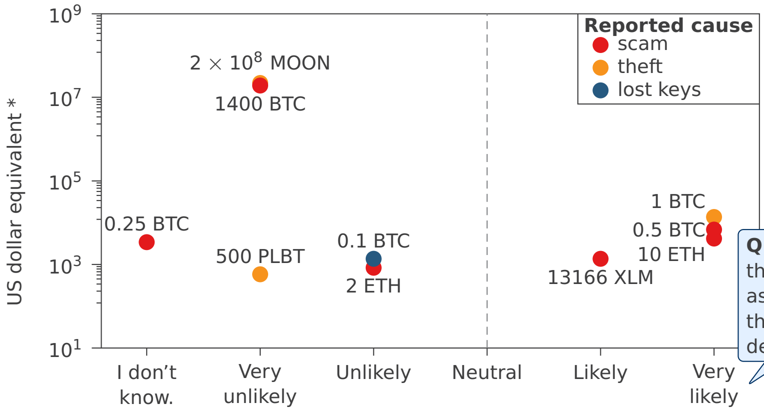
Measure harm

Examine consumer sentiments

Understand response behavior

Losses of Digital Assets

A few victims report financial losses, of which very few are ***likely*** caused by this breach.



Q: How likely is it that the loss of crypto-assets was caused by the data breach incident?

* Own conversion using the average market price of a cryptocurrency in the second half of 2020 as baseline.

Why Study High-Profile Data Breaches?

Measure harm

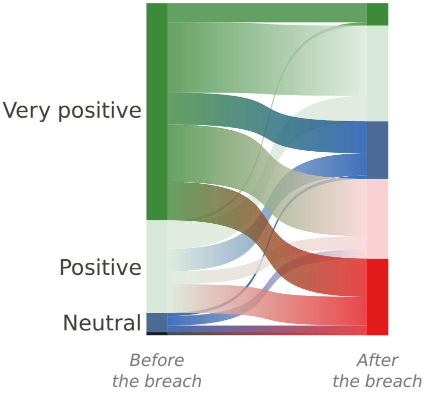
Examine consumer sentiments

Understand response behavior

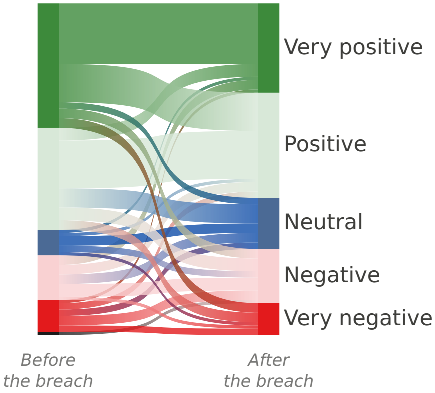
Changes in Consumer Attitudes

Surveyed victims differentiate between **vendor reputation** and **product security**.

Attitudes toward the vendor



Attitudes toward the product



Wilcoxon rank sum test: $p < 0.001$ – toward the vendor, $p = 0.095$ – toward the product

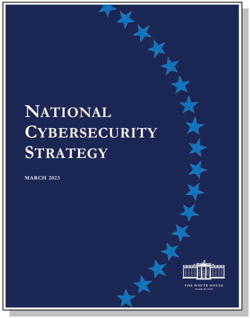
Why Study High-Profile Data Breaches ?

Measure harm

Examine consumer sentiments

Understand response behavior

“[We must] reshape laws that govern liability for data losses and harm caused by cybersecurity errors.”



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

WASHINGTON

Litigation Efforts

Surveyed victims appear **skeptical** about the success of litigation.

Harm is already done.

Too much effort with little perspective of success.

Time and money needed would not hold up against potential benefits.

Lessons We Learned

No ‘smoking gun’ is found in the aftermath of this breach.

Survey instrument: always ask for one’s confidence and differentiate harms as granular as possible (e. g., e-mail vs. phone scams)

Our risk analysis missed some unanticipated (small) costs on the stakeholders.

Sampling from leaked datasets is feasible, yet consumes time and effort.

universität innsbruck

Thank You for Your Interest !

Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case

Svetlana Abramova, Rainer Böhme

32nd USENIX Security Symposium · Anaheim, CA · 9 August 2023