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

Svetlana Abramova: Anatomy of a High-Profile Data Breach – Dissecting the Aftermath of a Crypto-Wallet Case
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]
Sampling Victims of a Data Breach

Have you experienced a data breach?

Imagine you fall victim to a data breach...

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

Population

Convenience sample

Victim population

Legend: ● high validity, ○ medium validity, • low validity (noise)
Sampling from Leaked Datasets

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

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

Svetlana Abramova: Anatomy of a High-Profile Data Breach · Dissecting the Aftermath of a Crypto-Wallet Case
Changes in Consumer Attitudes

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

**Attitudes toward the vendor**
- **Before the breach**: Neutral, Positive, Very positive
- **After the breach**: Neutral, Positive, Very positive

**Attitudes toward the product**
- **Before the breach**: Very negative, Negative, Neutral, Positive, Very positive
- **After the breach**: Very negative, Negative, Neutral, Positive, Very positive

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

Svetlana Abramova: Anatomy of a High-Profile Data Breach · Dissecting the Aftermath of a Crypto-Wallet Case
Litigation Efforts

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

- Too much effort with little perspective of success.
- Time and money needed would not hold up against potential benefits.
- Harm is already done.
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.
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