Mt. Gox Bitcoin Theft Case Study

Bastian Tenbergen

April 2021

Mt. Gox Bitcoin Theft Case

Background

In 2011, the Japan-based company and then-largest Bitcoin transaction processor Mt. Gox experienced a series of different security breaches that allowed thousands of bitcoins to be stolen with customer accounts, and millions of bitcoins more to be invalidated due to loss of private key information. These events unfolded a series of complications, including inabilities to meet newly issued privacy regulation in 2013. Moreover, in 2014, Mt. Gox announced their inability to "locate" over 7% of the universally finite amount of Bitcoin and admitted the possibility that these bitcoins may have been stolen by hackers. Damages exceed $473 million US. In May 216, Mt. Gox announced that creditors impacted by previous years' losses and thefts asking more than $2.4 trillion US in damages, rendering the company bankrupt.

Case Study Overview

The 2011 and 2014 bitcoin losses seem to have used different vectors of attack. Rather than financial and/or legal implications mostly discussed in available resources, this case study aims at technical reasons and possible mitigations for these hacks.

Student Instructions

Part 1

There are at least three different vectors of attack that were used in the theft of Bitcoin. Describe the attack vectors, malware used (if available, else give examples of suitable programs), and how Mt. Gox took notice of the attack.

Part 2

For each vector of attack from Part 1, define appropriate countermeasures. Explain how the countermeasures will disrupt malicious activity.

Part 3

Explain why Mt. Gox was unable to retrieve stolen funds. Describe how law enforcement and governmental oversight agencies aim to track down key actors in the theft.

Instructor notes

This case study may be assigned as an individual or team exercise, either in synchronous or asynchronous educational settings. A proven strategy is "Think-Pair-Share": use a similar CyBOK case study (Wilson et al. 2018) to discuss CyBOK KAs in class, then group learners into small teams of 2-3 and ask them to solve this assignment. Then, in a following class meeting, have teams present results and discuss implications.

The Mt. Gox case touches upon virtually every Knowledge Area of CyBOK, however with special emphasis on the Topic Areas outlined above.

Since this case study is in three parts, it could possible also be assigned as a term project or (asynchronous) exam. We recommend giving users at least the Wikipedia reference from the reference list below. At the time of writing, the Mt. Gox Wikipedia article references some of the most details and trustworthy articles on the subject. Remaining references below give the details outlined in the Example solution, however students might be able to find more and different solutions.

Example solution

Part 1

- Compromisation of User Passwords allowing user funds to be exchanged into Bitcoin, which were then withdrawn
    - Access logs showed successful log-in attempts on first try
- CSFR Exploit allowed theft of ca. 60,000 user account details from Mt. Gox database, sale to highest bidder
    - Mt. Gox did not notice until hacker offered database for sale on pastebin
- Disassociation of Private Keys from Blockchain
    - Two dozen transactions sent Bitcoin to invalid email addresses, thereby invalidating private key
    - all impacted bitcoin were in roughly sequential order within Block 150951, which is anomalous

Part 2

- Two-factor authentication will prevent malicious actors to gain access to an account even if they possess the user password. Two-factor authentication relies on having a second mode of authentication, e.g., a physical device such as a cell phone, which a hacker would need to steal as well before gaining access.
- CSRF stands for Cross-Site-Request-Forgery. A hacker sets up a vulnerable site and redirects the user to the site under control of the hacker. The hacker motivates the user to carry out regular activities (such as login in) or unintentional activities (e.g., showing a fake "password reset" page) to gain access to one or more users. Preventing CSRF requires hardened API endpoints and/or proper cookie-based session handling.
- Disassociation of private keys is a side-effect of missing node-side private key validation. While bitcoin clients perform private key validation, transaction nodes do not. This is a

weakness in the Bitcoin blockchain protocol. Stricter implementation by enforcing intranode key validation is required to harden the protocol and thereby prevent sending bitcoin to invalid recipient addresses.

Part 3

- It is unclear if Mt. Gox was able to retrieve stolen funds. The company effectively blamed the user for allowing their passwords to be stolen, assuming no responsibility. However, their weak authentication system made the theft possible.
- According to the hacker who claimed to have stolen the user account database, the CSRF vulnerability was closed by the time the individual offered the database for sale. Presumably, Mt. Gox informed the users and motivated them to change their passwords, however time delay between theft, user notification, and user action likely resulted in damages to occur even more. The nature of bitcoin makes thus-legal transactions valid; bitcoins were laundered by at least one individual associated with various bitcoin recipient accounts, per US Federal Investigators.
- Disassociation of private keys irretrievably destroys the bitcoin to the nature of the cryptographic algorithm.

References

Wikipedia: "Mt. Gox," online resource available at: https://en.wikipedia.org/wiki/Mt._Gox, no year. Accessed: 7 March 2021

Nilsson, K.: "The Missing MtGox bitcoins," online resource available at: https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html, 2015. Accessed 8 Feb 2021.

Dougherty, C. and Huan, G.: "Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss," online resource available at: https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy, 2014. Accessed 16 Feb 2021

Tabbaa, B.: "the Mt. Gox Hack – What's in your Bitcoin Wallet?," online resource available at: https://medium.com/dataseries/the-rise-and-fall-of-mt-gox-whats-in-your-bitcoin-wallet-bd5eb4106f4e, 2018. Accessed 11 March 2021.

Lee, T.: "Feds say they caught a key figure in the massive Mt. Gox Bitcoin hack," online resource available at: https://arstechnica.com/tech-policy/2017/07/feds-indict-a-leading-bitcoin-exchange-for-money-laundering/, 2017. Accessed 15 Feb 2021.

Wilson, K.; Brickman, P; Brame, C: Group Work. Life Sciences Education 17(1), 2018.