Analysis on Ronin Network Security Incident

LING Shengchen
Department of Computer Science
City University of Hong Kong
Hong Kong SAR, China
shengling2-c@my.cityu.edu.hk

***Abstract*—This article focuses on the security incident of Ronin Network, a typical decentralized finance (DeFi) security incident in the blockchain world. Firstly, this article introduces the brief summary and background of the incident, then make an in-depth discussion and analysis on how the attack happened, the countermeasures taken and inspirations for common users. Last, this article also gives some analysis of DeFi security development.**

Keywords—Blockchain, Decentralized Finance, Private Key, Whitelist, Phishing

I. Introduction

On March 29, 2022, Ronin Network, the Axie Infinity sidechain, issued a community alert about a security vulnerability incident, a total of 173,600 ETH and 25.5M USDC were stolen from Ronin Bridge [1], which equaled to more than $610 million at that time. The loss of this incident is even greater than that of the Poly Network hack in 2021, which lost over $600 million.

Notably, the hack occurred on March 23, but not being officially claimed discovery until some users reported that they were unable to withdraw 5,000 ETH from the bridge.

II. Background

A. Blockchain and DeFi

In November 2008, Satoshi Nakamoto published the famous article *Bitcoin: A Peer-to-peer Electronic Cash System*, which marked the birth of blockchain technology [2]. In the article, Satoshi Nakamoto elaborated the electronic cash concept system based on P2P network, cryptography, time stamp, blockchain and other technologies.

With the birth of smart-contract-chains represented by Ethereum and the development of cryptocurrencies, the crypto economy booms out there, as well as decentralized applications (DApp) and decentralized finance (DeFi), where you can lend, borrow, long/short, earn interest, and more.

Unfortunately, security incidents are accompanied by its growing popularity. According to the data from Liyi Zhou and Xihan Xiong [3], users, liquidity providers, speculators, and protocol operators suffered a total loss of at least $3.24 billion from April 30, 2018, to April 30, 2022.

B. Cross-chain Bridge Security

With the advancement of blockchain-related technology, cross-chain asset transfers and smart contracts interactions have become commonplace on the blockchains, which naturally leads to the security incidents of cross-chain bridges. There are several schemes to design a cross-chain bridge system, including Notary schemes, Sidechains/Relays and Hash-Locking, but none of them can avoid a relatively centralized mode.

According to the statistics by Dune Analytics, the total value locked (TVL) of Ethereum's 15 biggest cross-chain bridges was about $7.12 billion dollars as of Sept. 11, despite a 22% decrease in the last 30 days [4].

Because of the high quantity of liquidity and low degree of decentralization, cross-chain bridges have been deemed a "sweet spot" in the eyes of hackers. As of June 2022, there were seven cross-chain bridge security incidents, with losses totaling $1.043 billion, accounting for 64% of DeFi's total losses and 53% of total losses overall in the half past year [5].

Cross-chain bridges, as a crucial infrastructure of the multi-chain ecosystem, bear a large amount of capital flow and provide considerable ease to consumers. However, it poses numerous security and decentralization challenges, necessitating projects to increase its security, risk management, and other capabilities.

C. Ronin Network and Ronin Bridge

Ronin Network is an Ethereum sidechain created specifically for the leading GameFi, Axie Infinity, see in Fig.1. Sky Mavis, the team of Axie Infinity, wanted a reliable, fast and cheap network as a stable infrastructure that would support the game's future development. Thus, the Ronin Network was born.

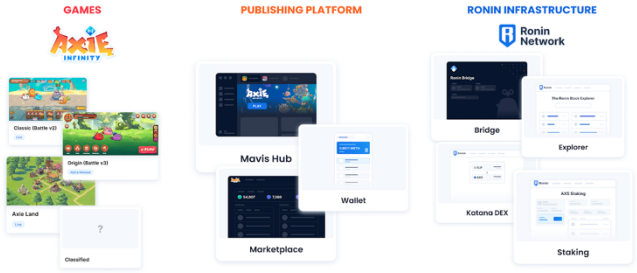

Fig. 1. Ecosystem of Ronin Network

The Ronin bridge is a cross-chain bridge of Ronin Network, mainly for transferring assets between Ronin and Ethereum. In this case, the stolen assets are from this bridge.

III. In-depth Discussion

A. Details about the Attack

This attack can be traced back to November 2021. At that time, Sky Mavis asked Axie DAO for assistance in distributing free transactions (transactions without paying gas fees). Considering the high volume of users and transactions, the Axie DAO whitelisted Sky Mavis for convenience, allowing it to sign various transactions on its behalf.

This demand ended in December 2021; however, the authentication was not cancelled, which formed a security vulnerability violating confidentiality. This means that once the attacker got access to Sky Mavis systems, they were able to sign the transactions on Axie DAO's behalf, directly from the Axie DAO validator nodes.

Therefore, the hackers implemented constant spear-phishing attacks on Sky Mavis employees [6], and eventually one of them was breached. Then the hackers penetrated Sky Mavis' IT infrastructure via the employee's access and gained access to four validator nodes.

They also found a backdoor of gas-free RPC node, offering them the fifth signature from the Axie DAO validator. However, the team did not disclose more details about the backdoor.

The Ronin Network totally consists of nine validator nodes and requires at least five signatures to identify a transaction. But unfortunately, the attackers still successfully gained control of five private keys of validators and forged the fake withdrawals, as is shown in Fig.2.

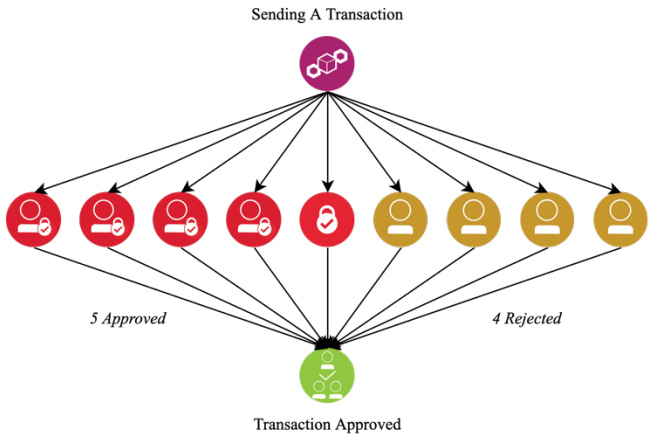

Fig. 2. The nine validators' condition when got hacked

The attackers used compromised private keys to establish withdrawals in two normal transactions, so it can also be considered as a private key leaking incident.

B. Countermeasures

After discovering the incident, the Ronin team has taken a series of actions to reduce users' further loss as far as possible, including:

1) cancelled the authorization of the four validator nodes controlled by Sky Mavis, which is the direct source of this incident.

2) increased the validator threshold from five to eight. Even if the hackers have owned five private keys, they still must get 3 more to implement another attack. This action can also result in some other transactions cannot get approved because of their fuzzy attributes or network delay.

3) migrated the nodes to brand-new physical machines, making them completely separated from old infrastructures, to prevent any possible risks from the hardwares.

4) temporarily paused Ronin Bridge and Katana DEX to ensure no more assets can be transferred out of Ronin Network, it actually frozened the capital flow between the network and other blockchains.

5) working with Chainalysis to monitor the stolen funds. Thanks for the transparency of blockchain, the funds can easily be monitored by anyone, and the transactions are open to the public.

Ronin Network then cooperated with U.S. government agencies including the FBI and other centralized and decentralized exchanges like Binance and Huobi, eventually identified the hackers and get the assets restored.

Fig.3 shows the screenshot of hacker address on Etherscan, a blockchain explorer of Ethereum. Up to Sept. 11th, the address balance is less than 1.80 Ether [7].

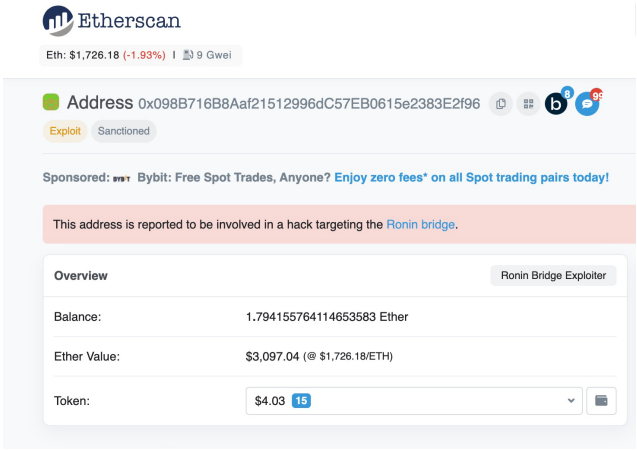

Fig. 3. Screenshot of hacker address on Etherscan

The Ronin team also conducted more countermeasures to further strengthen the security level of Ronin Network, for the purpose that similar incidents will not happen again:

1) implemented a network hardfork (a network upgrade of blockchain that old proposal will be incompatible with the new version), requiring all operators of validator nodes to update their node programs.

2) conducted three independent audits for the Ronin Bridge, including one internal audit and two external audits, led by Verichains and Certik.

3) increased the number of validator nodes from 9 to 14, and planed to further increase to 21 in the next three months, with the long-term goal of over 100 nodes.

4) implemented stricter internal management and review within the team.

IV. Analysis

A. Factors Leading to the Attack

1) *Improper whitelist management*

The improper whitelist management is of utter importance.

Firstly, as for protocols of public chains, it's not very often seen that the validators directly authenticate the permission of signature to a team or organization, especially only for sending transactions, which is a quite simple on-chain operation that can be addressed via smart contracts.

Secondly, whitelist authentication is a much too significant permission on the security of the network, the whole process and real-time status should have been paid close attention to, and the authentication should have been revoked as soon as it discontinued.

2) *Ignorance of the spear-phishing attacks*

The employee who fell into the phishing trap is another importance point. It's quite common to receive phishing emails, phonecalls and texts, but as for part of Sky Mavis system, employees should receive more numerous and more rigorous security trainings. After receiving massive amount of phishing messages in a short period of time, the whole team should have been on the alert and even taken some necessary precautions to prevent such incidents.

On Sept.7, 2022, USTC held a phishing email anti-scam drill, to test and remind students and staffs about the phishing attacks, which triggered a heated discussion.

3) *Lack of monitoring and alarm mechanism*

The attack actually occurred on March 23, but the team did not discover it until users reported unavailability of withdrawal 6 days later, on March 29. This demonstrates that the bridge, even the whole network, lacks a systematic monitoring and alarm mechanism to discover potential risks, and it might be better if giving special concern on transfers of large amounts of assets.

With a monitoring and alarm mechanism, the team can not only be informed of petential assets loss and abnormal behaviors on-chain, but also some other security warnings and analysis.

B. Precautions for Common Users

1) *Focus on DApp security*

There's no denying that it's quite hard for common users to discriminate whether a DApp is rather secure or not before using it. Despite most DApps claim open-source and welcome to check, the overwhelming majority of users do not have the capacity, or time, or willingness to check the source codes. Nonetheless, we can still check whether the DApp has been audited by authoritative auditing institutions like Certik, or introduced or recommended by some trustworthy KOLs.

2) *Protection of private keys*

It's significant for DApp teams to ensure the security of private keys, as well as for common users. The simplest and safest way is to write down your private keys or mnemonic words on a piece of paper and never send them via Internet. Some advanced ways such as hardware wallets or multi-sig wallets are also available options.

V. DeFi Security Future Development

Even it can be said that by far the most successful transition of roles from Web2 to Web3 has been hacking [8]. Thus, given the blockchain's transparency and increasing incident frequency, we can, and need to systematically measure, evaluate, and compare DeFi incidents.

A. Classifications of DeFi Security

In 2021, Sam M. Werner devided DeFi security into two classes: technical security and economic security [3]. The technical security means an agent can directly exploit the technical structure of a blockchain system including smart contract vulnerablities, while the economic security means manipulating the incentive structure and token-economy model of the protocol.

One year later, Liyi Zhou and Xihan Xiong proposed a more concrete description [9]. A security incident refers to unexpected asset loss on blockchain to some certain entities, which can be devided into two parts: attack and accident. An attack requires adversaries to exploit vulnerabilities and weaknesses aiming at disabling or alterring information, systems or other expected states. On the other hand, an accident may not involve adversaries, some design or logical flaws can still lead to bad results.

B. Future Development

As for technical security, the basic technical route and technology stack are gradually stablizing, and so many security teams are working on it, thanks to the Ethereum developer community and ecosystems. It means that the technical security risk will get lower as the time goes.

Nonetheless, we definitely should not ignore the emerging solutions, regardless of new blockchain structures like Aptos [10] and Sui, or new programming languages like Move [11]. New tools will not only bring developers convenience and effiency, but also new unknown risks.

As for economic security, the financial and economic traits give it more possibilities in both positive and negtive aspects, the high incentives attract both 'whitehats' and hackers.

The basis of blockchain system is that the system, so as the smart contracts, can run automately and cannot be modified or paused by any party, but taking human-beings into account may trigger more variables. Kelsie Nabben proposed an interesting concept named *People Security*, applying sociotechnical security to blockchain [12], offering an unique view that the differenciality of people's demands may lead to various cognition and definition of threats and risks.

References

[1] Ronin Network, "Community Alert: Ronin Validators Compromised", https://roninblockchain.substack.com/p/community-alert-ronin-validators.

[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf.

[3] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, “SoK: Decentralized Finance (DeFi) Incidents”, http://arxiv.org/abs/2208.13035, 2022-08-27.

[4] Dune, Ethereum Bridge Total TVL, 2022-09-11, https://dune.com/queries/145010/285622.

[5] SlowMist, “2022 Mid-Year Blockchain Security and AML Analysis Report”, https://www.slowmist.com/report/first-half-of-the-2022-report(EN).pdf.

[6] Ronin Network, “Back to Building: Ronin Security Breach Postmortem”, https://roninblockchain.substack.com/p/back-to-building-ronin-security-breach.

[7] Etherscan,https://etherscan.io/address/0x098B716B8Aaf21512996dC57EB0615e2383E2f96.

[8] Yuxian's Homepage, https://weibo.com/u/1652595727.

[9] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, SoK: Decentralized Finance (DeFi) [J/OL], http://arxiv.org/abs/2101.08778, 2021-09-26.

[10] Aptos Labs, “Aptos Developer Documentation”, https://aptos.dev/.

[11] Damir Shamanaev, “The Move Programming Language”, https://move-book.com/.

[12] K. Nabben, “Blockchain Security as ‘People Security’: Applying Sociotechnical Security to Blockchain Technology”, Frontiers in Computer Science, 2021-03-22.