Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Analysis of the "Dandruff Attack" on the Tron Network: Risks, Damage Assessment, and Solutions

Dmitry Mikhaylov[1*], Andrei Kutin[2], Joseph Anderson[2], Maxim Falaleev[2]
[1]National University of Singapore, Singapore.
[2]Match Systems, United Arab Emirates.

Received 31 Mar. 2023; Accepted 11 Jun. 2023; Available Online 22 Jun. 2023

Abstract

This study, conducted by employees of Match Systems in November-December 2022, presents a subjective opinion on the potential involvement of certain addresses and transactions in suspicious activity. This research was initiated in response to reports from Match Systems' clients, that identified a new pattern of network attacks distinct from the well-known "Dust Attacks." The study relies solely on publicly available data and does not incorporate any additional information. The assessment and conclusions drawn are based on observed patterns of suspicious activity and have not been corroborated by court decisions or law enforcement agencies. The findings of this study do reveal the existence of a new threat, that has had detrimental effects on numerous users who have experienced frustration and financial losses. The study also offers recommendations for users to safeguard themselves and their funds. It is important to note that because of the subjective nature of this study, it should be taken into consideration alongside other sources of information. Careful analysis is necessary before implementing any actions based on its findings. Furthermore, given the constantly evolving landscape of cyber threats, individuals and organizations must remain vigilant and stay informed about the latest threats and best practices for protecting their assets.

I. Introduction

Blockchain is considered a secure technology. The payment is not fraudulent, and the matter cannot be changed. However, even such a seemingly reliable system has some technical weaknesses. The threat of web attacks has revealed itself. As an example, in the early summer of 2022, a large number of Tron blockchain users reported receiving insignificant receipts from unknown addresses [1], [4]-[6]. This phenomenon was observed across the network, and a significant proportion of the transactions involved TRX and Tether (USDT) assets. While this type of attack did not have a specific name at first, it was commonly referred to as a "dust attack" due to its similarity to a similar type of attack observed on the Bitcoin (BTC) network[7]-[9].

However, it soon became apparent that this new attack differed from traditional dust attacks. As a result, a new name was required to differentiate it.

Keywords: dandruff attack, dust attack, network, tokens.

Production and hosting by NAUSS

* Corresponding Author: Dmitry Mikhaylov
Email: Mr.Dmitry.Mikhaylov@gmail.com
doi: 10.26735/KQGU9199

The research team behind this study has adopted the working name "dandruff attack" for this new form of attack, while the small transactions involved are referred to as "dandruff". While each issue may seem innocuous on its own, when combined, these attacks can have serious consequences for network performance, privacy and productivity.

It is important to note that while the naming of attacks can help to clarify the types of threats faced by a network, it is only one aspect of the overall response [11]. To effectively combat such attacks, a thorough understanding of the techniques used by attackers and the vulnerabilities in the network is essential. Additionally, implementing robust security measures and staying informed about the latest threats and best practices is crucial for minimizing the risk of such attacks [12],[14].

This study gives a thorough examination of the impact of 'dandruff' assaults on blockchain networks. We investigate the mechanics of dandruff attacks, including their motivation, mode of execution, and probable effects. By associating addresses and tracing transactions, we investigate how dust attacks might be used to breach user privacy.

We highlight open difficulties and future research prospects in the topic of dandruff attacks on blockchain networks. These include investigating machine learning and data analysis approaches for real-time detection, developing consensus protocol upgrades to limit the impact of dandruff attacks, and researching decentralized governance mechanisms for network resilience.

This study brings light on the growing threat of dandruff attacks on blockchain networks and emphasizes the significance of taking proactive actions to protect the network's integrity, privacy, and stability. Blockchain networks can continue to survive as secure and robust infrastructures in the future by identifying the individual elements of dandruff attacks and developing relevant defenses.

II. Dandruff Attacks Close-Up Severity

The "dandruff attack" is carried out by attackers who send multiple transactions to addresses that have recently made or received transactions. The attackers then wait for the recipient of the small transaction to mistakenly copy the attacker's address instead of the intended recipient's address and send assets to the attacker. Overall, the attack is executed by many attackers independently of each other, using various attack algorithms and principles of target selection [15],[16]. Our company has received appeals from at least a dozen victims of the attack, with the maximum amount of loss reaching several hundred thousand dollars.

The attack is characterized by:

- Many small transactions
- An extensive network of addresses used
- The transfer of the received assets to decentralized exchanges (DEX).

It has been observed that attackers can modify their approaches in order to evade detection. They may change the timing, frequency, and size of dandruff transactions, making it more difficult to build consistent detection patterns. To stay up with developing assault techniques, this dynamic behavior necessitates ongoing monitoring and analysis. As a result of this, we have identified six generations of this attack, and the most advanced attacking networks have been shown to be effective, with a level of success exceeding 3800%.

The total number of addresses sending the TRX token as part of such an attack was greater than 683 million transactions (namely 683 434 052), while for the USDT token, it was more than 85 million transactions (namely 85 304 707). The graphs below (Fig.1 and Fig.2) display the number of transactions related to the "dandruff attack" implementation in the TRX network in three periods. Until April 2021, there were only a few attacks, accounting for less than 0.01% of all network transactions. From May 2021 to September 2022, the number of attacks increased slightly, but the total volume increased by 20 times. However, since September 2022, the number of attacks has dramatically increased, accounting for up to 30% of total network transactions, and then increased to 47%. As of the time of writing, the daily volume of attacks reaches 60% of all transactions in the TRX network, with the expectation that this number will continue to rise in December 2022. The graphs are presented on a linear scale and a logarithmic scale to estimate the scale of the growth in the number of attacks in the network.

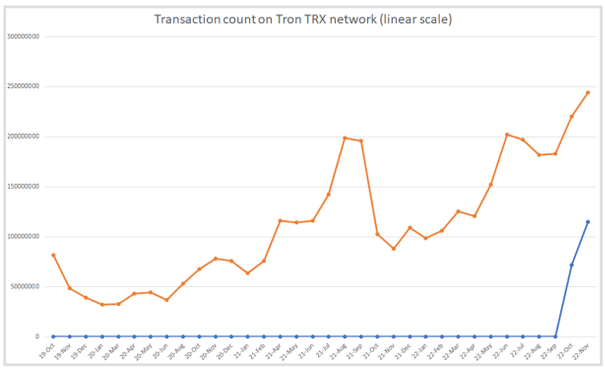

Fig.1. Attacks on a Linear Scale

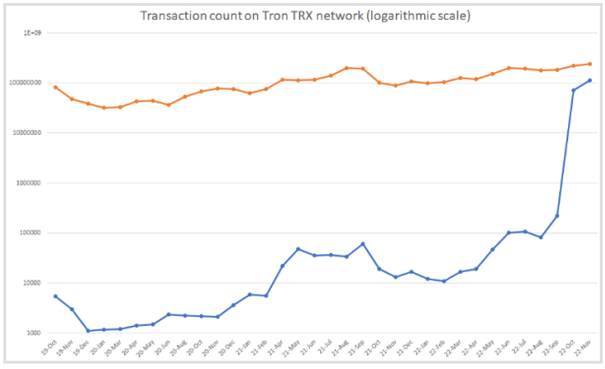

Fig.2. Attacks on a Logarithmic Scale

Fighting this kind of attack is possible! However, in order to address the challenge that dandruff attack presents it is imperative to have detection systems incorporate advanced algorithms, machine learning, and analytical methods capable of recognizing specific patterns of behavior. One must acknowledge that these advanced systems ought to be able to distinguish between illegal and legitimate transactions without jeopardizing user activity and privacy.

Machine learning algorithms can be applied to find vulnerabilities in the blockchain networks pertaining to dandruff attacks and predict possible errors in transactions. Here is an explanation of how such an account can be correct and send assets to attacker addresses:

1. Data collection: in order to develop the machine learning model, one must collect information on the previous transactions from the blockchain network [10]. The required information must include data on all transactions, those sent and received, their total number, and all the metadata attached.
2. Feature Extraction: these include potential transaction patterns, their frequency, total amount to specific addressees, and addressee types [13]. These variables are used for machine learning input and further analysis.
3. Model training: either a classification or regression method can be used for model training [10]. This model ought to be capable of recognizing patterns and relationships within the data that it is fed.
4. Vulnerability Prediction: Once the model is trained, it can be assigned to addresses that are most likely to cause red flags when sending transactions [2],[3]. These predictions are based on patterns and relationships observed during the training phase.
5. Flaws can be exploited: Attackers can target predicted critical addresses by creating connections that exploit the expected flaws [10]. Incorrect addresses, social engineering tactics, or fraudulent practices can be used to trick address owners into transferring assets to attacker addresses
6. Maximum return with minimum effort: Attackers can optimize their efforts and resources by focusing on addresses that are predicted to be vulnerable [13]. Specific mechanisms can be used to incentivize address owners to make mistakes, making it more likely that assets will be transferred from the managed address successfully This method reduces the amount of work and required resources.

The purpose of applying machine learning in this context is to identify any weaknesses or mistakes made by users while submitting services. It does not facilitate or encourage bad behavior.

The goal of using machine learning to identify vulnerable addresses is to improve security and avoid potential mistakes or errors that could lead to loss of revenue or undesirable behavior. The goal is to raise awareness and take action taking the initiative to mitigate risks, anticipate them.

However, it is important to note that attackers

may try to exploit these vulnerabilities themselves. Addresses identified by machine learning or other error-prone methods can be tracked and targeted. Attackers could do a variety of harmful things to trick address owners into moving assets to their managed addresses. This can include phishing attempts, social engineering, or creating fake transactions to trick consumers into committing fraud.

Specific suggestions to methods and techniques are described in the sections below.

III. Implementation Mechanisms of "Dandruff Attacks"

In the span of a few months since its inception in the summer of 2022, the "dandruff attack" has evolved rapidly from a basic mailing list to a sophisticated system with advanced methods of goal analysis. As of now, there are several generations of this attack that can be identified. The attackers have developed and refined their strategies over time to make the attacks more effective and harder to detect.

A. The First Generation

The mailing list is sent to all recently active addresses in a chaotic manner, utilizing TRX for transmission. This is due to TRX's capability to be sent without expending energy and solely using bandwidth, which will be elaborated on in the corresponding section [19].

Advantages:

- *The* simplicity of the mailing method.
- *The* network of addresses incurs low costs.

Disadvantages:

- *The* individual display of cryptocurrency assets in applications reduces the effectiveness of attacks on other tokens, including USDT.
- *The* scheme's efficiency is low.

An attacker's address, such as TGuuuq9asKwhGR2Zq21vQ1Nk4yFiTc8G3J, serves as an example (Fig.3) [17].

B. The Second Generation

The mailing process continues chaotically, but now employs USDT tokens instead. Although

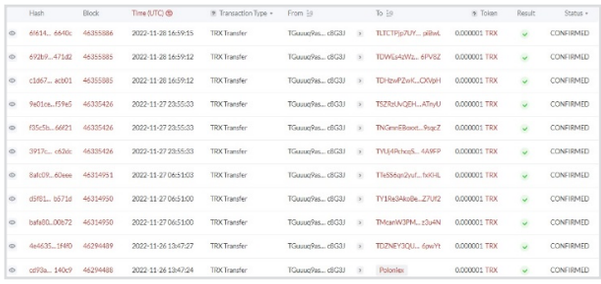

Fig.3. Example of attacker 1 address

there is only a slight difference in the value of the assets being transferred (still remaining at $0.01 or less), the cost of such a mailing increases due to the energy consumed in making transactions with any tokens [18]. Transactions with TRX only require daily renewable bandwidth, but transfers involving any other tokens will require both bandwidth and energy, which can be obtained by stacking TRX or burning it [19].

Advantages:

- *The* simplicity of the mailing method remains intact.
- *Mailing* efficiency is improved compared to the first generation.

Disadvantages:

- *Network* operation costs are increased compared to the first generation.
- *Optimizing* costs requires stacking a large amount of TRX.
- *The* network operation structure is complicated.

An example of an attacker's address is TEdi3CGdKewc1ZRen3SWkGf3YecoVT457j (Fig.4) [17].

C. The Third Generation

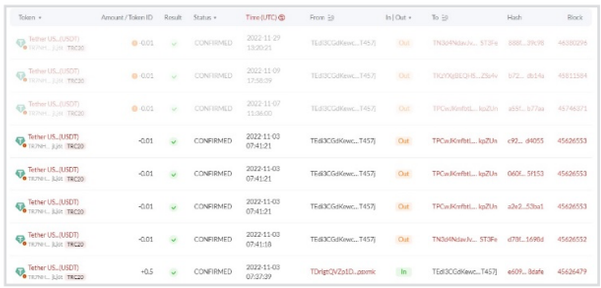

Fig.4. Example of attacker 1 address

The mailing continues to occur chaotically, now with the addition of filtering attack targets, representing an advancement from the second generation with some modified and altered filtering methods. These filters include factors such as the balance of the address, frequency of target transactions, and transaction time, among others. Each developer of the attacking network decides on the restrictions to implement at his/her discretion.

At this stage, there is an increase in the complexity of the work scheme, as analytics algorithms are introduced. This requires more requests to be made to the nodes of the network, which in turn provides technical capabilities for analyzing attackers.

Advantages:

- *The* attack is more targeted towards addresses with a large balance or other favorable initial data.

Disadvantages:

- *Technical* implementation is complicated.
- *Requests* to nodes become more noticeable from the general flow, especially in the absence of their own node.

D. The Fourth Generation

The attacker's network operation now includes an algorithm that selects addresses with a similar ending to the counterparty of the attacked address. This algorithm significantly increases the effectiveness of the attack, but requires a higher level of execution of the attacking network modules.

This attack generation utilizes a mechanism that matches the end of the crypto address, generating an address that has maximum similarity in the last characters. This significantly increases the chance of a successful attack, as it can combine various analytics methods available in the third generation. However, the choice of the attacked address and the generation of the attacker's address, similar to the target's counterparty, requires prompt replenishment of the attacker's addresses with assets and resources to complete the transaction. As a result, the mechanism of supplying the attacking network with Energy from staking is not applicable, and most networks attacking this generation pay commissions for making transactions by burning TRX [18].

Advantages:

- *The* effectiveness of the attack increases.

Disadvantages:

- *The* aforementioned disadvantages of the third generation apply.
- *Address* generation requires highly qualified specialists.
- *Increased* costs for each attack, as the use of staking is minimized.
- *In case* of an unsuccessful attack, the attacker's address cannot be used for attacks on other targets.

E. The Fifth Generation

The fifth generation of attacks introduces several changes, such as goal selection analysis, generating addresses similar to the counterparty, and transferring a number of assets similar to the one sent by the counterparty. This generation aims for the most selective attacks through duplicating a test payment between addresses. Through analysis, it was observed that duplicate amounts of up to 2 USDT were sent in certain conditions, including the absence of previous transactions between parties, significant balance on the target's account, and a test payment of no more than 2 USDT.

Advantages:

- *Extremely high effectiveness of the attack.*

Disadvantages:

- *The above disadvantages of the fourth generation;*
- *High costs for attacking a single address.*

F. The Sixth Generation

One of the main changes from the fifth generation is adding the attacker's address to the list of persons to whom the victim "sent" assets earlier. This means that the attacker is inserting his/her own address into a list of previous recipients that the victim has sent assets to. This can be done without any restrictions on sending 0 assets from any address on the Tron Network, even if the attacker does not have the private keys for the sending address.

This feature of the attack makes it less noticeable and more effective for attackers. It can be combined with mechanisms for generating cryptocurrency addresses that are similar to the counterparties under attack, which significantly increases the effectiveness of the attack. This combination can make it extremely difficult for victims to identify the source of the attack and to take measures to protect their assets.

However, this generation of attacks also requires a higher level of technical knowledge from the attacker, as well as a higher level of competition due to the popularity of this type of attack. Despite these challenges, the fifth generation has proven to be extremely efficient and cost-effective for attackers, making it a significant threat to the security of the crypto world.

Advantages:

- *This* attack generation is highly efficient, especially when using the address generation algorithm, and requires no costs for the asset being sent, as transaction costs are retained.
- *The* attack is less noticeable and more effective for attackers because the attacker inserts their address into the list of persons to whom the victim sent assets earlier, making it harder to detect.

Disadvantages:

- *Implementing* this attack generation require a higher level of technical knowledge and expertise.
- *There* is high competition as this generation of attacks has become more popular and displaces other generations in terms of the number of transactions in the network.

IV. The Economy of "Dandruff Attacks"

The expenses associated with the operation of the network can be divided among the following components:

- *Development* of modules for the attacking network: This includes the costs associated with creating and improving the various modules that form the attacking network.
- *Activation* of each address: To carry out attacks, each address in the attacking network needs to be activated. This process also incurs costs.
- *Transaction* costs: When assets are transferred to attacking addresses for use in the attacks, transaction costs are incurred. Additionally, "dandruff" transactions are sent to cover the tracks of the attacks, and these transactions also incur transaction costs.
- *Data* acquisition costs: Obtaining data on the activity of the Tron Network can be done either through external data providers or by launching and maintaining your own node. These expenses include the cost of obtaining and processing data, as well as the cost of maintaining the infrastructure necessary for data acquisition.

The profit that an attacker can obtain from an attack is determined by subtracting the costs of network operation from the assets obtained by the attacking addresses from victims. As the success and size of the attack are influenced by various random factors, it is crucial to base the assessment on a sizable sample of attacking network addresses to obtain a more accurate evaluation, even though it may not cover all possibilities.

The costs of network operation include the development of attacking network modules, the activation of each address of the attacking network, transaction costs for transferring assets to attacking addresses for attacks and sending "dandruff", as well as associated expenses for obtaining data on the Tron Network's activity, such as from external data providers or by launching and maintaining one's node. By analyzing these costs and comparing them with the potential profits, an attacker can assess whether the attack is profitable or not.

A. Development of attacking network modules

The cost for preparing the attacking network can be around $3000, which can be done by the attacker themselves or outsourced. Our technical experts estimate that developing all the modules of the most advanced fourth-fifth generation attacking network takes approximately 100 hours of work for a skilled specialist, including debugging and testing. At an average hourly rate of $30/hour, the total cost would be around $3,000. However, the development of first and third-generation networks is relatively less expensive,

around half the cost of the fourth-fifth generation, making it more accessible for a wider range of individuals.

B. Activation of each attacking address in the Tron Network

Activating a large network of addresses for the first-generation networks is quite resource-intensive, as it requires each address to have at least 1 TRX. This can make launching large networks, with tens of thousands of addresses, quite costly. However, the first-generation networks use large networks of addresses since each of these addresses can make up to 4 transactions in TRX daily for free, thanks to the daily renewable bandwidth [19]. For instance, activating 50,000 addresses requires approximately $2,600.

In contrast, the latest generation networks use fewer addresses, which reduces the cost of activating the network addresses.

C. Transaction costs cover

There are various ways in which the transaction costs of transferring assets to attacking addresses for attacks and sending "dandruff" can be covered. In the first generation, transaction costs are often not incurred as free daily renewable bandwidth of up to 1500 is used for each address [19]. On the other hand, the second and third generations use renewable bandwidth for free and TRX staking is used to cover the required number of energies in their optimal execution [19]. For instance, to make one daily transaction with the USDT token at one attacking address, about 550 TRX is required, and burning TRX can also be used to make transactions, consuming approximately 4.5 TRX to make each transaction (about $0.25).

An example of an address that supplies the Energy network of attacking addresses by staking its own TRX is TJUMW8UEAUCVTEMKSS3HLMTLDBKVHDH3C [17]. However, in the fourth and subsequent generations, staking is used less often due to the technical impossibility of staking TRX for a period of fewer than 72 hours. Additionally, the need to quickly change the attacking addresses generated for each target makes the most frequent use of the TRX burning mechanism to pay the commission for transactions in the networks of these generations.

D. Associated costs

Launching your own Tron node requires an initial investment of around $500 for setup and startup labor costs, as well as an ongoing cost of approximately $500 per month for renting a server with the appropriate technical specifications.

V. Profitability with the Example of A Separate Network

The evaluation of the attack's efficiency will be conducted on the attacking network that has received the assets from the address TTFGc88GU8LXrXNnSPZFeeivSwaBZoJGk1 (Fig.5). This network can be classified into several generations simultaneously due to the adaptable nature of the method it employs, containing

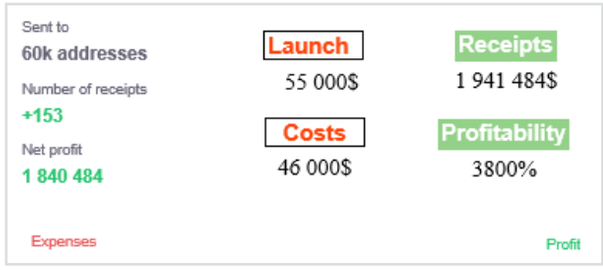

Fig.5. Profitability Calculation.

transactions from both the fourth and sixth generations.

The address TTFGc88GU8LXrXNnSPZFeeivSwaBZoJGk1 transferred 721,054 TRX and 1,750 USDT to over 60,000 addresses of the attacking network, incurring a commission of 90,443 TRX [17]. The total value of crypto assets used in this network was approximately $46,000, and combined with other costs, the estimated amount spent on launching the network was between $50,000 and $55,000.

The network generated 153 receipts to attacking addresses after the transaction was made from the attacked address, and the total amount of funds received in this way was at least 1,941,484 USDT. The overall profitability of this network was over 3,800%.

Justification:

1. Address selection: The address TTFGc88GU8LXrXNnSPZFeeivSwaBZoJGk1 was chosen for determining the effectiveness of the attack. This address was shown to send a large amount of TRX and USDT to over 60,000 addresses. We attempted to determine the impact and profitability of the attack by evaluating the activities and transactions linked with this address.
2. The attacking network has demonstrated several generations: transactions from the fourth and sixth generations were discovered. This suggests that the network used a flexible strategy, capable of adapting and changing over time. We hoped to represent the intricacy and effectiveness of the network's attack tactic by considering numerous generations and to monitor the activity in time progression.
3. Estimation of costs: the overall value of crypto assets used in the network was roughly $46,000, and when extra costs were considered, the anticipated cost of creating the network was between $50,000 and $55,000. This shed light on the attackers' investment and the potential profit they hoped to earn.
4. Receipts and funds received: Following the initial transaction from the attacked address (TTFGc88GU8LXrXNnSPZFeeivSwaBZoJGk1), the network generated 153 receipts to attacking addresses. The total sum received as a result of these receipts was at least 1,941,484 USDT. This data reveals that the attacking network successfully captured assets, emphasizing their profitability.
5. Overall profitability: Based on the calculations and statistics shown above, the attacking network's overall profitability was determined to be greater than 3,800%. This statistic shows the attackers' returns in relation to their investment in launching and operating the network.

VI. The Most Effective Counteraction Measures

After analyzing "dandruff attacks", we have identified several potential methods for reducing the risk of such attacks:

- *Cryptocurrency wallet developers could implement a default option to hide transactions under $1, rendering attacks of the first, fourth, and sixth generations almost ineffective.*
- *In-depth analysis and de-anonymization of staking address managers that supply energy to attacking networks could increase the difficulty and decrease the profitability of attacks of the second and third generations.*
- *Analyzing the TRX receipt sources in attacking address networks could put additional pressure on administrators of the first, fourth, and sixth generations.*
- *Implementing an automatic activity analysis algorithm to block Tether Ltd. USDT assets at attacking addresses when they receive amounts over a certain value after sending "dandruff" could render this type of attack economically unfeasible.*
- *Studying request logs of key services that provide transaction information on the Tron Network could enable identification of possible administrators of attacking networks of all generations, if the attacker does not use their own node.*
- *Authors of attacking algorithms can be identified by searching for similar attacks in the test network during the debugging stage. Many attacking networks are tested on Tron test nets for debugging and tuning, with tokens obtainable only through the official community in Discord. An example of such an attack is shown*

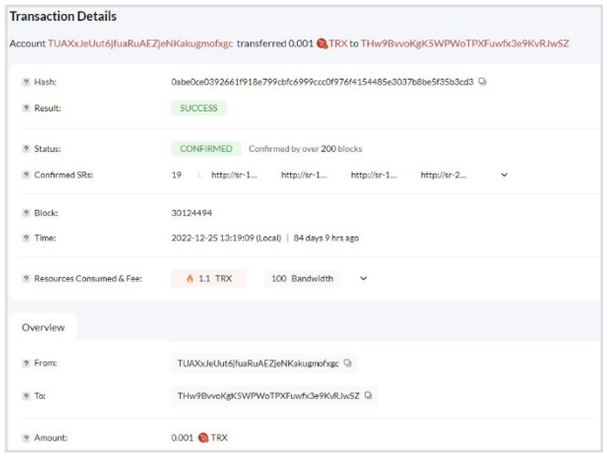

Fig.6. Transaction proof example

in a screen shot of a transaction below (Fig.6).

VII. Future Approach

Based on the above analysis, we present probable areas for future work:

1. Dandruff attack detection via machine learning. More research is required into the application of machine learning approaches to detection of these attacks in blockchain networks. This would mean that advanced algorithms, feature engineering, and advanced anomaly detection methods are required. This would allow to improve the accuracy of detection, and distinguishing dandruff transactions from valid ones. Real-time detection techniques would significantly up the bar of countering dandruff attacks through minimizing errors, thereby maintaining client satisfaction rate and positive experience.
2. Address clustering and behavioral analysis. It is important for future research to delve deeper into the analysis of implicated addresses behavior. Through correlation analysis, evaluation of transaction patterns, their frequency, researchers would be able to make the design of address clustering algorithms more effective. Naturally, this will help proactive and tailored mitigation tactics preventing dandruff attacks from succeeding.
3. Privacy-preserving dandruff attack detection. Dandruff attacks are primarily focused on jeopardizing user privacy. Thus, privacy-preserving methods are of primary importance. This involves developing cryptographic algorithms or secure multiparty computation protocols.
4. Dynamic defenses and adaptive fee systems. This may mean implementing adaptive pricing structures that make dandruff transactions dependent on the size of the transaction due to the changes in transaction interest prices. At the same time dynamic transaction filtering systems need to be made so as to recognize and filter out dandruff transactions in real-time.
5. Game-theoretical analysis. Game theory can be implemented to better understand the incentives and motivations driving dandruff attacks. By modeling interactions with network participants researchers can acquire insights into attackers' strategic behavior and develop countermeasures. In the long-term, this would make dandruff attacks more difficult to implement due to the known potential moves of the attackers.

To improve understanding of this emerging threat and develop effective countermeasures, future works in the field of dandruff attacks on blockchain networks should focus on advancing detection techniques, addressing privacy concerns, developing dynamic defenses, and conducting empirical analysis.

VIII. Conclusion

The "dandruff attack" on the Tron Network is a type of attack that is used to flood a victim's wallet with small amounts of cryptocurrency transactions, which creates difficulties for the victim in distinguishing between real transactions and those generated by the attacker. This attack is economically profitable for the attacker due to the low transaction fees on the Tron Network.

The attack has evolved through several generations, and each generation has different characteristics and requires different resources to execute.

The first generation of attacks was rudimentary and relied on randomly selecting addresses to send the small transactions to. However, as the attackers began to learn from their mistakes, they started using more complex methods to identify potential targets. The second generation of attacks involved analyzing the network for addresses that had recently sent or received large transactions, which indicated that they held a significant amount of assets.

In the third generation, the attackers started to use machine learning algorithms to identify the most vulnerable addresses. They analyzed patterns in the network to determine which addresses were likely to make mistakes while sending transactions,

making them more susceptible to sending assets to the attackers' addresses. This approach allowed the attackers to maximize their returns with minimal effort.

In the fourth and fifth generations, the attackers began to use more advanced methods of goal analysis, such as tracking the network for addresses that were likely to trade on decentralized exchanges (DEXs) and sending the assets received from "dandruff" transactions to those addresses. This allowed the attackers to launder their ill-gotten gains and further obfuscate their activities.

The sixth and most recent generation of attacks has seen the attackers using a combination of all the previously mentioned strategies, making the attacks highly effective and difficult to stop. The sophistication of these attacks has enabled the attackers to scale their operations and target a large number of users simultaneously.

As the "dandruff attack" continues to evolve, it is likely that attackers will develop even more advanced methods to achieve their goals. It is imperative that users remain vigilant and take necessary precautions to protect their assets.

The attack has been analyzed in detail, and several measures have been proposed to reduce the risk of such attacks, including introducing the ability to hide small transactions, de-anonymizing staking address managers, analyzing TRX receipt sources, and blocking USDT assets at attacking addresses.

It is important to note that the profitability of the attack remains high, and the proposed measures are not foolproof. Therefore, it is essential to remain vigilant and implement a combination of measures to reduce the risk of "dandruff attacks" and other similar attacks. The Tron community and application developers must work together to improve the network's security and protect users from potential attacks.

Enhancement of dandruff assault detection by the use of modern machine learning techniques and real-time detection systems is one area. Furthermore, deeper behavioral research and the development of more effective address grouping algorithms can aid in proactive mitigation measures.

Another critical component is the investigation of privacy-preserving systems for identifying dandruff attacks, which would allow for collective monitoring of transaction data while protecting individual privacy. Dynamic defenses, such as adaptive fee structures, along with real-time transaction filtering approaches, can help discourage dust transactions while improving overall network security.

Furthermore, using game theory to analyze attacker incentives allows for the development of successful defense methods.

Future research should focus on enhancing detection algorithms, addressing privacy problems, establishing dynamic defenses, and carrying out empirical analyses. These initiatives will aid in the creation of robust countermeasures for blockchain networks as well as a better understanding of dust attacks.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] O. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, pp. 1333, 2023, doi: 10.3390/electronics12061333.

[2] Z. Bilgin, M. A. Ersoy, E. U. Soykan, E. Tomur, P. Çomak, and L. Karaçay, "Vulnerability prediction from source code using machine learning," *IEEE Access*, vol. 8, pp. 150672-150684, 2020, doi: 10.1109/ACCESS.2020.3016774.

[3] S. Chakraborty, R. Krishna, Y. Ding, and B. Ray, "Deep learning based vulnerability detection: Are we there yet," *IEEE Trans. Softw.* Eng., vol. 48, no. 9, pp. 3280-3296, Sept. 2022, doi: 10.1109/TSE.2021.3087402.

[4] L. Chauhan, "Cyber Security and its Various Perspectives,"

IJRAMT, vol. 4, no. 4, pp. 64-69, 2023.

[5] A. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman, and A. Yadav, "A Survey on Consensus Protocols and Attacks on Blockchain Technology," *Appl. Sci.*, vol. 13, no. 4, pp. 2604, 2023, doi: 10.3390/app13042604.

[6] B. Hammi, S. Zeadally, and J. Nebhen, "Security threats, countermeasures, and challenges of digital supply chains," *ACM Comput. Surv.*, early access, Mar. 2023, doi: 10.1145/3588999.

[7] Y. Jiang and J. Zhang, "Vulnerability of Finitely-long Blockchains in Securing Data," *arXiv:2304.09965,* 2023. [Online]. Available: https://arxiv.org/abs/2304.09965

[8] D. S. Kerr, K. A. Loveland, K. T. Smith, and L. M. Smith, "Cryptocurrency *Risks,* Fraud Cases, and Financial Performance," Risks, vol. 11, no. 3, pp. 51, 2023, doi: 10.3390/risks11030051.

[9] S. Li, J. Li, Y. Tang, X. Luo, Z. He, Z. Li, X. Cheng, Y. Bai, T. Chen, and Y. Tang, "BlockExplorer: Exploring Blockchain Big Data via Parallel Processing," *IEEE Trans. Comput.,* early access, Feb. 2023, doi: 10.1109/TC.2023.3248280.

[10] R. Mahmood, J. Lucas, J. Alvarez, S. Fidler, and M. Law, "Optimizing data collection for machine learning," in *36th Conference on Neural Information Processing Systems (NeurIPS 2022),* in Advances in Neural Information Processing Systems 35, S. Koyejo et al. Eds., 2022, pp. 29915-29928.

[11] M. Paliwal, "A review on cyber security," in *AIP Conf. Proc.*, vol. 2427, no. 1, 2023, doi: 10.1063/5.0101190.

[12] P. Weichbroth, K. Wereszko, H. Anacka, and J. Kowal, "Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments," *Sensors,* vol. 23, no. 6, pp. 3155, 2023, doi: 10.3390/s23063155.

[13] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digit. Commun. Netw.*, early access, Sept. 2022, doi: 10.1016/j.dcan.2022.08.012.

[14] K. Schiller, F. Adamsky, and Z. Benenson, "Towards an Empirical Study to Determine the Effectiveness of Support Systems against E-Mail Phishing Attacks," in *2023 CHI Conf. Hum. Factors in Comput. Syst.,* Germany, Apr. 2023, pp. 1-15, doi: 10.1145/3544549.3585658.

[15] A. A. Sharadqh, H. A. M. Hatamleh, A. M. A. Alnaser, S. S. Saloum, and T. A. Alawneh, "Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment," *IEEE Access,* vol. 11, pp. 27433-27449, 2023, doi: 10.1109/ACCESS.2023.3256277.

[16] P. Sharma, K. Choi, O. Krejcar, P. Blazek, V. Bhatia, and S. Prakash, "Securing optical networks using quantum-secured blockchain: An overview," *Sensors*, vol. 23, no. 3, pp. 1228, 2023, doi: 10.3390/s23031228.

[17] Tronscan. [Online]. Available: https://tronscan.org/#/. [Accessed: 19-Mar-2023].

[18] Tron Calculators. [Online]. Available: https://tronstation.io/calculator. [Accessed: 19-Mar-2023].

[19] Tron Network. [Online]. Available: https://developers.tron.network/docs/resource-model. [Accessed: 19-Mar-2023].