Investigating Black-Market Jobs on Social Networking Service

Yamato Kawaguchi*, Kazuki Takada*†, Yin Minn Pa Pa*, Rui Tanabe*‡, Katsunari Yoshioka*, and Tsutomu Matsumoto*§
*Yokohama National University, Japan
†Hitachi Systems, Ltd.
‡Juntendo University, Japan
§National Institute of Advanced Industrial Science and Technology

***Abstract*—In this study, we investigate black market job advertisements on social networking services (SNS) through cross-platform observation of popular SNSs. Our findings reveal that black market job recruitment often begins with SNS posts designed to attract victims. Once a victim contacts the attackers via direct message (DM) or their public SNS account, the application process for the black market job is initiated, or they are redirected to fraudulent websites where they may fall victim to money transfer scams. Additionally, our study explores the relationship between accounts that post black-market job advertisements and their activity patterns.**

***Index Terms*—Job scams, black-market jobs**

I. Introduction

Black-market jobs on SNS have become a growing concern in Japan. According to the National Police Agency, from January to the end of July 2023, 46.9% of the suspects arrested for roles such as money mules had applied for these positions through social media [1]. However, the process of black-market job advertisements reaching the final destination, namely their potential victims, is poorly understood. To address this, we collect SNS posts related to black market jobs from a popular SNS platform in Japan and follow the directions in these posts to track their progression. Additionally, we examine SNS accounts associated with black-market job advertisements and analyze their relationships. We reveal three distinct pathways through which black-market job advertisements culminate. At the ends of the pathways, the job application process is started, or the victim is redirected to scam websites and falls into money transfer scams.

II. Methodology and Results

To automatically collect information from a popular SNS platform (referred to as SNS-A), we use the Web API provided by the service. This API allows us to search for posts using specific keywords and gather user and profile information for the matching posts. We search for posts containing the keyword 'high-paying part-time job' in Japanese between December 21, 2022, and January 29, 2023, collecting 31,390 posts from 4,025 accounts. Figure 1 shows the number of gathered posts and accounts per day relating to high-paying part-time job advertisement.

We then analyze these posts from SNS-A, follow the instructions such as sending direct messages (DMs) or joining the attacker's public SNS account, and trace the process to its destination. Our analysis identifies three distinct patterns: (1) The first pattern, associated with 13,484 posts, involves letting the victims send DMs to scammers' accounts on the same SNS-A platform. (2) The second pattern, linked to 4,246 posts, directs victims to join the attacker's public accounts on another SNS platform (referred to as SNS-B). (3) The third pattern, which involves only 8 posts, directs users to send DMs to a different SNS platform (referred to as SNS-C).We focus on the follow-up actions of the first and second patterns, as the third pattern represents a negligible amount.

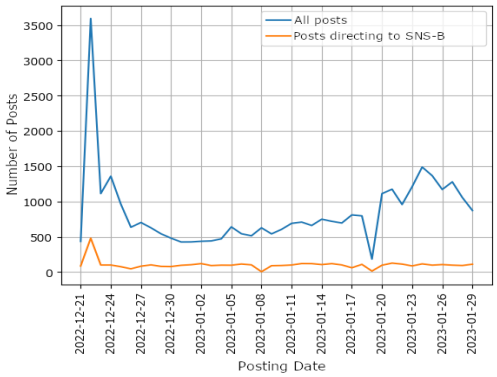

Fig. 1. Number of daily SNS posts and accounts matching "high-paying part-time job" (in Japanese) from December 21, 2022 to January 29, 2023.

Pattern one: Sending DM to Accounts on the Same SNS-A Platform: In the first pattern, 13,484 posts, including the 'high-paying part-time job' keyword, suggest the victims to send DM for further information. We randomly choose to send DM to 37 accounts relating to such posts and receive replies from 33 accounts. We receive messages associated with black-market jobs from 22 accounts. Figure 2 shows a translated example of the first received message shows that the job is related to crime.

Pattern two: Joining Public Account of SNS-B: In the second pattern, 4,246 posts from SNS-A, including the keyword 'high-paying part-time job', lead victims to join 15 public attacker accounts on the SNS-B platform.

We collect messages from these 15 public SNS-B accounts. Since SNS-B lacks an API for retrieving messages, making

”Consignee, the client is associated with a family business connected to organized crime. Since the main requests come from individuals involved in anti-social activities, please assume that these may involve firearms, drugs, or other illicit items.”

Fig. 2. The received message showing that the job is related to crime.

TABLE I
TYPE OF WEBSITES OF COLLECTED URLS

Page type	Number of URLs	URL source
Unknown	173	SNS-B
Sites requiring form input	150	SNS-B
Messaging SNS invitation links	96	SNS-B
Sites mimicking email services	52	SMS
Sites prompting email sending	42	SNS-B
Inaccessible sites	24	SNS-B
Sites prompting phone calls	9	SNS-B
Sites prompting purchases	5	SNS-B
Sites prompting bank transfers	0	SNS-B
Total	551	

automatic collection difficult, we install the SNS-B applicaion on an Android device and use Android Debug Bridge (adb) [2] and UI Automator [3], an Android app UI testing framework, to automate app operations from a PC. When we encounter additional SNS-B accounts in messages, we also join those. This approach allows us to collect 3,504 messages from 94 public SNS-B accounts.

From these messages, we are able to collect 551 URLs and access these on January 24, 2023. Table I shows the types of pages for these 551 URLs and their associated sources. When a URL leads to a website displaying an input form for personal information, we manually enter specific phone numbers we prepared for investigation. As a result, we receive 55 SMS messages on our phones. Of these, 52 direct users to scam sites that imitate email services, demanding registration fees or handling charges. The payment methods include convenience store payments, electronic money, bank transfers, and credit cards. Of the remaining 3, 1 contains a broken link, and 2 are legitimate Short Message Service (SMS) messages. We also check the number of other accounts (potential victims) joining these 96 pubic SNS-B accounts. The number of registrants (accounts) per day per attacker's public SNS account ranges from 60 to 100 accounts, meaning the potential victim reaches 100 in extreme cases.

Finding Black-market Job Advertisements on SNS-A:

In addition to our initial search with a keyword using 'high-paying part-time job', we also search black market job posts on SNS-A using keywords retrieved from the names of SNS-B accounts. Table II shows the results from January 29 to January 31, 2023. Search queries combining nouns related to money and 'side job' yield many matching posts. In particular, search queries like 'FX side job' guide to numerous accounts, suggesting the possibility of discovering new SNS-B accounts. This way, we can collect more information by providing feedback based on the collected data.

Relationship between Accounts: Figure 3 shows the relationship between accounts of SNS-A and SNS-B. In the graph, nodes represent SNS account IDs, and edges represent relationships between accounts. Blue nodes and blue edges represent SNS-A, while green ones represent SNS-B. This figure shows that the relation from SNS-A is directed to SNS-B accounts, which then link to additional SNS-B accounts, forming an extensive network and showing a strong connection between accounts of black-market jobs.

TABLE II
RESULTS BY SEARCH QUERY

Search query	Posts on SNS-A	Posts linked to SNS-B	SNS-B accounts
”FX side job”	14694	4140	205
”Gift side job”	2251	520	113
”Lottery side job”	467	44	14
”Horse racing side job”	402	94	13
”Boat racing side job”	220	72	2

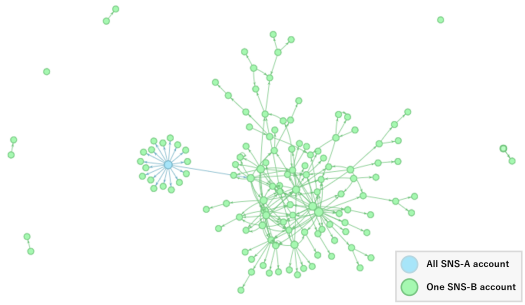

Fig. 3. Relationship between accounts on messaging SNS

Ethic: We carefully design our study and anonymize the SNS platforms investigated. In addition, we gather publicly available data and store it securely to ensure the privacy and confidentiality of individuals involved.

III. CONCLUSION

This study reveals that black-market job ads on SNS platforms involve complex networks of accounts guiding victims through multiple interactions. By analyzing 34,734 posts on SNS-A and tracking interactions on SNS-B, we identify three main engagement patterns, with many leading to scam sites requesting fees or personal data. Our findings show the organized nature of these scams, using interconnected SNS accounts to expand their reach, emphasizing the need for monitoring and analyzing social media interactions to mitigate online job scam risks.

Acknowledgements. This paper is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

REFERENCES

[1] “Investigation of dark work from sns to crime (translated),” https://prtimes.jp/main/html/rd/p/000000104.000034282.html, (Accessed on 27/07/2024).
[2] A. Developers, “Android debug bridgeadb,” https://developer.android.com/tools/adb?hl=ja, (Accessed on 26/08/2024).
[3] ——, “Ui automator,” https://developer.android.com/training/testing/ui-automator?hl=ja, (Accessed on 26/08/2024).