

December 6, 2023

SBI Holdings Inc.

SBI EVERSPIN Co., Ltd

**Notice of Attention Regarding Malicious Apps Detected by Fake Finder,
an AI-based Malicious App Detection App for Android OS**
- Report on the state of Malicious Apps in October 2023 -

SBI EVERSPIN Co., Ltd. (Head office: Minato-ku, Tokyo; Representative Director: Jamyung Yoon; hereinafter “the Company”), a consolidated subsidiary of SBI Holdings, Inc. (Head office: Minato-ku, Tokyo; Representative Director, Chairman, President & CEO: Yoshitaka Kitao), which provides an AI-based malicious app detection app “Fake Finder for SBI Group” free of charge to customers using services of SBI Group companies exclusively for Android hereby announces that it have found Malicious Apps, to call for attention.

1. Type of Malicious Apps

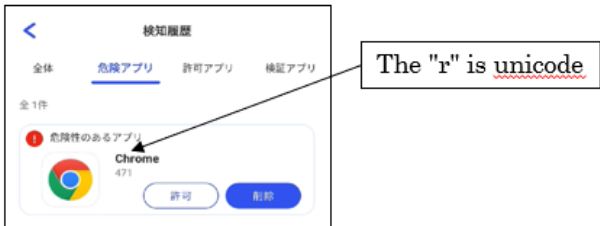

- 1.1. **Type** : Fake applications that impersonate financial institutions or public institutions, etc.
- 1.2. **Description**: Apps created for malicious purposes, such as plagiarizing the name or icon of the relevant institution, or updates to security programs, identity authentication or other financial app functions, or other Fake apps spoofed with additional programs, etc.
- 1.3. **Example**: When the app is installed, it automatically connects to the app developer's server and automatically downloads and installs other Malicious app on the smartphone.

2. Information and Initial Detection Time of Malicious Apps

Case	PACKAGE_NAME	Initial Detection Time
A	JPpost	2023-10-13 18:32:25
B	Chrome	2023-10-23 18:31:36

3. Characteristics of Malicious Apps (Chrome Case Study)

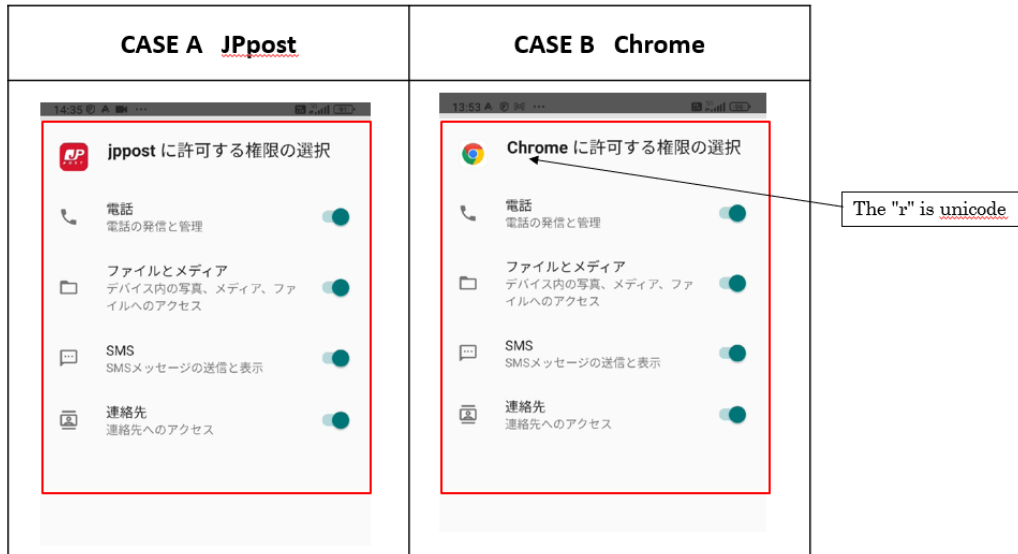
- 3.1. **Basics** : Fake Chrome App uses Unicode for "r" as a font that looks almost the same but is different from the usual (Unicode Info: U+0433)
- Request permission to access phone, files and media, SNS, and contacts
- 3.2. **Operation** : **Invisible " Malicious app" additionally installed after force close due to Android version issue**
- 3.3. **UI features** : Icons are hidden and not visible

3.1. Reproduction of "Fake Finder" Malicious app detection screen	3.2. Error message at application force close
	

4. Operation of Malicious Apps

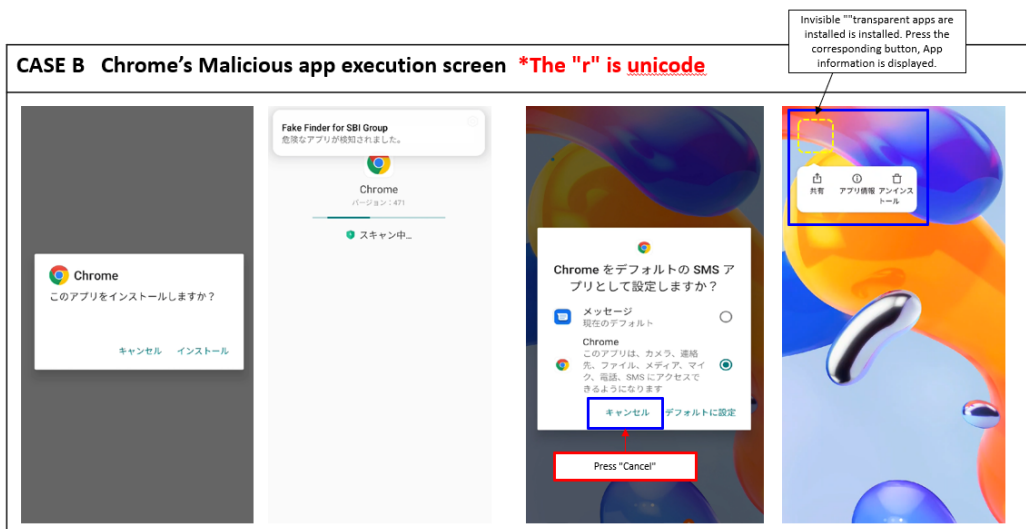
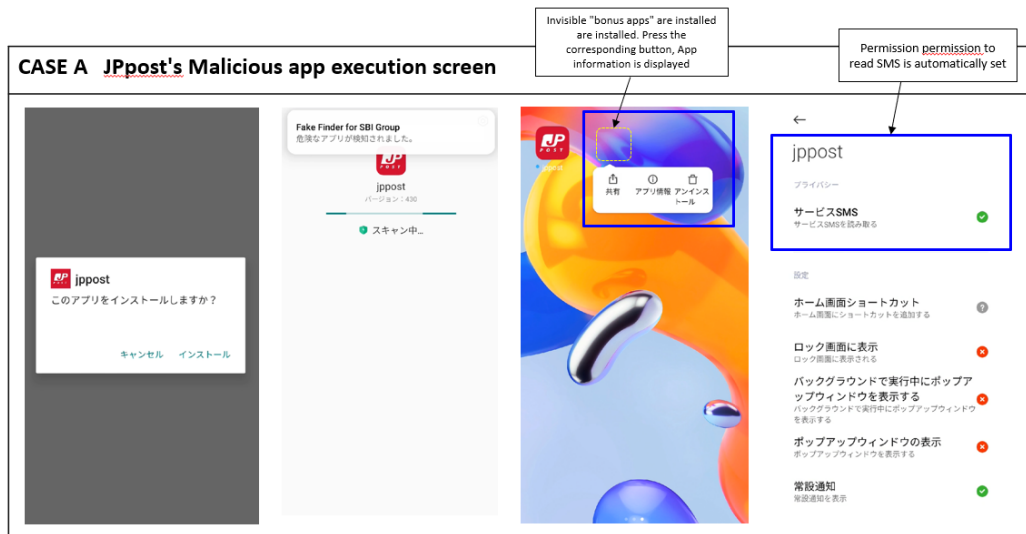
4.1. Initial screen after installation

: Request permission to access phone calls, files and media, SMS, contacts



4.2. Malicious apps execution screen

: Invisible "Malicious apps" are additionally installed



Malicious apps such as the above are often distributed outside of the official market, and since Android devices can obtain apps from providers other than Google Play, malicious apps are distributed by taking advantage of this. Nowadays, many smartphone apps are provided by various developers, and attackers take advantage of the fact that users install apps on a daily basis to lead them to malicious apps. Therefore, inadvertent download of apps may lead to unexpected damage.

In order to avoid damage from malicious apps, it is necessary to obtain apps from official markets in principle, and to carefully check the developer's reliability, functions of the app, terms of use, etc. when selecting apps. The Company currently offers a free malicious app detection app for Android, ["Fake Finder for SBI Group."](#) which it hopes users will take advantage of.

The Company will continue to focus on protecting the safety and security of its customers' smartphone usage environment by regularly distributing information on malicious apps and other topics to help prevent its customers from becoming victims of phishing scams, etc., and [as announced on October 6, 2023](#), as well as to inform related organizations about the current state of malicious apps by collaborating with the Japan Cybercrime Control Center (JC3), of which it is a regular member of. In addition, by collaborating with the Japan Cybercrime Control Center (JC3), the company will endeavor to promote awareness of malicious apps among related organizations, thereby leading to activities to prevent financial damage caused by use of smartphones.

Using the expertise that the Company has gained through continuous research on cutting-edge security technologies and years of security vulnerability assessments to protect its customers' systems from the ever-evolving damage caused by unauthorized access, such as hacking, the Company will endeavor to realize a secure society where customers can confidently use digital environments and focus on their core business services.

For further information, please contact:
SBI EVERSPIN Co., Ltd. contact@sbieverspin.com