

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

SBI EVERSPIN Co., Ltd. (Head office: Minato-ku, Tokyo; Representative Director and President: 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, etc., to call for attention.

### 1. Type of Malicious Apps

- 1.1. **Type** : Fraudulent applications that exploit personal information or 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
- 1.3. **Example**: Require excessive privileges to have full control over smartphones  
Automatically download and install other “malignant apps” on smartphones

### 2. Information and Initial Detection Time of Malicious Apps

Case	PACKAGE_NAME	Initial Detection Time
A	Chrome	2023-11-28 15:24:10
B	SyncService	2023-12-08 16:33:48
C	Chrome	2023-12-15 14:42:31

### 3. Characteristics of Malicious Apps (Chrome Case Study and SyncService (app name: hoverwatch) Case Study)

#### 3.1. Basics

**Case A and C** : Chrome fake application uses Unicode for “C” and “e” as a font that looks almost the same but is different from the usual

**Case B** : Fake app spoofing “hoverwatch (name of monitoring app)”


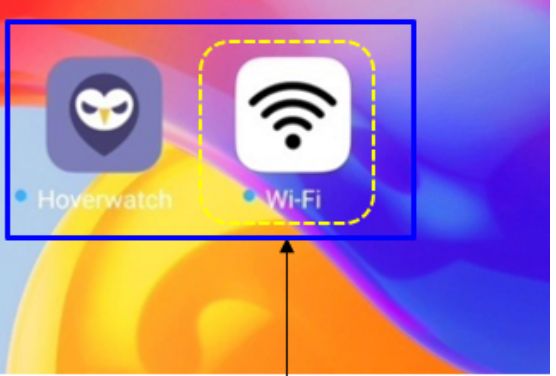
#### 3.2. Operation

**Case A and C** : Demand excessive authority to exploit personal information

**Case B** : Request excessive privileges to install additional invisible “malicious apps” and take full control of smartphones

- Request permission to access phone, files and media, SNS, and contacts


### 3.3. UI features : Icons are hidden and not visible, or additional “malicious apps” are installed

After installing “Chrome” spoofing apps, Icons are hidden and not visible	After installing “hoverwatch” spoofing apps, Malignant Apps are installed automatically
 <p data-bbox="300 651 820 779">After installing “Chrome”, Icons are hidden and not visible. Press the corresponding button to display the app information.</p>	 <p data-bbox="884 725 1422 779">Automatically install additional "malicious apps"</p>

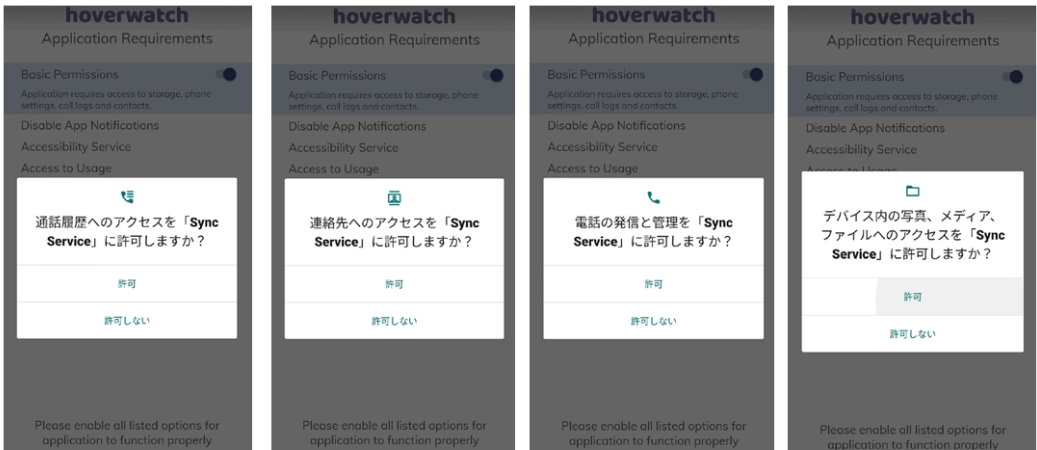
## 4. Operation of Malicious Apps

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

**Excessive authorization requests for “Chrome” spoofing apps**



**Excessive authorization requests for “hoverwatch” spoofing app**



5. Other remote control application(\*) detection results in “Fake Finder” during the same period

Total Period	Number of remote control apps detected
November-December 2023	1,482 cases

(\*) Remote control application: An application that monitors or operates a smartphone in a remote location

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 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](mailto:contact@sbieverspin.com)