October 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 September 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. Information and Detection Time of Malicious Apps

Case	PACKAGE_NAME	Detection Time
A	Anshin Security	2023-09-13 15:48:40
B	Softbank Security	2023-09-13 15:57:11
C	KDDI Security	2023-09-27 12:03:10

2. Characteristics of Malicious Apps

2.1. Basics : Guides setting as a default SMS app

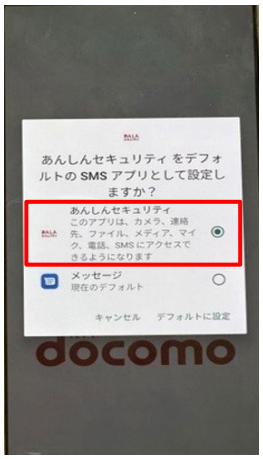
2.2. Operation : Spoof security apps to steal personal information such as address books, SMS, phone records, etc.

2.3. UI features : Disguises UI form of device management security apps (memory optimization, WIFI security, etc.), but does not work when actually performing operations.

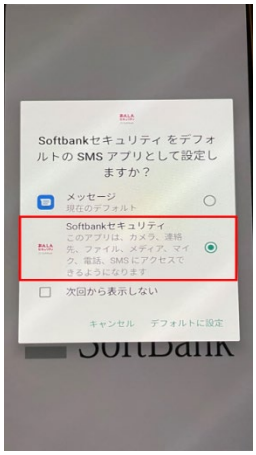
3. Operation of Malicious Apps

3.1. Guides setting as a default SMS app on initial screen after installation

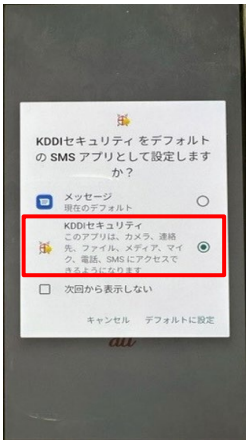
Case A



Case B

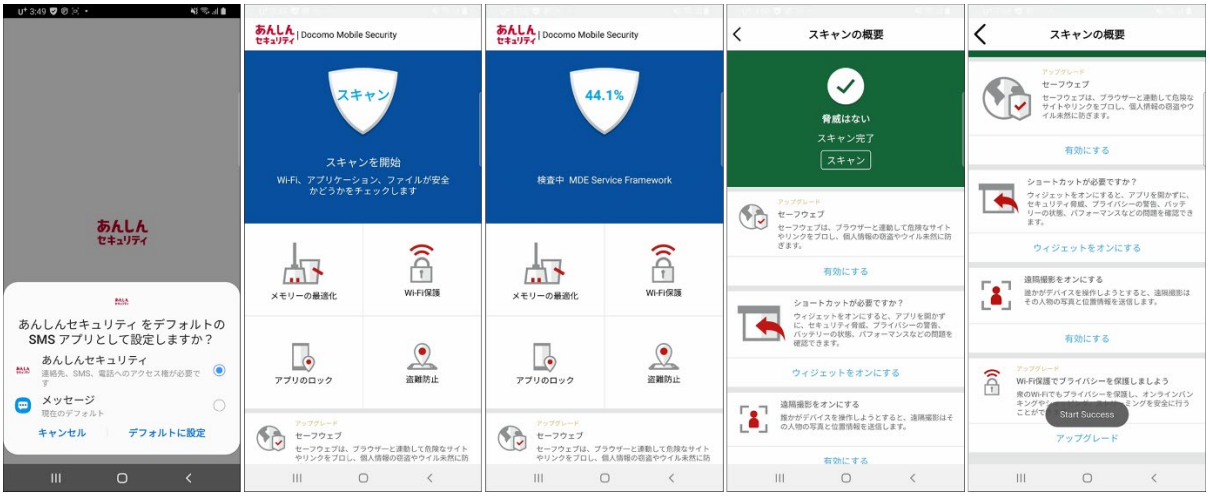


Case C

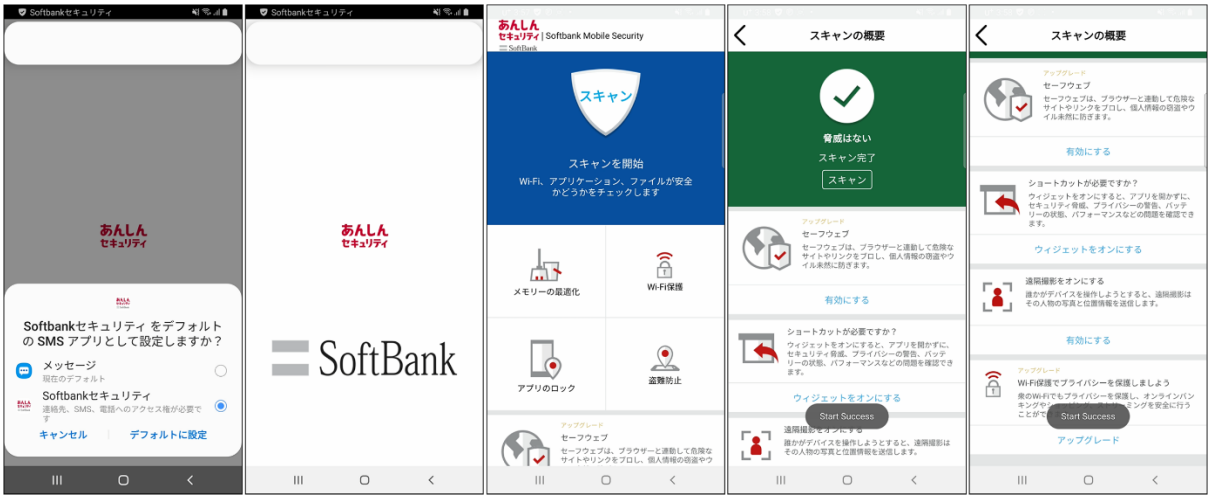


3.2. Malicious Application Execution Screen

[Case A :Anshin Security Malicious app]



[Case B: Softbank Security Malicious app]



[Case C：KDDI Security Malicious app]

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., 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.

(*) About the Japan Cybercrime Control Center (JC3):
The Japan Cybercrime Control Center (JC3) is a new framework among industry, academia, and government to achieve a preemptive and comprehensive response to threats. It includes accumulating and sharing experience in dealing with cyberspace threats collaborating with industry, academic research institutions, and law enforcement agencies together with more effective use of investigative authority by the police.
JC3 is a non-profit organization that seeks to identify, mitigate, and neutralize the major sources of cybercrime and other cyber threats in cyberspace by observing all of cyberspace from a bird's-eye view through sharing of information and building collaborative relationships with relevant Japanese domestic and overseas organizations such as the U.S. NCFTA.

Please visit the website below for information about the Japan Cybercrime Control Center (JC3)
https://www.jc3.or.jp/english/

****

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