The Google Android Security Team's Classifications for Potentially Harmful Applications

April 2016

android

Overview

This document covers the Android Security Team's taxonomy for classifying apps that pose a potential security risk to users or their data. These types of apps are often generically referred to as "malware." However, that term lacks a well-defined and universally accepted taxonomy, so we refer to such apps as "Potentially Harmful Applications" (PHAs) to avoid confusion.

The PHA classifications have changed over the years along with the ecosystem, and we expect them to continue to develop. By releasing this information, we hope to provide greater insight into our current approach to PHAs. We also believe it's best for users if the security community uses a consistent naming convention when referring to threats. While our classifications are not perfect, we hope that they provide a good start that sparks an ongoing discussion and helps others verify our externally released data.

How the classifications are used

Verify Apps warns the user if it detects the attempted installation of any app that falls into one or more of these categories on their device. When we detect that a PHA contains features from multiple categories, it is classified based on the most harmful characteristics. For example, if an app applies to both ransomware and spyware categories, the Verify Apps message would refer only to ransomware.

Google Play prohibits all PHAs, so we also use these classifications in our evaluations of apps that developers submit for publication.

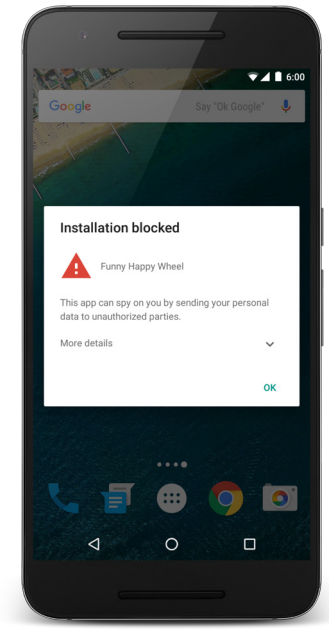

Figure 1: SMS Fraud Warning

Categories of Potentially Harmful Applications

Backdoors

This app lets hackers control your device, giving them unauthorized access to your data.
An application that allows the execution of unwanted, potentially harmful, remote-controlled operations on a device. The operations may include behavior that would place the app into one of the other PHA categories if executed automatically. In general, backdoor is more a description of how a potentially harmful operation can occur on a device and is therefore not completely aligned with categories like billing fraud or commercial spyware.

Billing fraud
An application that charges the user in an intentionally misleading way.

Here are some categories of Billing Fraud. Note that premium services are not necessarily flagged as Billing Fraud: only those that charge the user without an adequate consent.

SMS Fraud
An application that charges users to send premium SMS without consent. For example, a game app that, while the user plays it, secretly downloads a list of premium numbers and sends SMS messages from the user's device to the numbers.

Call Fraud
An application that can add charges to a user's mobile bill by making costly calls without informing them first.

Wireless Access Protocol (WAP) Fraud
An application that adds charges to a user's mobile bill by connecting to a third-party service without asking them first.

Commercial Spyware
An application that transmits personal information from the device without adequate notice or consent. The software is typically marketed as a tool intended for supervision (e.g., for parent), and may or may not reveal itself to the person being supervised.

Data Collection
An application that collects data about installed applications without adequate notice or consent. This may include collecting the actual list of installed apps, as well as partial information like the currently active apps.

Denial of Service
An application that, without the knowledge of the user, executes a denial-of-service attack or is a part of a distributed denial-of-service attack against other systems and resources. This can happen by sending a high volume of http requests to produce excessive load on remote servers.

Hostile Downloaders
An application that is not in itself potentially harmful, but downloads other potentially harmful apps. For example, a gaming app that does not contain malicious code, but persistently displays a misleading "Security Update" link that installs harmful apps.

Non-Android Threat
An application that contains non-Android threats. These apps are unable to cause harm to the user or Android device, but contain components that are potentially harmful to other platforms.

Phishing Applications
An application that pretends to come from a trustworthy source, requests a user's authentication credentials and/or billing information, and sends the data to a third-party. This category also applies to apps that intercept the transmission of user credentials in transit.

Privilege escalation apps
An application that compromises the integrity of the system by breaking the application sandbox and allowing one application to interact with other apps on the device or system in a manner that is forbidden by the intended design of the application sandbox. An example of this would be an app that prevents its removal by abusing device administrator APIs. Note: privilege escalation apps that root devices are classified separately as rooting apps.

Ransomware
An application that takes partial or extensive control of a device or data on a device, and demands payment to release control. Some ransomware apps encrypt data on the device and demand payment to decrypt data, and/or leverage the device administrator features so that the app can't be removed by the typical user.

Rooting apps
A privilege escalation app that roots the device.

There is a difference between malicious rooting apps and non-malicious rooting apps. Non-malicious rooting apps let the user know in advance that they are going to root the phone, and they do not execute other potentially harmful actions that apply to other PHA categories.

Malicious rooting apps do not let the user know in advance that they will root the phone, or they inform the user about the rooting in advance but also execute other actions that apply to other PHA categories.

Spam
An application that sends unsolicited commercial messages to the user's contact list or uses the device as an email spam relay.

Spyware
An app that attempts to take information from a device and send it to a third party without adequate notice or consent from the user of the device. For example, an app that sends the developer an email containing the names and phone numbers of all people on the device's contact list without user notification or in a manner that is unexpected to the user.

Trojan
An application that appears to be benign (e.g., a game that claims only to be a game) and performs undesirable actions against the user. This classification is usually used in combination with other categories of harmfulness. A trojan will have an innocuous app component and a hidden harmful component. For example, a tic-tac-toe game that, in the background and without the knowledge of the user, sends premium SMS messages from the user's device.