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

February 2017

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.

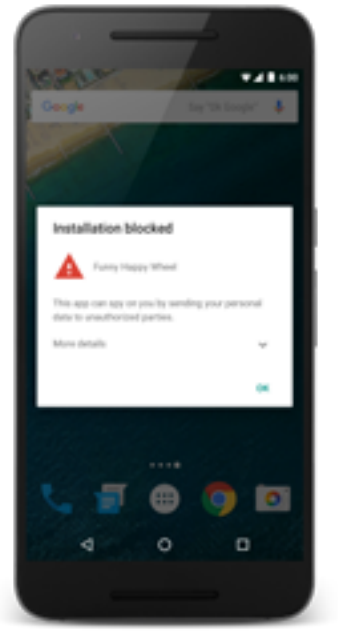

Figure 1: SMS Fraud Warning

Categories of Potentially Harmful Applications

Backdoors

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.

Commercial spyware
Any application that transmits sensitive information off the device without user consent and does not display a persistent notification that this is happening.

Commercial spyware apps transmit data to a party other than the PHA provider. Legitimate forms of these apps can be used by parents to track their children. However, these apps can be used to track a person (a spouse, for example) without their knowledge or permission if a persistent notification is not displayed while the data is being transmitted.

Data collection
Reclassified as Mobile Unwanted Software (MUwS).

Any application that collects at least one of the following without user consent:
— Information about installed applications
— Information about third-party accounts
— Names of files on the device

This includes collecting the actual list of installed applications as well as partial information like information about 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 downloader
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.

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

Mobile billing fraud is divided into SMS fraud, Call fraud, and Toll fraud based on the type of fraud being committed.

SMS fraud
An application that charges users to send premium SMS without consent, or tries to disguise its SMS activities by hiding disclosure agreements or SMS messages from the mobile operator notifying the user of charges or confirming subscription.

Some apps, even though they technically disclose SMS sending behavior introduce additional tricky behavior that accommodates SMS fraud. Examples of this include hiding any parts of disclosure agreement from the user, making them unreadable, conditionally suppressing SMS messages the mobile operator sends to inform user of charges or confirm subscription.

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

Toll fraud
An application that tricks users to subscribe or purchase content via their mobile phone bill.

Toll Fraud includes any type of billing except Premium SMS and premium calls. Examples of this include: Direct Carrier Billing, WAP (Wireless Access Point), or Mobile Airtime Transfer.

WAP fraud is one of the most prevalent types of Toll fraud. WAP fraud can include tricking users to click a button on a silently loaded transparent WebView. Upon performing the action, a recurring subscription is initiated, and the confirmation SMS or email is often hijacked to prevent users from noticing the financial transaction.

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
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.

Common targets of phishing include banking credentials, credit card numbers, or online account credentials for social networks and games.

Privilege escalation
An application that compromises the integrity of the system by breaking the application sandbox, or changing or disabling access to core security-related functions. Examples include:
— An app that violates the Android permissions model, or steals credentials (such as OAuth tokens) from other apps.
— An app that prevents its own removal by abusing device administrator APIs.
— An app that disables SELinux.

Note: Privilege escalation apps that root devices without user permission are classified 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.
Examples include:
— An app that locks a user out of their device and demands money to restore user control.
— An app that encrypts data on the phone and demands payment, ostensibly to decrypt data again.
— An app that leverages device policy manager features and cannot be removed by the user.

Rooting
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 device and they do not execute other potentially harmful actions that apply to other PHA categories.

Malicious rooting apps do not inform the user that they will root the device, 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 application that transmits sensitive information off the device.

Transmission of any of the following without disclosures or in a manner that is unexpected to the user are sufficient to be considered spyware:
— contact list
— photos or other files not owned by the application
— content from user email
— call log
— SMS log
— web history or browser bookmarks of the default browser
— information from the /data/ directories of other applications.

Behaviors that can be considered as spying on the user can also be flagged as spyware. For example: recording audio or recording calls made to the phone, stealing application data, etc.

Trojan
An application that appears to be benign 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.