Adware Apps Seen With Optimized Evasion Features

By Song Wang (words)

Published: 2019-10-18 · Archived: 2026-04-05 20:36:31 UTC

At the start of the year, Google updated its permission requests in Android applications, and in particular, restricted access to SMS and CALL Log permissions. Google also added requirements for non-default applications (or those that don't provide critical core features), allowing them to prompt and ask users for permission to access the device's data.

This restriction is meant to prevent fake or malicious apps from abusing these features to deliver malware, steal personally identifiable information, or perpetrate fraud. But as last year's mobile threat landscapeopen on a new tab showed, fraudsters and cybercriminals will always try to follow the money, whether fine-tuning their strategies, finding ways to bypass restrictions, or, in a recent case we've seen, revert to old but tried-and-tested techniques.

This is recently exemplified by an app we found on Google Play named "Yellow Camera" (detected by Trend Micro as AndroidOS_SMSNotfy), which poses as a camera and photo beautification or editing app — an increasingly common trick we've observed, what with the various information-stealing as well as malware- or adware-ridden apps we've uncovered so far this year. While the functions work as advertised, it is embedded with a routine that reads SMS verification codes from the System Notifications, and, in turn, activate a Wireless Application Protocol (WAP) billing. We disclosed our findings to Google, and the app, along with similar ones we saw, are no longer in the Play store.

Based on the name of the file downloaded by the app, it appears it is mostly targeting users in Southeast Asian countries (e.g., Thailand, Malaysia). However, we've also seen the app targeting Chinese-speaking users, so it won't be a surprise if the app to gradually shift or expand their targets. While Google already removed the app from the Play store, we found that the fraudsters uploaded similar apps to the Play Store, as shown in Figure 5.

WAP-billing services are widely used as an alternative payment method for users to buy content from WAP-enabled sites. These services charge purchases directly to the user's phone bill or credits without having to register for services, key in credentials, or use credit or debit cards. Unfortunately, fraudsters appear to have also taken advantage of this convenience. Based on the app's reviews on the Play Store (Figure 1), some of the users already lost phone credits to the app.

intelFigure 1. Screenshot showing reviews about the app; one user noted how she lost mobile credits after installing the appintel Figure 2. Infection chain of the malicious app

Yellow Camera's Infection Chain

Here are additional details of Yellow Camera's infection chain, as visualized in Figure 2:

- [MCC+MNC].log, which contains the WAP billing site address and JS payloads, is downloaded from hxxp://new-bucket-3ee91e7f[-]yellowcamera[.]s3[-]ap[-]southeast[-]1[.]amazonaws[.]com. MCC is the SIM provider's mobile country code; MNC is the mobile network code.
- The WAP billing site runs in the background; the site accessed/displayed is telco-specific, based on the [MCC+MNC].log.
- The JS payloads auto-clicks Type Allocation Code (TAC) requests — codes used to uniquely identify wireless devices.

For persistence, the malicious app uses the startForeground API to put the service in a foreground state, where the system considers it to be something the user is actively aware of and thus would not be terminated even if the device is low on memory.

We also found other apps (Figure 5), posing as photo filtering or beautifying apps, bearing the same routine of fraudulently subscribing the device to a WAP service. While they do share similar codes, we can't fully confirm if these apps came from the same operators, or the group behind the Yellow Camera app.

intelFigure 3. Code snippet showing the file being downloaded by the app

intelFigure 4. Snapshot of WAP-billing site where TAC is requested and subscription is confirmed

intelFigure 5. Screenshots of apps with malicious routines similar to those of the Yellow Camera app

Best practices and Trend Micro solutions

The fraudsters' technique may appear undistinguished, as WAP billing scams and fraudulent subscriptionservices to premium services aren't new. However, this can be seen as a different approach or response to security controls designed to mitigate threats or deter abuse of device functionalities, particularly the Notifications feature. Previous scams, for example, relied on SMS to fetch verification codes, and would often require the device to switch connections between Wi-Fi and mobile data. Given how it affected the users who installed the apps, the malicious app showed how it can conveniently steal money by abusing the device's other functionalities.

Also of note is how scammers and cybercriminals adapt their tactics — or the way they ride social networking trends — in their social engineering lures, as we've seen increased incidence in using photo editing or beautification apps as decoys to entice unwitting users into downloading fraudulent or malicious apps.

For the end-users' part, however, it pays to read an app's reviews before installing them, as they can help identify apps with fraudulent or suspicious behaviors. Users should also adopt best practicesopen on a new tab for securing mobile devicesopen on a new tab, especially against socially engineered threats.

Users can also benefit from security solutions that can thwart stealthy adware, such as Trend Micro™ Mobile Security for Android™products (also available on Google Play), which blocks malicious apps. End users can also benefit from its multilayered security capabilities that secure the device owner's data and privacy and that safeguard them from ransomware, fraudulent websites, and identity theft.

For organizations, the Trend Micro™ Mobile Security for Enterpriseproducts suite provides device, compliance and application management, data protection, and configuration provisioning, as well as protects devices from

attacks that exploit vulnerabilities, prevents unauthorized access to apps and detects and blocks malware and fraudulent websites. Trend Micro's Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learningopen on a new tab technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

The indicators of compromise (IoCs) are in this appendixopen on a new tab.

MITRE ATT&CK techniques

Tactic	Technique	ID	Description
Initial Access	Deliver Malicious App via Authorized App Store	T1475	Used to upload malware to Google Play store
Persistence	App Auto-Start at Device Boot	T1402	Used to listen for the BOOT_COMPLETED broadcast
Impact	Premium SMS Toll Fraud	T1448	Used to autofill content on WAP billing page by embedded JS
Exfiltration	Alternate Network Mediums	T1438	Used to connect cellular networks rather than Wi-Fi
Command and Control	Standard Application Layer Protocol	T1437	Used to communicate with remote C&C server

---