REPORT

McAfee
Together is power.

McAfee Mobile Threat Report

Mobile Malware Is Playing Hide and Steal

McAfee Mobile Threat Report Q1, 2020

Mobile Malware Is Playing Hide and Steal

Consider the number of applications on your smartphone today. Which ones are actively used? Which ones are no longer used? While this is a simple check, more important questions often go unanswered. For example, **do you know what data each app collects**? What they do with the data? Or even who they share it with? Although it may be possible to find answers to some of these questions, chances are some, even most of them, will remain unanswered.

Of course, these questions are based on the apps that you can see. There is a **growing trend for certain apps to hide themselves**, stealing precious resources and data from mobile devices that are the passport to our digital world. The objective of these hidden apps is relatively straightforward: generate money for the developer. And it is a growing threat, with almost half of all malware on the mobile platform consisting of hidden apps.

In this edition of our mobile threat report we take a closer look into the world of hidden apps and the fraudulent compromise of the mobile space with fake reviews. In addition, we dive into the use of mobile platforms as a tool to deliver targeted spyware. Combined with the summary of threat statistics, this particular report demonstrates the **growing capability of adversaries targeting our smartphones** and where we, as defenders, need to focus our efforts.

We hope this provides an excellent resource for protecting your mobile devices and welcome your feedback.

Raj Samani
McAfee Fellow, Chief Scientist
(**Twitter@Raj_Samani**)

Authors

This report was researched and written by:

- **Raj Samani**
- **Contributions from the McAfee Advanced Threat Research and Mobile Malware Research team**

Connect With Us

You Are the Click Farm

Ratings and reviews have a significant impact on an app's ranking, so generating fake reviews is becoming another way of monetizing cybercrime. A new malware family, called LeifAccess or Shopper, takes advantage of the accessibility features in Android to create accounts, download apps, and post reviews.

We first identified this malware in May 2019, and it has been globally active since then with localized versions, especially in the United States and Brazil.

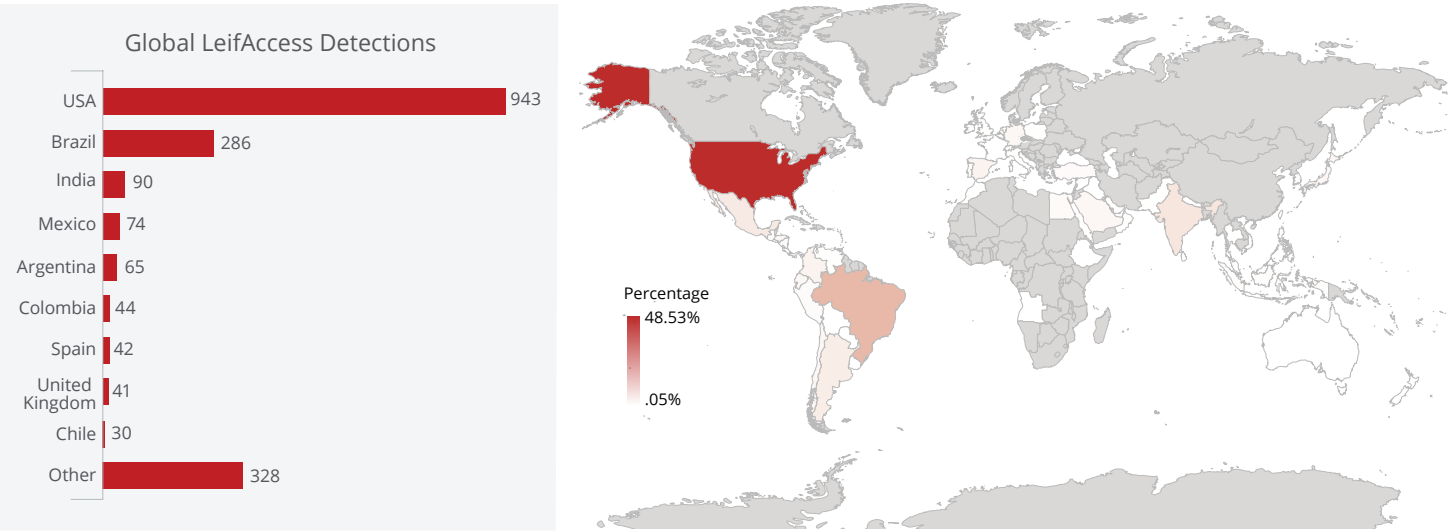

Figure 1. Worldwide detections of LeifAccess, 2019

LEIFACCESS/ SHOPPER

What is it?
Android-based malware that abuses single sign-on and accessibility services to create accounts and post fake reviews

Current threats

- Distributed via malvertising and found uploaded to Discord chat service
- No icon or shortcut visible after installation
- Posts fake reviews on Google Play to affect app rankings
- Advertising click fraud
- Automatically download other apps from Google Play

Future threats

- Can act as an installer for other malware

Connect With Us

Fake Security Notifications

LeifAccess is known to be distributed via fraudulent advertising and also found uploaded to Discord, a chat service for gamers. Once installed, the variant we analyzed calls itself "SystemSecurityService" to gain legitimacy and scare the user. **No icon or shortcut is displayed**, making it difficult for users to find and remove the malicious app. Fake warnings are used to get the user to activate accessibility services, enabling the full range of the malware's capabilities. These cover a range of vague but scary system warnings, such as "system needs to upgrade your video decoder,", "application reduces your phone performance, please check it now," and "security error should be dealt with immediately." In an effort to separate the warnings from installation, the malware waits up to eight hours before showing the fake notification.

Abusing Accessibility

Android's accessibility features are intended to help people overcome obstacles to using their devices, whether from disability or other situations. For example, it is possible to use voice commands instead of the touch screen. Google has restricted the permissions on accessibility features and moved functions to new application programming interfaces (API) in an effort to combat abuse of these tools, but criminals are still able to abuse this functionality. One of the key features being abused is **the ability to automate actions in the graphical interface in the background**. Users can combat this by checking their accessibility permission settings and turning them off if they are not needed. However, this malware can still perform click fraud and install other apps without accessibility functions.

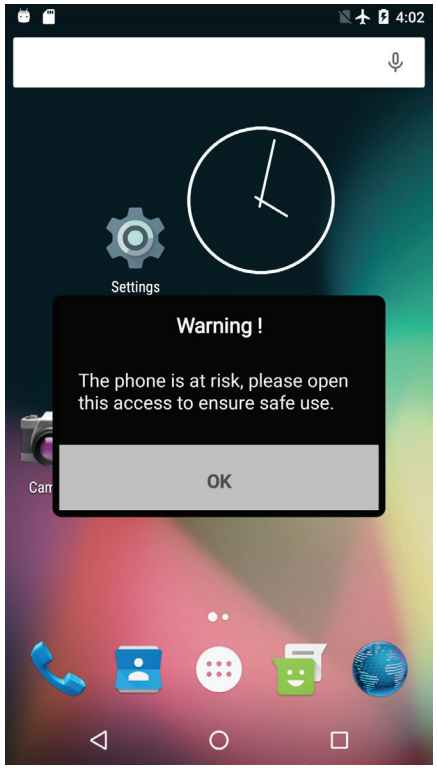

Figure 2. Toast notification displaying fake warning to launch settings view.

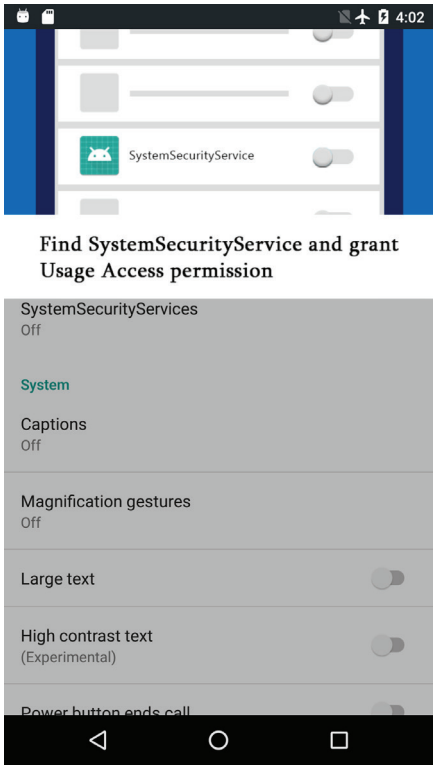

Figure 3. Settings view with GIF animation displaying how to activate Accessibility Services.

Connect With Us

Ad Fraud and Fake Reviews

One example of an app that appears to have many fake reviews is *Super Clean-Phone Booster, Junk Cleaner & CPU Cooler*. This app had a 4.5 star average rating and more than 7,000 reviews, many of them containing phrases provided by LeifAccess command and control server such as "very simple and useful," "very good mobile app cleaner", "Great, works fast and good," and **25 other phrases in more than one language** that can be used alone or in combination to make them appear varied and more genuine. LeifAccess also looks for reviews that match words and phrases related to positive reviews and can give them a five-star rating to boost their visibility and ranking. At best, this increases the likelihood of users downloading poor quality apps. At worst, these fake reviews may legitimize malicious apps and perpetrate additional frauds. *Super Clean-Phone Booster, Junk Cleaner & CPU Cooler* has since been removed from Google Play because it was found to be distributing LeifAccess via malvertising.

Finally, this malware is an ad fraud accomplice, requesting ad traffic from its control servers and then simulating clicks to fraudulently boost ad revenue. Some of these ads are displayed to the user while others are requested but not displayed, generating far more fake displays and clicks than the user is aware of and consuming memory and processing capacity of the victim's phone.

What You See Is Not What You Get

Hidden apps are the most active mobile threat category, generating almost half of all malicious telemetry this year, a 30% increase from 2018. Thousands of apps are actively hiding their presence after installation, making them difficult to locate and remove while annoying victims with invasive ads.

Digital ad revenue comes from raw numbers—screens displayed and clicks captured. Fraudulently increasing these numbers is becoming a very popular **malware monetization technique**. Criminals are tricking users into installing adware on their devices that redirects them to a range of different ad types and topics. Built-in intervals and event triggers control the frequency of the ad redirects, so that many users will not realize that their device is infected.

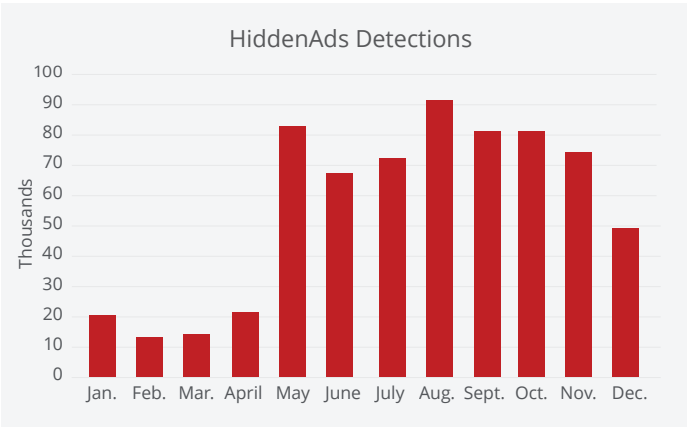

Figure 4. HiddenAds telemetry, 2019.

Hiding During Installation

We analyzed two HiddenAds variants, one pretending to be the game Call of Duty and the other a photo tool called *FaceApp*. Both used file names similar to their genuine counterparts and were distributed, not in Google Play, but as links in YouTube videos and other search results of people looking for free or cracked apps. The **fake apps used icons that closely mimic the real apps** for additional authenticity. Once the app is installed on the phone, the icon is changed to one that mimics Settings. When the user clicks on this, the malicious app displays a fake error message—"Application is unavailable in your country. Click OK to uninstall." However, clicking OK completes the installation and then hides the fake *Settings* icon, making it difficult for the user to find and delete the malware.

Hiding From Analysis

In an effort to hide from malware analysis and discovery, HiddenAds also tries to obfuscate the code. Similar to many malware apps, the initial app is just a downloader or dropper for the real malicious program. This code is typically encrypted, the first layer of concealment. In

HIDDENADS MALWARE

What is it?
Android-based malware that hides itself and redirects users to to ads, then gets them to click on ads to collect fraudulent ad revenue

Current threats
- Masquerades as genuine apps, with similar names and icons, or apps with basic functionality
- Changes icon to hide after installation
- Redirects user to various types of ads and collects user data

Future threats
- Libraries also include click fraud functionality
- Can act as an installer for other malware
- Multiple event monitoring and trigger control functions for future exploitation

Connect With Us

addition, the functions are split into multiple sub-functions, spreading the actions throughout the code and **making it more challenging to evaluate and compare to known malware**. The sub-functions are also padded with many nonsense operations to further confuse investigators and escape detection.

Triggering Ad Requests

Earlier variants of HiddenAds displayed ads frequently, trying to generate as much fraudulent revenue as possible before being removed. These new versions use a **time interval to manage the number of ads displayed in the hopes of remaining undiscovered**. The version that McAfee Mobile Research analyzed contained two timers: *Install Frequency* and *Start Delay*. *Install Frequency*, which was set to 1,000 seconds (16 minutes and 40 seconds), limits the rate of install requests. This timer is triggered when the app is launched, and during our analysis many of the install responses were empty, making analysis more difficult. *Start Delay* was set to 30,000 seconds (5 hours and 20 minutes) and limits the frequency of web requests for ad content. These web page requests are triggered by various user or device events, such as opening or closing apps, unlocking the phone, receiving notifications, installing or uninstalling apps, and even changing the device orientation. Responses to web requests from the adware include not just the ad URL, but also code updates and some tracking and status data. Other event triggers in the malware, including browser history and YouTube cache, may be used to target ads to make them appear more legitimate. For example, when victim is

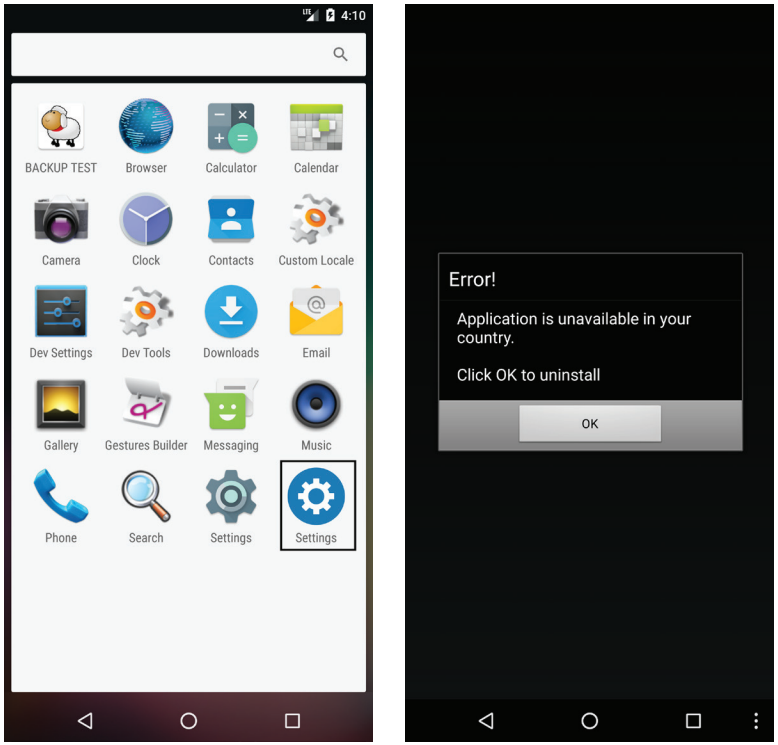

Figure 5. Fake Settings icon and application unavailable error

browsing or watching a video, the malware controller can select a full screen ad that appears to be a genuine part of the activity, reducing the chance that the user will look for and remove the infection.

HiddenAds poses multiple threats to mobile consumers beyond the annoying ads. This malware can collect device and user information, invading the user's privacy. It can also suggest and distribute other malicious applications, based on the event triggers and monitoring the user's behavior.

Watch Out for the MalBus

McAfee Mobile Research team **discovered** Daegu Bus was one of four popular Korean-language bus information apps in South Korea to be compromised in this attack. The malware tries to phish for the user's Google account information, **scans the device for sensitive military and political keywords**, and uploads any matching documents. These apps, which have provided regional transit information, such as bus stop locations, route maps, and schedule times for more than five years, have now been removed from Google Play. The infected apps contain an additional library that reaches out to one of several hacked web servers to get a malicious plugin, disguised as a media file with a .mov extension.

Legitimate App Hacked

MalBus represents a new attack method. Instead of building a fake app and pushing it up the ranking with fake reviews, **these criminals went after the account of a legitimate developer** of a popular app with a solid reputation. Two variants of this app reported more than 100,000 and 500,000 installs. After the threat actors got into the account, they added an additional library to the apps and uploaded them to Google Play. During installation the malicious library checks whether it is already installed, and, if not, runs an update process to download and dynamically load a malicious Trojan disguised as a media file.

Phish for Google Account

After completing the installation, MalBus opens a local web page that mimics the Google login screen. Filled with JavaScript, this page collects the registered user's email address, pre-fills the page with that email as the username, and then prompts for the password. If this step is successful, the malware then **attempts to change the recovery email** for the account to an address they control, and then trigger a password recovery event. This would enable them to change the password and take over the account. In the event that a new Google account is created by the user, they also attempt to set the recovery email to their own. Fortunately, these attempts to change or set the recovery email are unsuccessful.

MALBUS SPYWARE

What is it?
Targeted attack hidden in a legitimate South Korean transit app by hacking the original developer's Google Play account

Current threats
- Phishes for victim's Google user id and password with a fake login page
- Drops malicious Trojan on device
- Searches user's device for specific military and political keywords and exfiltrates files
- Malware can run commands and download, upload, or delete files

Future threats
- Infected device is fully compromised

Connect With Us

Search for Keywords

The primary objective of this spyware appears to be scanning the user's device for specific keywords and exfiltrating documents and files that reference them. MalBus indexes the directory structure to enable a walk-through of all of the files on the device. Then it scans each for specific keywords, including "National defense," "National Intelligence Service," "Defect," "Military operation," and a **long list of military and political terms and titles**. Files matching any of these words are uploaded to a remote server.

Summary

Mobile malware is finding new ways to hide

2020 is looking like the year of mobile sneak attacks. Last year, cybercriminals and nation-states increased their mobile attacks with a wide variety of methods, from backdoors to mining cryptocurrencies. This year, they have expanded the ways of hiding their attacks and frauds, making them increasingly difficult to identify and remove.

Still Going for the Easy Money

With the exception of nation-state attacks, most mobile cybercriminals seem to want the quickest and easiest path to money. After trying several different ways of monetizing their efforts over the last few years, click fraud, fake reviews, and malvertising appear to be the easy money. Advertisers pay small amounts for each ad display or click-through, so the trick is to **trigger as many fraudulent actions as possible before getting caught**. Initially, these malicious apps would act early and quickly, but now they are slowing down, hoping to remain unnoticed.

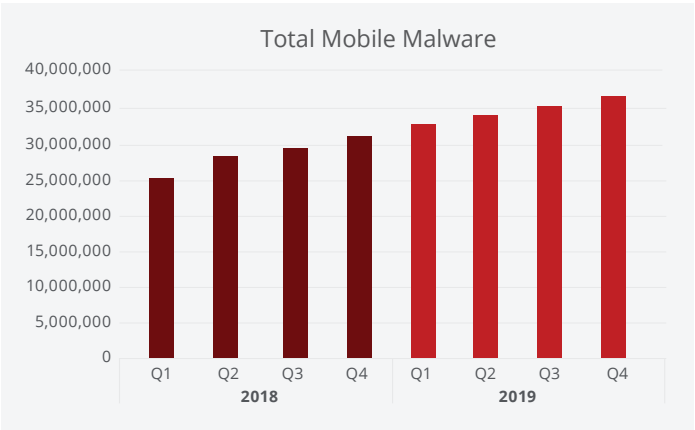

Figure 6. Total mobile malware detections by quarter.

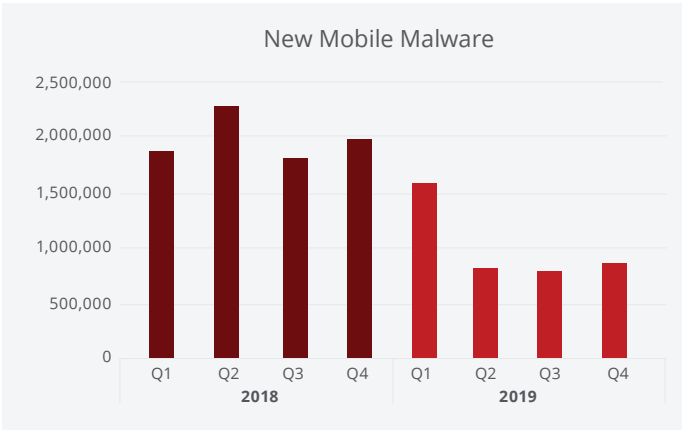

Figure 7. New mobile malware detections by quarter.

Connect With Us

You Cannot Fix What You Cannot Find

Criminals are not only finding new ways to generate fraudulent ad numbers, they are doing them out of sight, and, hopefully, out of mind, of the user. By hiding their app icons, users have to take more steps to find and remove unwanted apps. To help stay undetected, they are also using different techniques to **make their activities appear more legitimate**. By slowing down the number and frequency of ad displays and other fraudulent activities, they can hopefully produce a larger and more consistent revenue stream.

Laptop, Tablet, Smartphone, Spy

Regardless of what device you are using, nation-states and criminal organizations are constantly looking for data. From military information, to corporate intelligence, to personal behavior, there are people trying to steal it, aggregate it, and use it. As mobile devices grow in capacity and usage, they present an **increasingly rich and desirable target** for these spies. Data collection and personal privacy is an ongoing but growing challenge for companies, users, and regulators.

What to Do

While threat tactics continue to change as criminals adapt and respond to detection and enforcement techniques, there are a few steps users can take to limit their exposure and risk.

Stay on the app stores
While some malicious apps do make it through the screening process, the majority of the attack downloads appear to be coming from social media, fake ads, and other unofficial app sources. Before downloading something to your device, do some quick research about the source and developer. Many of these have been flagged by other users.

Read reviews with a critical eye
Reviews and rankings are still a good method of determining whether an app is legitimate. However, watch out for reviews that reuse the same simple phrases, as they are probably an indication of fake reviews pumping up a suspicious or malicious app.

Use security software
Comprehensive security software across all devices, whether they are computers, tablets, or smartphones, continues to be a strong defensive measure to protect your data and privacy from cyberthreats.

Update software
Developers are actively working to identify and address security issues. Both operating systems and apps should be frequently updated so that they have the latest fixes and security protections.

Monitor your IDs
Use ID monitoring tools to be aware of changes or actions that you did not make. These may have been caused by malware and could indicate that your phone or account has been compromised.

Findings represent threat analysis detected by the McAfee Threat Research Team after looking at incidents of mobile malware globally between October-December 2019. Predictions for future trends are based on prior findings and provided for informational purposes only.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com