Google Play Apps Drop Anubis, Use Motion-based Evasion

blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

January 17, 2019

Malware

We found malicious apps on Google Play trying to drop a banking malware payload on unsuspecting users. Motion sensor data was used to evade detection.

By: Kevin Sun January 17, 2019 Read time: (words)

We recently found two malicious apps on Google Play that drop wide-reaching banking malware. The two apps were disguised as useful tools, simply named Currency Converter and BatterySaverMobi. Google has confirmed that both these apps are no longer on the Play Store.

The battery app logged more than 5,000 downloads before it was taken down, and boasted a score of 4.5 stars from 73 reviewers. However, a close look at the posted reviews show signs that they may not have been valid; some anonymous usernames were spotted and a few review statements are illogical and lack detail.

We looked into this campaign and found that the apps dropped a malicious payload that we can safely link to the known banking malware Anubis (detected by Trend Micro as ANDROIDOS_ANUBISDROPPER). Upon analysis of the payload, we noted that the code is strikingly similar to known Anubis samples. And we also saw that it connects to a command and control (C&C) server with the domain *aserogeege.space*, which is linked to Anubis as well.

Besides *aserogeege.space*, 18 other malicious domains map to the IP address 47.254.26.2 and we confirmed that Anubis uses the subpath of these domains. These domains change IP addresses quite frequently and may have switched six times since October 2018, showing just how active this particular campaign is.

Fig 1.

Fig 1.

Fig 1.

Figure 1. Images of the malicious apps on Google Play

Table 1.

Table 1. Victim distribution for all BatterySaveMobi samples

How the apps evade detection

These apps don’t just use traditional evasion techniques; they also try to use the user and device’s motions to hide their activities.

As a user moves, their device usually generates some amount of motion sensor data. The malware developer is assuming that the sandbox for scanning malware is an emulator with no motion sensors, and as such will not create that type of data. If that is the case, the developer can determine if the app is running in a sandbox environment by simply checking for sensor data.

The malicious app monitors the user's steps through the device motion sensor. If it senses that the user and the device are not moving (if it lacks sensor data and thus, might be running in a sandbox environment), then the malicious code will not run.

Fig 2.

Figure 2. The malware tracks the user's movement; the malicious code will run if it senses motion

Command	Action

“::apk::”	*Download apk and trick user to install*
“kill”	*Stop running malicious code*

Table 2. C&C server commands

If the malicious code runs, then the app will try to trick the users into downloading and installing its payload APK with a fake system update.

Fig 3.

Figure 3. Fake system update

One of the ways the app developers hide the malicious server is by encoding it in Telegram and Twitter webpage requests. The bank malware dropper will request Telegram or Twitter after it trusts the running device. By parsing the response’s HTML content, it gets the C&C server (*aserogeege.space*). Then, it registers with the C&C server and checks for commands with an HTTP POST request. If the server responds to the app with an APK command and attaches the download URL, then the Anubis payload will be dropped in the background. It will try and trick users into installing it with the fake system update seen in Figure 3.

Fig 4.

Figure 4. The encoded server URL, showing the text results in the URL of the C&C server

The Anubis payload

The Anubis malware masquerades as a benign app, prompts the user to grant it accessibility rights, and also tries to steal account information. Banking trojans usually launch a fake overlay screen when the user accesses a target app and tries to steal information when the user inputs account credentials into the overlay. However, Anubis’ process is a little different. It has a built-in keylogger that can simply steal a users’ account credentials by logging the keystrokes. The malware can also take a screenshot of the infected users’ screen, which is another way to get the victims credentials.

Our data shows that the latest version of Anubis has been distributed to 93 different countries and targets the users of 377 variations of financial apps to farm account details. We can also see that, if Anubis successfully runs, an attacker would gain access to contact lists as well as location. It would also have the ability to record audio, send SMS messages, make calls, and alter external storage. Anubis can use these permissions to send spam messages to contacts, call numbers from the device, and other malicious activities. Previous research from security company Quick Heal Technologies shows that versions of Anubis even function as a ransomware.

Fig 5.

Figure 5. Some of the financial apps Anubis targets

Gaps in mobile security can lead to severe consequences for many users because devices are used to hold so much information and connect to many different accounts. Users should be wary of any app that asks for banking credentials in particular and be sure that they are legitimately linked to their bank.

Trend Micro Solutions

Trend Micro's Mobile App Reputation Service

Indicators of Compromise

SHA256 and URLs	***Definitions***
b012eb5538ad1d56c5bdf9fe9562791a163dffa4 bc87c9fffcdac4eea1b84c62842ce1138fd90ed6 7e025e21d445be9b6b12a9181ada4bab3db5819c e29c814c2527ebbac11398877beea2bc75b58ffd	IoCs
16fc9bc96f58ba35a04ade2d961b0108d135caa5	Payload
areadozemode.space selectnew25mode.space twethujsnu.cc project2anub.xyz taiprotectsq.xyz uwannaplaygame.space projectpredator.space nihaobrazzzahit.top aserogeege.space hdfuckedin18.top dingpsounda.space wantddantiprot.space privateanbshouse.space seconddoxed.space firstdoxed.space oauth3.html5100.com dosandiq.space protect4juls.space wijariief.space scradm.in	Command and control

Tags

Mobile | Malware | Research