Coin Miner Mobile Malware Returns, Hits Google Play

blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/

October 30, 2017

Malware

We found apps with malicious cryptocurrency mining capabilities on Google Play. These apps used dynamic JavaScript loading and native code injection to avoid detection.

By: Trend Micro October 30, 2017 Read time: (words)

Content added to Folio

The efficacy of mobile devices to actually produce cryptocurrency in any meaningful amount is still doubtful. However, the effects on users of affected devices are clear: increased device wear and tear, reduced battery life, comparably slower performance.

Recently, we found that apps with malicious cryptocurrency mining capabilities on Google Play. These apps used dynamic JavaScript loading and native code injection to avoid detection. We detect these apps as ANDROIDOS_JSMINER and ANDROIDOS_CPUMINER.

This is not the first time we've found these types of apps on app stores. Several years ago, we found malicious apps on the Google Play store detected as ANDROIDOS_KAGECOIN, a malware family with hidden cryptocurrency mining capabilities.

ANDROIDOS_JSMINER: Mining via Coinhive We've previously seen tech support scams and compromised websites used to deliver the Coinhive JavaScript cryptocurrency miner to users. However, we're now seeing apps used for this purpose, which we detect as ANDROIDOS_JSMINER. We found two apps; one supposedly helps users pray the rosary, while the other provides discounts of various kinds.

Figures 1 and 2. JSMINER Malware on Google Play

Both of these samples do the same thing once they are started: they will load the JavaScript library code from Coinhive and start mining with the attacker's own site key:

Figure 3. Code to start mining when the app starts

This JavaScript code runs within the app's webview, but this is not visible to the user because the webview is set to run in invisible mode by default.

Figure 4. Webview is set to invisible mode

When the malicious JavaScript code is running, the CPU usage will be exceptionally high.

ANDROIDOS_CPUMINER: Trojanized versions of legitimate apps

Another family of malicious apps takes legitimate versions of apps and adds mining libraries, which are then repackaged and distributed. We detect these as ANDROIDOS_CPUMINER.

One version of this malware is in Google Play and disguised as a wallpaper application:

Figure 5. Mining malware on Google Play store

The mining code appears to be a modified version of the legitimate *cpuminer* library. The legitimate version is only up to 2.5.0, whereas this malicious version uses 2.5.1. The code is added to normal applications, as seen below:

Figure 6. Code added to normal apps by CPUMINER

Please note that the above code layout was taken from a sample that is not found on Google Play, but belongs to the same family.

Figure 7. Malware with modified code

The mining code fetches a configuration file from the cybercriminal's own server (which uses a dynamic DNS service) that provides information on its mining pool via the Stratum mining protocol.

Figure 8. Cryptocurrency mining profits

The figure above shows that the attacker is mining various cryptocurrencies, with varying amounts of currencies mined. It also shows that the value of the coins mined over an unknown period amounts to just over 170 US dollars; total profits aren't known.

We have identified a total 25 samples of ANDROIDOS_CPUMINER. Trend Micro Mobile Security already detects these variants, as well as the JSMINER variants mentioned earlier in this post.

These threats highlight how even mobile devices can be used for cryptocurrency mining activities, even if, in practice, the effort results in an insignificant amount of profit. Users should take note of any performance degradation on their devices after installing an app.

We have reached out to Google, and the apps mentioned in this post are no longer on Google Play.

Indicators of Compromise The following malicious apps were found on Google Play and are connected to this threat:

SHA256 hash	App name	Package name	Detection name
22581e7e76a09d404d093ab755888743b4c908518c47af66225e2da991d112f0	Recitiamo Santo Rosario Free	prsolutions.rosariofacileads	ANDROIDOS_JSMIN
440cc9913d623ed42563e90eec352da9438a9fdac331017af2ab9b87a5eee4af	SafetyNet Wireless App	com.freemo.safetynet	ANDROIDOS_JSMIN
d3c0bed627edab9ac1bbc2bcc6e8c3ff45b4708afa527790e42a4a6fe2c045f0	Car Wallpaper HD: mercedes, ferrari, bmw and audi	com.yrchkor.newwallpapers	ANDROIDOS_CPUM