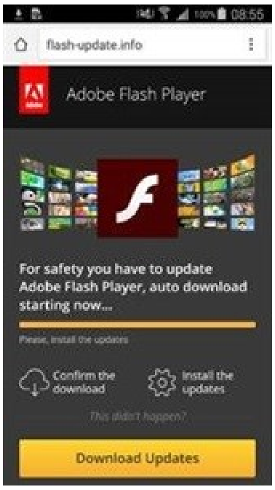
BIZCOMMUNITY

Dangerous new app masquerading as Flash Player update

ESET researchers discovered a dangerous new app targeting Android devices is capable of downloading and executing additional malware.



For safety you have to update Adobe Flash Player, auto download starting now...

Please, install the updates

Detected by ESET security software as Android/TrojanDownloader.Agent.JI, the trojan is distributed via compromised websites and masquerades as a Flash Player update. Unwary users who fall for installing the malware might find their mobile devices held ransom or bank accounts emptied.

Following installation, the malware creates a fake ‘Saving Battery’ service in the Android system and urges the victim to grant it crucial permissions within Android’s Accessibility functions. If granted, these permissions - "Monitor your actions", "Retrieve window content" and "Turn on Explore by Touch" - enable the attacker to mimic the user’s actions and display whatever they want on the user’s screen.

Designed for syphoning off funds from bank accounts

“In cases we investigated, this trojan was built to download another trojan designed for syphoning off funds from bank accounts. However, it would take only a small change in the code for the user to get served with spyware or ransomware,” warns Lukáš Štefanko, the ESET malware researcher who led the analysis.

The key indicator of whether a device has been infected with this malware is the presence of a “Saving Battery” option amongst Services in the Accessibility menu. In such a case, the user should either employ a reputable mobile security app, such as ESET Mobile Security & Antivirus, to remove the threat or uninstall the app manually by going to Settings ->

Application Manager -> Flash-Player.

In some instances, the user has been successfully tricked into granting Device administrator rights to the app. In such a case, it is necessary to deactivate the administrator rights first, by going to Settings -> Security -> Flash-Player.

Uninstalling doesn't remove malicious aps

“Unfortunately, uninstalling the downloader doesn’t remove malicious apps the downloader might have installed. As with the downloader itself, the best way for cleaning up the device is using a mobile security solution,” recommends Štefanko.

ESET security experts have prepared a set of basic recommendations for preventing infection with mobile malware:

- Only download apps or updates from a trustworthy source – in the case of an Adobe Flash Player update, the only safe place to get it from is the official Adobe website. Always check the URL address in your browser.
- Pay attention to what permissions and rights your apps request.
- Use a reputable mobile security solution.