New Android trojan mimics user clicks to download dangerous malware

welivesecurity.com/2017/02/14/new-android-trojan-mimics-user-clicks-download-dangerous-malware/

February 14, 2017

Android users are exposed to a new malicious app imitating Adobe Flash Player and serving as an entrance gate for potentially any kind of dangerous malware

Lukas Stefanko
14 Feb 2017 - 02:00PM

Android users are exposed to a new malicious app imitating Adobe Flash Player and serving as an entrance gate for potentially any kind of dangerous malware

Android users have been exposed to a new malicious app imitating Adobe Flash Player that serves as a potential entrance for many types of dangerous malware. The application, detected by ESET security software as Android/TrojanDownloader.Agent.JI, tricks its victims into granting it special permissions in the Android accessibility menu and uses these to download and execute additional malware of the attackers' choice.

According to our analysis, the trojan targets devices running Android, including the latest versions. It is distributed via compromised websites – adult video sites, but also via social media. Under the pretense of safety measures, the websites lure users into downloading a fake Adobe Flash Player update. If victims fall for the legitimate-looking update screen and runs the installation, they have more deceptive screens to look forward to.

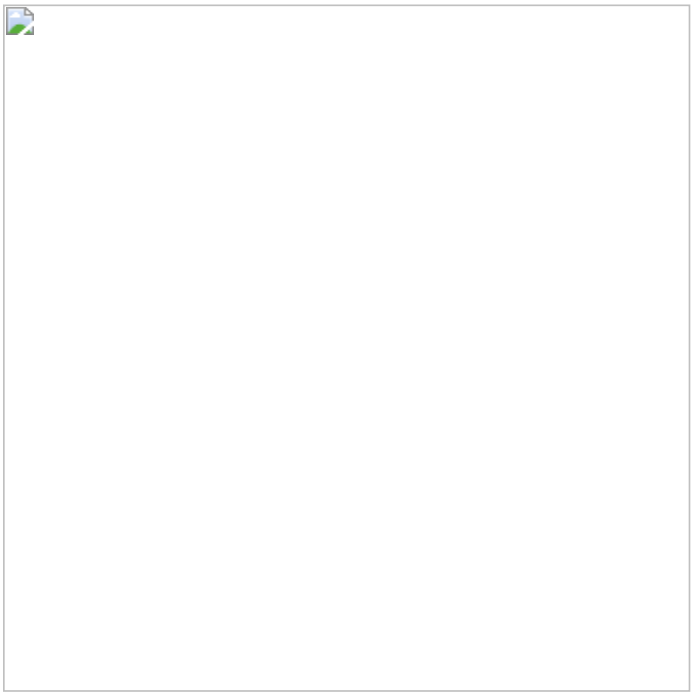

Figure 1: Fake Flash Player update screen

How does it work?

The next phony screen pops up following successful installation, claiming "too much consumption of energy" and urging the user to turn on a fake "Saving Battery" mode. Like most malicious pop ups, the message won't stop appearing until the victim gives in and agrees to enable the service. This opens the Android Accessibility menu, showing a list of services with accessibility functions. Among the legitimate ones, a new service (created

by the malware during installation) named “Saving battery” appears. The service then requests permissions to *Monitor your actions*, *Retrieve window content* and *Turn on Explore by Touch* – all crucial for future malicious activity, enabling the attacker to mimic the user’s clicks and select anything displayed on their screen.

Figure 2: Pop-up screen requesting “Saving Battery” after install

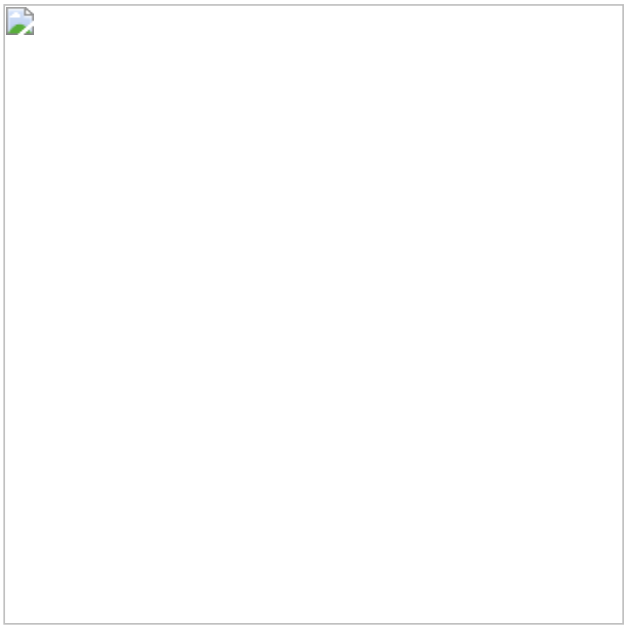

Figure 3: Android Accessibility menu with the malicious service

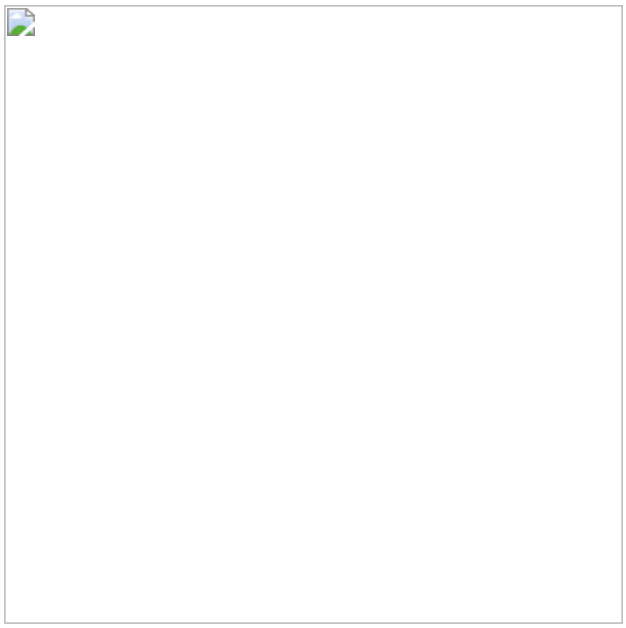

Figure 3: Android Accessibility menu with the malicious service

Once the service is enabled, the fake Flash Player icon hides from the user. However, in the background, the malware is busy contacting its C&C server and providing it with information about the compromised device. The server responds with a URL leading to a malicious app of the cybercriminal's choice – in the detected case, banking malware (though it could be any malware ranging from adware through spyware, and on to ransomware). After acquiring the malicious link, the compromised device displays a bogus lock screen with no option to close it, covering the ongoing malicious activity beneath it.

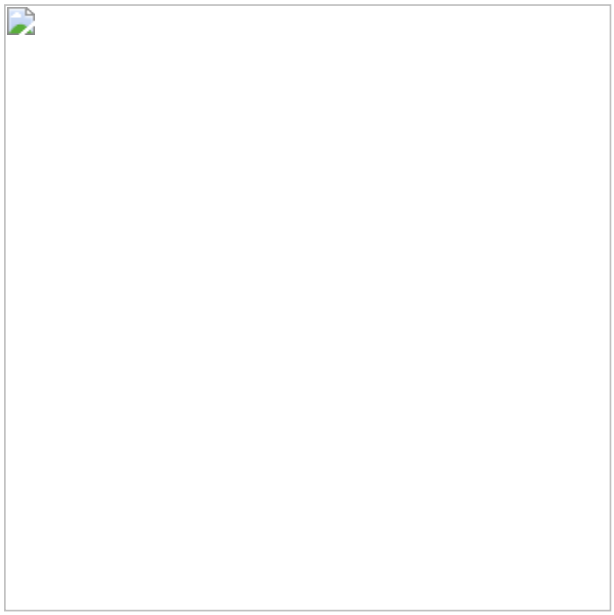

Figure 5: Lock screen covering malicious activity

This is when the permission to mimic the user's clicks comes in handy – the malware is now free to download, install, execute and activate device administrator rights for additional malware without the user's consent, all while remaining unseen under the fake lock screen. After the app's secret shenanigans are done, the overlay screen disappears and the user is able to resume using the mobile device – now compromised by the downloaded malware.

Has my device been infected? How do I clean it?

If you think you might have installed this fake Flash Player update in the past, you can easily verify by checking for ‘Saving Battery’ under Services in the Accessibility menu. If listed under the services, your device may very well be infected.

Denying the service its permissions will only bring you back to the first pop up screen and will not get rid of Android/TrojanDownloader.Agent.JI.

To remove the downloader, try manually uninstalling the app from Settings -> Application Manager -> Flash-Player.

In some instances, the downloader also requests that the user activate Device administrator rights. If that turns out to be the case and you can’t uninstall the app, deactivate the administrator rights by going to Settings -> Security -> Flash-Player and then proceed with uninstalling.

Even after doing so, your device might still be infected by countless malicious apps installed by the downloader. To make sure your device is clean, we recommend using a reputable mobile security app as a hassle-free way to detect and remove threats.

How to stay safe

To avoid dealing with the consequences of nasty mobile malware, prevention is always the key. Apart from sticking to trustworthy websites, there are a couple more things you can do to stay safe.

If you’re downloading apps or updates in your browser, always check the URL address to make sure you’re installing from the intended source. In this particular case, the only safe place to get your Adobe Flash Player update is from the official Adobe website.

After running anything you’ve installed on your mobile device, pay attention to what permissions and rights it requests. If an app asks for permissions that don’t seem appropriate to its function, don’t enable these without double checking.

Last but not least, even if all else fails, a reputable mobile security solution will protect your device from active threats.

If you’d like to find out more about Android-based malware, look into our latest research on the topic. You’re also welcome to stop by ESET’s stand at this year’s Mobile World Congress.

Video capture from an infected device (time edited)

Watch Video At: https://youtu.be/2Ozl5KZrUIs

Analyzed sample's Indicators of Compromise (IoCs)

Package Name	Hash	Detection name
loader.com.loader	4F086B56C98257D6AFD27F04C5C52A48C03E9D62	Android/TrojanDownloader.Agent.JI
cosmetiq.fl	C6A72B78A28CE14E992189322BE74139AEF2B463	Android/Spy.Banker.HD

14 Feb 2017 - 02:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion