Facestealer Trojan Hidden in Google Play Plunders Facebook Accounts

By Tara Seals

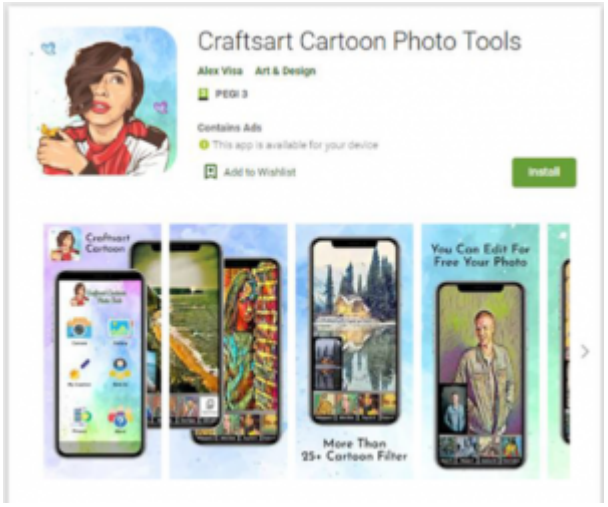
Published: 2022-03-21 · Archived: 2026-04-06 01:38:43 UTC

The trojanized Craftsart Cartoon Photo Tools app is available in the official Android app store, but it's actually spyware capable of stealing any and all information from victims' social-media accounts.

A popular mobile app in the official Google Play store called "Craftsart Cartoon Photo Tools" has racked up more than 100,000 installs – but unfortunately for the app's enthusiasts, it contains a version of the Facestealer Android malware.

That's according to researchers at Pradeo, who said the app performs somewhat as promised, pretending to be a legitimate photo editing tool. Specifically, it claims to allow users to convert photos into cartoon or "painting"-style versions using a few different filters. However, behind this mask lies a "small piece of [malicious] code that easily slips under the radar of store's safeguards," they explained.

Facestealer is a known Android threat that has made its way into Google Play in the past via trojanized apps. According to past Malwarebytes analysis, when the application is first launched, it guides the user to the legitimate main Facebook login page and asks users to log in before they can use the app. Then, "injected malicious JavaScript steals the login credentials and sends them to a command-and-control server," according to the firm. "The C2 server makes use of login credentials to authorize access to the [account]."



Splash page for the Craftsart Cartoon Photo Tools app, from Google Play.

From there, the trojan is off to the data-stealing races: It lifts information from victims' Facebook accounts, including email addresses and IP addresses, phone numbers, conversations and messaging histories, credit-card details, friend lists and more.

"When your login credentials for a social-media account have been stolen this can have serious consequences," explained Pradeo researchers, in a Monday writeup. "It gives threat actors a base from which to gather more information." They added, "Facebook credentials are used by cybercriminals to compromise accounts in multiple ways, the most common being to commit financial fraud, send phishing links and spread fake news."

A Pradeo analysis of Craftsart Cartoon Photo Tools found that the app makes connections to a Russian-registered domain that has been used for at least seven years as the command-and-control (C2) address for various malicious Android apps.

"[The domain] is connected to multiple malicious mobile applications that were at some points available on Google Play and later deleted," they explained. "To maintain a presence on Google Play, repackaging mobile apps is common practice for cybercriminals. Sometimes, we even observed cases in which repackaging was entirely automated."

Pradeo researchers said they alerted the Google Play team about the app, but as of Monday, it was still available in the official store. Obviously, users should delete the app immediately from their phones.

Avoiding Google Play Malware

Kaspersky, in a February posting, noted that malware was increasingly popping up in Google Play, using the same tactic that Craftsart Cartoon Photo Tools uses.

"The most common way to sneak malware onto Google Play is for a trojan to mimic a legitimate app already published on the site (for example, a photo editor or a VPN service) with the addition of a small piece of code to decrypt and launch a payload from the trojan's body or download it from the attackers' server," researchers explained. "Often, to complicate dynamic analysis, unpacking actions are performed through commands from the attackers' server and in several steps: each decrypted module contains the address of the next one, plus instructions for decrypting it."

User should thus always be wary of any app with warning signs. In this current case, even though the app has managed to attract a large number of installs, there are definite red flags in the reviews.

Some users flagged the forced Facebook login, commenting that it must be "some kind of phishing." Others comments included, "fake fake fake" and "very very very bad app," which sum up the overall reactions of reviewers. Also, some noted that the functionality the app claims to have is limited or nonexistent – always a sign to stay away.

In all, Craftsart Cartoon Photo Tools has a 2.1-star rating, with the majority of the reviews being one-star assessments, balanced out by a handful of obviously fake five-star reviews. There are no two-, three- or four-star ratings, which is clearly telling.

Moving to the cloud? Discover emerging cloud-security threats along with solid advice for how to defend your assets with our FREE downloadable eBook, "Cloud Security: The Forecast for 2022." We explore organizations' top risks and challenges, best practices for defense, and advice for security success in such a dynamic computing environment, including handy checklists.
