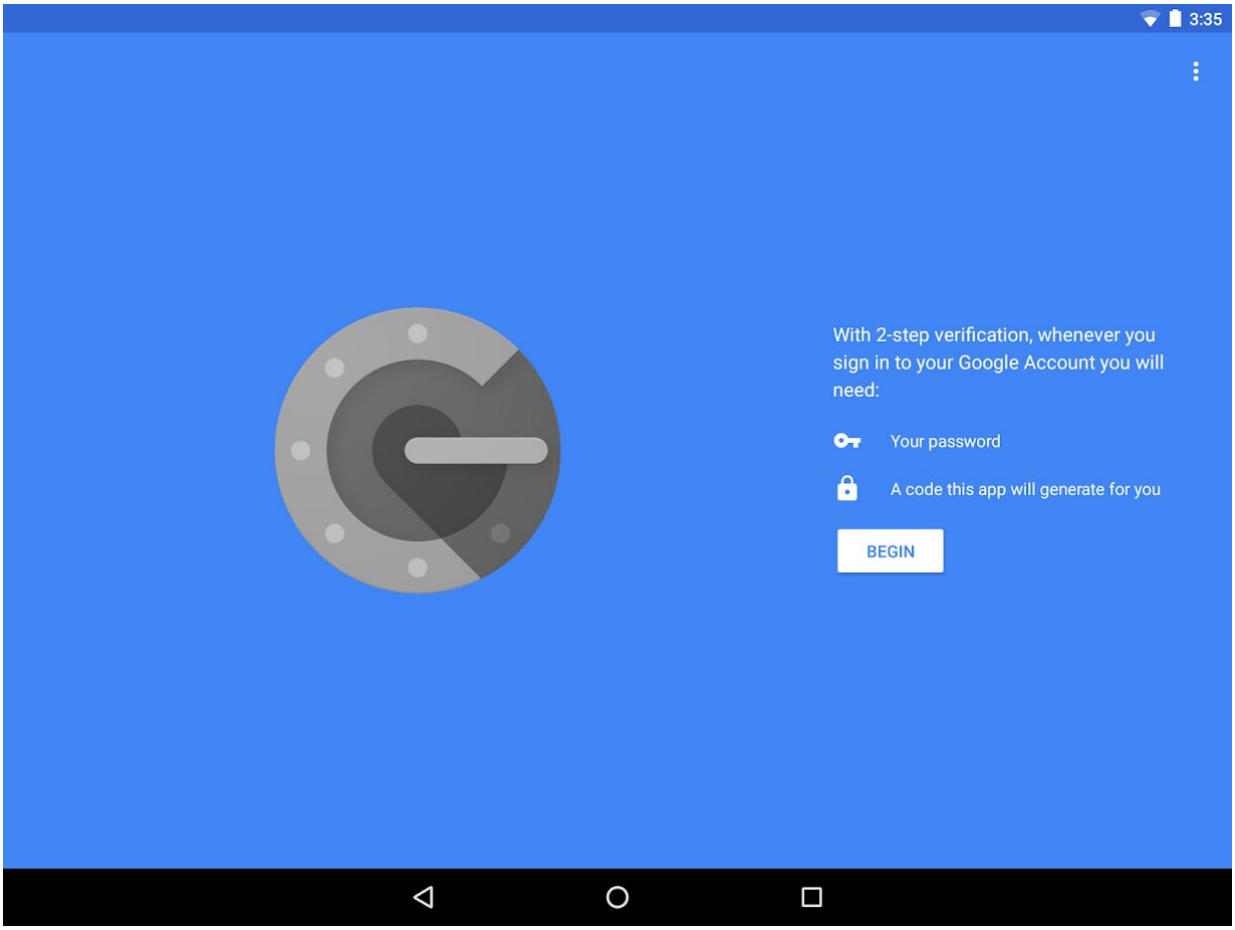
Google Authenticator app susceptible to malware attacks

March 3 2020, by Jelani Harper



New research indicates the Google Authenticator app on Android

devices is vulnerable to a form of malware known as Cerberus. According to financial cyber security specialist ThreatFabric, this banking Trojan can steal one-time pass codes generated by the app and potentially enable hackers to access bank accounts.

Google Authenticator provides a two-factor authentication (2FA) layer for protecting online accounts. Accessible through smartphones, it was conceived as a preferable alternative to SMS-based passcodes that are sent through mobile networks with varying (and dubious) levels of security.

Hackers that gain Google Authenticator's passcodes with Cerberus could access any of the accounts safeguarded by it, including email inboxes, social media, and most other user-based platforms of online activity.

Cerberus works by targeting the accessibility privileges on Android devices. Its capabilities are viewed as effective as those of remote access trojans (RATs), highly sophisticated malware that enables hackers to remotely control a user's mobile device, and which were "designed and used primarily to access and steal information that facilitates financial fraud," according to ThreatFabric.

As is the case with most RATs, once Cerberus is used to control an Android OS mobile device, infiltrators can leverage their credentials to take over the owner's bank account. They can then use the malware's features for stealing Google Authenticator's passcodes to evade any 2FA security measures.

Cerberus' potential for fraudulent activities doesn't end there. Once it's used to compromise mobile devices, it can alter device settings, access any existing apps, delete or install apps, and "also provide valuable insight into victims' behaviors and habits," according to ThreatFabric. The banking Trojan can scour the device's entire file system,

downloading anything it accesses.

Cerberus initially emerged on the threat landscape in June of 2019. Its RAT capabilities are distinct improvements over the strain detected over the summer, which was transacted on underground forums. Its capacity to compromise 2FA is extremely rare for malware, placing it in the upper echelons of this form of cyber attacks.

Currently, there are no reports of the present Cerberus strain being transacted on dark web forums. Still, members of the Android community are alarmed at its potential for misuse, citing its obvious ramifications for data privacy and online safety.

According to ThreatFabric, this banking Trojan is particularly formidable: "Having an exhaustive target list including institutions from all over the world, combined with its new RAT capability, Cerberus is a critical risk for financials offering online banking services. Whether in its target list or not, it is easy for its operators to enhance the list to target additional apps."

Google has yet to respond with any potential patches or solutions for this vulnerability.

More information: www.threatfabric.com/blogs/202 … year_of_the_rat.html

Citation: Google Authenticator app susceptible to malware attacks (2020, March 3) retrieved 25 April 2024 from https://techxplore.com/news/2020-03-google-authenticator-app-susceptible-malware.html