ESET Research discovers financial fraud using novel phishing method tailored to Android and iPhone users

DUBAI, UNITED ARAB EMIRATES, August 20, 2024 /EINPresswire.com/ -- ESET Research discovered an uncommon type of phishing campaign targeting mobile users, and analyzed a case observed in the wild that targeted clients of a prominent Czech bank. This technique is noteworthy because it installs a phishing application from a third-party website without the user having to allow third-party app installation. On Android, this could result in the silent installation of a special kind of APK, which even appears to be installed from the Google Play store. The threat targeted iPhone (iOS) users as well.

The phishing websites targeting iOS instruct victims to add a Progressive Web Application (PWA) to their home screens, while on Android, the PWA is installed after confirming custom pop-ups in the browser. At this point, on both operating systems, these phishing apps are largely indistinguishable from the real banking apps that they mimic. PWAs are essentially websites bundled into what feels like a stand-alone application, with this feeling being enhanced by the use of native system prompts. PWAs, just like websites, are cross-platform, which explains how these PWA phishing campaigns can target both iOS and Android users. The novel technique was observed in Czechia by ESET analysts working on the ESET Brand Intelligence Service, which provides monitoring of threats targeting a client's brand.

"For iPhone users, such an action might break any 'walled garden' assumptions about security," says ESET researcher Jakub Osmani, who analyzed the threat.

ESET analysts' discovery of a series of phishing campaigns, targeting mobile users, used three different URL delivery mechanisms. These mechanisms include automated voice calls, SMS messages, and social media malvertising. The voice call delivery is done via an automated call that warns the user about an out-of-date banking app, and asks the user to select an option on

the numerical keyboard. After the correct button is pressed, a phishing URL is sent via SMS, as was reported in a tweet. Initial delivery by SMS was performed by sending messages indiscriminately to Czech phone numbers. The message sent included a phishing link and text to socially engineer victims into visiting the link. The malicious campaign was spread via registered advertisements on Meta platforms like Instagram and Facebook. These ads included a call to action, like a limited offer for users who “download an update below.”

After opening the URL delivered in the first stage, Android victims are presented with two distinct campaigns, either a high-quality phishing page imitating the official Google Play store page for the targeted banking application, or a copycat website for that application. From here, victims are asked to install a “new version” of the banking app.

The phishing campaign and method are possible only because of the technology of progressive web applications. In short, PWAs are applications built using traditional web application technologies that can run on multiple platforms and devices. WebAPKs could be considered an upgraded version of progressive web apps, as the Chrome browser generates a native Android application from a PWA: in other words, an APK. These WebAPKs look like regular native apps.

Furthermore, installing a WebAPK does not produce any of the “installation from an untrusted source” warnings. The app will even be installed if installation from third-party sources is not allowed.

One group used a Telegram bot to log all entered information into a Telegram group chat via the official Telegram API, while another used a traditional Command & Control (C&C) server with an administrative panel. “Based on the fact that the campaigns used two distinct C&C infrastructures, we have determined that two separate groups were operating the PWA/WebAPK phishing campaigns against several banks,” concludes Osmani. Most of the known cases have taken place in Czechia, with only two phishing applications appearing outside of the country (specifically in Hungary and Georgia).

All sensitive information found by ESET research on this matter was promptly sent to the affected banks for processing.

ESET also assisted with the takedowns of multiple phishing domains and C&C servers.

For more technical information about this novel phishing threat, check out the blogpost “Be careful what you pwish for – Phishing in PWA applications” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

Sanjeev Kant
Vistar Communications
0559724623
email us here