AL2024_32 Hackers Steal Banking Credentials from iOS, Android Users via PWA Apps (22nd August 2024)

Description

Threat actors have started leveraging progressive web applications (PWAs) to impersonate banking apps and steal credentials from both Android and iOS users. These attacks allow hackers to bypass traditional app store security measures and install malicious software directly from the browser.

Details

Cybersecurity experts have observed that PWAs, which offer a native-like experience with features such as push notifications and background data syncing, are being used in phishing campaigns to impersonate banking apps. These apps evade detection and gain access to sensitive device permissions without alerting the user.

The first recorded instance of this attack method was in July 2023 in Poland, with a subsequent campaign targeting Czech users later that year. ESET, a cybersecurity firm, is currently tracking two separate campaigns using this technique: one targeting OTP Bank in Hungary and another targeting TBC Bank in Georgia. The campaigns employ a variety of methods to reach their victims, including automated calls, smishing (SMS phishing), and malvertising on social media platforms like Facebook.

Once the victim clicks on the malicious link or ad, they are redirected to a fake Google Play or App Store page, depending on their device. Here, they are prompted to install a malicious PWA posing as a legitimate banking app. In some cases, on Android devices, the app is installed as a WebAPK, a native APK generated by the Chrome browser, which makes it nearly indistinguishable from a legitimate application.

These malicious PWAs not only mimic the appearance of official banking apps but also declare the Google Play Store as their software source. This level of sophistication allows attackers to gain trust and successfully harvest credentials from unsuspecting users.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- Phishing emails, SMS messages, or social media ads urging the installation of a banking app update.
- Installation prompts for PWAs or WebAPKs from sources outside official app stores.
- Unexpected or unusual behavior from recently installed banking apps.

Remediation

To mitigate the risks associated with these malicious PWAs, organizations and users can:

- Verify the source of any app installation prompts, especially those related to banking applications.
- Avoid clicking on links or ads promoting app updates; instead, download apps directly from official app stores.
- Educate employees and users about the dangers of PWAs and how they can be used in phishing campaigns.
- Regularly update security solutions to detect and block malicious activities.
- Monitor network traffic for unusual patterns that may indicate malware activity.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- BleepingComputer. (2024, August 21). Hackers steal banking creds from iOS, Android users via PWA apps. Retrieved from https://www.bleepingcomputer.com/news/security/hackers-steal-banking-creds-from-ios-android-users-via-pwa-apps/
- ESET Research. (2024, August 20). Be careful what you PWish for: Phishing in PWA applications. Retrieved from https://www.welivesecurity.com/en/eset-research/be-careful-what-you-pwish-for-phishing-in-pwa-applications/