TECH HIVE ADVISORY

SECURITY ADVISORY SERIES

Cybersecurity, News, Events and Threat Advisories. Volume 1. Issue 6

ANDROID MALWARE 'FLYTRAP' COMPROMISES FACEBOOK ACCOUNTS

TLDR: A new android malware named 'Flytrap' reported to be spread via malicious android apps has been uncovered by researchers at Zimperium. These android apps were available on Google Playstore but have been brought down. However, they are still available on third-party app stores. The Flytrap malware is used to hijack users Facebook accounts and spread its tentacles through social engineering. The malware has compromised about 10,000 Facebook accounts since March 2021.

See detailed information here.

What is the issue?

The nine malicious android apps pose to offer free Netflix coupon codes, Google AdWord coupon codes and allow users to vote for their favourite team or player in the just concluded Euro 2020 games. However, the apps then direct users to Facebook login page and ensure that users cannot complete their voting or collect the coupon codes until they log into their Facebook accounts. So, in the end, users are neither offered any coupon nor able to cast votes.

The malware is designed to steal the Facebook ID, email address, (internet protocol) IP address, location, and cookie and tokens associated with the Facebook account. "These hijacked Facebook sessions can be used to spread the malware by abusing the victim's social credibility through personal messaging with links to the Trojan, as well as propagating propaganda or disinformation campaigns using the victim's geolocation details," Researchers at Zimperium wrote.

Impacts

The malware has affected users in 144 countries and compromised 10,000 Facebook accounts. The affected countries include the United States, Canada, Brazil, Russia, Australia, Nigeria and most African countries. In addition, the malicious apps are still available for download on other third-party app stores.

Furthermore, FlyTrap's command-and-control (C2) server's security flaw could be exploited to leak the database found in the stolen cookies and would be accessible to just anyone on the internet. This exposes users to more danger.
There is also the fear that Flytrap and similar malware may be restructured to go after more critical information.

Lessons for android users

- When apps demand social media login to access coupons or deals, be wary. Ask yourself if such personal data is integral to the action being completed.

- When suspected activities are sensed on your Facebook account, change password, enable multi-factor authentication (MFA), and log out of the account.

- Disallow android from downloading apps from unknown sources. This can be done by going to settings>security>unknown apps.

Curated by Tojola Yusuf
@tojolabilqis Tojola Yusuf

contact@techhiveadvisory.org.ng @Hiveadvisory
www.techhiveadvisory.org.ng