PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Be wary of fake e-shops, android malware siphoning banking data
Language: English
Publication/Portal: Daily Express (Sabah)
Section: Business / Bizbytes
Date: 7 April 2022
Page: 13

Be wary of fake e-shops, android malware siphoning banking data

KUALA LUMPUR: Malaysian bank customers should be wary of malicious Android applications and fake e-shop websites aimed at siphoning their banking credentials.

Lukáš Štefanko, a researcher from global digital company ESET, warned that the company has detected fake websites posing as legitimate services, with similar domain names, in the country.

Štefanko said unsuspecting online shoppers are lured to copycat websites through campaigns run by the cyber attackers via Facebook advertisements, but these websites do not provide an option to shop directly through them. Instead, they include buttons that entice users to download apps from Google Play.

However, clicking on these buttons does not lead to the Google Play Store, but to servers under the cyber attackers' control.

When the time comes to pay, users are presented with payment options of transferring the required amount from their bank accounts, after which the "victims" are presented with a fake financial process exchange (FPX) payment page, and asked to choose one of eight Malaysian banks provided.

FPX is a Malaysia-based payment method that allows customers to complete transactions online using their bank credentials.

"The targeted banks are Maybank, Affin Bank, Public Bank, CIMB Bank, BSN, RHB, Bank Islam Malaysia, and Hong Leong Bank," the company said in a report.

After the victims submit their banking credentials, they receive an error message telling them that the user ID or password they had provided was invalid. At this point, the entered credentials have been sent to the malware operators.

To ensure the cyber attackers can access the victims' bank accounts, the fake e-shop applications also forward all SMS messages received by the victim to the perpetrators in case they contain the two-factor authentication (2FA) codes sent by the bank.

Štefanko warned online users to be wary of clicking advertisements and paid search engine results because they do not lead to the official website and to ensure that the application is only downloaded from Google Play Store, as well as to verify the security of websites.

Users should also use software or hardware 2FA instead of SMS when possible and use mobile security solutions to better secure their online accounts, the company advised.

According to the report, seven fake websites and three malicious Android applications were identified recently in the country.

The cyber criminals have targeted Malaysia exclusively for now, but they may expand to other countries and banks later. The attackers are after banking credentials, but they may steal credit card information in the future, Štefanko said. – Bernama