Issued 11/6/17

New 'Marcher' Malware Attacks Android Users' Banking Accounts

Marcher has been around since March 2013, initiating in Russian forums, and has escalated to a global threat. The newest form of Marcher pairs credential and credit card phishing with banking Trojans into one scheme, targeting Android users who are also customers of large Austrian banks, Proofpoint found. The current scheme has been ongoing since January, impacting almost 20,000 people, according to the report.

Phishing emails are the first step of the attack, using a bit[.]ly link to direct users to a fake Bank of Austria page, according to the report. From there, a customer is prompted to enter their banking login information, followed by their email address and phone number. That contact information is later used by the attackers to send users messages directing them to download the fake "Bank Austria Security App," or face their account being blocked, the report said.

When downloading the fake app, instructions prompt the user to change their security settings to allow apps with unknown sources to download. The app also requires several permissions, including permission to act as a device administrator, which the report says should rarely be granted to an app. Once granted access to the device, Marcher can now deploy credit card phishing scams, both in and outside of the fake app. For example, the malware will ask for credit card details when logging into the Google Play Store, the report said. Further personal details are requested as well.