EINPRESSWIRE

ESET Research discovers NGate: Android malware, which relays NFC traffic to steal victim’s cash from ATMs

DUBAI, UNITED ARAB EMIRATES, August 23, 2024 /EINPresswire.com/ -- ESET researchers uncovered a crimeware campaign that targeted clients at three Czech banks. The malware used, which ESET has named NGate, has the unique ability to relay data from victims’ payment cards via a malicious app installed on their Android devices, to the attacker’s rooted Android phone. The primary goal of this campaign was to facilitate unauthorized ATM withdrawals from the victims’ bank accounts. This was achieved by relaying near field communication (NFC) data from the victims’ physical payment cards, via their compromised Android smartphones, by using the NGate Android malware, to the attacker’s device. The attacker then used this data to perform ATM transactions. If this method failed, the attacker had a fallback plan to transfer funds from the victims’ accounts to other bank accounts.

“We haven’t seen this novel NFC relay technique in any previously discovered Android malware. The technique is based on a tool called NFCGate, designed by students at the Technical University of Darmstadt, Germany, to capture, analyze, or alter NFC traffic; therefore, we named this new malware family NGate,” says Lukáš Štefanko, who discovered the novel threat and technique.

Victims downloaded and installed the malware after being deceived into thinking they were communicating with their bank and that their device was compromised. In reality, the victims had unknowingly compromised their own Android devices by previously downloading and installing an app from a link in a deceptive SMS message about a potential tax return.

It’s important to note that NGate was never available on the official Google Play store.

NGate Android malware is related to the phishing activities of a threat actor that has operated in

Czechia since November 2023. However, ESET believes these activities were put on hold following the arrest of a suspect in March 2024. ESET Research first noticed the threat actor targeting clients of prominent Czech banks starting at the end of November 2023. The malware was delivered via short-lived domains impersonating legitimate banking websites or official mobile banking apps available on the Google Play store. These fraudulent domains were identified through the ESET Brand Intelligence Service, which provides monitoring of threats targeting a client's brand. During the same month, ESET reported the findings to its clients.

The attackers leveraged the potential of progressive web apps (PWAs), as ESET reported in a previous publication, only to later refine their strategies by employing a more sophisticated version of PWAs known as WebAPKs. Eventually, the operation culminated in the deployment of NGate malware.

In March 2024, ESET Research discovered that NGate Android malware became available on the same distribution domains that were previously used to facilitate phishing campaigns delivering malicious PWAs and WebAPKs. After being installed and opened, NGate displays a fake website that asks for the user's banking information, which is then sent to the attacker's server.

In addition to its phishing capabilities, NGate malware also comes with a tool called NFCGate, which is misused to relay NFC data between two devices – the device of a victim and the device of the perpetrator. Some of these features only work on rooted devices; however, in this case, relaying NFC traffic is possible from non-rooted devices as well. NGate also prompts its victims to enter sensitive information like their banking client ID, date of birth, and the PIN code for their banking card. It also asks them to turn on the NFC feature on their smartphones. Then, victims are instructed to place their payment card at the back of their smartphone until the malicious app recognizes the card.

In addition to the technique used by the NGate malware, an attacker with physical access to payment cards can potentially copy and emulate them. This technique could be employed by an attacker attempting to read cards through unattended purses, wallets, backpacks, or smartphone cases that hold cards, particularly in public and crowded places. This scenario, however, is generally limited to making small contactless payments at terminal points.

"Ensuring protection from such complex attacks requires the use of certain proactive steps against tactics like phishing, social engineering, and Android malware. This means checking URLs of websites, downloading apps from official stores, keeping PIN codes secret, using security apps on smartphones, turning off the NFC function when it is not needed, using protective cases, or using virtual cards protected by authentication," advises Štefanko.

For more technical information about the novel NFC threat, check out the blogpost "NGate Android malware relays NFC traffic to steal cash" 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
+971 55 972 4623
email us here