NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Circular No: NPCI/2019-20/IS/001 Dated: 12 July 2019

Advisory to Banks on Agent Smith Malware

To,

All Member Banks

There are reports emanating from media that "Agent Smith" malware has infected 1.5 million android smartphones in India. The "Agent Smith" virus, which serves ads to these infected smartphones spreads to users via third-party app stores. Once installed, it masquerades itself by changing its application name to a genuine looking app.

The malware is known to exploits existing known Android vulnerabilities and automatically replaces already existing installed apps with malicious versions silently, without users' knowledge or interaction. The malware currently uses its broad access to such large number of devices resources to show advertisements for financial gain, but this level of access could easily be used for far more intrusive and harmful objectives such as banking credential theft, card data stealing and eavesdropping on mobile OTPs or voice communication.

To combat against such intrusions, we advise Banks to follow the listed measures & not just restricted to the below.

1. Customer Awareness: advise customer to download Bank App from trusted app stores only.
2. Install an Antivirus: ask customers to install an antivirus on their phones to scan for known bad applications.
3. Vigilant Monitoring: monitor third party app stores and scan them for malicious or rebuild version of the Bank App, and initiate takedown if necessary.
4. Encrypting stored data: no financial data should be stored in plain text. Always store your app's data in an encrypted format.
5. Media monitoring: keep a watch on further development and change in nature of such malwares, which can target your customers.

Banks are also advised to report CYBER INTRUSION OF ANY NATURE immediately to

1. National Cyber Security Co-ordinator, National Security Council Secretariat, 2nd floor, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110001 (ncsc@gov.in) or Director General, Indian Computer Emergency Response Team (CERT-In) at Electronics Niketan, CGO Complex, New Delhi – 110003 (incident@cert-in.org.in)
2. Reserve Bank of India, CSITE Cell – csite@rbi.org.in
3. NPCI – ciso@npci.org.in

Thanking you,

Yours faithfully,

Mathan Babu Kasilingam

CISO