Solution Guide:

Voice phishing using malware



Modus Operandi (MO)

Attackers convince victims to install an app containing malware, compromising their devices and allowing attackers to commit fraud.

Phone call to victim

Let victim install malicious app

Use malware to commit fraud



- Mimic bank or other known institute
- Build trust
- Psychological tricks
- Practical guidance for app installation
- Transfer money
- Order goods with different shipping address (often with 1-click payment)

of malware has ATO capabilities

YoY-increase in 40% On-Device Fraud*

Voice phishing is a form of APP fraud where fraudsters call their victims and pretend to be a the bank. In voice phishing using convince their victims to install a malicious app and then use the compromised device to commit fraud.

Realtime Visibility

Manage fraud risks from the earliest stage using layered detection.

Behavioral risk:

- On-call while opening app store

Device risk:

- App installed from 3rd-party app store

Device risk:

 Automated script banking app

Behavioral risk:

- Form filling timing

Using ThreatFabric's Fraud Risk Suite, every step in the fraudster's attack attempt is detectable using one or more detection layers. Our unique integration of technical and behavioural detection layers will lead to early warnings and a high signal-to-noise ratio. Combined with internal knowledge, it allows our customers to stop fraud attempts before people become fraud victims.









Realtime risk events & scores, fraud alerts, reports, etc.

Demo?





+31 (0)20 8950650



info@threatfabric.com

PII, account, address book, transactions, (order) history, interests, and more.

Fraud team & systems