Mobile Phishing Killchain

Phishing attacks pose a dangerous threat to mobile users and their employers. While each attack is unique, they share the end goal of stealing sensitive corporate data.

Lookout defends mobile users against phishing, app, device, and network-based attacks. By protecting users, Lookout secures the corporate data accessed from those devices from malicious actors. In the case of phishing attacks, Lookout intervenes immediately to reduce risk and mitigate data loss.

1

ATTACKER SENDS A MESSAGE AIMED AT SOCIAL ENGINEERING VICTIM

SMS

Email

Messaging Apps

Ad Networks in Apps

88%

of credential theft is achieved using phishing links[1]

2

ATTACKER SUCCESSFULLY TRICKS VICTIM INTO CLICKING A PHISHING LINK

56%

More than half of Lookout users have clicked on a phishing link.

WITH LOOKOUT

Lookout Phishing and Content Protection blocks the connection

WITHOUT LOOKOUT

WITH LOOKOUT

Default or Custom policies automatically quarantine the device

3

MALICIOUS LINK CAN LEAD TO A OR B

A

B

UPON CLICKING THE LINK, VICTIM IS BROUGHT TO A PHISHING SITE MEANT TO LOOK LEGITIMATE

60%

Mobile phishing is reported as a more frequent mobile security incident than physically lost/stolen devices (30%)[1]

LINK SILENTLY DOWNLOADS SURVEILLANCEWARE TO THE DEVICE

Pegasus

Aggressive surveillanceware allows attackers to silently jailbreak a device, spy on the user, and steal data

4A

ATTACKER GAINS ACCESS TO EVERYTHING ON THE DEVICE

300%

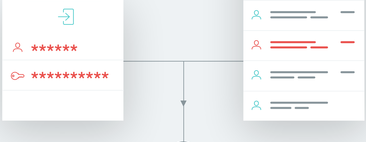
Enterprise users are three times as likely to fall for a phishing link on a mobile device

4B

SURVEILLANCEWARE MONITORS AND HARVESTS ALL ACTIVITY ON DEVICE

1 Click

One action is all it takes for Pegasus to be silently installed on the victim's device



5

ATTACKER IMPERSONATES, TRACKS, OR SPIES ON THE VICTIM, LEADING TO SENSITIVE CORPORATE DATA LEAKAGE

Research Data

Emails

PII

Financial Data

Corporate Data

DATA BREACH COST PER RECORD

To learn more, visit lookout.com

Lookout

1 2019 Phishing Trends and Intelligence Report, PhishLabs