# NOCTURNUS | THREAT ALERT

# EVENTBOT MOBILE TROJAN

## OVERVIEW

THREAT TYPE:
MOBILE BANKING TROJAN

TARGET INDUSTRY:
FINANCIAL

ATTACK GOAL:
USER & CORPORATE DATA

IMPACTED GEO:
EUROPE & USA

## RECOMMENDATIONS

Do not download mobile apps from unofficial sources.

Always apply critical thinking and consider whether you should give an app permissions.

When in doubt, check the APK signature and hash in sources like VirusTotal before installing it on your device.

EXPERIENCED A BREACH?
EMAIL US AT

INFO@CYBEREASON.COM

## WHAT'S HAPPENING?

The Cybereason Nocturnus team is investigating EventBot, a new type of Android mobile malware that emerged around March 2020. EventBot is a mobile banking trojan and infostealer that abuses Android's accessibility features to steal user data from financial applications, read user SMS messages, and steal SMS messages to allow the malware to bypass two-factor authentication.

## KEY OBSERVATIONS & TTPS

- EventBot targets users of over 200 different financial applications, including banking, money transfer services, and crypto-currency wallets. Those targeted include applications like Paypal Business, Revolut, Barclays, UniCredit, CapitalOne UK, HSBC UK, Santander UK, TransferWise, Coinbase, paysafecard, and many more.
- It specifically targets financial banking applications across the United States and Europe, including Italy, the UK, Spain, Switzerland, France, and Germany.
- EventBot is particularly interesting because it is in such early stages of development. This brand new malware has real potential to become the next big mobile malware, as it is under constant iterative improvements, abuses a critical operating system feature, and targets financial applications.
- Read the full length research and a full list of targeted apps here.

## CYBEREASON CUSTOMERS

DETECTED BY THE CYBEREASON DEFENSE PLATFORM

We highly recommend every customer enable the following features:

- If you do not have Cybereason Mobile, consider adding it to your portfolio to prevent against threats like these.
- For Cybereason MDR customers, the Cybereason team will monitor and triage as well as assist in the mitigation of potential infections.