

Week 5: Lab- Android App Reverse Engineering

Date: 6/14/20

BY: Jason Rodriguez

CFDI-310-40A

Question 1: md5 value for facebook_otp.apk

Md5: 021d55c415ff951c8e7b1ce3f94399bb

Question 2: Malicious code

Md5: 021d55c415ff951c8e7b1ce3f94399bb

SHA256: f448c6d8e2e970020c1993be69120a6a8761df7be978f989d41da8c531c33063

Other associated file names

- Facebook.apk
- Myfile.exe
- Sample.apk
- Fskr9.apk
- Base.apk
- Apk.apk

Question 3: IP address associated

172.217.16.195

Question 4: Locator

The destination of the IP is in Mountain view, California.

Question 5: Hardcoded IP

There was no hardcoded IP within this apk.

First time in the wild was 2015-01-28

Question 11: Strings Identified

Bxateca.net, twitter.com, facebook.com, and linkedin.com

Question 12: APK Permissions

- Access location
- Call Phone
- Change wifi state
- Read contacts
- Read SMS
- Record audio
- Disable keyguard
- Receive SMS
- Write SMS
- Write external storage

Question 13:

It was utilizing three IP host located in mountain view, California

Question 14: Issued Apk

Luisa Santos

Czech

Question 15:

It is an Android banking trojan used to capture SMS pin to evade two-factor authentication from some banks.

