

CYBER GYAN VIRTUAL INTERNSHIP PROGRAM

**Centre for Development of Advanced
Computing (CDAC), Noida**

Submitted By: SHASHWAT MISHRA

Project Trainee, (July-August) 2024

TOPIC NAME

RANSOMWARE IMPLEMENTATION AND DETECTION

PROBLEM STATEMENT

Ransomware encrypts victim's files, demanding payment for decryption keys. It's often delivered via phishing emails or exploit kits. Detection involves monitoring for unusual file access patterns, unexpected encryption activity, and using antivirus software. Employing regular backups and educating users about phishing attacks are key preventive measures.

TECHNOLOGY/TOOLS TO BE USED

SARA (Simple Android Ransomware Attack) is a tool available on GitHub for creating ransomware for Android devices. It's designed for educational purposes and allows users to generate custom ransomware (file lockers) and trojans. SARA can be installed on Kali Linux, Ubuntu, Debian, and Termux. The GitHub link of this tool is provided below-

<https://github.com/termuxhackers-id/SARA.git>

ABOUT THE ATTACK/TOPIC/PROBLEM STATEMENT

For implementation of ransomware attack first we'll install the tool SARA in our KALI LINUX machine using GitHub link. Now when we'll run the tool it will ask about which type of ransomware you are trying to apply, in this project we'll apply screen lock ransomware in which when any user install any app or run any extension in his system his screen will be encrypted and user will be unable to use his device, for unlocking it he will have to decrypt it for decryption he'll need decryption key that we have entered while creating a ransomware application.



```

<sara> : you can fill or leave blank for using default config
the default configuration is name = 'Screen Locker'
head = 'Your Phone Is Locked'
desc = 'locked by sara@termuxhackers-id'
icon = 'data/tmp/icon.png' and keys = 's3cr3t'

custom lock screen apk (passprhase)

set app name: chrome fake
set app head: you are hacked
set app desc: web
set app icon: /home/imshashwat007/Downloads/bf467a396e714afb74d1af12fd72e8b5.png
set app keys: 12345678910

<sara> : well this process takes a few minutes,
please be patient until the process is complete

<sara> : decompile 'chromefake.apk' using apktool ... done
<sara> : add 'app_name">chrome...' on 'strings.xml' ... done
<sara> : add 'you are hacked' on 'strings.xml' ... done
<sara> : add 'web' on 'strings.xml' ... done
<sara> : add '12345678910' as 'passprhase' ... done
<sara> : add 'bf467a396e714afb74d1af12fd72e8b5.png' into 'ic_launcher' ... done
<sara> : add '8' into 'chromefake/apktool.yml' ... done
<sara> : add '8.0 by @chromefake' into 'chromefake/apktool.yml' ... done
<sara> : recompile 'chromefake' using apktool ... done
<sara> : signing 'chromefake.apk' using uber-apk-signer ... done

<sara> : do you want to upload 'chromefake.apk' ?

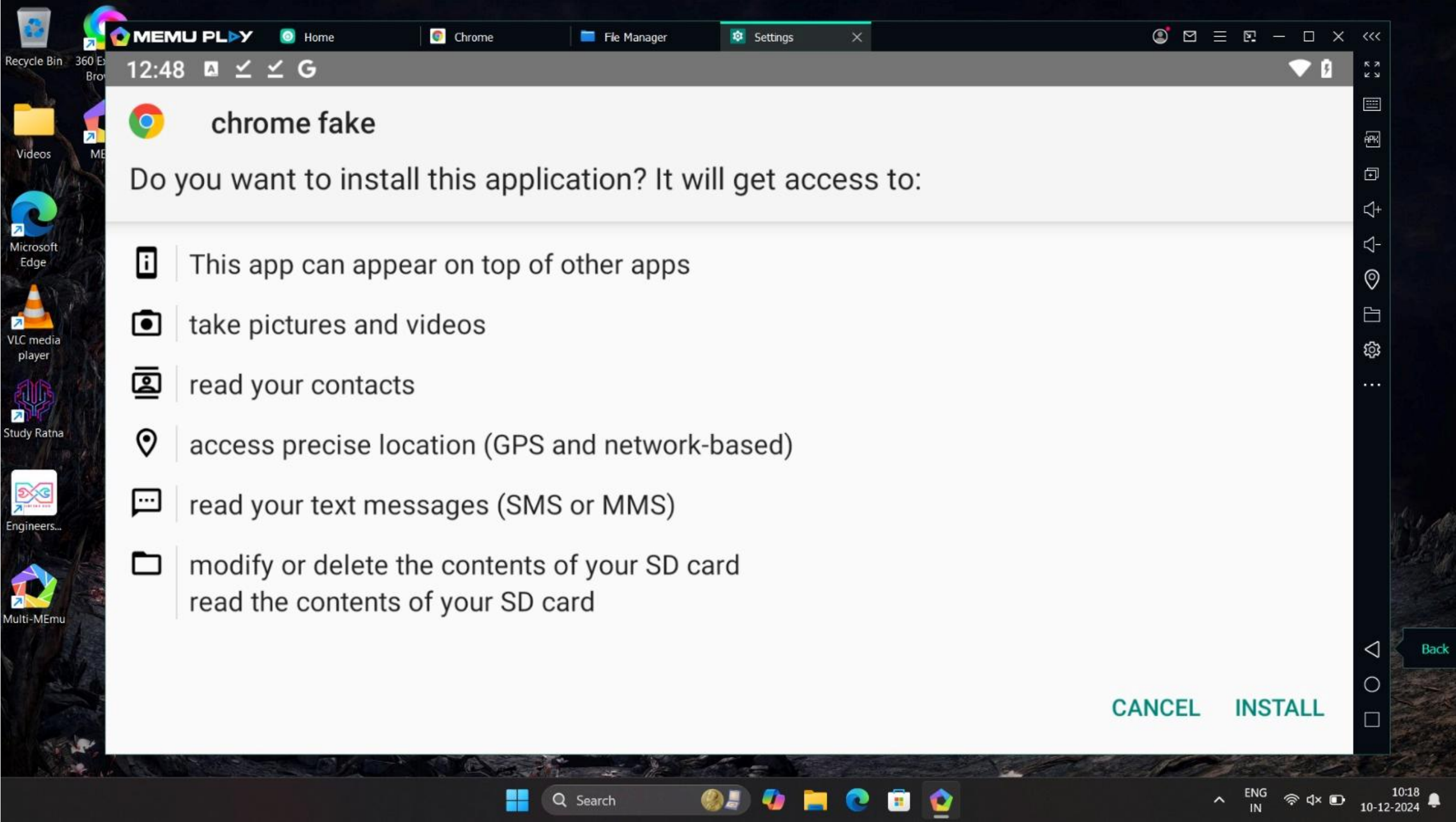
(1) yes, i want to upload
(2) no thanks

<user> : 2

<sara> : your screen locker apps successfully created
the application is saved as 'chromefake.apk'
the secret key (passprhase) '12345678910'

<sara> : press enter for back to 'main menu' (enter)







```



12:48

chrome fake

Do you want to install this application? It will get access to:

-  This app can appear on top of other apps
-  take pictures and videos
-  read your contacts
-  access precise location (GPS and network-based)
-  read your text messages (SMS or MMS)
-  modify or delete the contents of your SD card
read the contents of your SD card

CANCEL INSTALL

Back



Search

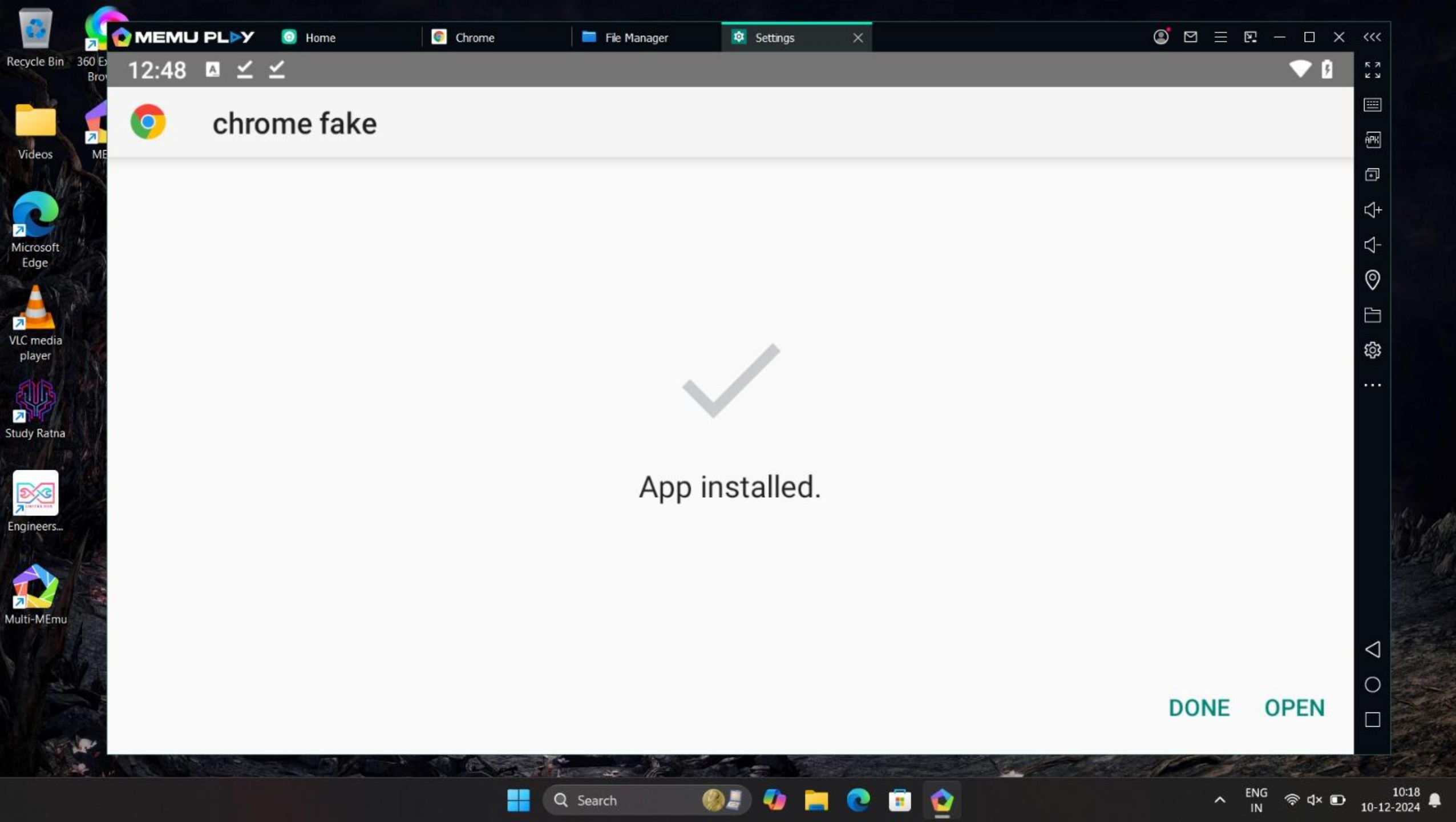


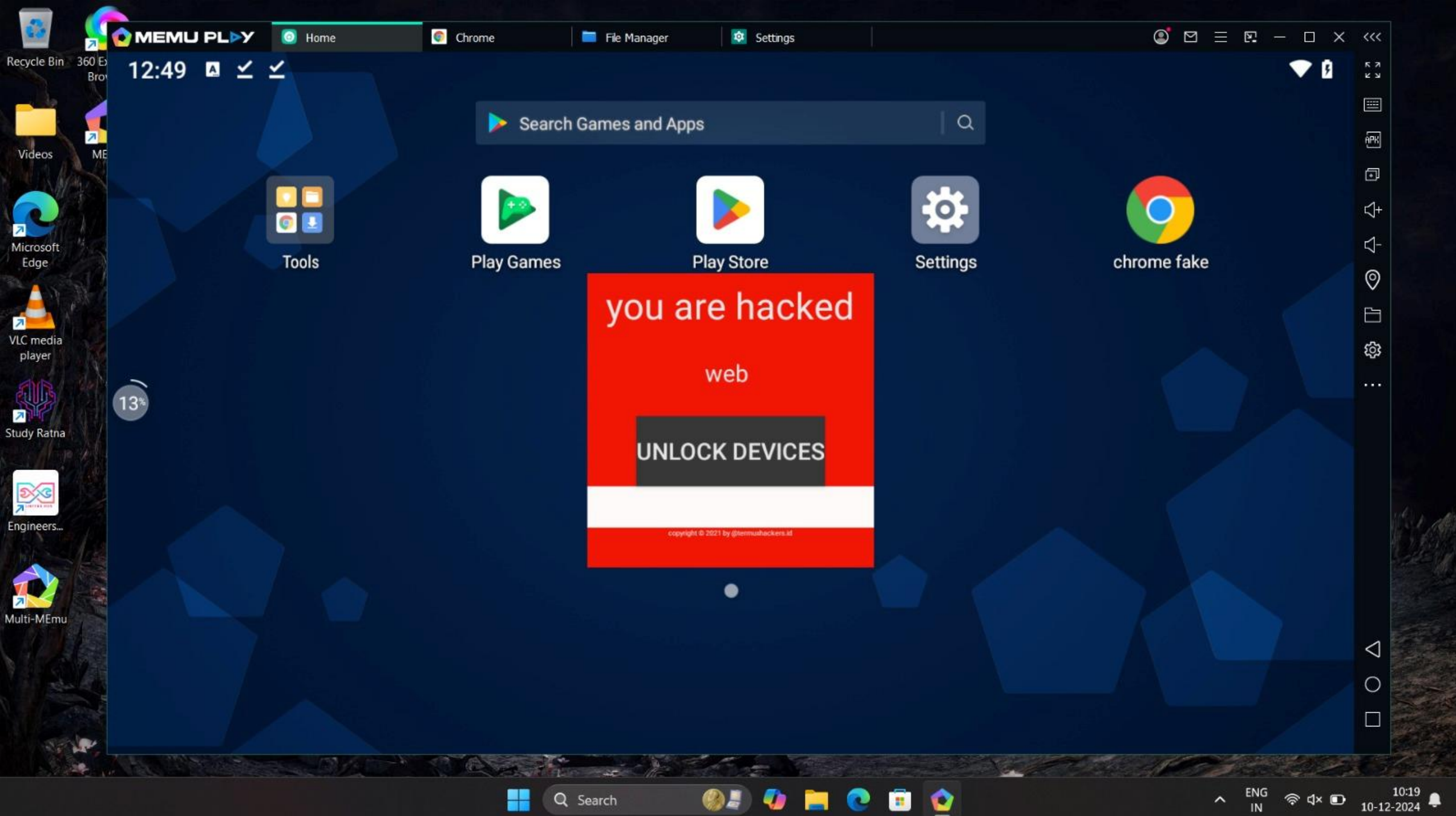
ENG
IN



10:18

10-12-2024













WHAT ARE THE REASONS BEHIND THE PROBLEM(TELL ABOUT THE ISSUES WHY THIS PROBLEM/ATTACKS ARE HAPPENING)

Ransomware problems stem from several factors: security-poor organizations, cryptocurrency monetization, and jurisdictional evasion by criminals. Cybercriminals exploit weak security, use unregulated digital currencies for payments, and operate across borders to avoid law enforcement. These elements make ransomware a persistent and evolving threat.

SUGGEST SOME POSSIBLE SOLUTIONS/COUNTERMEASURES

In the Android devices there are a lot of methods to detect the Ransomware attack-

The First and very simple method is to turn on Google Play Protection, in which if we install any unauthorized application in our android device it detects it and stop it while installing and it shows that your application is not installed.

The Second method is to upload the application on some trusted websites that detects all the problems exist in any application and after some process it makes a report about all the parameters in which it is risky to install so that we'll know that we have to install it or not.

- Recycle Bin
- Videos
- Microsoft Edge
- VLC media player
- Study Ratna
- Engineers...
- MEmu


MEMU PLAY

Home

Google Play Store

1:01


← Play Protect



Turn on Play Protect scanning

For your security, turn on Play Protect to check apps from outside the Play Store. Play apps are automatically scanned.

Turn on



- Recycle Bin
- Videos
- Microsoft Edge
- VLC media player
- Study Ratna
- Engineers...
- MEmu

MEMU PLAY

Home

Google Play Store

1:01

← Play Protect

No harmful apps found

1 security notification

Scan

Removing permissions for unused apps



Search



ENG IN



10:31

10-12-2024



MEMU PLAY

Home

File Manager

1:01

chrome fake

Do you want to install this application? It will get access to:

This app can appear on top of other apps

take pictures and videos

read your contacts

access precise location (GPS and network-based)

read your text messages (SMS or MMS)

modify or delete the contents of your SD card
read the contents of your SD card

CANCEL

INSTALL



Search



ENG
IN



10:31
10-12-2024

- Recycle Bin
- Videos
- Microsoft Edge
- VLC media player
- Study Ratna
- Engineers...
- MEmu

MEMU PLAY

Home

File Manager


Google Play Store

1:02

chrome fake

Google Play Protect

Harmful app blocked

chrome fake

This app may be harmful.

More details

Got it

CANCEL

- Recycle Bin
- Videos
- Microsoft Edge
- VLC media player
- Study Ratna
- Engineers...
- MEmu

MEMU PLAY


Home

File Manager

Google Play Store

1:03

chrome fake



App not installed.

DONE



Home Chrome

1:04

<https://www.immuniweb.com/mobile/> 1

ImmuniWeb
AI for Application Security

Important Update: ImmuniWeb inaugurates regional offices in London, Washington and Dubai. [Learn more.](#)

Mobile App Security Test

Free online tool to test mobile app's security

✓ iOS/Android Security Test

✓ Mobile App Privacy Check

✓ OWASP Mobile Top 10 Test

✓ Mobile Security Scan

871,658 mobile applications tested

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:34



10-12-2024



Home Chrome Files

1:06

ImmuniWeb[®]
AI for Application Security

Privacy Policy was not found in application

Misconfiguration or weakness

Suspicious Functionality

The mobile application uses the following suspicious functionality:

Background Services

The application uses functionality for starting services in the background. Some actions, such as location tracking or file uploading, can be performed without the user noticing, which could be used for malicious purposes, potentially violating privacy and security.

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:36
10-12-2024



Home Chrome Files

1:07

ImmuniWeb®
AI for Application Security

location tracking or file uploading, can be performed without the user noticing, which could be used for malicious purposes, potentially violating privacy and security.

Read/Write Contacts

The application uses functionality for reading/writing contacts. If misused, this could deceive the user by substituting names or phone numbers in the contact list.

Overlays

The mobile application uses overlay interfaces. This functionality allows to display content over other applications, which could potentially be exploited to deceive users by mimicking legitimate app interfaces, obscuring important details or modifying visible text.

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:37
10-12-2024



MEMU PLAY

Home

Chrome

Files

1:07

available. Malicious applications can use this to determine where you are and may consume additional battery power.

CAMERA

dangerous

Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

READ_CONTACTS

dangerous

Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

READ_EXTERNAL_STORAGE

dangerous

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:37
10-12-2024



Home Chrome Files

1:07

ImmuniWeb[®]
AI for Application Security

app interfaces, obscuring important details or modifying visible text.

Mobile Application Permissions

The mobile application requests the following permissions that may endanger user's privacy under certain circumstances:

ACCESS_FINE_LOCATION

 dangerous

Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:37
10-12-2024



MEMU PLAY

Home

Chrome

Files

1:08

entire screen of the phone.

WRITE_EXTERNAL_STORAGE

dangerous

Allows an application to write to external storage.

INTERNET

normal

Allows an application to create network sockets.

RECEIVE_BOOT_COMPLETED

normal

Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:38
10-12-2024





Home Chrome Files

1:07

ImmuniWeb®
AI for Application Security

READ_EXTERNAL_STORAGE

dangerous

Allows an application to read from external storage.

READ_SMS

dangerous

Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.

SYSTEM_ALERT_WINDOW

dangerous

Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

DEMO

TALK TO SALES

STAY IN TOUCH



Search



ENG
IN



10:37
10-12-2024



THANKYOU