Mobile Malware Analysis

De Silva K.R.K.D

Table of contents

Introduction To The Topic

Mobile malware has become a much greater concern in our increasingly connected society where mobile devices are components of our daily lives. Smartphones and tablets, two examples of mobile devices, have developed into powerful computing platforms that provide a wide range of services and applications. However, because of their adaptability, they have become attractive targets for hackers looking to steal user data and exploit security flaws. People, companies, and even organizations are at serious risk from mobile malware, a specific type of malicious software created for mobile platforms like iOS and Android. These dangerous programs, which can infect devices and cause trouble on both a personal and professional level, exist in a variety of varieties, ranging from advertising and spyware to Trojans and malware.

To comprehend, analyze, and reduce the risks caused by these threats, malware for mobile device analysis is a crucial subject in the area of cybersecurity. To find and eliminate dangerous parts, this analytical technique looks at mobile applications, analyzes code structures, and evaluates behavior. The main objectives for smartphone malware analysis are to strengthen security protocols, preserve user privacy, and secure sensitive data. “Mobile malware is an increasing danger to consumer devices even if it is not as common as malware that targets conventional desktops. As assaults multiply and are more powerful, mobile malware is posing a threat to the mobile safety sector.”[1]

In addition to giving you the necessary skills, the “Mobile Malware Analysis” program also gives you the ability to contribute to the ongoing fight against mobile device malware threats. By the completion of this training, you’ll be better equipped to guard against the always-changing array of mobile threats, protecting both your digital life and the mobile ecosystems that we all depend on a daily basis. Come along with me as I study the exciting, difficult, and important topic of mobile malware investigation.

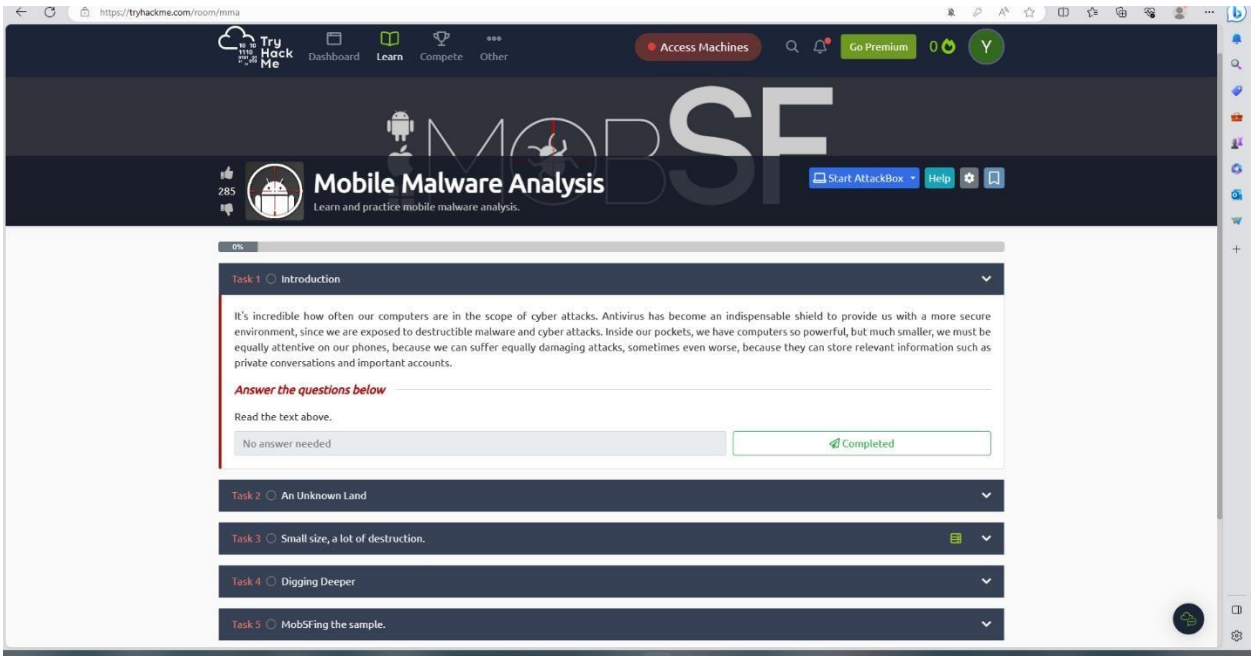
Methodology

Analysis of mobile malware is a complex, diverse process that is essential to cybersecurity. These mobile powerhouses are essential to our everyday lives in an age where mobile devices rule, but they are also excellent targets for hackers looking to exploit flaws, compromise user data, or engage in various other crimes. As the guide for understanding, analyzing, and minimizing the risks offered by these digital adversaries, an effective approach for mobile malware investigation is crucial.

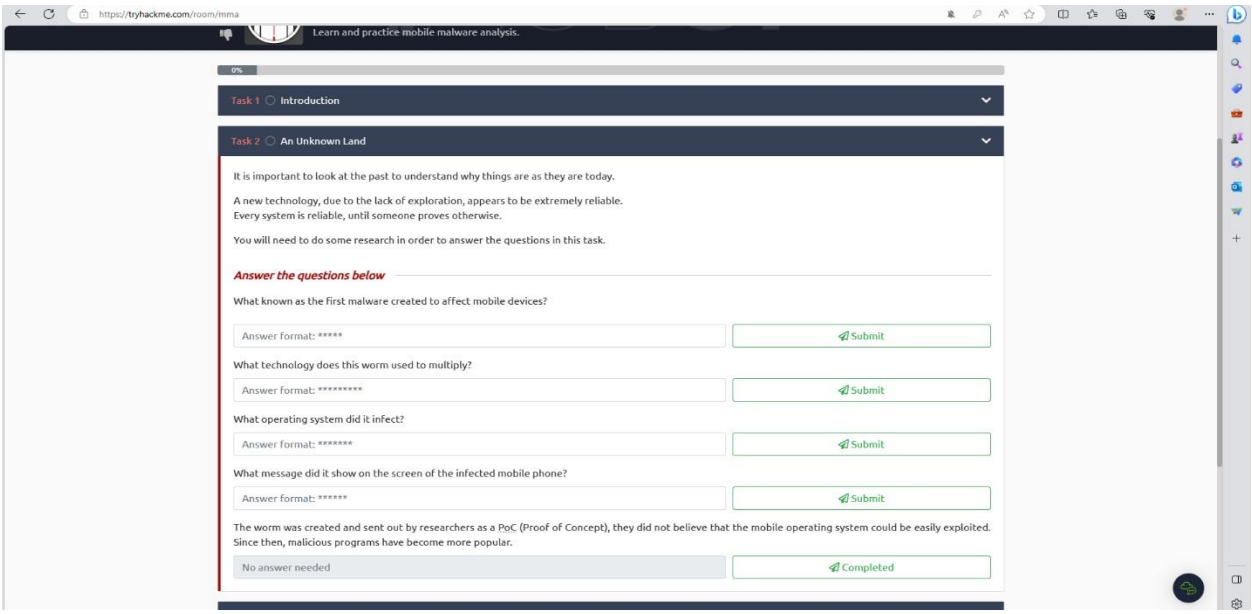
It starts with careful planning, guaranteeing the availability of necessary tools and forms for documenting findings. Following sample gathering, there is a focus on confirming the legitimacy and applicability of the malware. Putting up a separate analysis environment is a key next step since it stops malware from spreading accidentally. While dynamic analysis entails running the virus in a secure setting and watching its activity, including network traffic, static analysis looks at the app's code, credentials, and API calls to find possible dangers.

TryHackMe lab link: [TryHackMe | Mobile Malware Analysis]

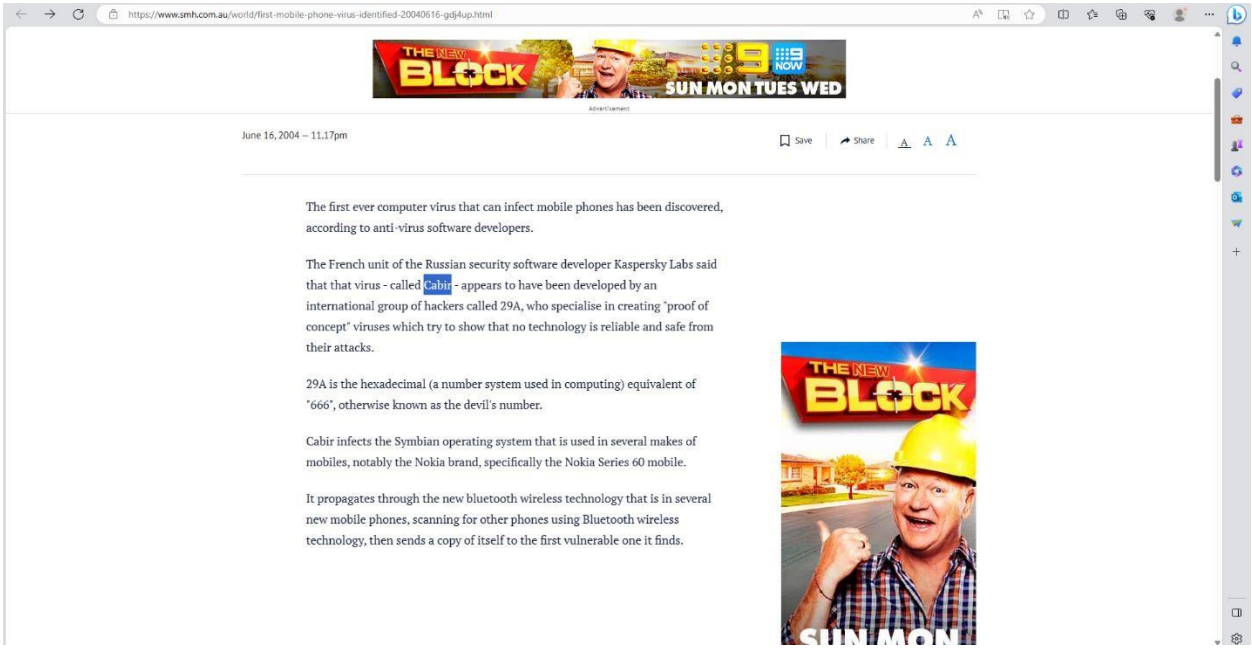
Task 1: Introduction – Read the text – No answer is needed



Task 2:



What is known as the first malware created to affect mobile devices? Read : https://www.smh.com.au/world/first-mobile-phone-virus-identified-20040616-gdj4up.html



June 16, 2004 – 11.17pm

The first ever computer virus that can infect mobile phones has been discovered, according to anti-virus software developers.

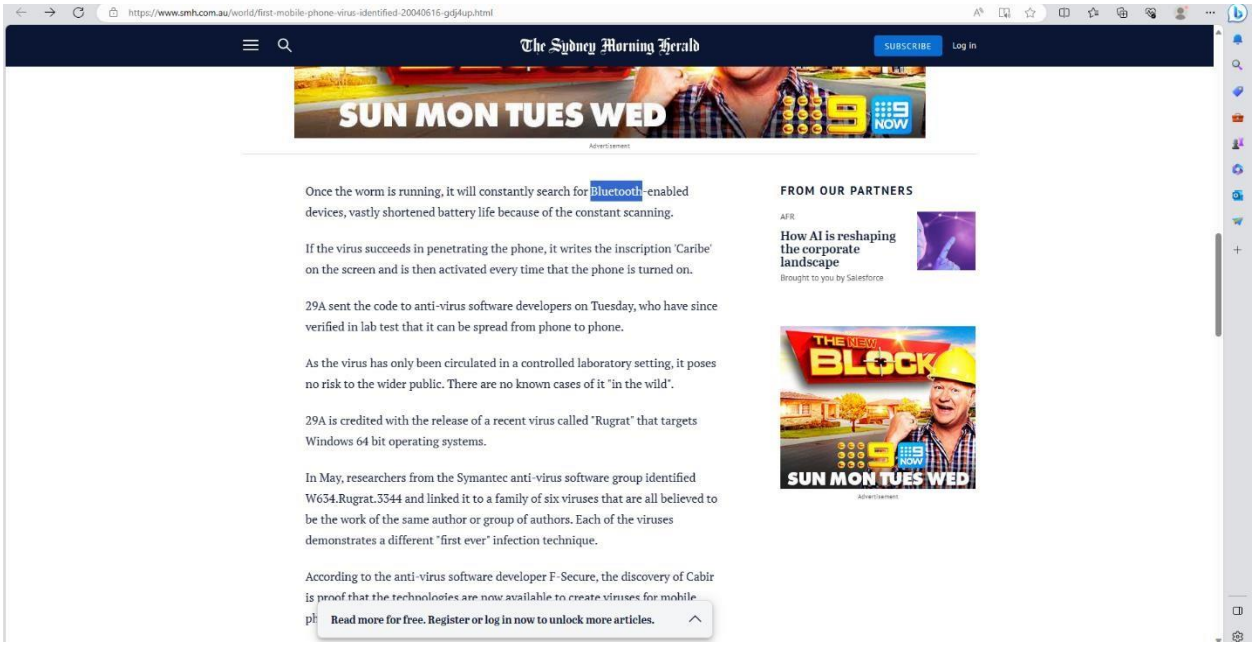
The French unit of the Russian security software developer Kaspersky Labs said that that virus - called Cabir - appears to have been developed by an international group of hackers called 29A, who specialise in creating "proof of concept" viruses which try to show that no technology is reliable and safe from their attacks.

29A is the hexadecimal (a number system used in computing) equivalent of "666", otherwise known as the devil's number.

Cabir infects the Symbian operating system that is used in several makes of mobiles, notably the Nokia brand, specifically the Nokia Series 60 mobile.

It propagates through the new bluetooth wireless technology that is in several new mobile phones, scanning for other phones using Bluetooth wireless technology, then sends a copy of itself to the first vulnerable one it finds.

What technology does this worm used to multiply? Read: First mobile phone virus identified (smh.com.au)



The Sydney Morning Herald

Once the worm is running, it will constantly search for Bluetooth-enabled devices, vastly shortened battery life because of the constant scanning.

If the virus succeeds in penetrating the phone, it writes the inscription 'Caribe' on the screen and is then activated every time that the phone is turned on.

29A sent the code to anti-virus software developers on Tuesday, who have since verified in lab test that it can be spread from phone to phone.

As the virus has only been circulated in a controlled laboratory setting, it poses no risk to the wider public. There are no known cases of it "in the wild".

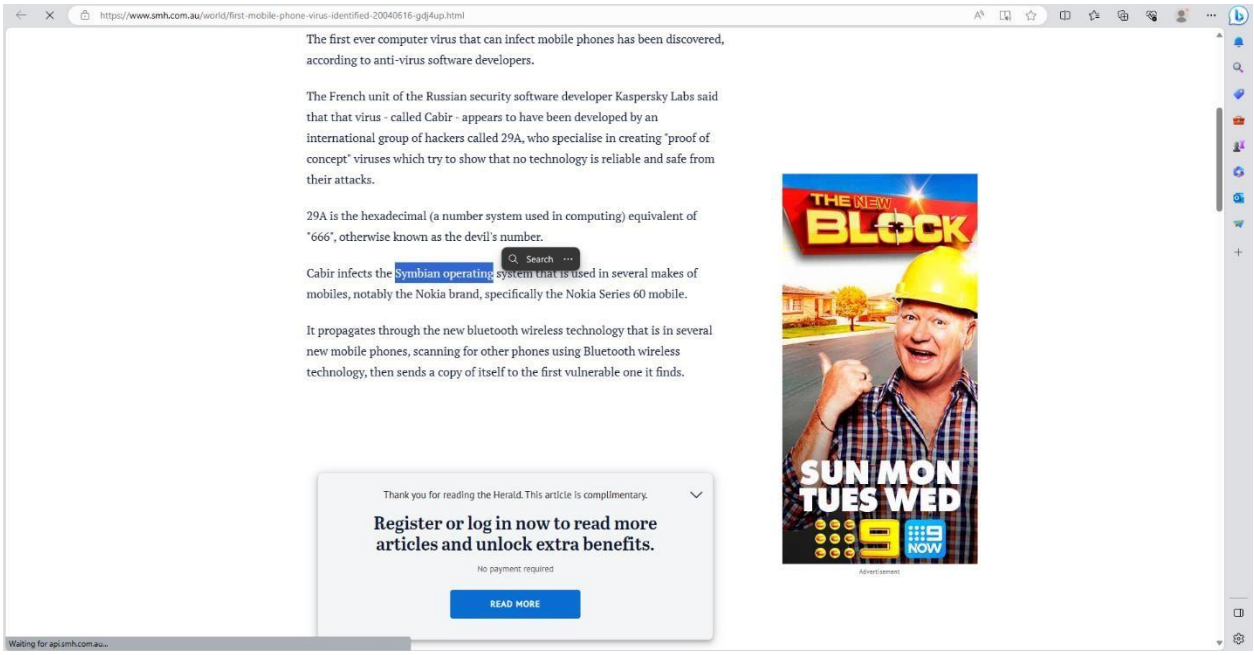
29A is credited with the release of a recent virus called "Rugrat" that targets Windows 64 bit operating systems.

In May, researchers from the Symantec anti-virus software group identified W64.Rugrat.3344 and linked it to a family of six viruses that are all believed to be the work of the same author or group of authors. Each of the viruses demonstrates a different "first ever" infection technique.

According to the anti-virus software developer F-Secure, the discovery of Cabir is proof that the technologies are now available to create viruses for mobile

Read more for free. Register or log in now to unlock more articles.

What operating system did it infect? : https://www.smh.com.au/world/first-mobile-phone-virusidentified-20040616-gdj4up.html



The first ever computer virus that can infect mobile phones has been discovered, according to anti-virus software developers.

The French unit of the Russian security software developer Kaspersky Labs said that that virus - called Cabir - appears to have been developed by an international group of hackers called 29A, who specialise in creating "proof of concept" viruses which try to show that no technology is reliable and safe from their attacks.

29A is the hexadecimal (a number system used in computing) equivalent of "666", otherwise known as the devil's number.

Cabir infects the Symbian operating system that is used in several makes of mobiles, notably the Nokia brand, specifically the Nokia Series 60 mobile.

It propagates through the new bluetooth wireless technology that is in several new mobile phones, scanning for other phones using Bluetooth wireless technology, then sends a copy of itself to the first vulnerable one it finds.

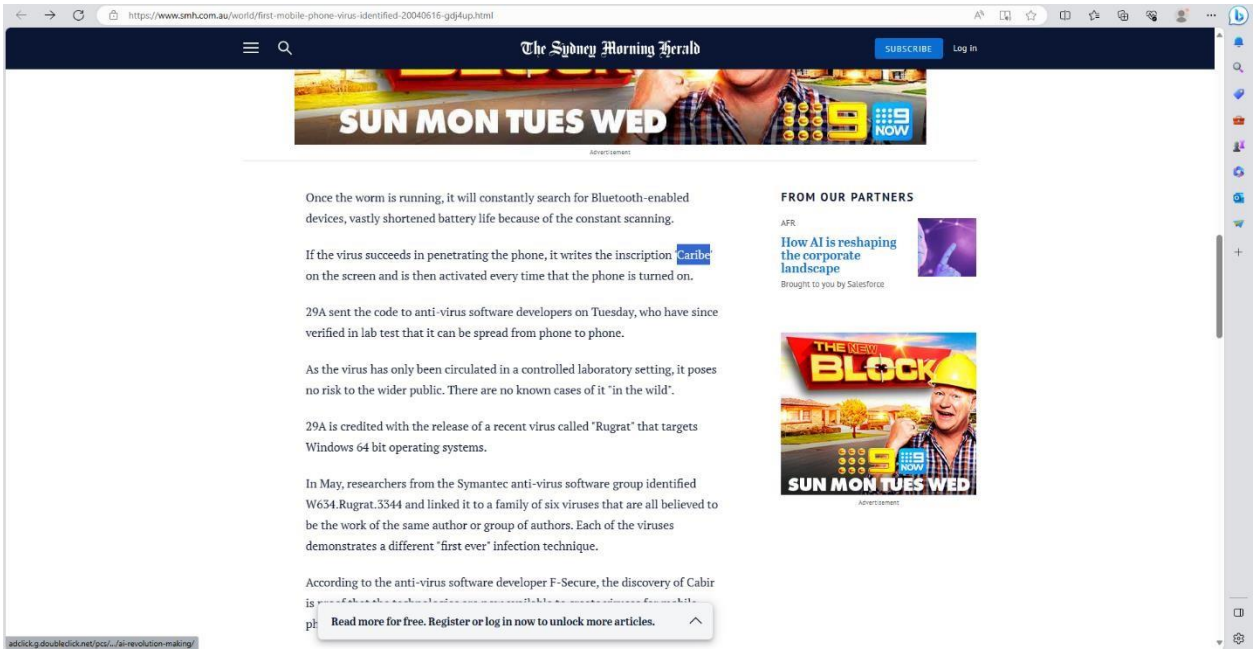
Thank you for reading the Herald. This article is complimentary.

Register or log in now to read more articles and unlock extra benefits.

No payment required

READ MORE

What message did it show on the screen of the infected mobile phone?: https://www.smh.com.au/world/first-mobile-phone-virus-identified-20040616-gdj4up.html



The Sydney Morning Herald

SUBSCRIBE Log in

Once the worm is running, it will constantly search for Bluetooth-enabled devices, vastly shortened battery life because of the constant scanning.

If the virus succeeds in penetrating the phone, it writes the inscription "Caribe" on the screen and is then activated every time that the phone is turned on.

29A sent the code to anti-virus software developers on Tuesday, who have since verified in lab test that it can be spread from phone to phone.

As the virus has only been circulated in a controlled laboratory setting, it poses no risk to the wider public. There are no known cases of it "in the wild".

29A is credited with the release of a recent virus called "Rugrat" that targets Windows 64 bit operating systems.

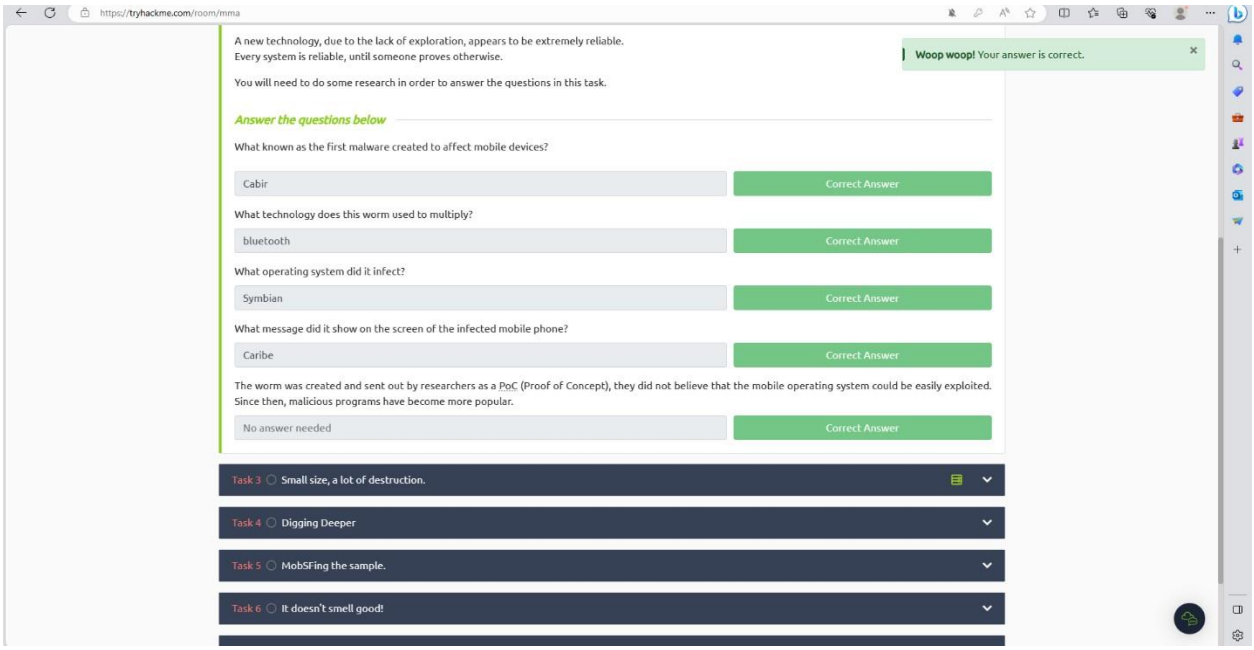
In May, researchers from the Symantec anti-virus software group identified W634.Rugrat.3344 and linked it to a family of six viruses that are all believed to be the work of the same author or group of authors. Each of the viruses demonstrates a different "first ever" infection technique.

According to the anti-virus software developer F-Secure, the discovery of Cabir

Read more for free. Register or log in now to unlock more articles.

FROM OUR PARTNERS

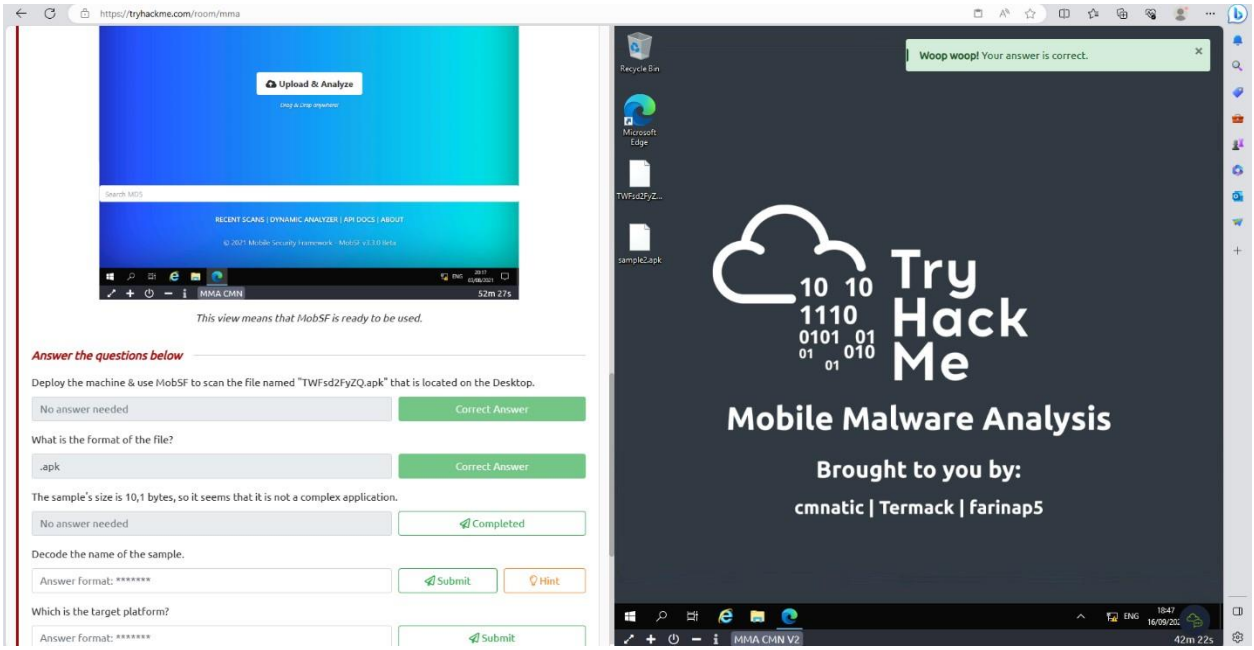
How AI is reshaping the corporate landscape



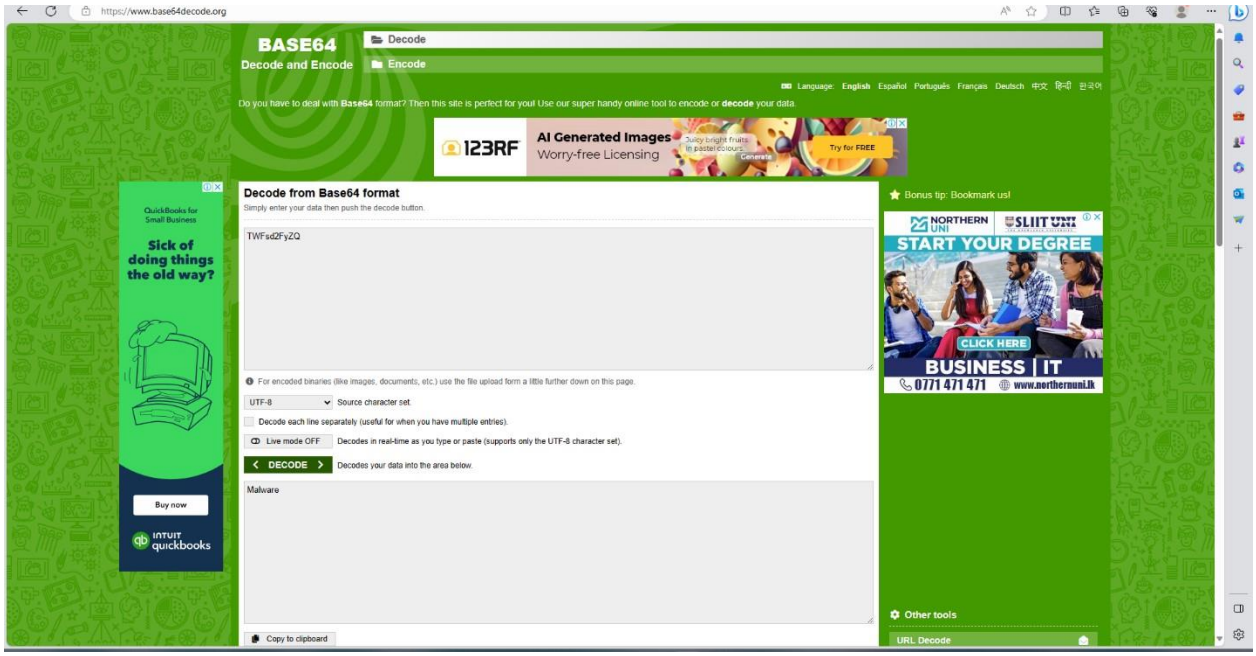
Task 3

What is the format of the file?

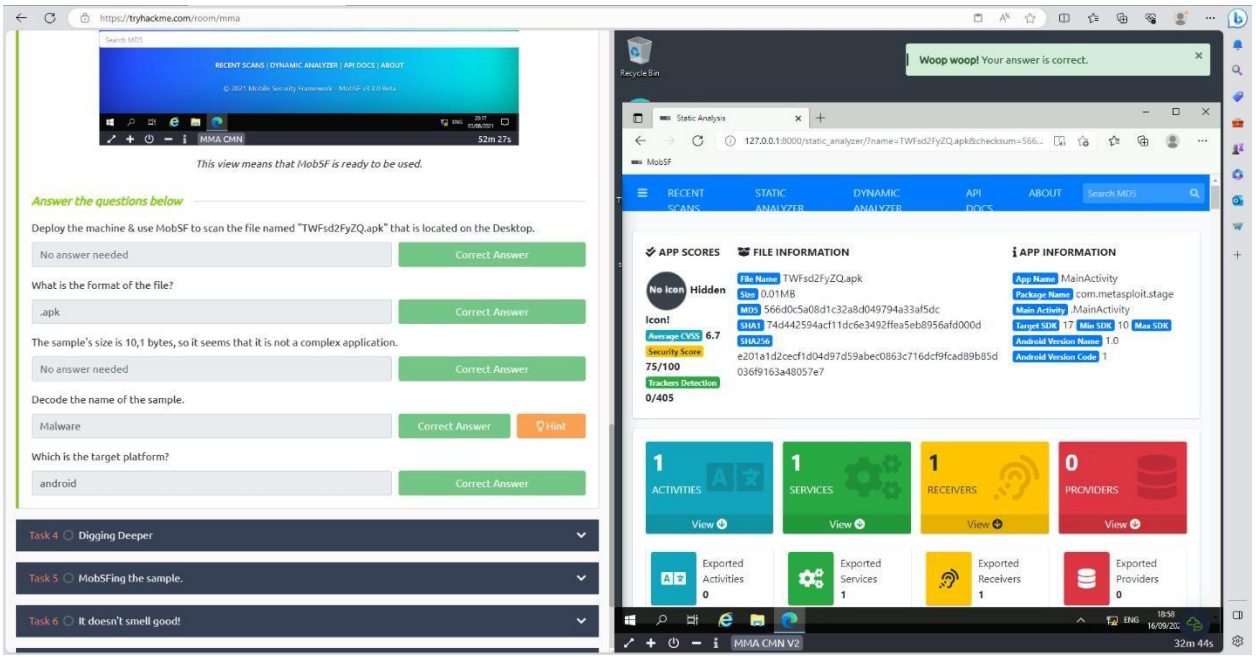
`TWFsd2FyZQ.apk`



Decode the name of the sample. Decode Link : https://www.base64decode.org/

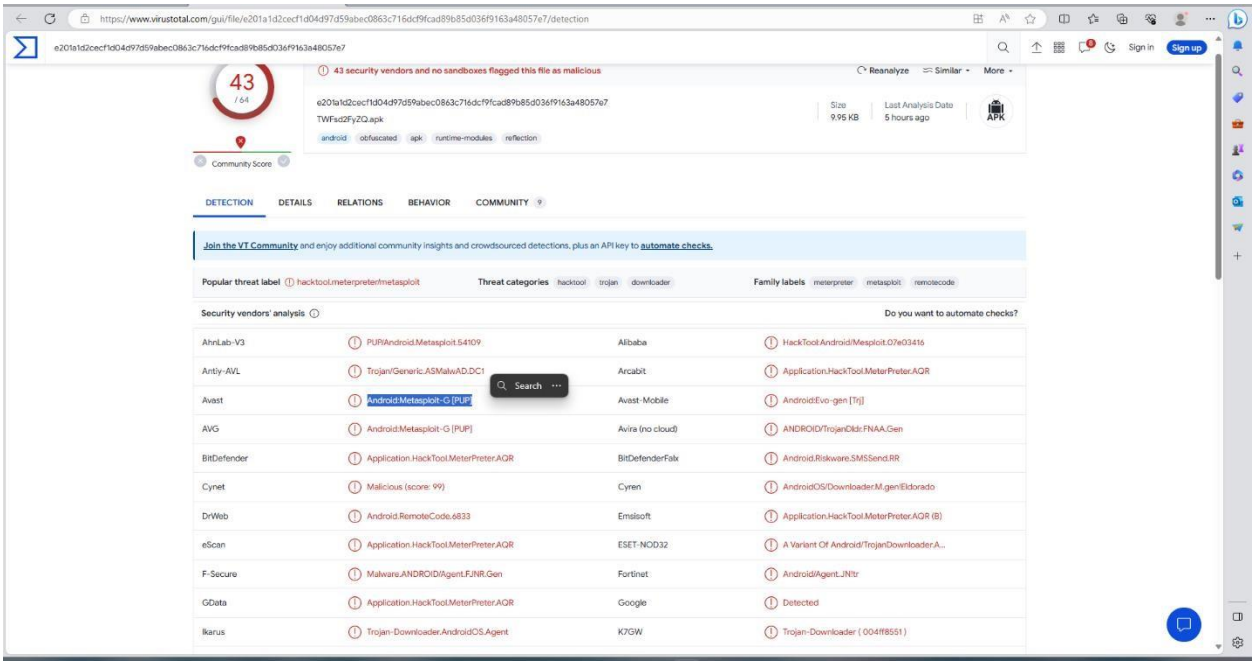


Which is the target platform? Read: https://fileinfo.com/extension/apk

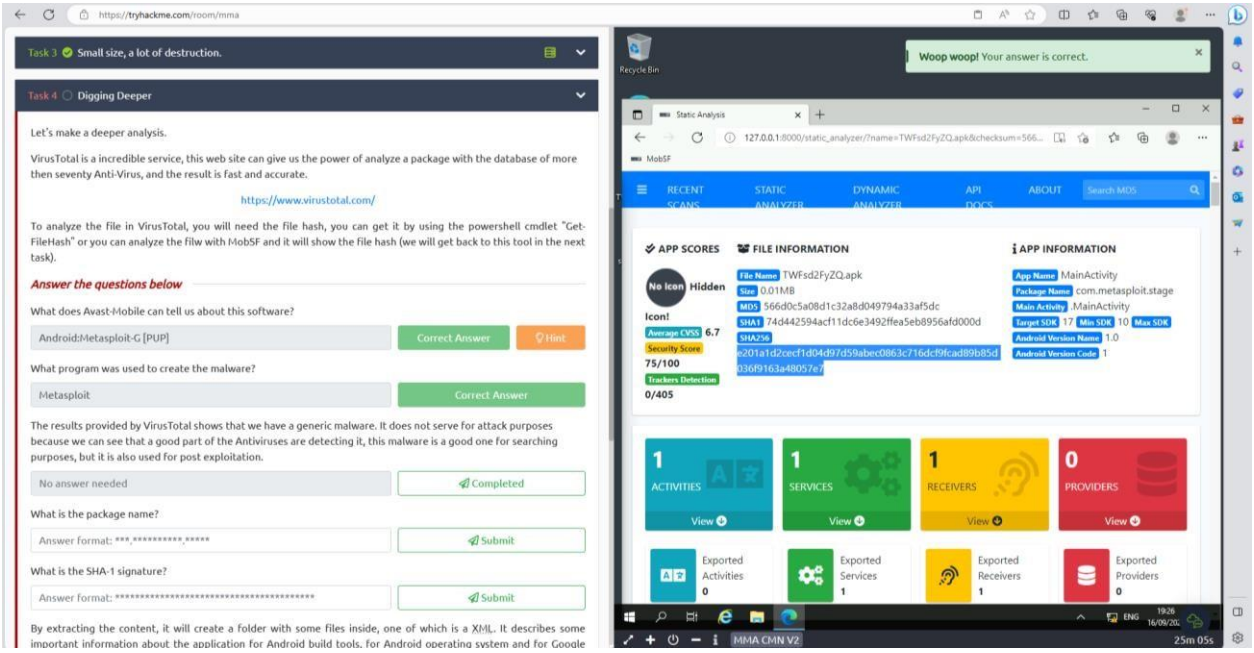


Task 4

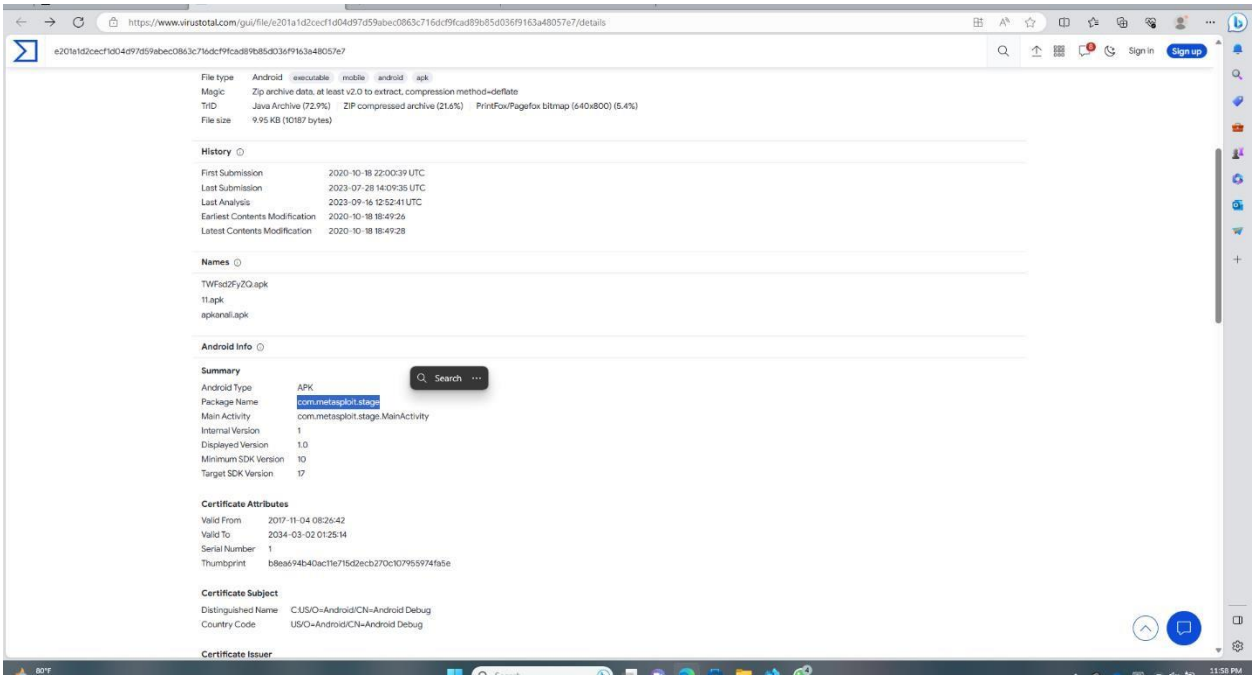
What does “Avast-Mobile” can tell us about this software?
https://www.virustotal.com/gui/file/e201a1d2cecf1d04d97d59abec0863c716dcf9fcad89b85d036



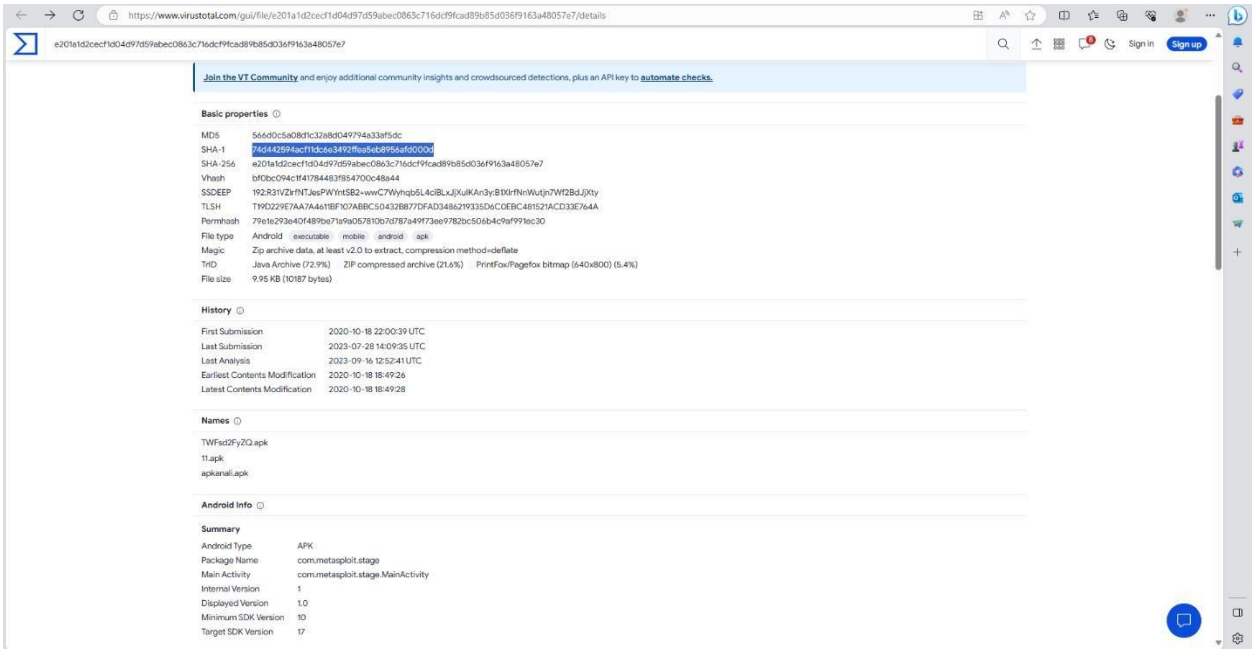
What program was used to create the malware?



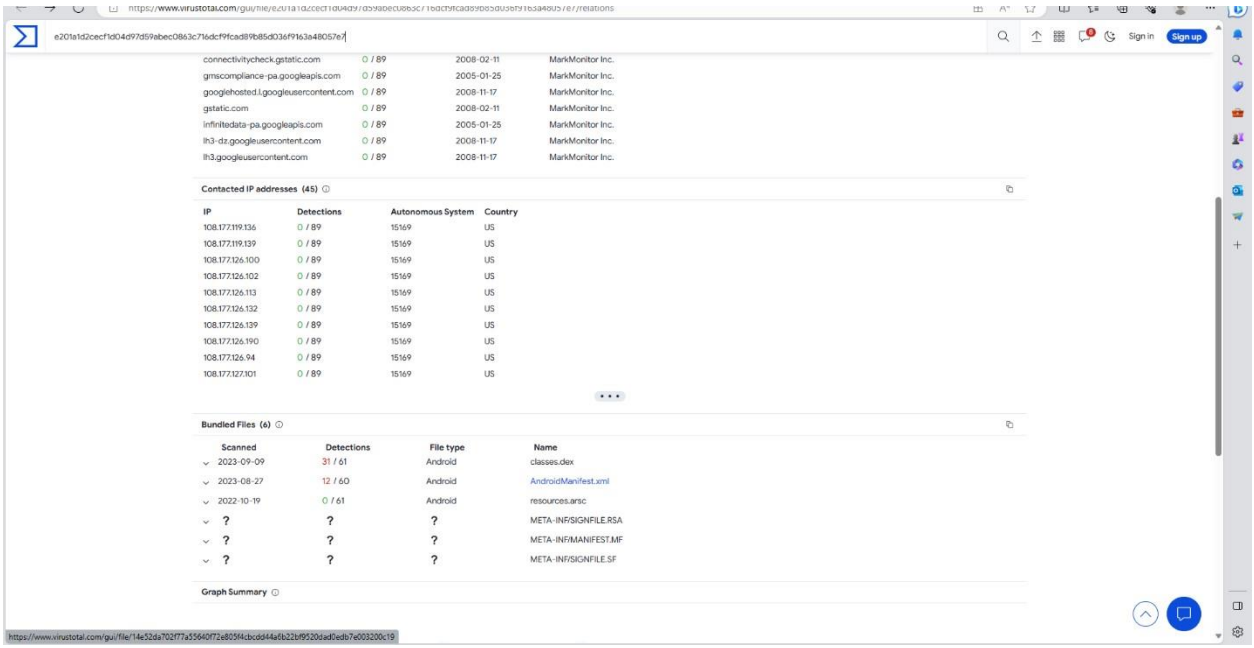
What is the package name?



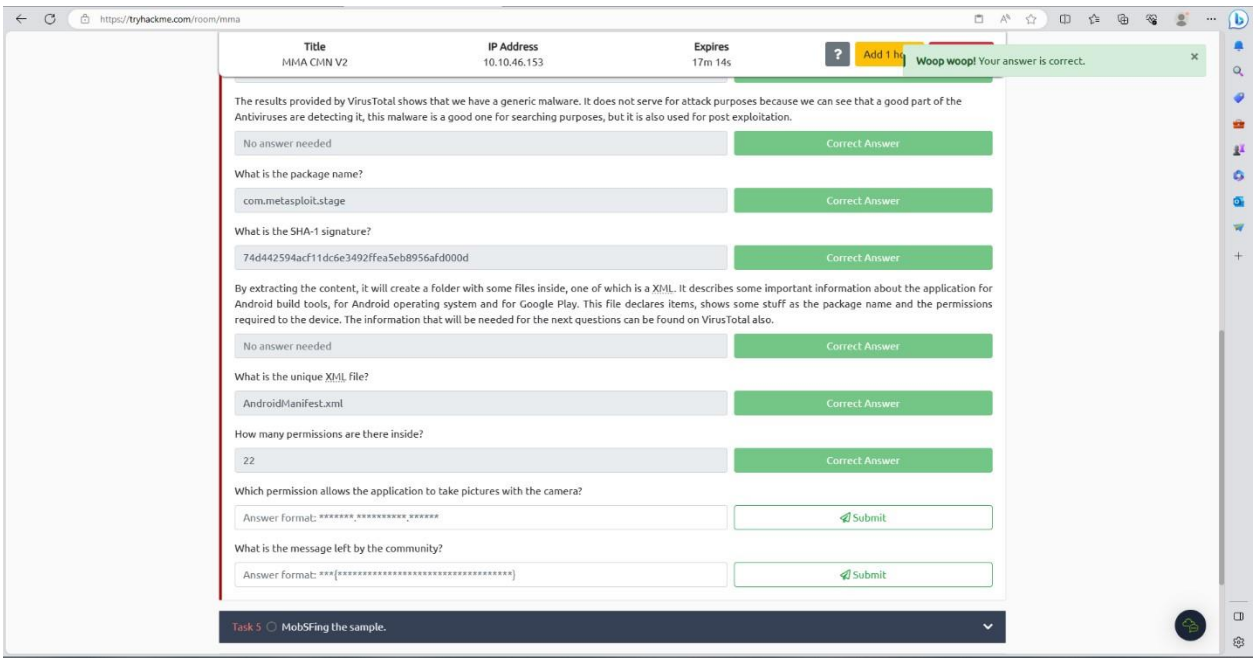
What is the SHA-1 signature?



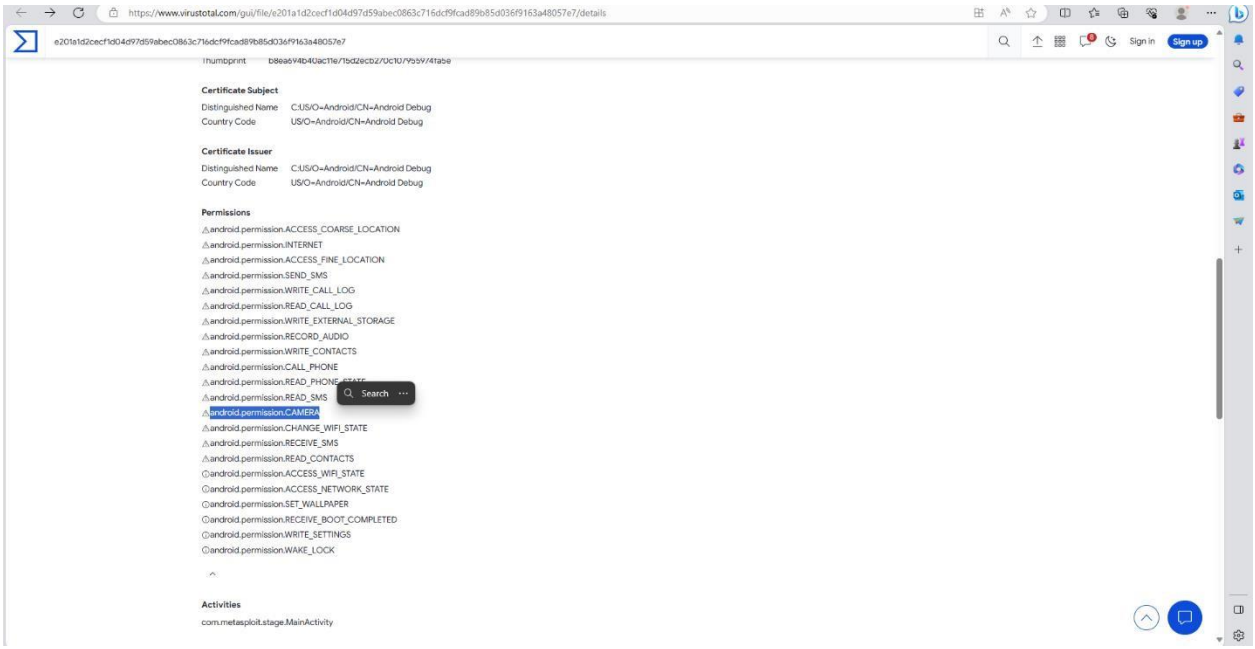
What is the unique XML file?



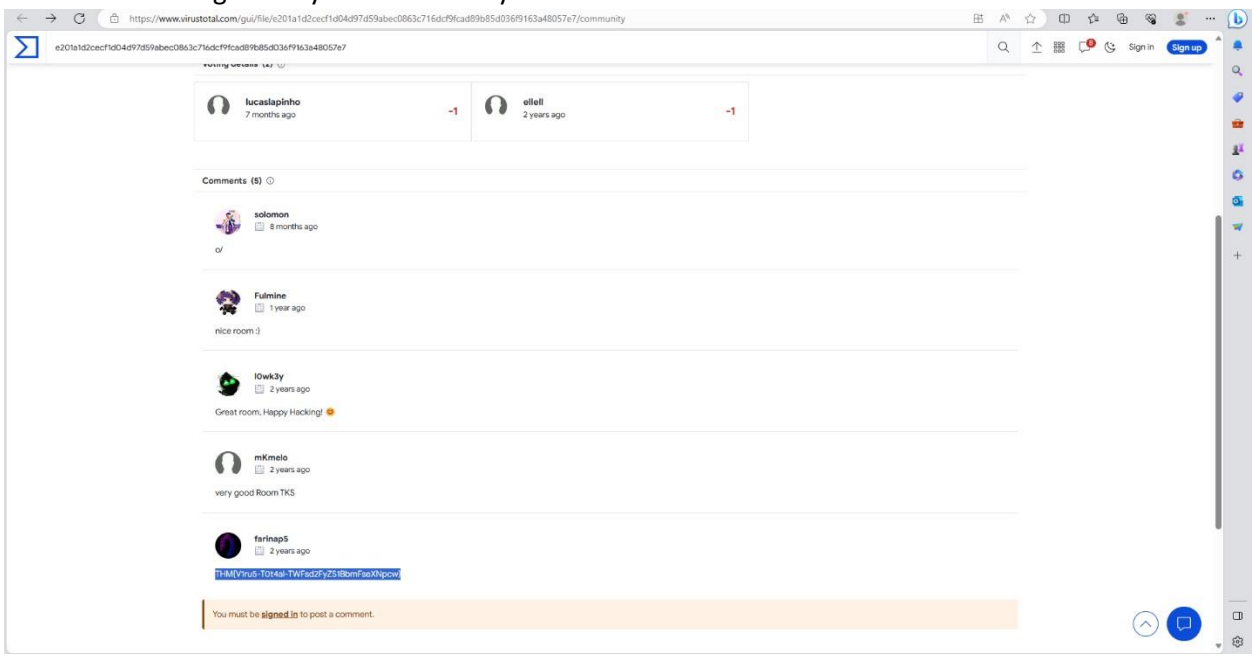
How many permissions are there inside?

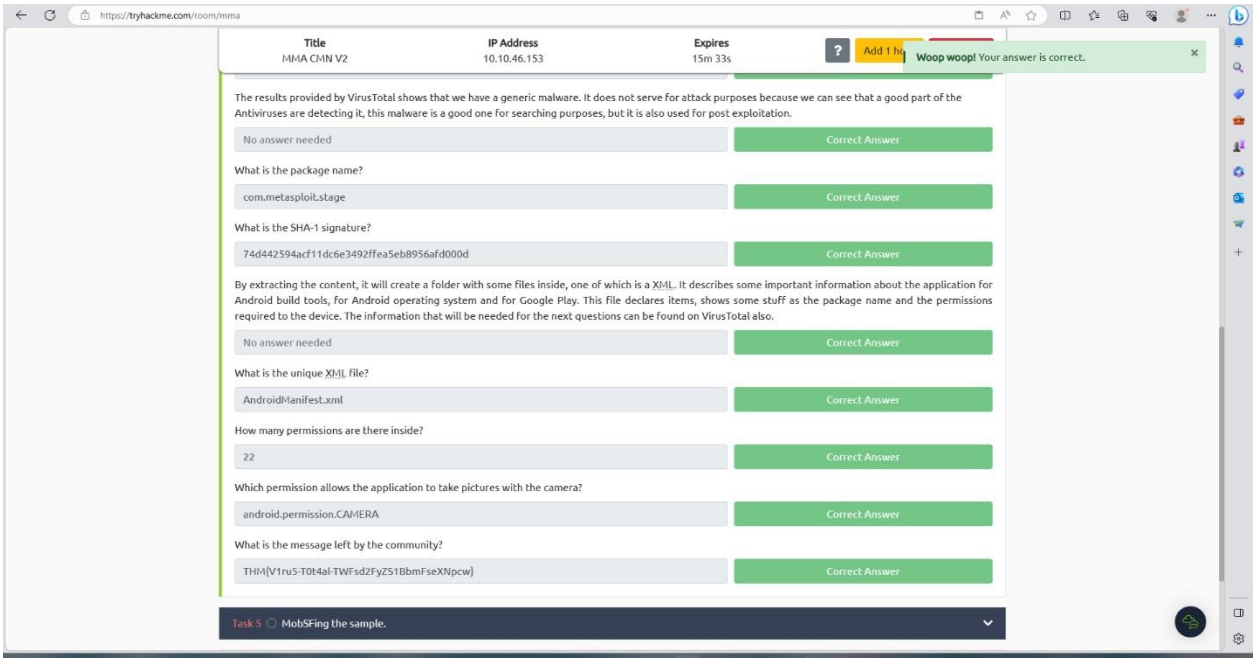


Which permission allows the application to take pictures with the camera?



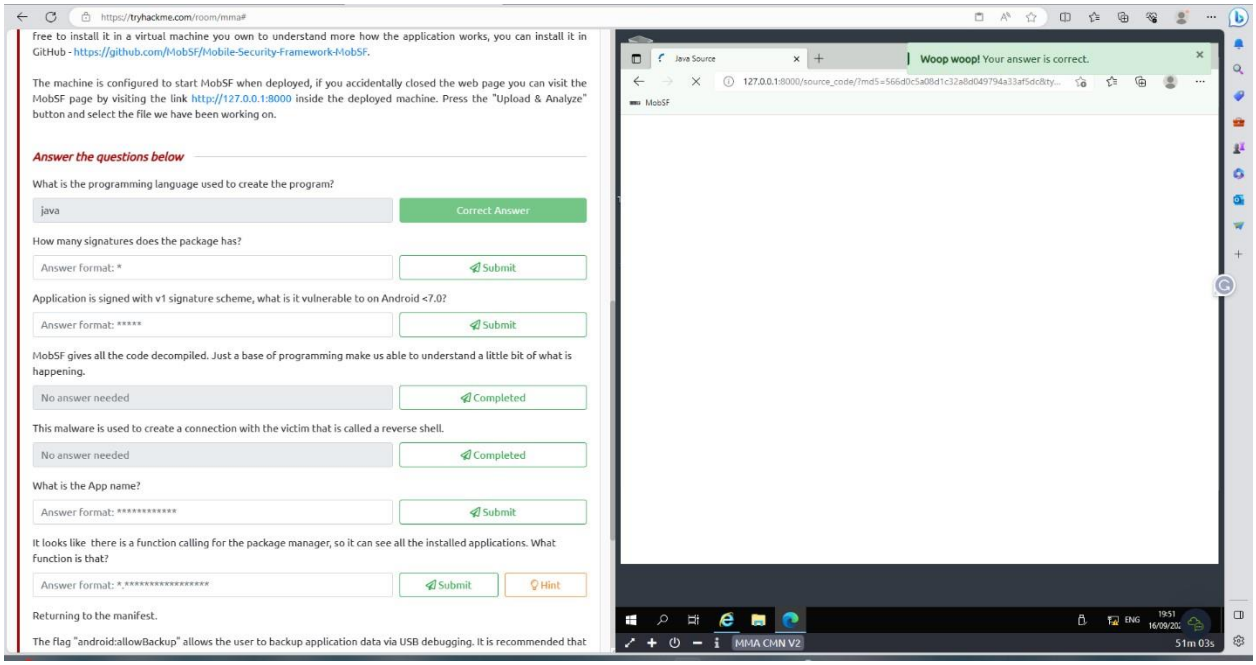
What is the message left by the community?



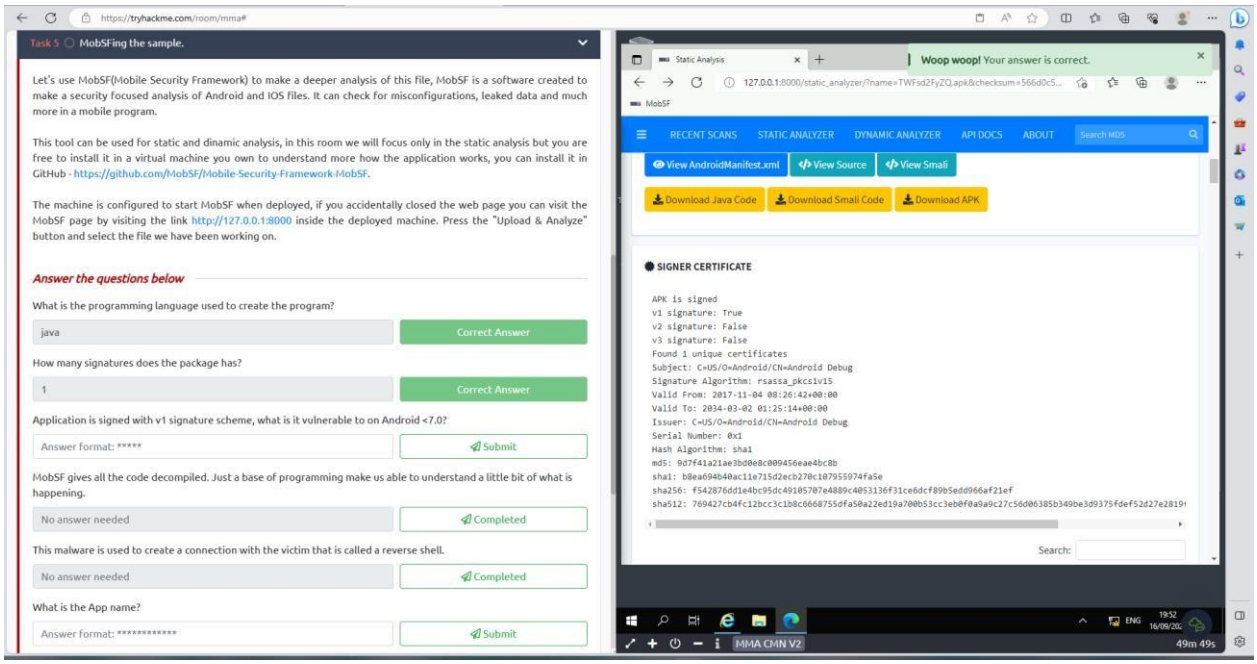


Task 5

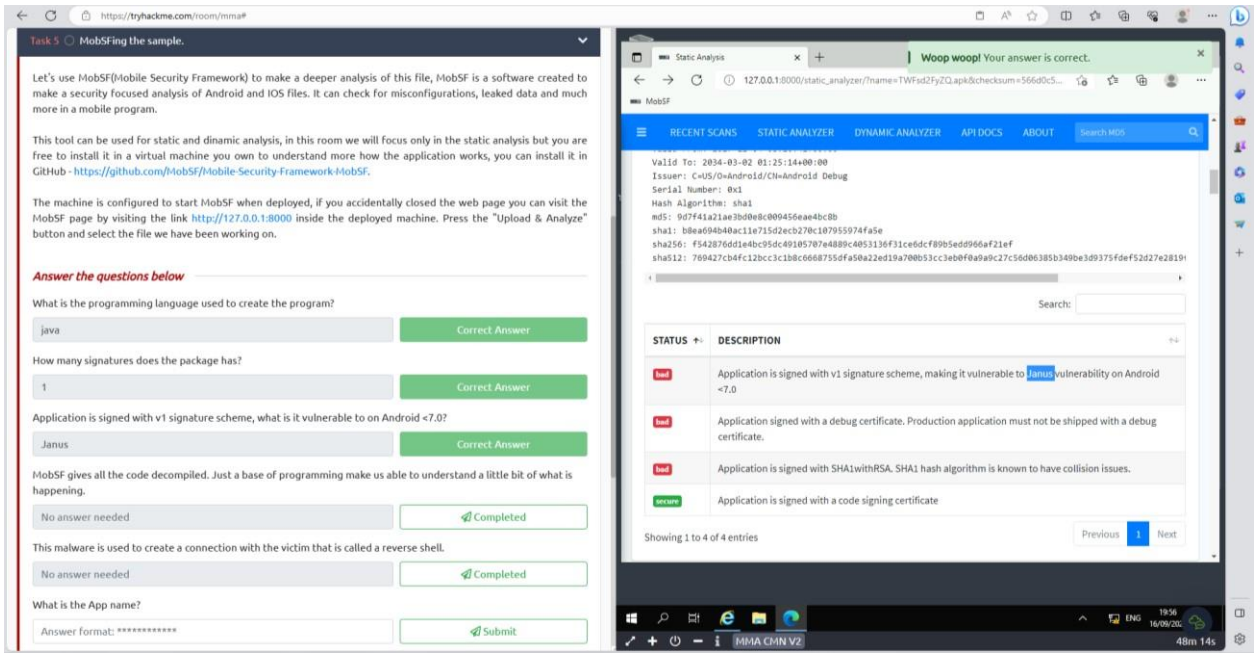
What is the programming language used to create the program?



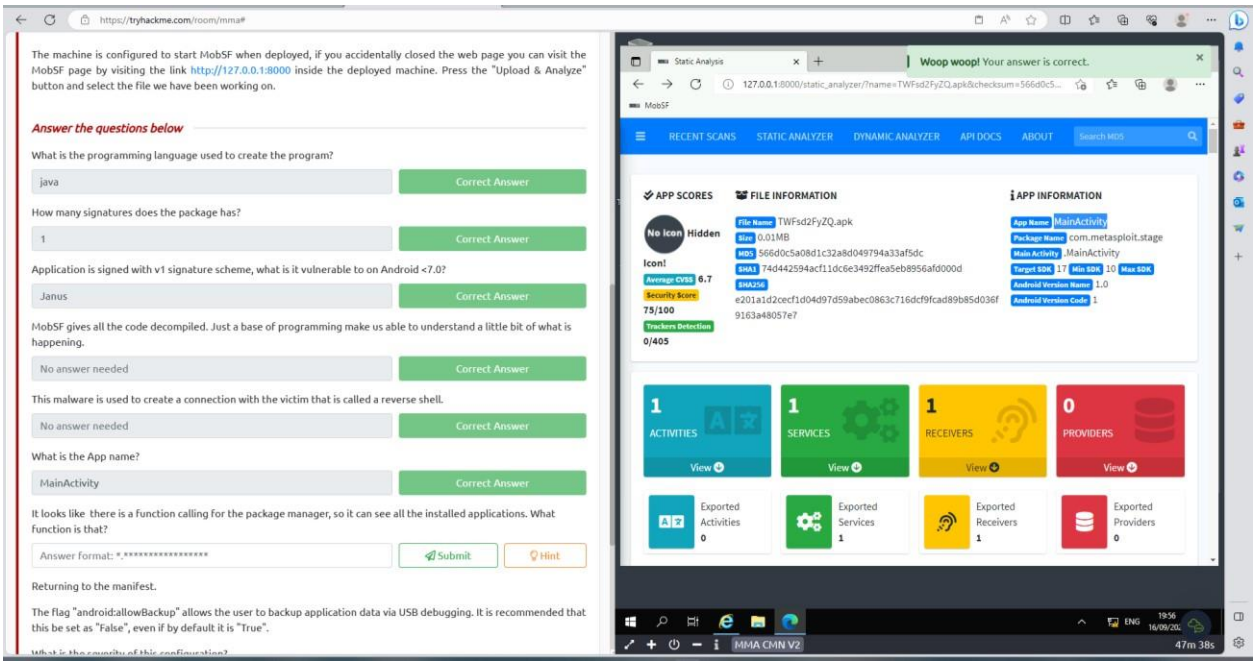
How many signatures does the package has?



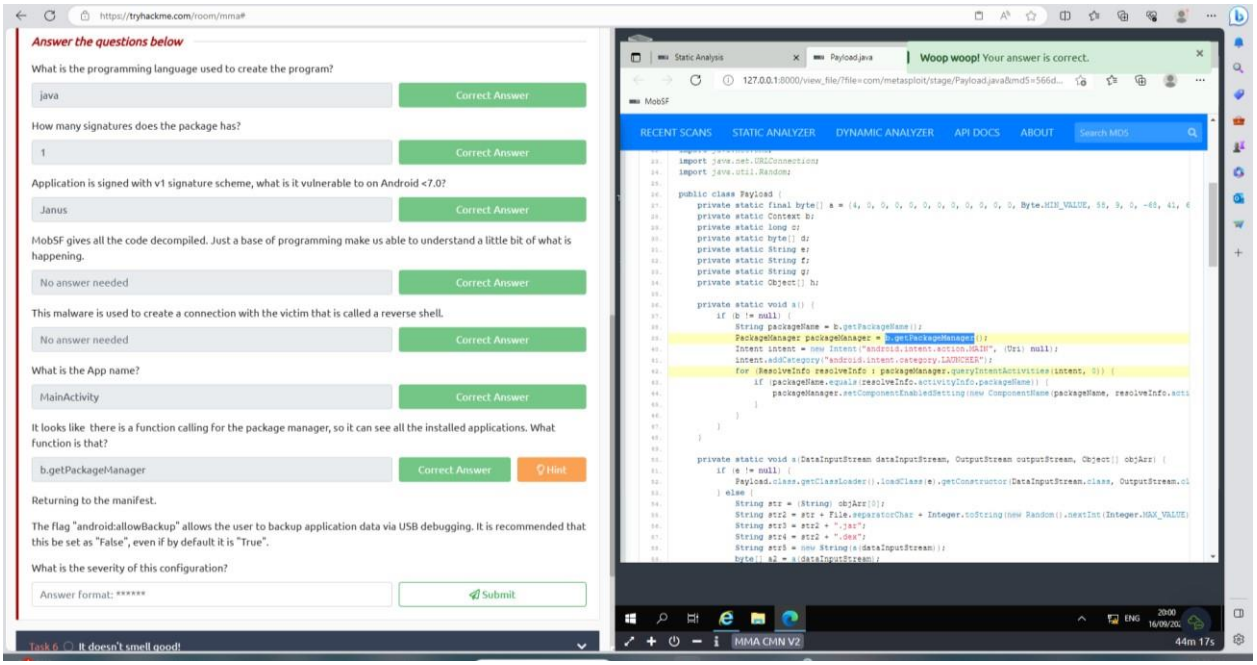
Application is signed with v1 signature scheme, what is it vulnerable to on Android<7.0?



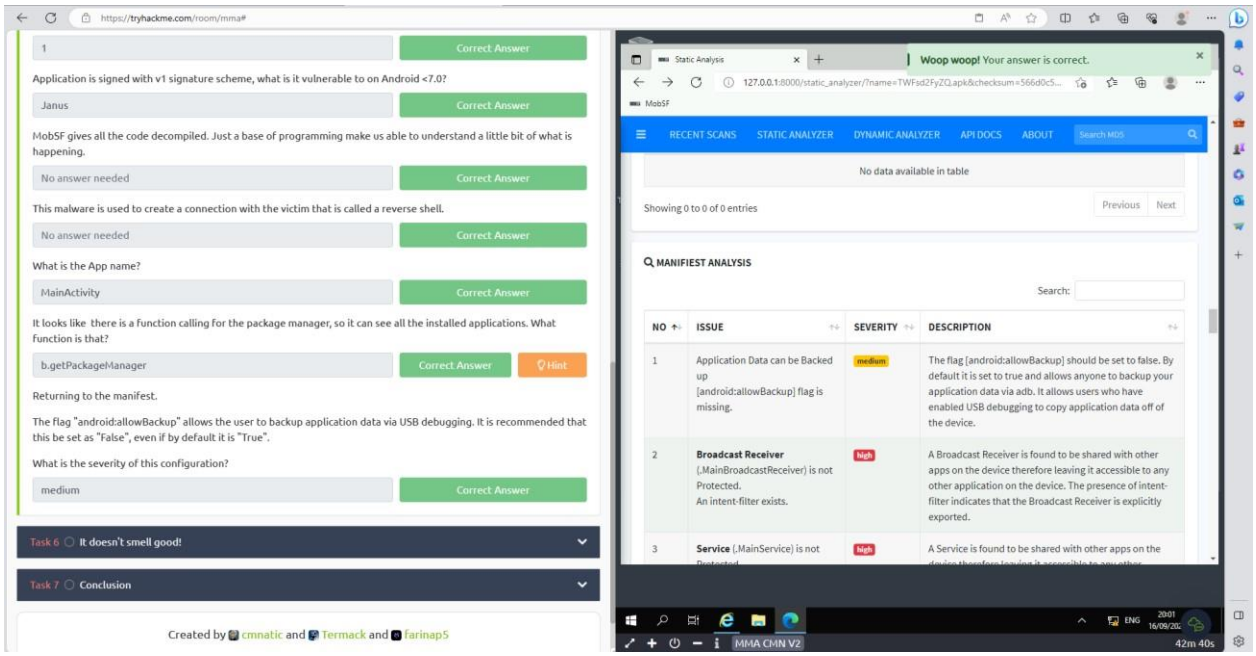
What is the App name?



It looks like there is a function calling for the package manager, so it can see all the installed applications. What function is that?

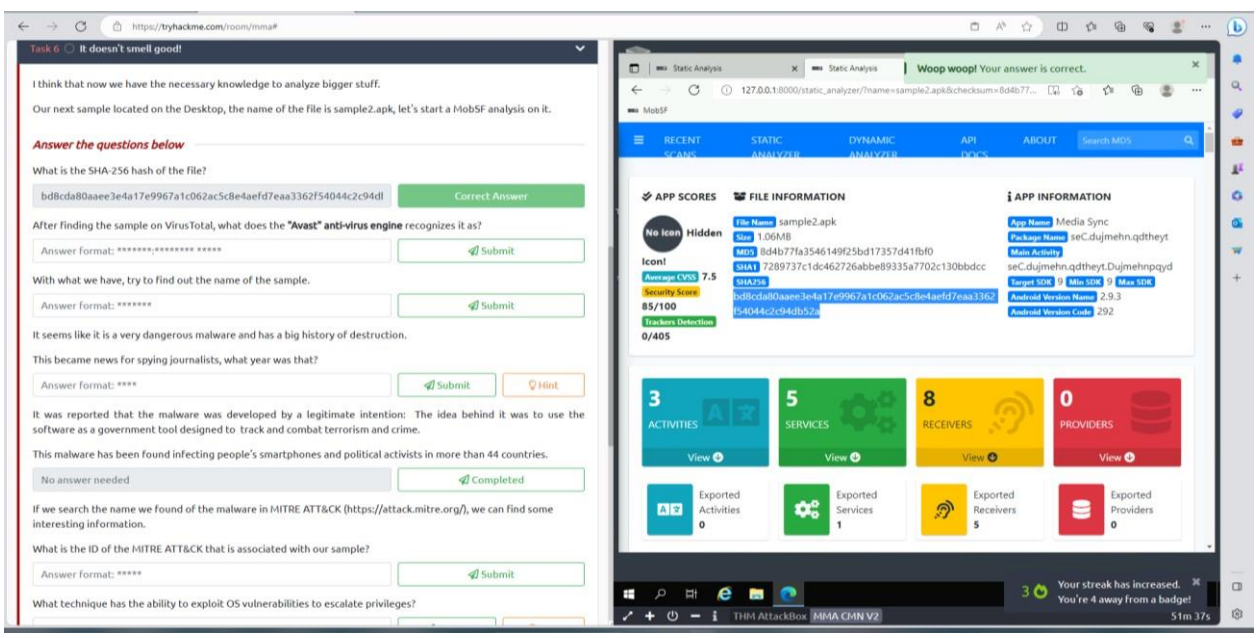


The flag “android:allowBackup” allows the user to backup application data via USB debugging. It is recommended that this be set as “False”, even if by default it is “True”. ● What is the severity of this configuration?



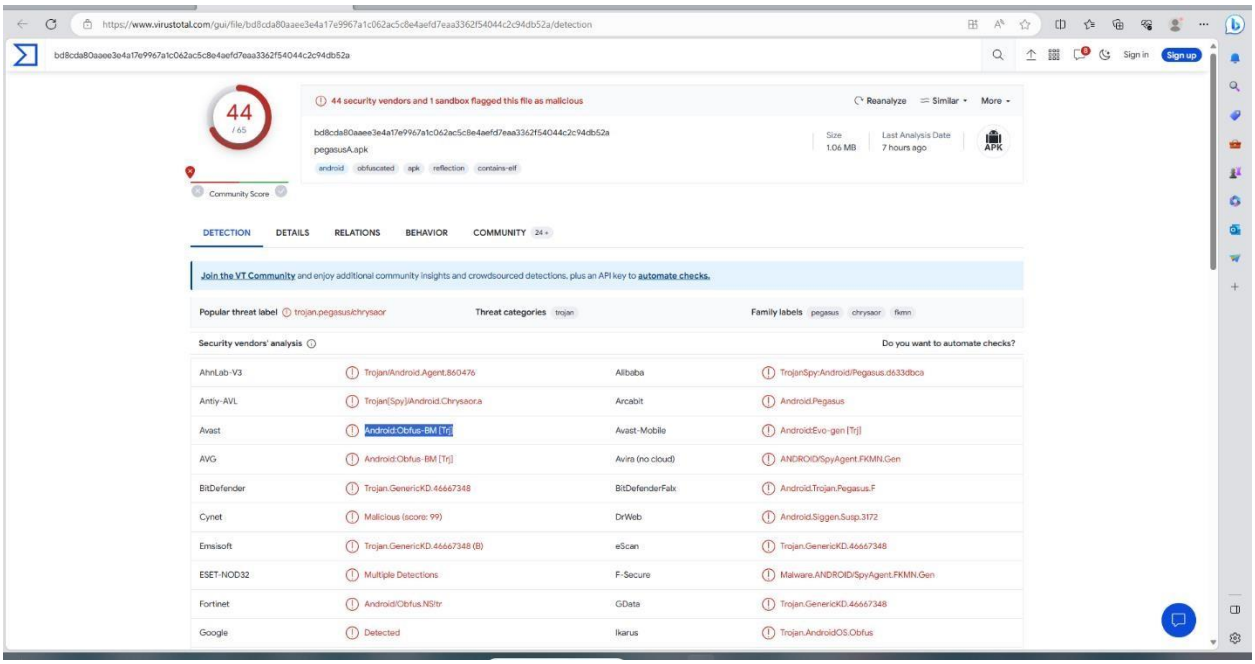
Task 6

Our next sample located on the Desktop, the name of the file is sample2.apk, let’s start a MobSF analysis on it.What is the SHA-256 hash of the file?

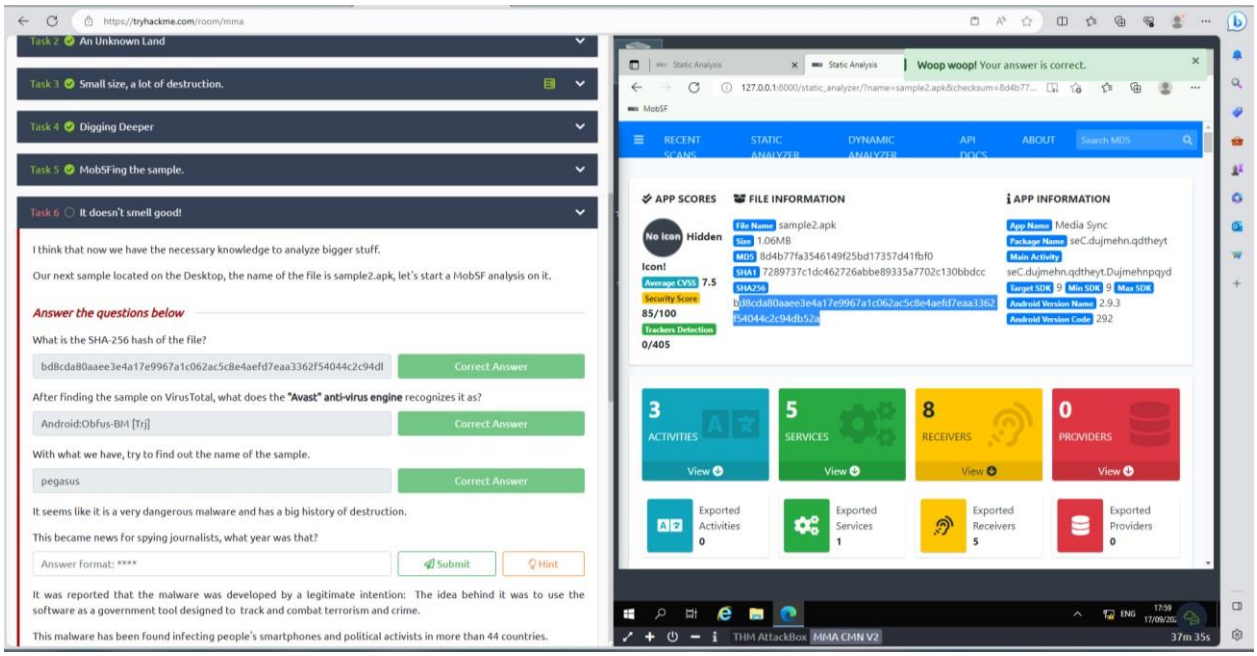


After finding the sample on VirusTotal, what does the “Avast” anti-virus engine recognizes it as?

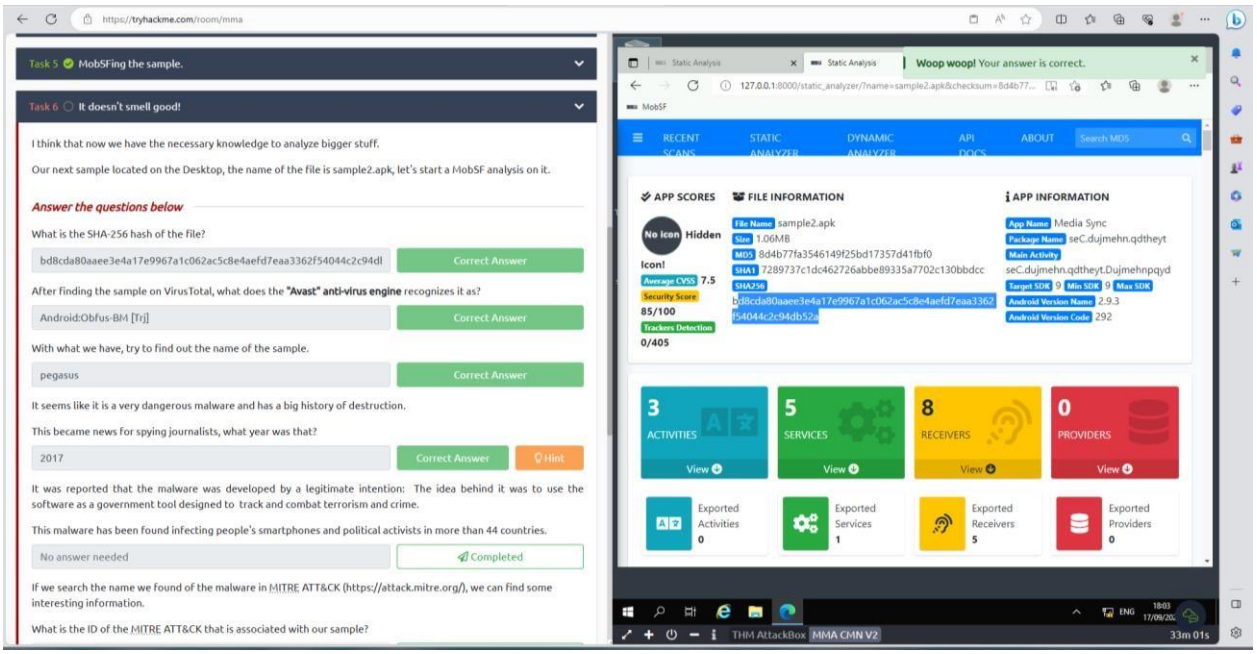
https://www.virustotal.com/gui/file/bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f540



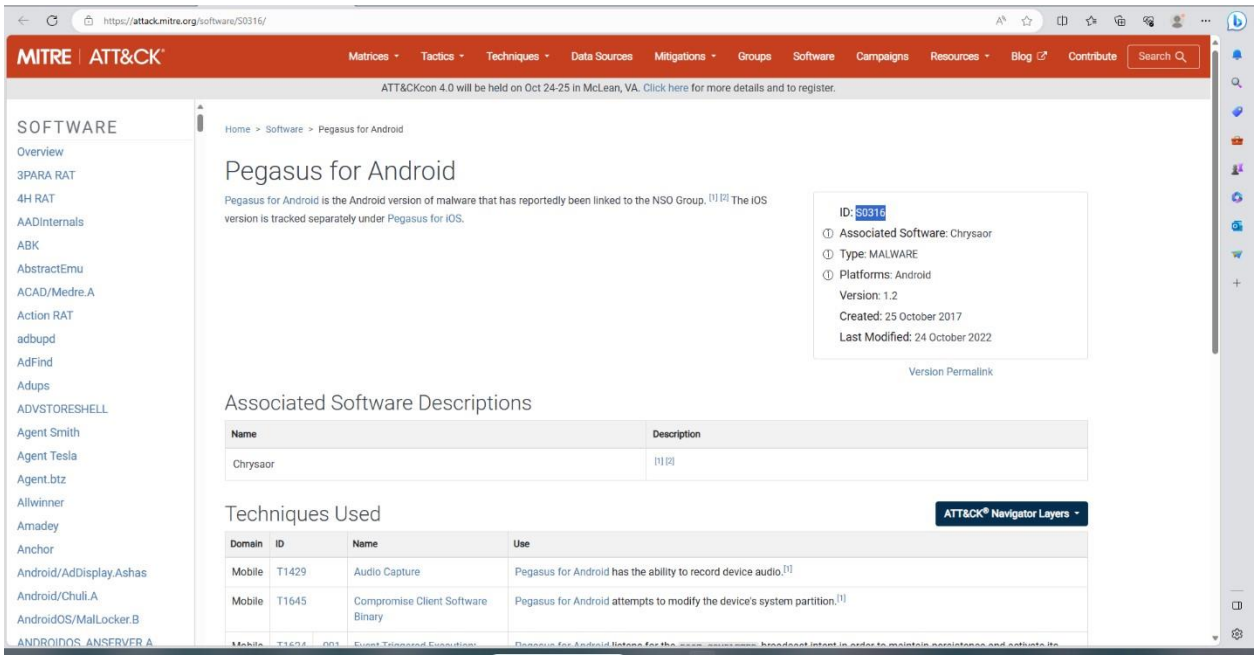
With what we have, try to find out the name of the sample.



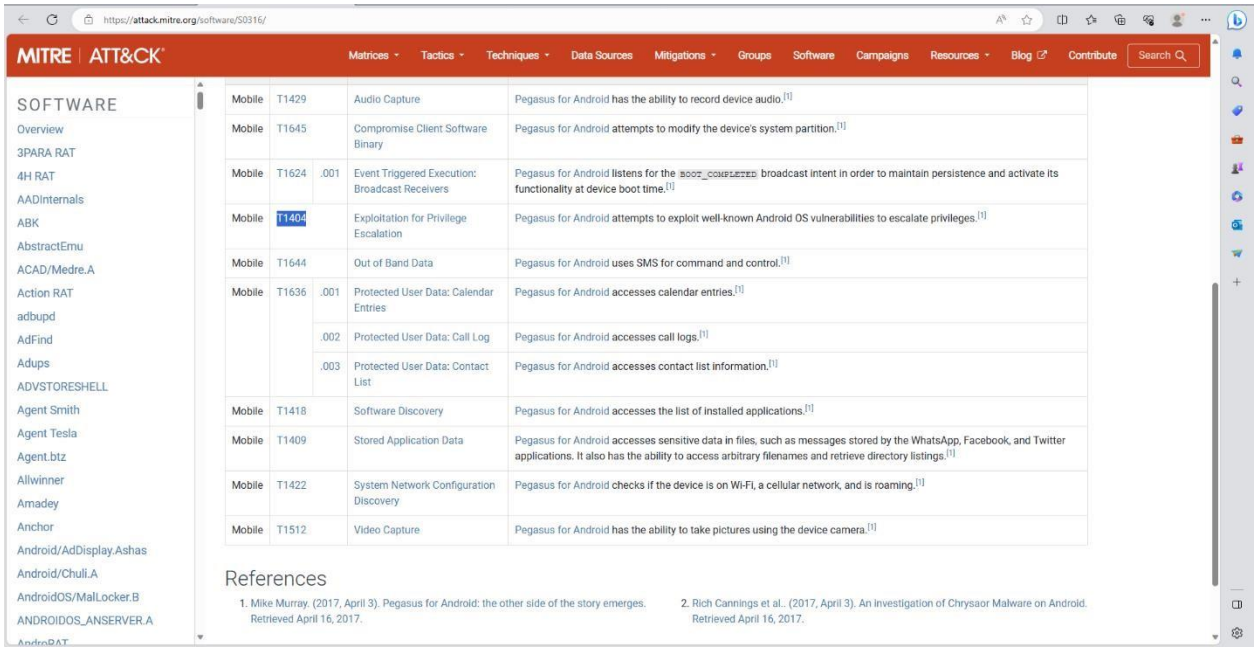
This became news for spying journalists, what year was that? Read:
https://en.wikipedia.org/wiki/Pegasus_(spyware)



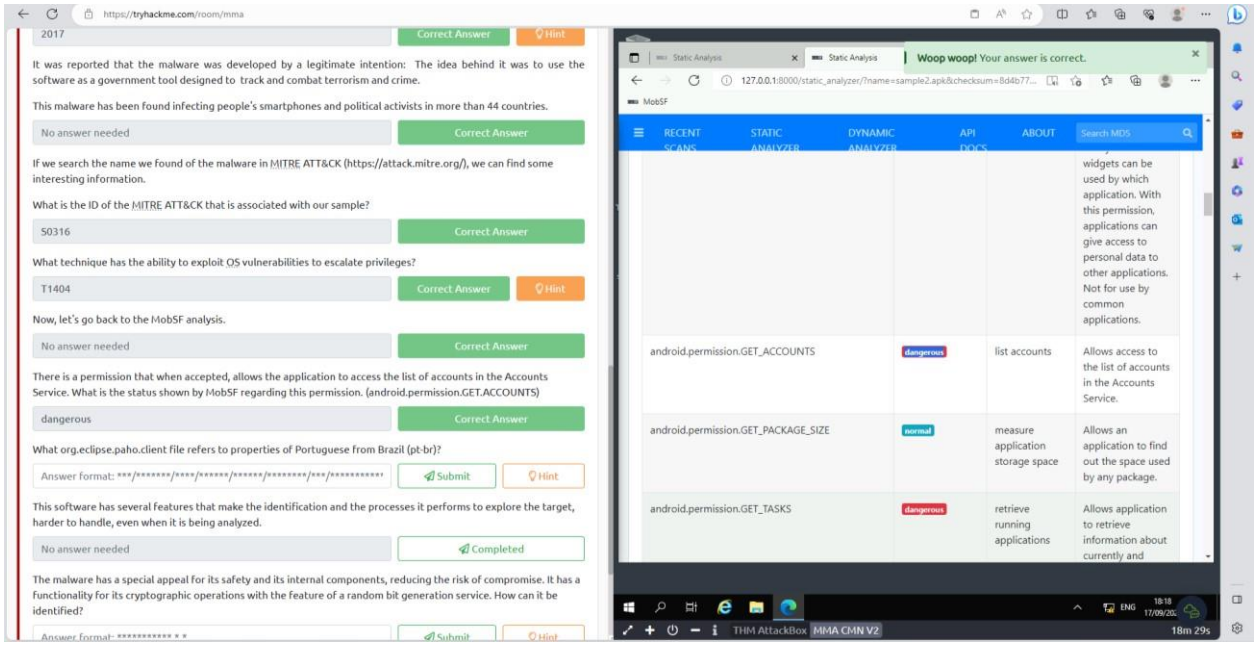
What is the ID of the MITRE ATT&CK that is associated with our sample? Review:
https://attack.mitre.org/software/S0316/



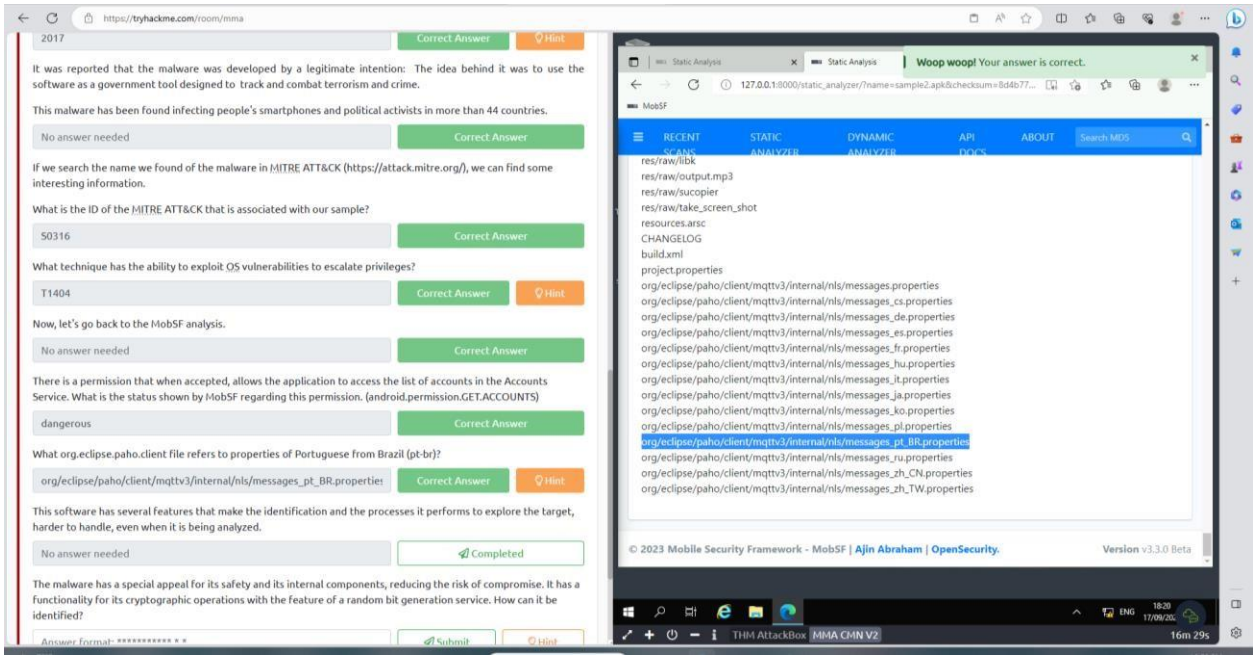
What technique has the ability to exploit OS vulnerabilities to escalate privileges? Review: https://attack.mitre.org/techniques/T1404/



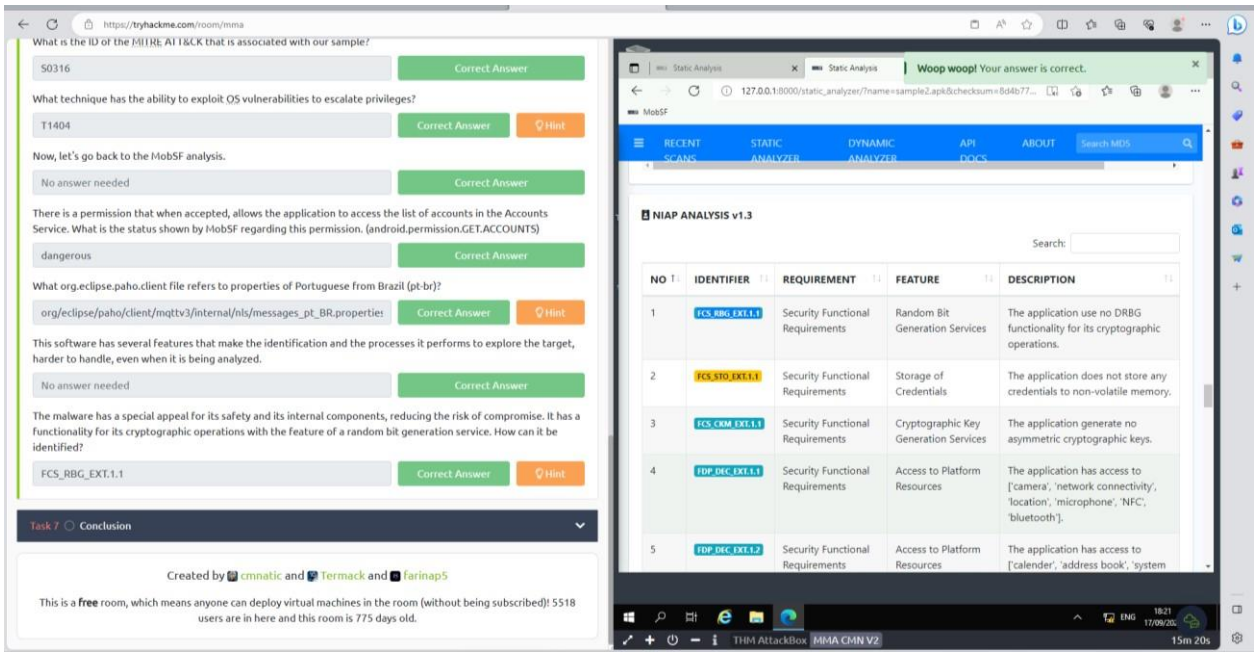
There is a permission that when accepted, allows the application to access the list of accounts in the Accounts Service. What is the status shown by MobSF regarding this permission. (android.permission.GET.ACCOUNTS)

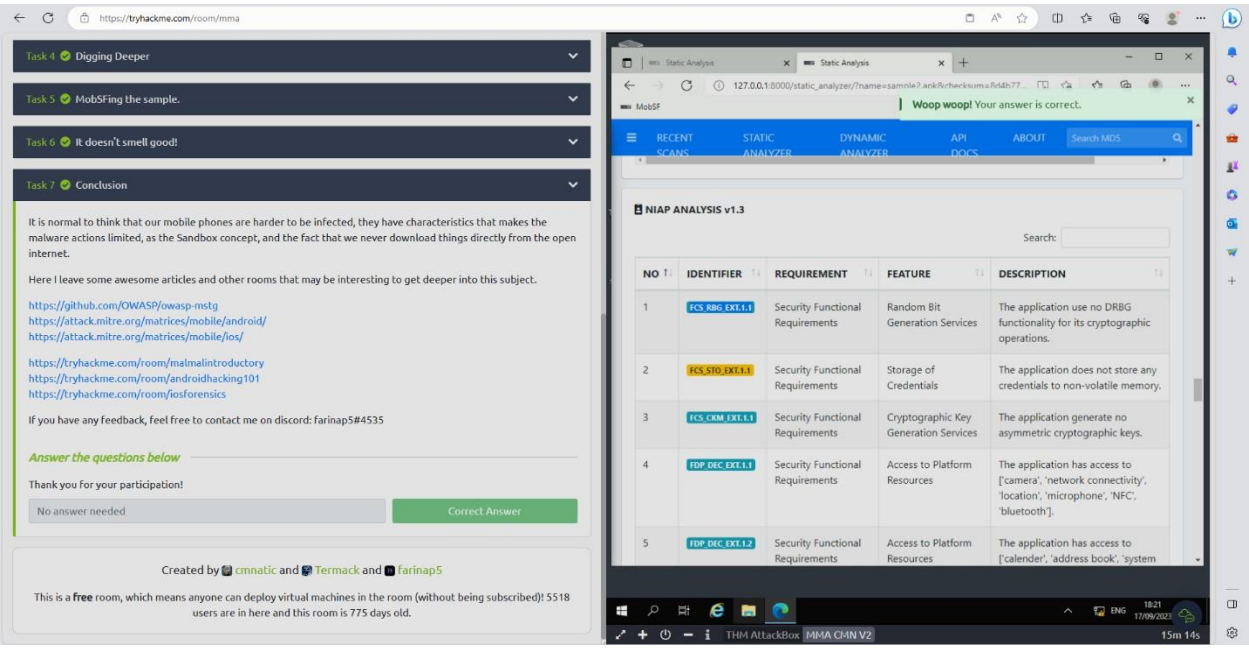


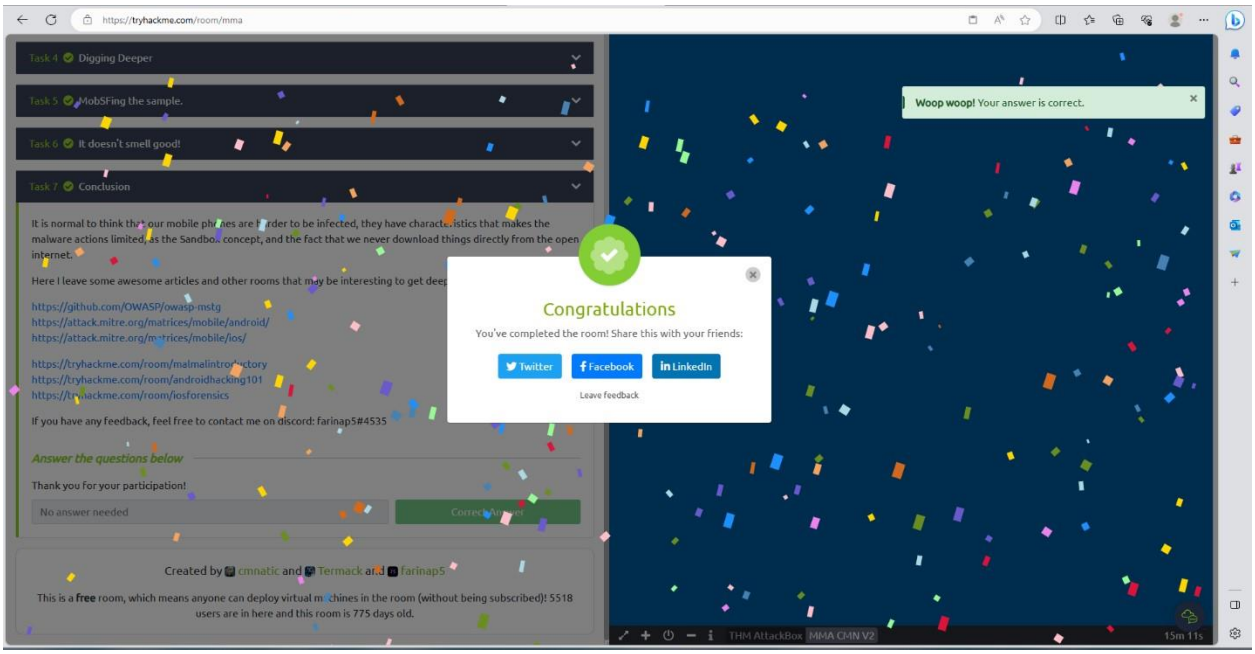
What org.eclipse.paho.client file refers to properties of Portuguese from Brazil (pt br)?



The malware has a special appeal for its safety and its internal components, reducing the risk of compromise. It has a functionality for its cryptographic operations with the feature of a random bit generation service. How can it be identified?




https://tryhackme.com/room/mma
Task 4 Digging Deeper
Task 5 MobSFing the sample.
Task 6 It doesn't smell good!
Task 7 Conclusion
It is normal to think that our mobile phones are harder to be infected, they have characteristics that makes the malware actions limited, as the Sandbox concept, and the fact that we never download things directly from the open internet.
Here I leave some awesome articles and other rooms that may be interesting to get deeper into this subject.
https://github.com/OWASP/owasp-mstg
https://attack.mitre.org/matrices/mobile/android/
https://attack.mitre.org/matrices/mobile/ios/
https://tryhackme.com/room/malmalintroductory
https://tryhackme.com/room/androidhacking101
https://tryhackme.com/room/iosforensics
If you have any feedback, feel free to contact me on discord: farinap5#4535
Answer the questions below
Thank you for your participation!
No answer needed
Correct Answer
Created by cmnatic and Termack and farinap5
This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 5518 users are in here and this room is 775 days old.
Woop woop! Your answer is correct.
MobSF
RECENT SCANS
STATIC ANALYZER
DYNAMIC ANALYZER
API DOCS
ABOUT
Search MD5
NIAP ANALYSIS v1.3
Search:
NO
IDENTIFIER
REQUIREMENT
FEATURE
DESCRIPTION
1 FCS_RBG_EXT.1.1 Security Functional Requirements Random Bit Generation Services The application use no DRBG functionality for its cryptographic operations.
2 FCS_STO_EXT.1.1 Security Functional Requirements Storage of Credentials The application does not store any credentials to non-volatile memory.
3 FCS_CKM_EXT.1.1 Security Functional Requirements Cryptographic Key Generation Services The application generate no asymmetric cryptographic keys.
4 FDP_DEC_EXT.1.1 Security Functional Requirements Access to Platform Resources The application has access to ['camera', 'network connectivity', 'location', 'microphone', 'NFC', 'bluetooth'].
5 FDP_DEC_EXT.1.2 Security Functional Requirements Access to Platform Resources The application has access to ['calender', 'address book', 'system
THM AttackBox
MMA CMN V2
15m 14s


https://tryhackme.com/room/mma
Task 4 Digging Deeper
Task 5 MobSFing the sample.
Task 6 It doesn't smell good!
Task 7 Conclusion
Woop woop! Your answer is correct.
Congratulations
You've completed the room! Share this with your friends:
Twitter
Facebook
LinkedIn
Leave feedback
Answer the questions below
Thank you for your participation!
No answer needed
Created by cmnatic and Termack and farinap5
THM AttackBox
MMA CMN V2
15m 11s

Conclusion

In the field of cybersecurity, mobile malware analysis is a crucial discipline that is necessary for securing user data and preserving the security of mobile ecosystems in a time when tablets and smartphones have become commonplace. Analysts may analyze harmful software and comprehend its inner workings using a methodical and precise approach, enabling the creation of efficient defenses against changing digital threats. Analysts are prepared to meet the challenges offered by mobile malware by following a well-defined approach that includes planning, sample collecting, system setup, dynamic and static analysis, and traffic analysis. This proactive approach not only strengthens security measures but also gives people, organizations, and governments the power to protect against the never-ending swell of cyber-threats.

References

[1] - https://www.techtarget.com/searchmobilecomputing/definition/mobilemalware - Mobile malware

[2] TryHackMe - TryHackMe | Mobile Malware Analysis

[3] https://www.smh.com.au/world/first-mobile-phone-virus-identified-20040616gdj4up.html - First mobile phone virus identified