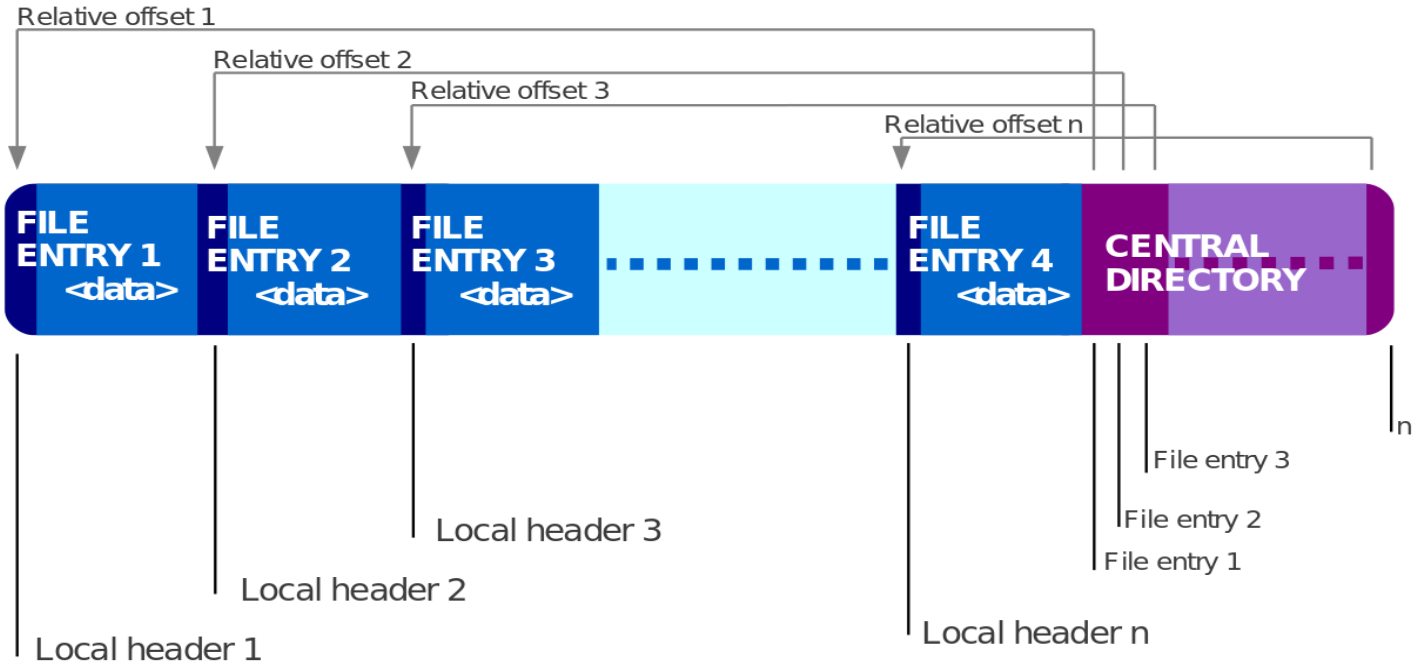
Leaving Our ZIP Undone

How to Abuse ZIP to Deliver Malware Apps

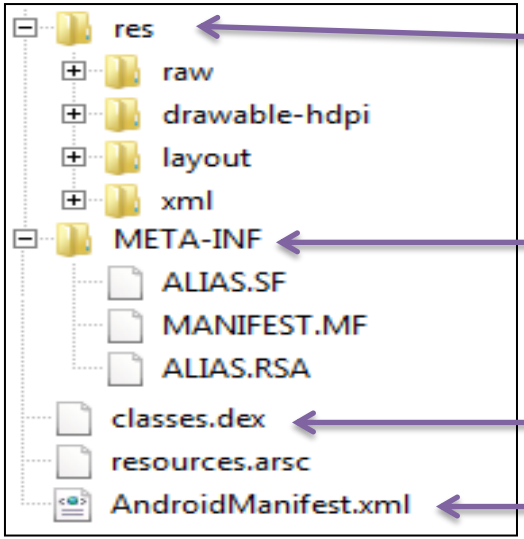
Gregory Panakkal
K7 Computing

APK Primer: ZIP Format

K7 COMPUTING™



APK Primer: Layout



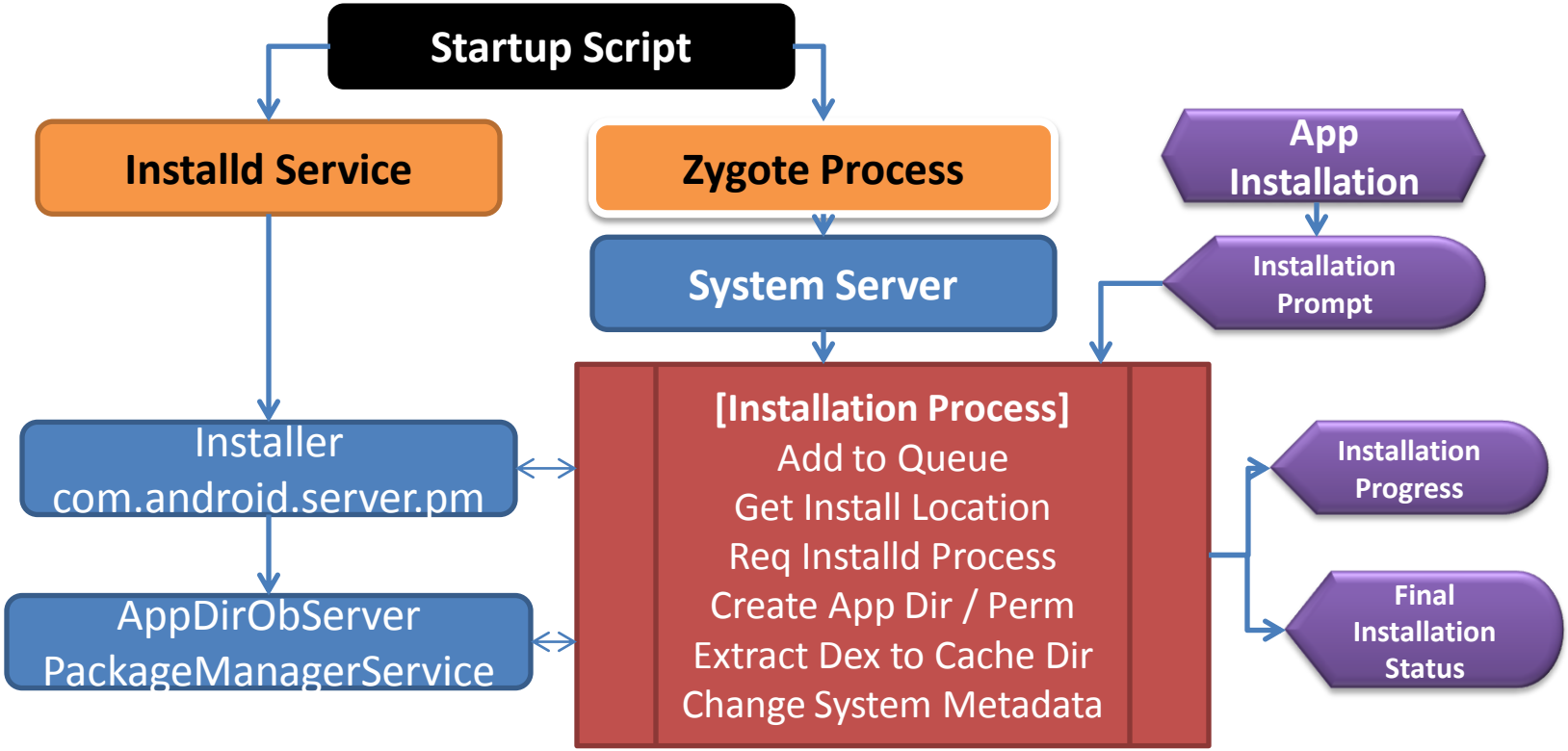
Resources

Signing Information

Dalvik Executable

Manifest – Permissions etc.

APK Primer: Verification & Installation



APK Primer: Verification & Installation

APK Verification

Hello.

APK Installation

Adios!

MasterKey Vulnerability (#8219321)

K7 COMPUTING™

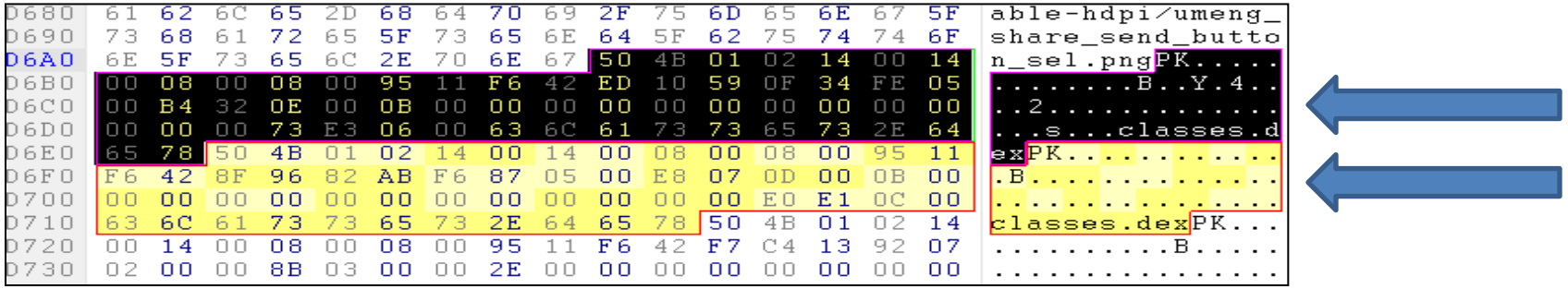
Java

Multiple classes.dex! I'll pick the last.

C++

I'll pick the first one I saw. Supposed to be only one.

It's like I've been ripped apart



Negative ExtraData (#9695860)

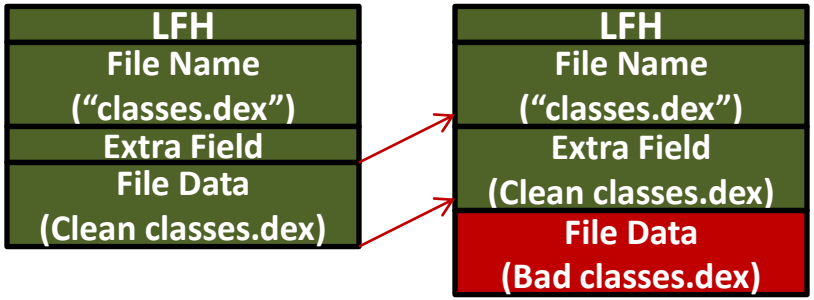
'U' Wot ?

I'll stick to the spec

Member	Value (dec)	Value (hex)
00000C41 struct LocalFileHeader	{...}	
00000C41 SIGNATURE Signature	LocalFileHead...	04034B50
00000C45 uint16 VersionNeededToEx...	20	0014
00000C47 uint16 GeneralPurposeBitFl...	2056	0808
00000C49 COMPRESSION_METHOD ...	STORED (0)	0000
00000C4B DOSDATE LastModFileTime	08:59:48 PM	A778
00000C4D DOSTIME LastModFileDate	06-07-2013	42E6
00000C4F uint32 Crc32	0	00000000
00000C53 uint32 CompressedSize	32885	00008075
00000C57 uint32 UncompressedSize	32885	00008075
00000C5B uint16 FileNameLength	11	000B
00000C5D uint16 ExtraFieldLength	65533	FFFD
00000C5F char FileName[FileNameLe...	classes.dex	
00000C6A blob ExtraField[ExtraFieldL...		

-3 (Java)

Oh no! Java just tore through my eye...



CDH LFH FileNameLen (#9950697)

Data Pos = **LFH** Pos + **CDH** FileNameLen + **LFH** ExtraDataLen

Data Pos = **LFH** Pos + **LFH** FileNameLen + **LFH** ExtraDataLen

Java just took my head off...

Member	Value (dec)	Value ...	Size
00042BD6 struct CentralDirectoryFile...	{...}		0000005D
00042BD6 SIGNATURE Signature	CentralDirect...	02014B50	00000004
00042BDA VERSION_MADE_BY Versi...	20	0014	00000002
00042BDC uint16 VersionNeededTo...	20	0014	00000002
00042BDE uint16 GeneralPurposeBit...	2056	0808	00000002
00042BE0 COMPRESSION_METHOD...	STORED (0)	0000	00000002
00042BE2 DOSDATE LastModFileTime	08:59:48 PM	A778	00000002
00042BE4 DOSTIME LastModFileDate	06-07-2013	42E6	00000002
00042BE6 uint32 Crc32	1357835533	50EEED0D	00000004
00042BEA uint32 CompressedSize	32885	00008075	00000004
00042BEE uint32 UncompressedSize	32885	00008075	00000004
00042BF2 uint16 FileNameLength	11	000B	00000002

Member	Value (dec)	Value ...	Size
00039E80 struct LocalFileHeader	{...}		0000004D
00039E80 SIGNATURE Signature	LocalFileHea...	04034B50	00000004
00039E84 uint16 VersionNeededToE...	20	0014	00000002
00039E86 uint16 GeneralPurposeBit...	2056	0808	00000002
00039E88 COMPRESSION_METHOD...	STORED (0)	0000	00000002
00039E8A DOSDATE LastModFileTi...	08:59:48 PM	A778	00000002
00039E8C DOSTIME LastModFileDate	06-07-2013	42E6	00000002
00039E8E uint32 Crc32	0	00000000	00000004
00039E92 uint32 CompressedSize	32885	00008075	00000004
00039E96 uint32 UncompressedSize	32885	00008075	00000004
00039E9A uint16 FileNameLength	65533	FFFD	00000002
00039E9C uint16 ExtraFieldLength	0	0000	00000002
00039E9E char FileName[FileNameL...	classes.dex		0000000B

APK: Compression Methods

Member	Value (dec)	Value (hex)	Size
00042BD6 struct CentralDirectoryFileHeader	{...}		0000005D
00042BD6 SIGNATURE Signature	CentralDirectory...	02014B50	00000004
00042BDA VERSION_MADE_BY VersionMadeBy	20	0014	00000002
00042BDC uint16 VersionNeededToExtract	20	0014	00000002
00042BDE uint16 GeneralPurposeBitFlag	2056	0808	00000002
00042BE0 COMPRESSION_METHOD Compressi...	STORED (0)	0000	00000002
00042BE2 DOSDATE LastModFileTime	08:59:48 PM	A778	00000002
00042BE4 DOSTIME LastModFileDate	06-07-2013	42E6	00000002

STORE

DEFLATE

Member	Value (dec)	Value (hex)	Size
00042BD6 struct CentralDirectoryFileHeader	{...}		0000005D
00042BD6 SIGNATURE Signature	CentralDirectory...	02014B50	00000004
00042BDA VERSION_MADE_BY VersionMadeBy	20	0014	00000002
00042BDC uint16 VersionNeededToExtract	20	0014	00000002
00042BDE uint16 GeneralPurposeBitFlag	2056	0808	00000002
00042BE0 COMPRESSION_METHOD Compressi...	DEFLATED (8)	0008	00000002
00042BE2 DOSDATE LastModFileTime	08:59:48 PM	A778	00000002
00042BE4 DOSTIME LastModFileDate	06-07-2013	42E6	00000002
00042BE6 uint32 Crc32	1357835533	50EEED0D	00000004

APK: Lost in Translation (C++/Java)

Android 4.4+

If Method==Stored
RawDataCopy(…)
Else
InflateAndCopy(…)

Android 4.4+

If Method==Stored
RawDataCopy(…)
Else
InflateAndCopy(…)

Android 4.3 and below

If Method==Stored
RawDataCopy(…)
Else
InflateAndCopy(…)

Android 4.3 and below

If Method==Deflate
InflateAndCopy(…)
Else
RawDataCopy(…)

I'm having the last laugh here!

AV Scanning Bypass: Crafted APK Test Results

AntiVirus
Strict Checks

Android
Relaxed Checks

File Name	Android OS <= 4.3	Android OS >= 4.4
Droidsheep_v15_Det	DROIDSHEEP	stall - SUCCESS tection - SUCCESS
Droidsheep_v15_Crafted_43.apk	Install - SUCCESS AV Detection - FAILED	Install - FAILED AV Detection - FAILED
Droidsheep_v15_Crafted_44.apk	Install - FAILED AV Detection - FAILED	Install - SUCCESS AV Detection - FAILED

AV Scanning Bypass: Structural Analysis of Original APK

Original: Droidsheep_v15_DetectCheck.apk

```
00042BC0  3E A6 5D 7A CE 01 51 47 DF DD 36 36 CF 01 51 47  >.]z..QG..66..QG
00042BD0  DF DD 36 36 CF 01 50 4B 01 02 14 00 14 00 08 08  ..66..PK........
00042BE0  08 00 78 A7 E6 42 0D ED EE 50 75 80 00 00 8C 53  ..x..B...Pu....S
00042BF0  01 00 0B 00 24 00 00 00 00 00 00 00 00 00 00 00  ....$...........
00042C00  80 9E 03 00 63 6C 61 73 73 65 73 2E 64 65 78 0A  ....classes.dex.
00042C10  00 20 00 00 00 00 00 01 00 18 00 00 BE 3E A6 5D  . ...........>.]
00042C20  7A CE 01 B2 A8 E1 DD 36 36 CF 01                 z......66..
00042C30  36 CF 01 50 4B 05 06 00 00 00 00
00042C40  0C 00 00 52 1F 04 00 00 00
```

Structures | zip structures (zip-format.hsl)

Member	Value (dec)	Value (hex)
00042BD6 struct CentralDirectoryFileHeader	{...}	
00042BD6 SIGNATURE Signature	CentralDirect...	02014B50
00042BDA VERSION_MADE_BY VersionMadeBy	20	0014
00042BDC uint16 VersionNeededToExtract	20	0014
00042BDE uint16 GeneralPurposeBitFlag	2056	0808
00042BE0 COMPRESSION_METHOD CompressionMethod	DEFLATED (8)	0008
00042BE2 DOSDATE LastModFileTime	08:59:48 PM	A778
00042BE4 DOSTIME LastModFileDate	06-07-2013	42E6
00042BE6 uint32 Crc32	1357835533	50EEED0D
00042BEA uint32 CompressedSize	32885	00008075
00042BEE uint32 UncompressedSize	86924	0001538C
00042BF2 uint16 FileNameLength	11	000B
00042BF4 uint16 ExtraFieldLength	36	0024
00042BF6 uint16 FileCommentLength	0	0000
00042BF8 uint16 DiskNumberStart	0	0000

AV Scanning Bypass: Structural Analysis of Crafted APK (Android 44+)

K7 COMPUTING™

Crafted: Droidsheep_v15_Crafted_44.apk

```
0  18 00 3D 62 A7 E3 36 36 CF 01 39 AD 15 8D 66 37  ..=b..66..9...f7
0  CF 01 39 AD 15 8D 66 37 CF 01 50 4B 01 02 14 00  ..9...f7..PK....
0  14 00 08 08 01 00 78 A7 E6 42 0D ED EE 50 75 80  ......x..B...Pu.
0  00 00 8C 53 01 00 0B 00 24 00 00 00 00 00 00 00  ...S....$.......
0  00 00 00 00 41 0C 00 00 63 6C 61 73 73 65 73 2E  ....A...classes.
0  64 65 78 0A 00 20 00 00 00 00 00 01 00 18 00 00  dex.. ..........
0  BE 3E A6 [illegible] 7A CE 01 D9 4B 13 8D 66 37 CF 01 D9  .>.jz...K..f7...
0  4B 13 8D [illegible] 37 CF 01 50 4B 01 02 14 00 1[illegible]
0  08 08 00 78 A7 E6 42 20 1C D9 F9 9C 43 0[illegible]
```

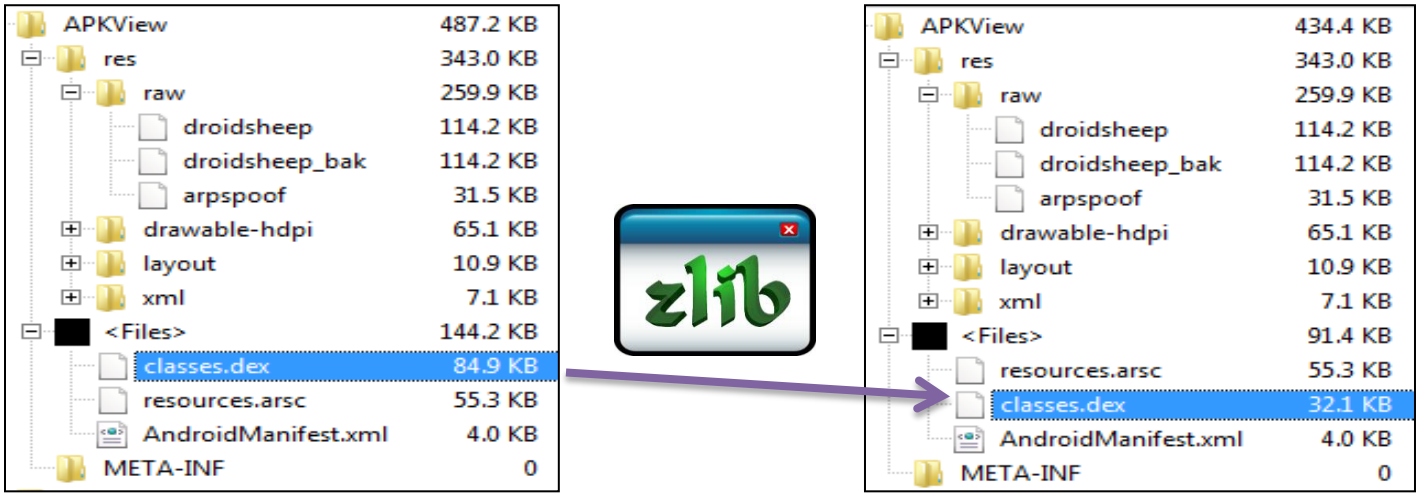
Java C/C++
If Method==Stored
RawDataCopy(…)
Else
InflateAndCopy(…)

Structures | zip structures (zip-format.hsl)

Member	Value (dec)	Value ...
0004206A struct CentralDirectoryFileHeader	{...}	
0004206A SIGNATURE Signature	CentralDirect...	02014B50
0004206E VERSION_MADE_BY VersionMadeBy	20	0014
00042070 uint16 VersionNeededToExtract	20	0014
00042072 uint16 GeneralPurposeBitFlag	2056	0808
00042074 COMPRESSION_METHOD CompressionMethod	SHRUNK (1)	0001
00042076 DOSDATE LastModFileTime	08:59:48 PM	A778
00042078 DOSTIME LastModFileDate	06-07-2013	42E6
0004207A uint32 Crc32	1357835533	50EEED0D
0004207E uint32 CompressedSize	32885	00008075
00042082 uint32 UncompressedSize	86924	0001538C
00042086 uint16 FileNameLength	11	000B
00042088 uint16 ExtraFieldLength	36	0024
0004208A uint16 FileCommentLength	0	0000
0004208C uint16 DiskNumberStart	0	0000

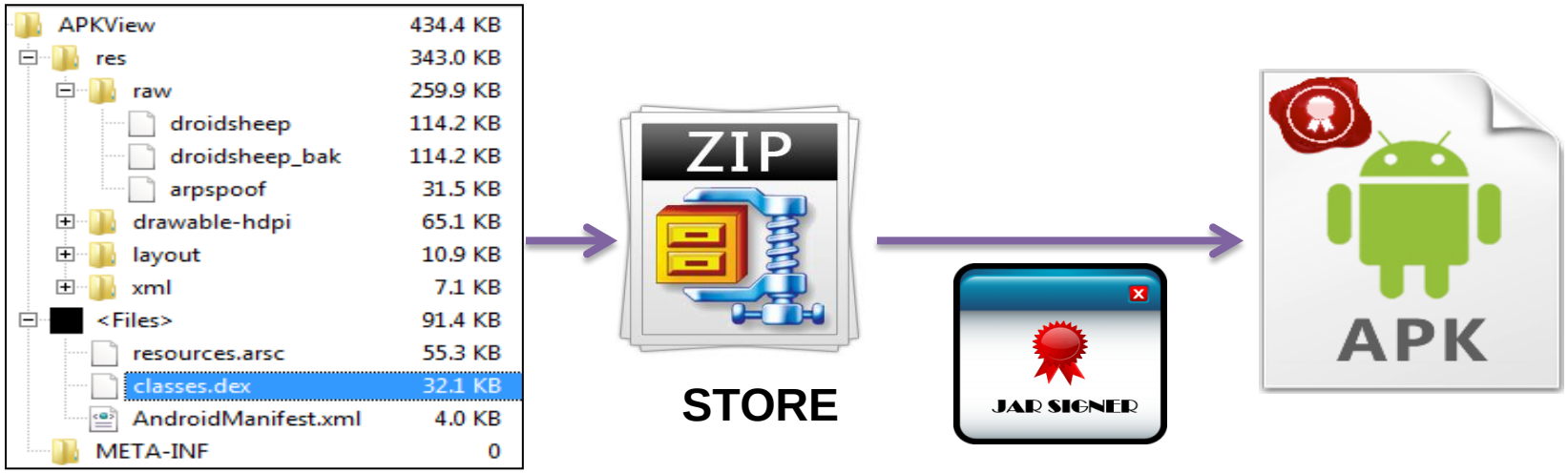
AV Scanning Bypass: Structural Analysis of Crafted APK (<=Android 4.3)

Crafted: Droidsheep_v15_Crafted_43.apk



AV Scanning Bypass: Structural Analysis of Crafted APK (<=Android 4.3)

Crafted: Droidsheep_v15_Crafted_43.apk



AV Scanning Bypass: Structural Analysis of Crafted APK (<=Android 4.3)

Crafted: Droidsheep_v15_Crafted_43.apk

Member	Value (dec)	Value (hex)
0006DB67 struct CentralDirectoryFileHeader	{...}	
0006DB67 SIGNATURE Signature	CentralDirector...	02014B50
0006DB6B VERSION_MADE_BY VersionMadeBy	31	001F
0006DB6D uint16 VersionNeededToExtract	10	000A
0006DB6F uint16 GeneralPurposeBitFlag	0	0000
0006DB71 COMPRESSION_METHOD Compressio...	STORED (0)	0000
0006DB73 DOSDATE LastModFileTime	10:24:38 PM	B313
0006DB75 DOSTIME LastModFileDate	02-03-2014	4462
0006DB77 uint32 Crc32	4232675189	FC497F75
0006DB7B uint32 CompressedSize	32885	00008075
0006DB7F uint32 UncompressedSize	32885	00008075
0006DB83 uint16 FileNameLength	11	000B
0006DB85 uint16 ExtraFieldLength	36	0024
0006DB87 uint16 FileCommentLength	0	0000
0006DB89 uint16 DiskNumberStart	0	0000
0006DB8B uint16 InternalFileAttributes	0	0000
0006DB8D uint32 ExternalFileAttributes	32	00000020
0006DB91 uint32 RelativeOffsetOfLocalHeader	413446	00064F06
0006DB95 char FileName[FileNameLength]	classes.dex	

Member	Value (dec)	Value (hex)
0006EC58 struct CentralDirectoryFileHeader	{...}	
0006EC58 SIGNATURE Signature	CentralDirect...	02014B50
0006EC5C VERSION_MADE_BY VersionMadeBy	31	001F
0006EC5E uint16 VersionNeededToExtract	10	000A
0006EC60 uint16 GeneralPurposeBitFlag	2048	0800
0006EC62 COMPRESSION_METHOD Compression...	SHRUNK (1)	0001
0006EC64 DOSDATE LastModFileTime	10:24:38 PM	B313
0006EC66 DOSTIME LastModFileDate	02-03-2014	4462
0006EC68 uint32 Crc32	4232675189	FC497F75
0006EC6C uint32 CompressedSize	32885	00008075
0006EC70 uint32 UncompressedSize	86924	0001538C
0006EC74 uint16 FileNameLength	11	000B
0006EC76 uint16 ExtraFieldLength	36	0024
0006EC78 uint16 FileCommentLength	0	0000
0006EC7A uint16 DiskNumberStart	0	0000
0006EC7C uint16 InternalFileAttributes	0	0000
0006EC7E uint32 ExternalFileAttributes	0	00000000
0006EC82 uint32 RelativeOffsetOfLocalHeader	417554	00065F12
0006EC86 char FileName[FileNameLength]	classes.dex	

Java
If Method==Deflate
InflateAndCopy(…)
Else
RawDataCopy(…)

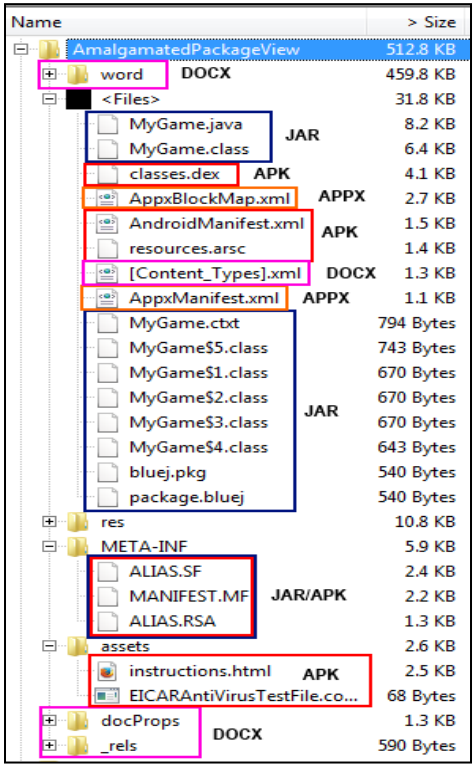
C/C++
If Method==Stored
RawDataCopy(…)
Else
InflateAndCopy(…)

AV Scanning Bypass - Mitigation

- **Suggested Fix (For Android OS Developers)**
  - Android OS can place a more strict check on the compression method fields. (Issue #69184)
- **Suggested Fix (For Antivirus Vendors)**
  - Heuristically flag files with unsupported compression method
  - Extract files based on Android OS assumptions

Chameleon ZIP

Format	FileNames
JAR	META-INF/MANIFEST.MF META-INF/*.SF META-INF/*RSA *.class
APK	META-INF/MANIFEST.MF META-INF/*.SF META-INF/*RSA AndroidManifest.xml classes.dex
DOCX	[Content_Types].xml Word docProps _rels
APPX	AppxManifest.xml AppxBlockMap.xml



Chameleon ZIP

Format/Extension	Application	Status
APK	Android OS	Success
JAR	Java Runtime	Success
DOCX	OpenOffice	Success
DOCX	Microsoft Word	Failed
APPX	Windows 8	Failed

Zipping it Up

- ZIP Format – flexible & versatile. Continuing format abuse expected.
- Crafted APK – Antivirus products (Windows & Android) affected equally.
  - IEEE Taggant for APKs – Actively discussed
- Chameleon ZIP – Possible effect on automation systems not evaluated.

K7 COMPUTING™

Thank You!