Annex 1: Technical Appendix

Table of contents

A. CONFIGURATION OPTIONS

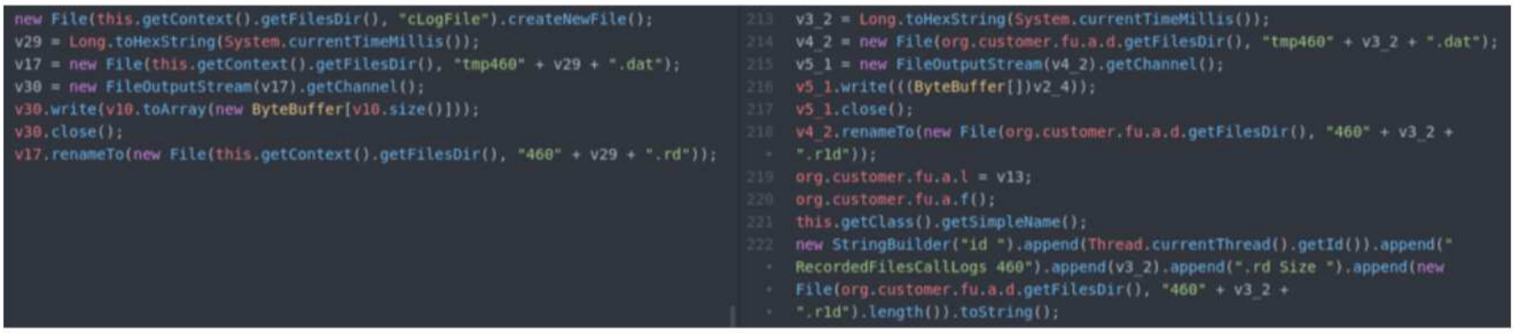
Forensic comparisons of a version of FinSpy that became public in the year 2014 with the A-Malware show that the source code of the two pieces of malware are practically identical, so that they are definitely different versions of the same malware, cf. Malware A in Annex 1 and FinSpy 2014 in Annex 2. For example, the configuration options of the A-Malware and of the version of FinSpy that became public in 2014 are almost the same,

> Annex 2: FinSpy Malware of August 2014; for a detailed overview of the functions of FinSpy see https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/.; https://www.symantec.com/security-center/writeup/2012-072615-4146-99?tabid=2; both last accessed 4 July 2019.

This refers to those parts of the source code that have a determining influence on how the malware works precisely, for example which pieces of information about the user of the end-user device are captured.

It is easy to reconstruct that the A-Malware from Annex 1 is exactly the malware with which opposition politicians were attacked on the Turkish Adalet website in the year 2017. To do so, one must merely compare the file enclosed with this criminal complaint with the file available on the Adalet website archived by archive.org. In the process, it becomes apparent that both files have the same cryptographic checksum (hash). This type of checksum is a distinct digital fingerprint of a file; in other words, if two checksums match, as they do here, then it is the same file.

Yet the A-Malware is not only practically identical to the FinSpy sample published by researchers in August 2014. The A-Malware also shares more than 90% of its source code with a newer version from July 2015. Apart from cosmetic differences – namely changes intended to conceal the manufacturer – the A-Malware uses the same code as earlier FinSpy samples. For example, the code used to record telephone calls is practically identical, even down to using the same pattern for the file names of the recorded data (‘tmp460’ + time stamp in milliseconds + ‘.dat’). It is purely a theoretical possibility, and can be ruled out, that two surveillance programmes developed independently of one another would purely coincidentally use exactly the same naming convention.



```java
new File(this.getContext().getFilesDir(), "cLogFile").createNewFile();
v29 = Long.toHexString(System.currentTimeMillis());
v17 = new File(this.getContext().getFilesDir(), "tmp460" + v29 + ".dat");
v30 = new FileOutputStream(v17).getChannel();
v30.write(v10.toArray(new ByteBuffer[v10.size()]));
v30.close();
v17.renameTo(new File(this.getContext().getFilesDir(), "460" + v29 + ".rd"));
```

```java
v3_2 = Long.toHexString(System.currentTimeMillis());
v4_2 = new File(org.customer.fu.a.d.getFilesDir(), "tmp460" + v3_2 + ".dat");
v5_1 = new FileOutputStream(v4_2).getChannel();
v5_1.write(((ByteBuffer[])v2_4));
v5_1.close();
v4_2.renameTo(new File(org.customer.fu.a.d.getFilesDir(), "460" + v3_2 +
".rld"));
org.customer.fu.a.l = v13;
org.customer.fu.a.f();
this.getClass().getSimpleName();
new StringBuilder("id ").append(Thread.currentThread().getId()).append("
RecordedFilesCallLogs 460").append(v3_2).append(".rd Size ").append(new
File(org.customer.fu.a.d.getFilesDir(), "460" + v3_2 +
".rld").length()).toString();
```

Left: Code of the FinSpy malware from the year 2014; Right: Code of the A-Malware

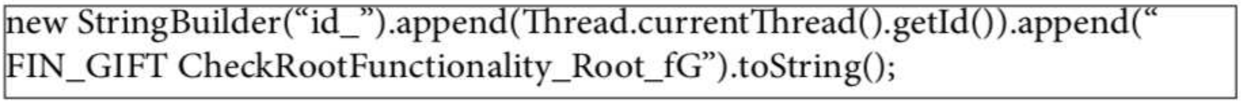
B. REFERENCES IN THE TEXT

Various German words are to be found in the code of the A-Malware, mainly in the preferences files with the name ‘einstellung.xml’.

Appendix 1: Sample of the A-Malware; Access Now Report, p. 9.

This speaks for development by a German manufacturer, and in any case, against Turkish authorities developing it themselves.

In addition, there are references embedded deep in the code that refer to the original name of the A-Malware, for example the text ‘FIN_GIFT’.



```
new StringBuilder(“id_”).append(Thread.currentThread().getId()).append(“
FIN_GIFT CheckRootFunctionality_Root_fG”).toString();
```

Extract from the A-Malware code including ‘FIN_GIFT’.

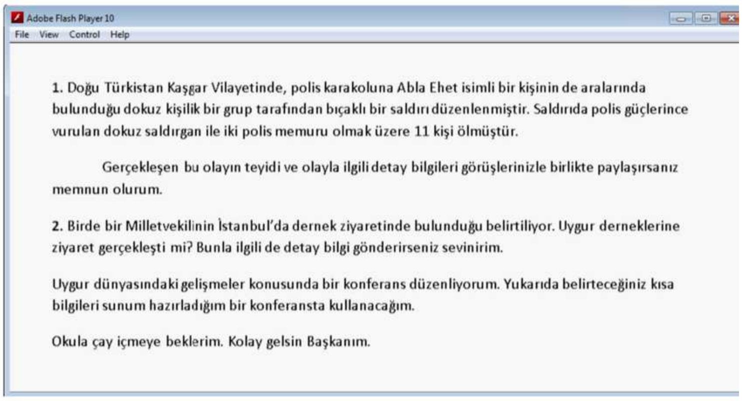
Taken together, both pieces of evidence refer unequivocally to FinFisher, a manufacturer headquartered in Germany.

C. MICROSOFT SECURITY REPORT

Additional indications of the fact that Turkey purchased FinSpy arise from the Microsoft Security Intelligence Report for January through June 2016 (Volume 21).

In December 2016, Microsoft reported the emergence of a zero-day exploit, that is, an exploitation of a security vulnerability in the Windows operating system that is unknown to the manufacturer. Attackers used Adobe Flash Player to compromise the Windows security architecture. This security vulnerability was exploited to install malware that Microsoft identified as FinSpy. Here, Microsoft used its own naming scheme, calling FinFisher ‘Neomydium’ and FinSpy ‘Wingbird’.

In addition, Microsoft declared that dozens of victims were affected by the security vulnerability; the overwhelming majority of them were in Turkey. Microsoft also concluded that Turkey had been selected as the primary target of the attack from the fact that the malware was disseminated as spear-phishing through websites and Tweets in Turkish.



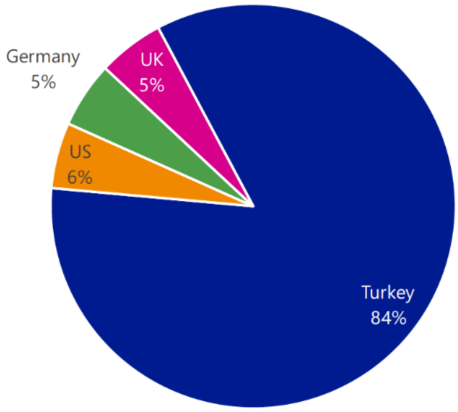
1. Doğu Türkistan Kaşgar Vilayetinde, polis karakoluna Abla Ehet isimli bir kişinin de aralarında bulunduğu dokuz kişilik bir grup tarafından bıçaklı bir saldırı düzenlenmiştir. Saldırıda polis güçlerince vurulan dokuz saldırgan ile iki polis memuru olmak üzere 11 kişi ölmüştür.

Gerçekleşen bu olayın teyidi ve olayla ilgili detay bilgileri görüşlerinizle birlikte paylaşırsanız memnun olurum.

2. Birde bir Milletvekilinin İstanbul'da dernek ziyaretinde bulunduğu belirtiliyor. Uygur derneklerine ziyaret gerçekleşti mi? Bunla ilgili de detay bilgi gönderirseniz sevinirim.

Uygur dünyasındaki gelişmeler konusunda bir konferans düzenliyorum. Yukarıda belirteceğiniz kısa bilgileri sunum hazırladığım bir konferansta kullanacağım.

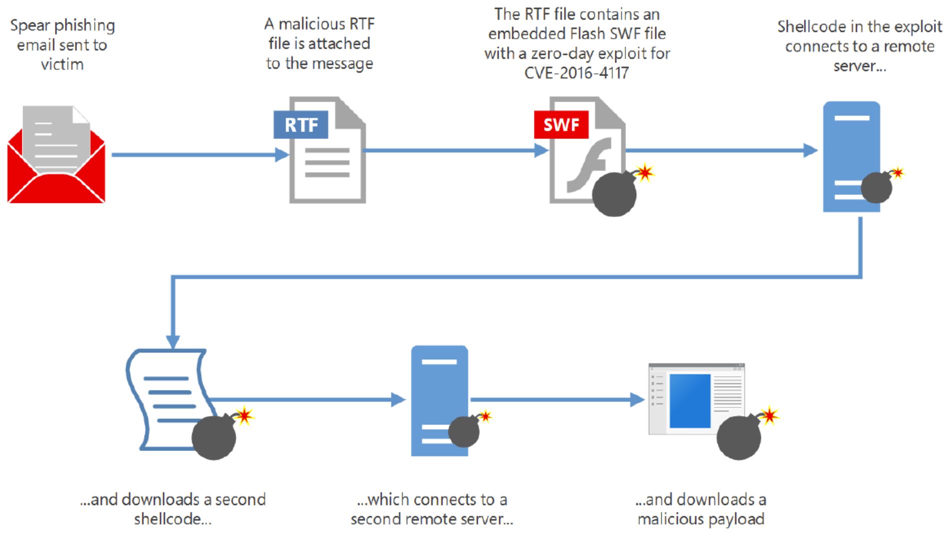
Okula çay içmeye beklerim. Kolay gelsin Başkanım.



Left: The Turkish-language spear-phishing message with which FinSpy was disseminated in Turkey, according to Microsoft. Right: FinSpy victims by country, according to Microsoft

Furthermore, the Microsoft results confirm the forensic software analysis presented under 1. and 2. The behaviour of the version of FinSpy identified by Microsoft and that of the A-Malware, including the use of the same domain service provider, are so similar that they could be mistaken for one another.

Microsoft Security Intelligence Report, Volume 21, January through June, 2016, pp. 22 ff.; Access Now Report, p. 10.


Spear phishing email sent to victim
A malicious RTF file is attached to the message
RTF
The RTF file contains an embedded Flash SWF file with a zero-day exploit for CVE-2016-4117
SWF
Shellcode in the exploit connects to a remote server...
...and downloads a second shellcode...
...which connects to a second remote server...
...and downloads a malicious payload

Representation of the functionality of the FinSpy version identified by Microsoft.

D. ADDITIONAL FINSPY MALWARE IN TURKEY

The version of FinSpy called A-Malware here was, however, not the only one used in Turkey. On the contrary: on 21 July 2017, a file hereinafter called B-Malware was uploaded to the website ‘VirusTotal’, an Internet service for identifying and archiving malware. It is available to this day at the following link:

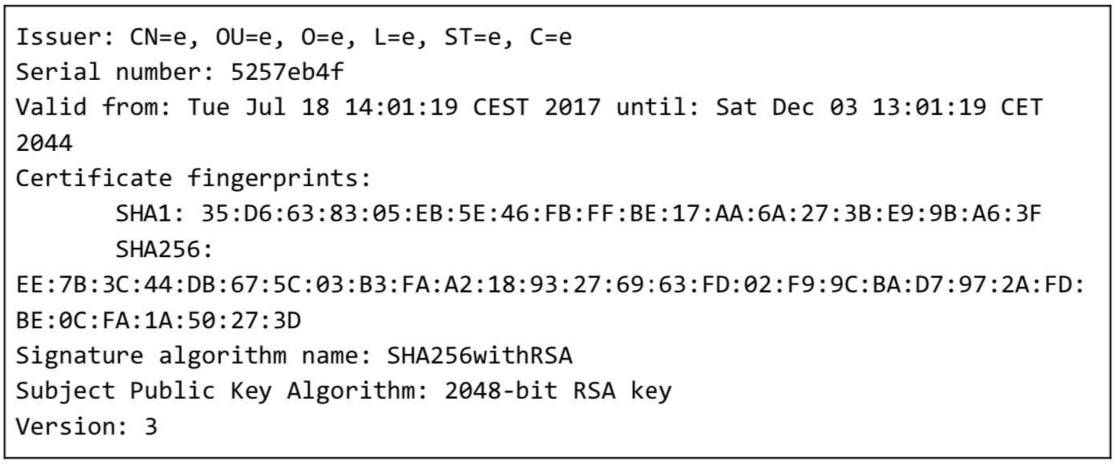
> https://www.virustotal.com/gui/file/23f154723213452634abe6063fd07bd3a38700a6b0ba4117db3224ae1411dada/detection; last accessed 4 July 2019.

The file can be clearly identified using the SHA-256-hash ‘23f154723213452634 abe6063fd07bd3a38700a6b0ba4117db3224ae1411dada’.

It was identified by VirusTotal as ‘FinSpy’ or ‘Belesak’. The latter is an alternative name for FinSpy commonly used by antivirus experts. Since the B-Malware uses the same character strings internally as the A-Malware, it must be part of the same malware family. For example, both identify a programme component as org.customer.fu.S5tartVers10n and also use the package name org.tech.fu. Hence, it appears highly likely that the B-Malware was also manufactured by FinFisher.

The mechanisms for identifying viruses used by VirusTotal are highly reliable. VirusTotal, which is offered by Google, uses ‘Yara binary identification’, a recognised industry standard. It searches for and compares certain characteristic features in the executable file – for example character strings. So if VirusTotal identifies the uploaded file as FinSpy, then, as it is the industry standard, that must be assumed to be true. It can also be deduced from the B-Malware that the Turkish FinFisher customers had access to FinSpy until July 2017, in other words, that FinFisher exported its own malware up to that time.

The digital signature of the B-Malware evidences that the file was signed only on 18 July 2017. The following sections will show that since the signature is attached by the manufacturer, who is based in Munich, it is impossible for the software to have been exported prior to this date.



```
Issuer: CN=e, OU=e, O=e, L=e, ST=e, C=e
Serial number: 5257eb4f
Valid from: Tue Jul 18 14:01:19 CEST 2017 until: Sat Dec 03 13:01:19 CET
2044
Certificate fingerprints:
       SHA1: 35:D6:63:83:05:EB:5E:46:FB:FF:BE:17:AA:6A:27:3B:E9:9B:A6:3F
       SHA256:
EE:7B:3C:44:DB:67:5C:03:B3:FA:A2:18:93:27:69:63:FD:02:F9:9C:BA:D7:97:2A:FD:
BE:0C:FA:1A:50:27:3D
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

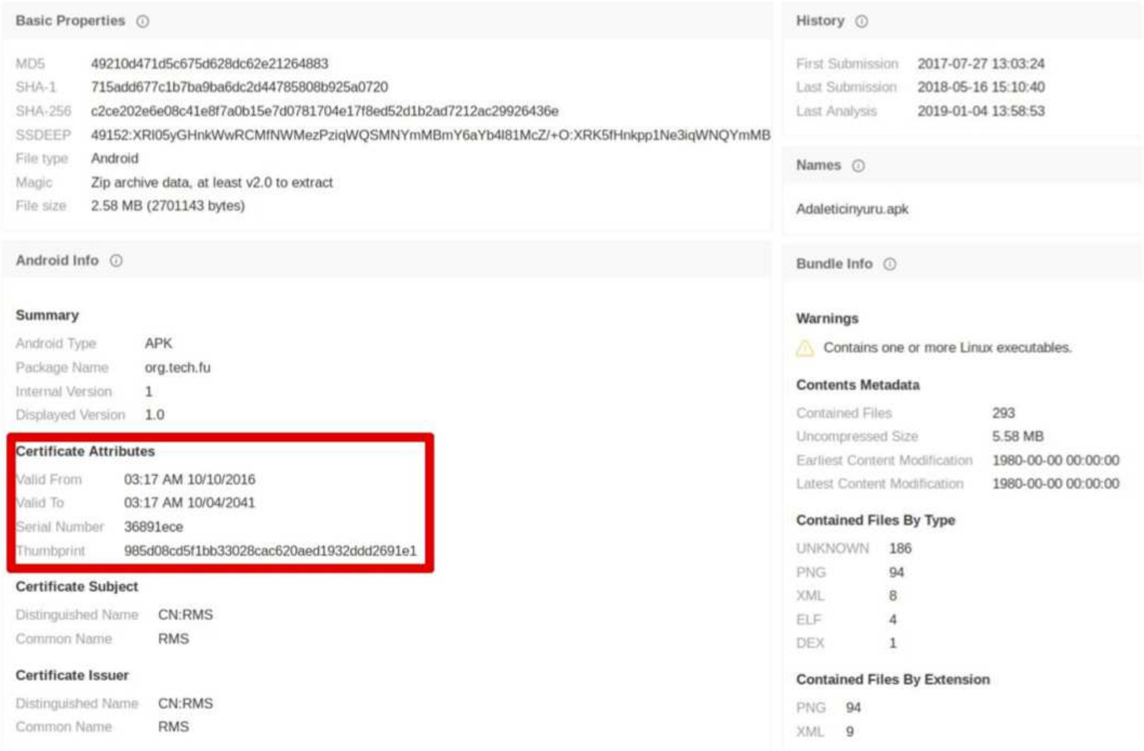
In this digital signature of the B-Malware, the creation date of the signature in the third line is given as 18 July 2017. All the analytical steps can be followed employing an analysis of the B-Malware attached to this criminal complaint,

Annex 3: B-Malware of 21 July 2017.

E. FINSPY SAMPLE IN LIBYA

The comparison of two FinSpy versions digitally signed with the same certificate proves that these digital signatures were actually attached by the manufacturer.

First, an analysis of the metadata and the software characteristics of the malware uploaded to the VirusTotal website from Libya evidences that it too must be FinSpy. For the Libyan malware was signed with the same cryptographic key and the same certificate as the A-Malware.



Basic Properties

MD5	49210d471d5c675d628dc62e21264883
SHA-1	715add677c1b7ba9ba6dc2d44785808b925a0720
SHA-256	c2ce202e6e08c41e8f7a0b15e7d0781704e17f8ed52d1b2ad7212ac29926436e
SSDEEP	49152:XRI05yGHnkWwRCMfNWMezPziqWQSMNYmMBmY6aYb4I81McZ/+O:XRK5fHnkpp1Ne3iqWNQYmMB
File type	Android
Magic	Zip archive data, at least v2.0 to extract
File size	2.58 MB (2701143 bytes)

History

First Submission	2017-07-27 13:03:24
Last Submission	2018-05-16 15:10:40
Last Analysis	2019-01-04 13:58:53

Names

Adaleticinyuru.apk

Android Info

Summary

Android Type	APK
Package Name	org.tech.fu
Internal Version	1
Displayed Version	1.0

Certificate Attributes

Valid From	03:17 AM 10/10/2016
Valid To	03:17 AM 10/04/2041
Serial Number	36891ece
Thumbprint	985d08cd5f1bb33028cac620aed1932ddd2691e1

Certificate Subject

Distinguished Name	CN:RMS
Common Name	RMS

Certificate Issuer

Distinguished Name	CN:RMS
Common Name	RMS

Bundle Info

Warnings

⚠ Contains one or more Linux executables.

Contents Metadata

Contained Files	293
Uncompressed Size	5.58 MB
Earliest Content Modification	1980-00-00 00:00:00
Latest Content Modification	1980-00-00 00:00:00

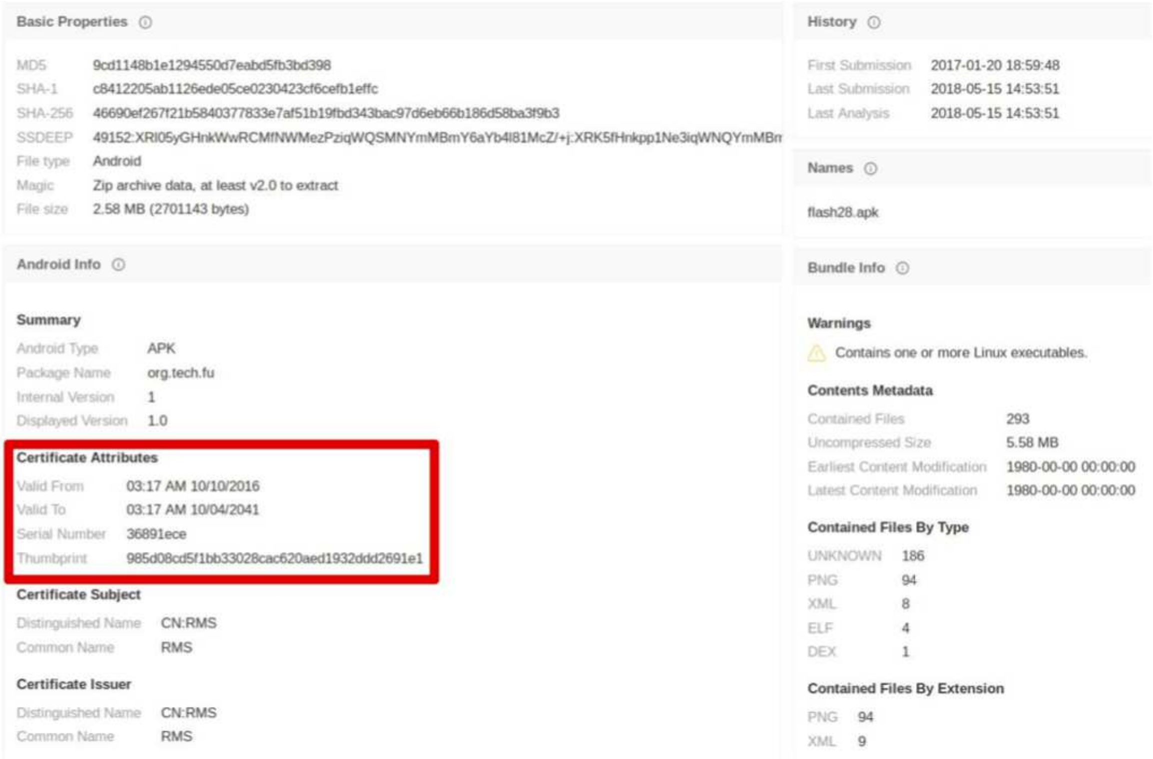
Contained Files By Type

UNKNOWN	186
PNG	94
XML	8
ELF	4
DEX	1

Contained Files By Extension

PNG	94
XML	9

Metadata of the A-Malware



Basic Properties

MD5	9cd1148b1e1294550d7eabd5fb3bd398
SHA-1	c8412205ab1126ede05ce0230423cf6cefb1effc
SHA-256	46690ef267f21b5840377833e7af51b19fbd343bac97d6eb66b186d58ba3f9b3
SSDEEP	49152:XRI05yGHnkWwRCMfNWMezPziqWQSMNYmMBmY6aYb4I81McZ/+j:XRK5fHnkpp1Ne3iqWNQYmMBm
File type	Android
Magic	Zip archive data, at least v2.0 to extract
File size	2.58 MB (2701143 bytes)

History

First Submission	2017-01-20 18:59:48
Last Submission	2018-05-15 14:53:51
Last Analysis	2018-05-15 14:53:51

Names

flash28.apk

Android Info

Summary

Android Type	APK
Package Name	org.tech.fu
Internal Version	1
Displayed Version	1.0

Certificate Attributes

Valid From	03:17 AM 10/10/2016
Valid To	03:17 AM 10/04/2041
Serial Number	36891ece
Thumbprint	985d08cd5f1bb33028cac620aed1932ddd2691e1

Certificate Subject

Distinguished Name	CN:RMS
Common Name	RMS

Certificate Issuer

Distinguished Name	CN:RMS
Common Name	RMS

Bundle Info

Warnings

⚠ Contains one or more Linux executables.

Contents Metadata

Contained Files	293
Uncompressed Size	5.58 MB
Earliest Content Modification	1980-00-00 00:00:00
Latest Content Modification	1980-00-00 00:00:00

Contained Files By Type

UNKNOWN	186
PNG	94
XML	8
ELF	4
DEX	1

Contained Files By Extension

PNG	94
XML	9

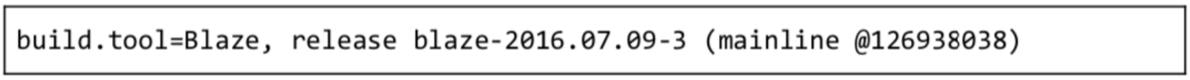
Metadata of the Libyan malware It is clear: the metadata are identical.

The two files share the same certificate, the same creation date, and the same serial number. The use of the same certificate to sign software that is to communicate with two different command servers and that was used in two different countries provides evidence for the fact that these keys were used by the original developers – i.e., FinFisher – and that they were not signed digitally by the end customers or operators.

F. TIME OF EXPORT

The forensic analysis of the A-Malware also shows that it must have been exported after 1 January 2015. The European Dual-Use Regulation has required companies to obtain a licence when selling surveillance technology outside of the EU since that date. Various characteristics of the A-Malware ‘Adaleticinyuru.apk’ refer to September and October 2016 as the creation dates.

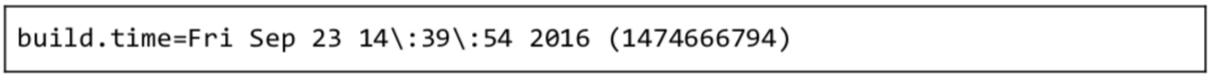
The first piece of evidence is in the file ‘build-data.properties’, which can be reviewed by simply unpacking the original APK file (which is basically just a zip archive). This file contains metadata for creating a library named ‘GMSCore’, which is part of the A-Malware. It emerges from these metadata that the ‘Blaze’ system was used to create ‘GMSCore’. The version of the ‘Blaze’ system used was published only on 9 July 2016:



```
build.tool=Blaze, release blaze-2016.07.09-3 (mainline @126938038)
```

For this reason, the ‘GSMCore’ component of the A-Malware cannot have been created before this day, and thus, this is also true of the A-Malware itself.

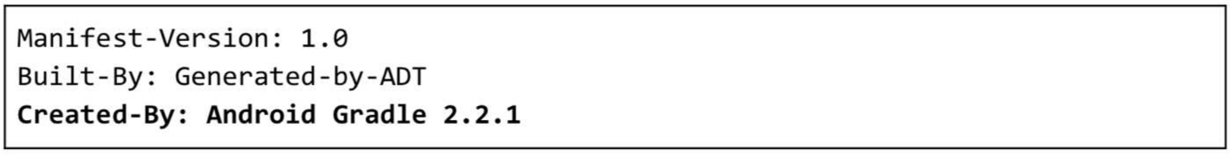
Secondly, these data include the date on which the version of ‘GSMCore’ in the A-Malware was created, namely 23 September 2016:



```
build.time=Fri Sep 23 14\:39\:54 2016 (1474666794)
```

Since ‘GMSCore’ is an integral functional component of the malware, it follows that the FinSpy version of the A-Malware cannot have been created and thus cannot have been exported before 23 September 2016.

The same also results from another file. There is a reference in the file component ‘META-INF/MANIFEST.MF’ to the ‘Android Gradle Version 2.2.1.’ software. Android Gradle is one of the software tools used by programmers when developing Android programmes. However, Android Gradle version 2.2.1 was published only in September 2016.



```
Manifest-Version: 1.0
Built-By: Generated-by-ADT
Created-By: Android Gradle 2.2.1
```

https://developer.android.com/studio/releases/gradle-plugin; last accessed 5 May 2019.

Creating and exporting a piece of software that refers to Android Gradle version 2.2.1 – as is true of the A-Malware – was, naturally, not possible before publication of that version.

In addition, the file component ‘AndroidManifest.xml’ contains the following metadata:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
android:versionCode="1" android:versionName="1.0" package="org.tech.fu"
platformBuildVersionCode="24" platformBuildVersionName="7">
```

This shows that the A-Malware was coded using version 24 of the Android development system. Version 24 refers to Android 7.0 ‘Nougat’, which was also published only in September 2016.

In addition, according to the information included in the digital signature of the A-Malware, the digital signature was created only on 10 October 2016:

```
Owner: CN=RMS
Issuer: CN=RMS
Serial number: 36891ece
Valid from: Mon Oct 10 05:17:01 CEST 2016 until: Fri Oct 04 05:17:01 CEST
2041
Certificate fingerprints:
       SHA1: 98:5D:08:CD:5F:1B:B3:30:28:CA:C6:20:AE:D1:93:2D:DD:26:91:E1
       SHA256:
1E:62:1A:88:3B:CD:9D:1B:D6:D5:61:11:C4:88:EE:10:D4:67:1D:2C:A6:64:F7:27:FE:
72:59:47:8A:68:79:67
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

All of the above-mentioned elements point to the fact that the A-Malware cannot have been created before September or October 2016, and thus cannot have been exported before this point in time.