Update on the Fancy Bear Android malware (poprd30.apk)

blog.crysys.hu/2017/03/update-on-the-fancy-bear-android-malware-poprd30-apk/

By Boldizsar Bencsath March 2, 2017

About the APK:

The APK file, that was investigated by Crowd Strike and us is actually corrupt, unzipping yields two warnings and a CRC Error.

$ unzip 6f7523d3019fa190499f327211e01fcb.apk
Archive: 6f7523d3019fa190499f327211e01fcb.apk
warning [6f7523d3019fa190499f327211e01fcb.apk]: 1 extra byte at beginning or within zipfile
(attempting to process anyway)
file #1: bad zipfile offset (local header sig): 1
(attempting to re-compensate)
inflating: META-INF/MANIFEST.MF
inflating: META-INF/CERT.SF
inflating: META-INF/CERT.RSA
inflating: AndroidManifest.xml
inflating: classes.dex
extracting: res/drawable-hdpi/dmk.png
extracting: res/drawable-hdpi/ic_launcher.png
extracting: res/drawable-mdpi/fon_1.jpg
extracting: res/drawable-mdpi/fon_2.png
extracting: res/drawable-mdpi/fon_3.png
extracting: res/drawable-mdpi/ic_action_search.png
extracting: res/drawable-mdpi/ic_launcher.png
extracting: res/drawable-mdpi/panel_2.gif
extracting: res/drawable-mdpi/panel_4.png
extracting: res/drawable-mdpi/panel_5.png
extracting: res/drawable-mdpi/panel_6.png
extracting: res/drawable-mdpi/panel_7.png
extracting: res/drawable-mdpi/warnings.png bad CRC 73cded37 (should be 902e9cdb)
file #19: bad zipfile offset (local header sig): 660433
(attempting to re-compensate)
extracting: res/drawable-xhdpi/ic_launcher.png
extracting: res/drawable-xxhdpi/ic_launcher.png
inflating: res/layout/activity_reg_form.xml
inflating: res/layout/byleten.xml
inflating: res/layout/dan_dmk.xml

inflating: res/layout/dan_meteo.xml
inflating: res/layout/dan_vr_2.xml
inflating: res/layout/meteo_podg_form.xml
inflating: res/layout/o_avtope_form.xml
inflating: res/layout/pomow_form.xml
inflating: res/layout/promt.xml
extracting: resources.arsc

In this form, it is not possible to install the APK, trying so results in the phone yielding the following error message:
$ adb install 6f7523d3019fa190499f327211e01fcb.apk
Failed to install 6f7523d3019fa190499f327211e01fcb.apk: Failure [INSTALL_PARSE_FAILED_UNEXPECTED_EXCEPTION: Failed to parse /data/app/vmdl135131206.tmp/base.apk: AndroidManifest.xml]

From the error messages we suspected, that an extra byte somehow ended up in the APK file.
The repair process consisted of finding and removing an extra byte from the file “warnings.png”. By changing only this byte and getting a valid APK file, this might be the original file. After repair, we got the following file.
$ sha256sum REPAIRED.apk
5b6ea28333399a73475027328812fb42259c12bb24b6650e5def94f4104f385e REPAIRED.apk

$ unzip -vt REPAIRED.apk
Archive: REPAIRED.apk
testing: META-INF/MANIFEST.MF OK
testing: META-INF/CERT.SF OK
testing: META-INF/CERT.RSA OK
testing: AndroidManifest.xml OK
testing: classes.dex OK
testing: res/drawable-hdpi/dmk.png OK
testing: res/drawable-hdpi/ic_launcher.png OK
testing: res/drawable-mdpi/fon_1.jpg OK
testing: res/drawable-mdpi/fon_2.png OK
testing: res/drawable-mdpi/fon_3.png OK
testing: res/drawable-mdpi/ic_action_search.png OK
testing: res/drawable-mdpi/ic_launcher.png OK
testing: res/drawable-mdpi/panel_2.gif OK
testing: res/drawable-mdpi/panel_4.png OK
testing: res/drawable-mdpi/panel_5.png OK
testing: res/drawable-mdpi/panel_6.png OK
testing: res/drawable-mdpi/panel_7.png OK

testing: res/drawable-mdpi/warnings.png OK
testing: res/drawable-xhdpi/ic_launcher.png OK
testing: res/drawable-xxhdpi/ic_launcher.png OK
testing: res/layout/activity_reg_form.xml OK
testing: res/layout/byleten.xml OK
testing: res/layout/dan_dmk.xml OK
testing: res/layout/dan_meteo.xml OK
testing: res/layout/dan_vr_2.xml OK
testing: res/layout/meteo_podg_form.xml OK
testing: res/layout/o_avtope_form.xml OK
testing: res/layout/pomow_form.xml OK
testing: res/layout/promt.xml OK
testing: resources.arsc OK
No errors detected in compressed data of REPAIRED.apk.

$ jarsigner -verbose -verify REPAIRED.apk

s 2215 Thu Feb 28 18:33:46 CET 2008 META-INF/MANIFEST.MF
2268 Thu Feb 28 18:33:46 CET 2008 META-INF/CERT.SF
1714 Thu Feb 28 18:33:46 CET 2008 META-INF/CERT.RSA
sm 6108 Thu Feb 28 18:33:46 CET 2008 AndroidManifest.xml
sm 543000 Thu Feb 28 18:33:46 CET 2008 classes.dex
sm 7047 Thu Feb 28 18:33:46 CET 2008 res/drawable-hdpi/dmk.png
sm 1703 Thu Feb 28 18:33:46 CET 2008 res/drawable-hdpi/ic_launcher.png
sm 68364 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/fon_1.jpg
sm 153893 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/fon_2.png
sm 182654 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/fon_3.png
sm 311 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/ic_action_search.png
sm 1853 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/ic_launcher.png
sm 2241 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/panel_2.gif
sm 4420 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/panel_4.png
sm 450 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/panel_5.png
sm 1448 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/panel_6.png
sm 551 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/panel_7.png
sm 25089 Thu Feb 28 18:33:46 CET 2008 res/drawable-mdpi/warnings.png
sm 2545 Thu Feb 28 18:33:46 CET 2008 res/drawable-xhdpi/ic_launcher.png
sm 4845 Thu Feb 28 18:33:46 CET 2008 res/drawable-xxhdpi/ic_launcher.png
sm 4356 Thu Feb 28 18:33:46 CET 2008 res/layout/activity_reg_form.xml
sm 20332 Thu Feb 28 18:33:46 CET 2008 res/layout/byleten.xml
sm 10584 Thu Feb 28 18:33:46 CET 2008 res/layout/dan_dmk.xml
sm 20852 Thu Feb 28 18:33:46 CET 2008 res/layout/dan_meteo.xml
sm 10208 Thu Feb 28 18:33:46 CET 2008 res/layout/dan_vr_2.xml
sm 2772 Thu Feb 28 18:33:46 CET 2008 res/layout/meteo_podg_form.xml

sm 2076 Thu Feb 28 18:33:46 CET 2008 res/layout/o_avtope_form.xml
sm 2944 Thu Feb 28 18:33:46 CET 2008 res/layout/pomow_form.xml
sm 952 Thu Feb 28 18:33:46 CET 2008 res/layout/promt.xml
sm 13296 Thu Feb 28 18:33:46 CET 2008 resources.arsc

s = signature was verified
m = entry is listed in manifest
k = at least one certificate was found in keystore
i = at least one certificate was found in identity scope

> Signed by “EMAILADDRESS=android@android.com, CN=Android, OU=Android, O=Android, L=Mountain View, ST=California, C=US”
> Digest algorithm: SHA1
> Signature algorithm: SHA1withRSA, 2048-bit key

jar verified.

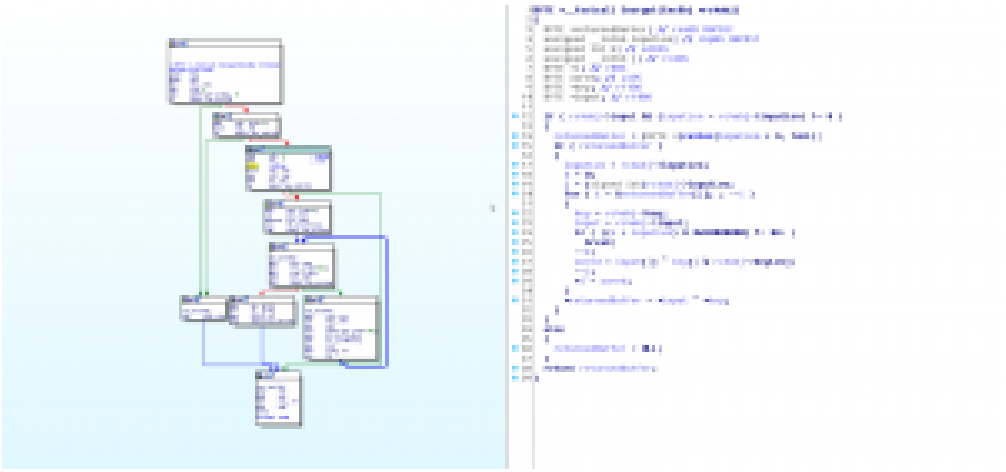
Warning:
This jar contains entries whose certificate chain is not validated.
This jar contains signatures that does not include a timestamp. Without a timestamp, users may not be able to validate this jar after the signer certificate’s expiration date (2035-07-17) or after any future revocation date.

Re-run with the -verbose and -certs options for more details.

About the RC4/encryption key:

By decompiling and manually “refactoring” the encryption algorithm, we discovered a “textbook” RC4 implementation as the encryption routine, which uses the hard-coded key as a first-part to the encryption key, with the second-part coming as a parameter from the function call:

Analyzing the XAgent linux sample, which also contained this RC4 key, we did not found an RC4 implementation, but a simple XOR based encryption routine:



We found one function call, which used the encryption key from the APK as input, but surprisingly, it was not used as key parameter, but input parameter.

For checking HTTP GET and POST messages a different XOR based check routine can be found, and a Base64-like encoding. After decoding, the XOR based routine checks the http result's body. It xors the 4-11 bytes with the first 4 bytes as a key. It then should be equal to a hardcoded value (7 bytes) which the sample uses to check whether the recv succeeded or not.

```
length = 0;
v4 = (void *)operator new(0x18u);
constructor_a((int)v4);
ct = decode((int)v4, a2, a3, (int)&length);
if ( v4 )
{
  destructor_a((int)v4);
  operator delete(v4);
}
unionEax.i = 0;
if ( ct && length > 3 )
{
  do
    ct[unionEax.i++ + 4] ^= ct[unionEax.i & 3];
  while ( unionEax.i != 11 );
  v7 = memcmp(checkValue, ct + 4, 7u);
  unionEax.pt = 0;
  if ( !v7 )
  {
    ptLen = length - 11;
    *outLen = length - 11;
    v10 = ptLen;
    unionEax.pt = calloc(ptLen, 1u);
    if ( unionEax.pt )
    {
      qmemcpy(unionEax.pt, ct + 11, v10);
      tmp = unionEax.pt;
      free(ct);
      unionEax.pt = tmp;
    }
  }
}
return unionEax.pt;
}
```

These XAgent linux samples are very similar to a Windows version that has been found in november, 2013 (5f6b2a0d1d966fc4f1ed292b46240767f4acb06c13512b0061b434ae2a692fa1).

Recommended yara for the linux versions:

```
rule sofacy_xagent {
meta:
author = "AKG"
description = "Sofacy - XAgent"
strings:
$service = "ksysdefd"
$x1 = "AgentKernel"
$x2 = "Cryptor"
$x3 = "AgentModule"
$x4 = "ChannelController"
$x5 = "RemoteKeylogger"
$a1 = "UNCORRECT DISPLAY NAME"
$a2 = "Keylogger started"
$a3 = "Keylog thread exit"
$a4 = "Keylogger yet started"
condition:
$service or (2 of ($x)) or (2 of ($a))
}
```