Dynamically analyzing system apps on Android

June 3, 2022

cisco | TALOS

Who am I?

CyberSecurity Researcher at Cisco Talos

- Mobile malware lover
- APT hunter
- Reverse engineer

Located in Portugal

Vitor Ventura

@_vventura

Talos
Cisco Security Research

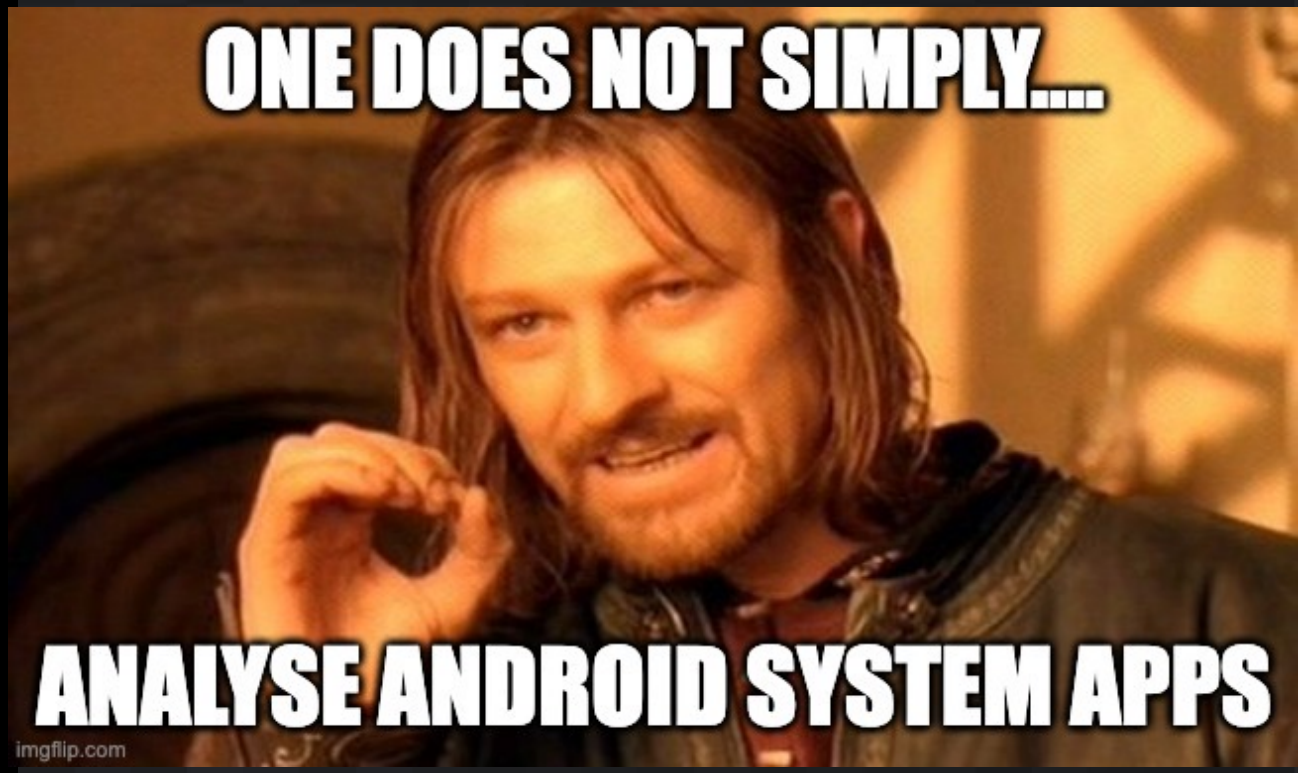
How did I got here?

WHY?

WHY

- Google was splitting Google Play Protect Services from the overwall Google Play
- So how are they doing their anti-malware solution?

What happened?



Background

The problem

Android Operating system

- Open operating system used by the majority of the phones
- Multiple types of applications
- Multiple permissions levels

Two types of applications

- System
  - Pre-installed with the OS.
  - Don’t need to be signed by Google
- Non-system
- User-level

System applications

- Especifically with the system.img
- Added by vendor, telecoms, Google or others at device creation

System Apps dynamic analysis

- Most don’t have a UI to be launched
- Can share process or UserID
- Can have signature level permissions
- Cannot be deleted by the user

cisco | TALOS

The objective

Perform dynamic analysis

Dynamic analysis of system applications

Instrument the target application

To perform dynamic analysis we will use Frida to instrument the target application.

We can do both dynamic analysis for reverse engineering

fuzzing of the application inputs for offensive researach

Use stock images

Keep the images as pristine as possible

Keep vendor kernel tweaks

Google Play protect Services

- Optimized with ProGuard
- No anti-analysis techniques
- Lots of interesting native code
- Native code not obfuscated

..... and the Journey begins

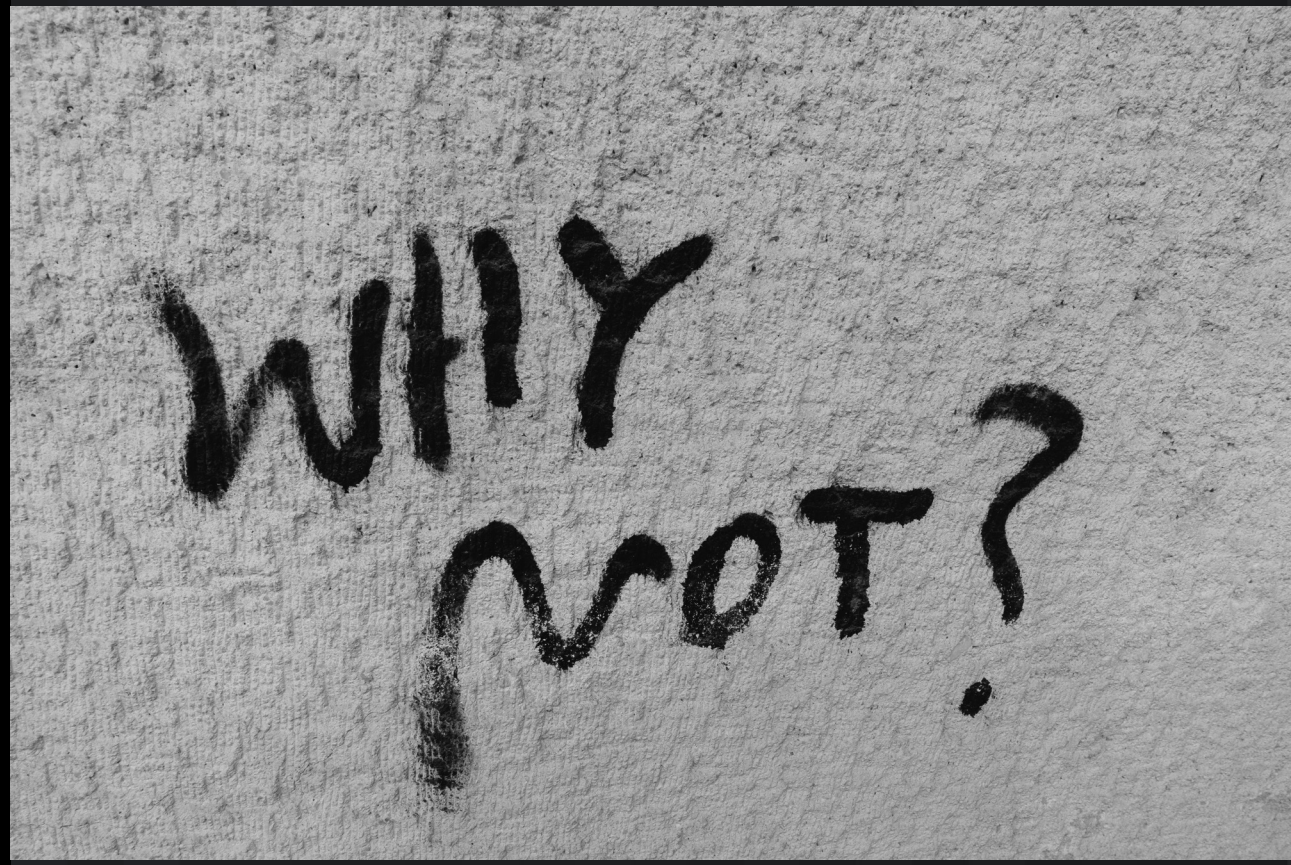
Direct approach

Indirect approach

I’m in trouble

I’m in trouble

- Its SIGNED by Google
  - …… and they don’t share their private key
  - … nor will they sign my code!



I’m in trouble

- It’s pre-installed !!
  - Can’t install over it with different signatures….
  - ….. DAMN YOU Google!!!

I’m in trouble

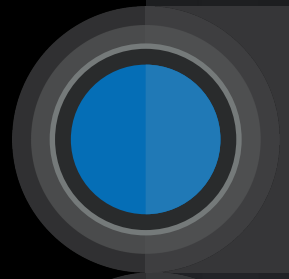
- I can’t uninstall either because it’s a pre-installed system app


SO IN SUMMARY
makeameme.org

I’m in trouble

Can’t run GPPS
- because there is no MAIN

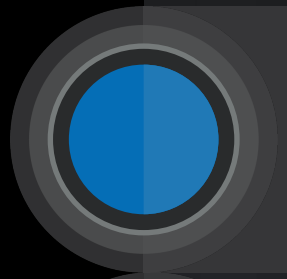
I’m in trouble



Can’t run GPPS
- because there is no MAIN

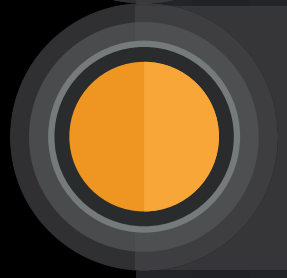
Can’t insert Frida gadget
- because I don’t have Google private key

I’m in trouble



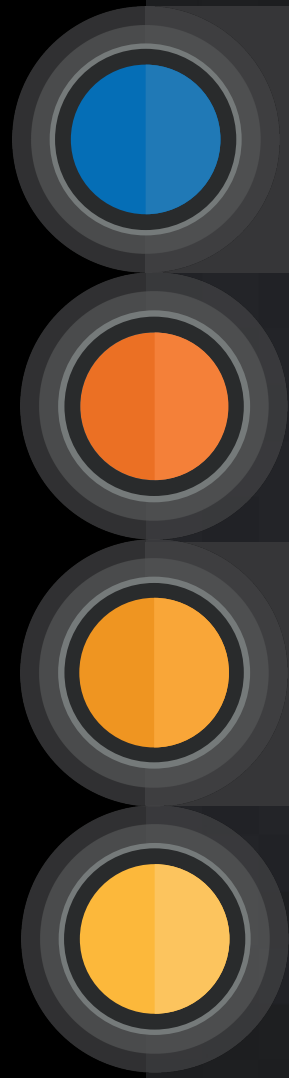
Can’t run GPPS
- because there is no MAIN

Can’t insert Frida gadget
- because I don’t have Google private key



Can’t uninstall Google Play Protect Services
- Because it is a pre-installed system application

I’m in trouble



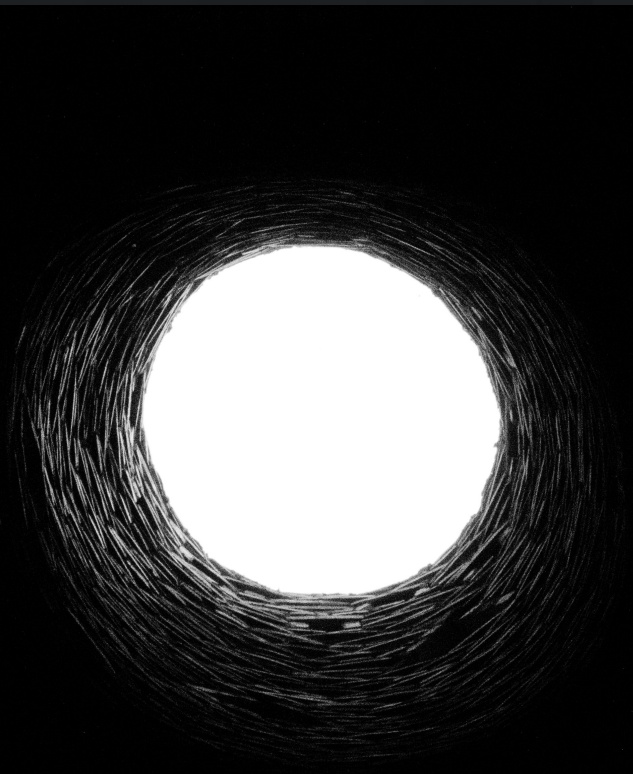
Can’t run GPPS
- because there is no MAIN

Can’t insert Frida gadget
- because I don’t have Google private key

Can’t uninstall Google Play Protect Services
- Because it is a pre-installed system application

What can I do?!!!

Need to get out of this hole



Steps

1. Remove the pre-installed version
2.
3.
4.
5.
6.

What is Magisk??

Magisk is a suite of open source software for customizing Android, supporting devices higher than Android 5.0.

Some highlight features:

- **MagiskSU**: Provide root access for applications
- **Magisk Modules**: Modify read-only partitions by installing modules
- **MagiskBoot**: The most complete tool for unpacking and repacking Android boot images
- **Zygisk**: Run code in every Android applications' processes

Source: https://github.com/topjohnwu/Magisk

Magisk to the rescue

- With Magisk we can create a module to hide and/or replace a previous package.
- Basically you can patch the file system with any content upon boot.
- Including simply making empty dirs

```
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 TetheringEntitlement
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 TipsPrebuilt
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 TurboPrebuilt
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 USCCDM
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 Velvet
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 WellbeingPrebuilt
drwxr-xr-x  3 root root 4096 2008-12-31 19:00 WfcActivation
coral:/system/product/priv-app # cd OdadPrebuilt/
coral:/system/product/priv-app/OdadPrebuilt # ls -la
total 7
drwxr-xr-x  2 root root 3488 2022-05-30 06:24 .
drwxr-xr-x 57 root root 4096 2008-12-31 19:00 ..
-rw-r--r--  1 root root    0 2022-03-28 09:12 .replace
```

Steps

1. Remove the pre-installed version
2. Patch the application to load Frida gadget
3.
4.
5.
6.

How to add the Frida Gadget?

Find the appropriate place to load the library.

This being a system application the BOOT_COMPLETED

Handler is the perfect place.

```
# virtual methods
.method public final onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 8

    .line 1
    .line 2
    const-string v0, "gadget"
    invoke-static {v0}, Ljava/lang/System;-> loadLibrary(Ljava/lang/String;)V

    const-string v0, "VV-Talos"
    const-string v1, "Odad: onReceive"
    invoke-static {v0,v1}, Landroid/util/Log;->v(Ljava/lang/String;Ljava/lang/String;)I
    invoke-virtual {p0, p1}, Latb;->a(Landroid/content/Context;)V

    .line 3
    invoke-static {}, Lark;->b()Z

    move-result p1

    if-eqz p1, :cond_0

    return-void

    .line 4
    :cond_0
    invoke-virtual {p2}, Landroid/content/Intent;->getAction()Ljava/lang/String;
```

How to add the Frida Gadget?

We just add the smali code to load the native library

```
# virtual methods
.method public final onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 8

    .line 1
    .line 2
    const-string v0, "gadget"
    invoke-static {v0}, Ljava/lang/System;-> loadLibrary(Ljava/lang/String;)V

    const-string v0, "VV-Talos"
    const-string v1, "Odad: onReceive"
    invoke-static {v0,v1}, Landroid/util/Log;->v(Ljava/lang/String;Ljava/lang/String;)I
    invoke-virtual {p0, p1}, Latb;->a(Landroid/content/Context;)V

    .line 3
    invoke-static {}, Lark;->b()Z

    move-result p1

    if-eqz p1, :cond_0

    return-void

    .line 4
    :cond_0
    invoke-virtual {p2}, Landroid/content/Intent;->getAction()Ljava/lang/String;
```

How to add the Frida Gadget?

This will load the frida gadget

We just add the smali code to load the native library

```
# virtual methods
.method public final onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 8

    .line 1
    .line 2
    const-string v0, "gadget"
    invoke-static {v0}, Ljava/lang/System;-> loadLibrary(Ljava/lang/String;)V

    const-string v0, "VV-Talos"
    const-string v1, "Odad: onReceive"
    invoke-static {v0,v1}, Landroid/util/Log;->v(Ljava/lang/String;Ljava/lang/String;)I
    invoke-virtual {p0, p1}, Latb;->a(Landroid/content/Context;)V

    .line 3
    invoke-static {}, Lark;->b()Z

    move-result p1

    if-eqz p1, :cond_0

    return-void

    .line 4
    :cond_0
    invoke-virtual {p2}, Landroid/content/Intent;->getAction()Ljava/lang/String;
```

How to add the Frida Gadget?

This will load the frida gadget

We just add the smali code to load the native library

Good old println debug

```
# virtual methods
.method public final onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 8

    .line 1
    .line 2
    const-string v0, "gadget"
    invoke-static {v0}, Ljava/lang/System;-> loadLibrary(Ljava/lang/String;)V

    const-string v0, "VV-Talos"
    const-string v1, "Odad: onReceive"
    invoke-static {v0,v1}, Landroid/util/Log;->v(Ljava/lang/String;Ljava/lang/String;)I
    invoke-virtual {p0, p1}, Latb;->a(Landroid/content/Context;)V

    .line 3
    invoke-static {}, Lark;->b()Z

    move-result p1

    if-eqz p1, :cond_0

    return-void

    .line 4
    :cond_0
    invoke-virtual {p2}, Landroid/content/Intent;->getAction()Ljava/lang/String;
```

How to add the Frida Gadget?

We just add the smali code to load the native library

Then we need to add both the shared library file and its configuration to the package.

```
'work/recon_22/pixel/patched_gpps_GADGET/lib
└── arm64-v8a
    ├── libcpuutils.so
    ├── libgadget.config.so
    ├── libgadget.so
    ├── libtartarus.so
    ├── libtask_text_jni.so
    └── libtensorflowlite_jni.so
```

How to add the Frida Gadget?

This configuration will simply run a Frida JavaScript.

Located in the Android temporary directory

```
└──>cat libgadget.config.so
{
  "interaction": {
    "type": "script",
    "path": "/data/local/tmp/gpps.js",
    "on_change": "reload"
  }
}
```

Steps

1. Remove the pre-installed version
2. Patch the application to load Frida gadget
3. Install patched version has system
4.
5.
6.

Without Magisk

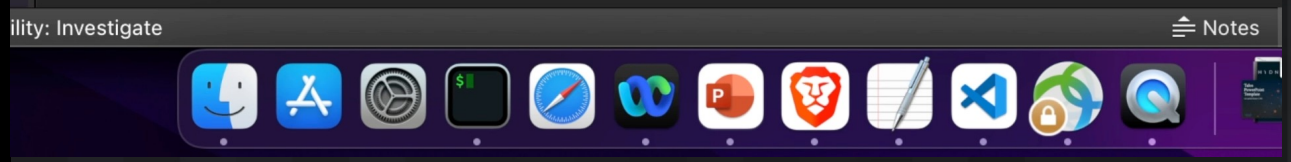
```
└──> <ANDROID> --> adb install -r patched_gpps_GADGET_patched.apk
Performing Incremental Install
Serving...
All files should be loaded. Notifying the device.
Failure [INSTALL_FAILED_SESSION_INVALID: Incremental installation of this package is not allowed.]
Performing Streamed Install

adb: failed to install patched_gpps_GADGET_patched.apk: Failure [INSTALL_FAILED_UPDATE_INCOMPATIBLE:
Package com.google.android.odad signatures do not match previously installed version; ignoring!]
```

With Magisk

```
└──> <ANDROID> --> adb install -r patched_gpps_GADGET_patched.apk
Performing Incremental Install
Serving...
All files should be loaded. Notifying the device.
Success
Install command complete in 1039 ms
```

When I run it

```
06-02 09:41:23.698  7379  7379 V VV-Talos: Odad: onReceive
^C
┌─[vitorventura@Vitors-MacBook-Pro:~/work/recon_22/pixel
└──> <ANDROID> --> adb logcat | egrep -i '(frida|talos)'
06-02 09:41:23.683  7379  7379 V VV-Talos: Have fun!
06-02 09:41:23.698  7379  7379 V VV-Talos: Odad: onReceive
┌─[vitorventura@Vitors-MacBook-Pro:~/work/recon_22/pixel
└──> <ANDROID> --> adb logcat | egrep -i '(frida|talos)'
- waiting for device -
```



Steps

1. Remove the pre-installed version
2. Patch the application to load Frida gadget
3. Install patched version has system
4. Search for the right place to patch
5.
6.

Was the receiver the right place to patch?

```
public final class StartPeriodicWorkReceiver extends atb {
    public static final cfe a = cfe.m("com/google/android/apps/miphone/odad/work/impl/StartPeriodicWorkReceiver");
    public cnh b;
    public dej c;

    @Override // defpackage.atb, android.content.BroadcastReceiver
1   public final void onReceive(Context context, Intent intent) {
2       System.loadLibrary("gadget");
        Log.v("VV-Talos", "Odad: onReceive");
        a(context);
3       if (ark.b() || intent.getAction() == null) {
            return;
        }
5       if ("android.intent.action.BOOT_COMPLETED".equals(intent.getAction()) || "android.intent.action.MY_PACKAGE_REPLACED".equals
6           BroadcastReceiver.PendingResult goAsync = goAsync();
7           ade b = ade.b(this.c.a);
8           abz abzVar = new abz(PeriodicClassificationWorker.class, Duration.ofDays(1L));
9           abh abhVar = new abh();
            abhVar.a = true;
            abhVar.b();
10          abzVar.c(abhVar.a());
11          ahn ahnVar = ((ack) b.a("periodic-classification-work", abzVar.b())).c;
            dej dejVar = this.c;
12          abz abzVar2 = new abz(PeriodicRefreshWorker.class, Duration.ofHours(18L));
13          abh abhVar2 = new abh();
            abhVar2.a = true;
14          abhVar2.b();
            abhVar2.d = 2;
16          abzVar2.c(abhVar2.a());
19          ahn ahnVar2 = ((ack) ade.b(dejVar.a).a("periodic-astrea-refresh-work", abzVar2.b())).c;
20          ade b2 = ade.b(this.c.a);
21          abz abzVar3 = new abz(PeriodicHygienationWorker.class, Duration.ofDays(1L));
22          abh abhVar3 = new abh();
            abhVar3.a = true;
            abhVar3.b();
23          abzVar3.c(abhVar3.a());
26          ej.w(ej.o(ahnVar, ahnVar2, ((ack) b2.a("periodic-hygienation-work", abzVar3.b())).c), new ate(goAsync), this.b);
        }
```


Well yes, but actually no

Search for the right place to patch

```
public final class StartPeriodicWorkReceiver extends atb {
    public static final cfe a = cfe.m("com/google/android/apps/miphone/odad/work/impl/StartPeriodicWorkReceiver");
    public cnh b;
    public dej c;

    @Override // defpackage.atb, android.content.BroadcastReceiver
1   public final void onReceive(Context context, Intent intent) {
2       System.loadLibrary("gadget");
        Log.v("VV-Talos", "Odad: onReceive");
        a(context);
3       if (ark.b() || intent.getAction() == null) {
            return;
        }
5       if ("android.intent.action.BOOT_COMPLETED".equals(intent.getAction()) || "android.intent.action.MY_PACKAGE_REPLACED".equals
6           BroadcastReceiver.PendingResult goAsync = goAsync();
7           ade b = ade.b(this.c.a);
8           abz abzVar = new abz(PeriodicClassificationWorker.class, Duration.ofDays(1L));
9           abh abhVar = new abh();
            abhVar.a = true;
            abhVar.b();
10          abzVar.c(abhVar.a());
11          ahn ahnVar = ((ack) b.a("periodic-classification-work", abzVar.b())).c;
            dej dejVar = this.c;
12          abz abzVar2 = new abz(PeriodicRefreshWorker.class, Duration.ofHours(18L));
13          abh abhVar2 = new abh();
            abhVar2.a = true;
14          abhVar2.b();
            abhVar2.d = 2;
16          abzVar2.c(abhVar2.a());
19          ahn ahnVar2 = ((ack) ade.b(dejVar.a).a("periodic-astrea-refresh-work", abzVar2.b())).c;
20          ade b2 = ade.b(this.c.a);
21          abz abzVar3 = new abz(PeriodicHygienationWorker.class, Duration.ofDays(1L));
22          abh abhVar3 = new abh();
            abhVar3.a = true;
            abhVar3.b();
23          abzVar3.c(abhVar3.a());
26          ej.w(ej.o(ahnVar, ahnVar2, ((ack) b2.a("periodic-hygienation-work", abzVar3.b())).c), new ate(goAsync), this.b);
        }
```

Steps

1. Remove the pre-installed version
2. Patch the application to load Frida gadget
3. Install patched version has system
4. Search for the right place to patch
5. What if there was a sharedUserId?
6.

sharedUserId

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://sche
mas.android.com/apk/res/android" android:compileSdkVersion="30" android:compileSdkVersionC
odename="11" android:sharedUserId="android.media" package="com.android.mtp" platformBuildV
ersionCode="30" platformBuildVersionName="11">
    <uses-feature android:name="android.hardware.usb.host"/>
    <uses-permission android:name="android.permission.ACCESS_MTP"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.MANAGE_USB"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.MANAGE_USERS"/>
    <uses-permission android:name="android.permission.INTERACT_ACROSS_USERS"/>
    <uses-permission android:name="android.permission.WRITE_MEDIA_STORAGE"/>
    <uses-permission android:name="android.permission.MANAGE_EXTERNAL_STORAGE"/>
    <application android:allowBackup="false" android:appComponentFactory="androidx.core.ap
p.CoreComponentFactory" android:extractNativeLibs="true" android:label="@string/app_label"
 android:process="android.process.media" android:usesCleartextTraffic="true" android:usesN
onSdkApi="true">
        <provider android:authorities="com.android.mtp.documents" android:exported="true"
android:grantUriPermissions="true" android:name="com.android.mtp.MtpDocumentsProvider" and
roid:permission="android.permission.MANAGE_DOCUMENTS">
            <intent-filter>
                <action android:name="android.content.action.DOCUMENTS_PROVIDER"/>
            </intent-filter>
                                                                    1,1           Top
```

Steps

1. Remove the pre-installed version
2. Patch the application to load Frida gadget
3. Install patched version has system
4. Search for the right place to patch
5. What if there was a sharedUserId?
6. Have fun

Future work

- Actually perform dyamic analysis on the Google Play Protect Services
- Fuzz Google Play Protect Services native code
- Perform dynamic analysis on other system applciations
- Move the gadget injection into the zygote throught Magisk.

Questions?

Thank you!

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity


CISCO
TALOS
TALOSINTELLIGENCE.COM