

# Как я собирался фазить YotaPhone

11/02/2014

DCG #7812

г. Санкт-Петербург

by  
@evdokimovds

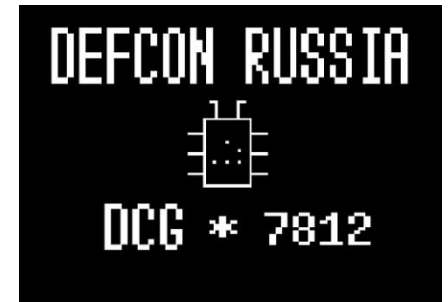


## #whoami

- Исследователь информационной безопасности в **Digital Security Research Group**.
- Редактор рубрик в журнале **Xakep**.
- Один из организаторов конференций **DEFCON Russia** и **ZeroNights**.



Специализируюсь на поиске уязвимостей в бинарных приложениях без исходного кода.



# ilovemobile

Firefox OS

Android

iPhone 4S

Android (YotaPhone)



WindowsPhone 7

WindowsPhone 8

iPhone 5

# YotaPhone

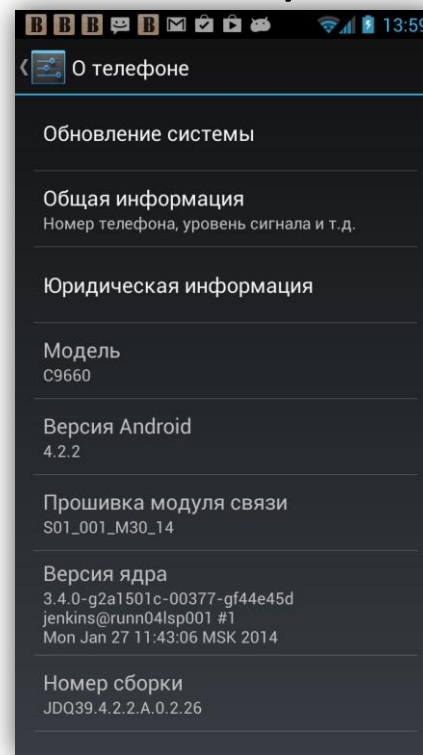


# Designed in Russia



# Internals

- Qualcomm dual core 1.7GHz Krait  
MSM8960Pro
  - Snapdragon S4 Pro (ARMv7, ~Cortex-A15)
- Android 4.2.2

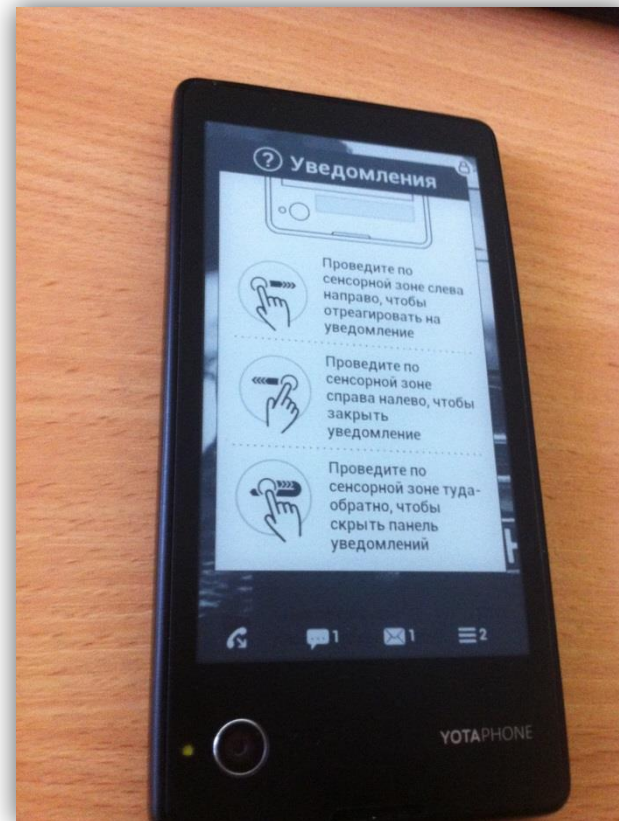




# New attack surface

- New features = new attack surface
- New:
  - E-ink display
  - Apps from YotaDevices
  - ... (?!)

```
root@android:/data/app # find . -name "*yotadevices*"
find . -name "*yotadevices*"
./com.yotadevices.yotaphone.organizer-1.apk
./com.yotadevices.yotaphone.internethub-1.apk
./com.yotadevices.yotaphone.notepad-1.apk
./com.yotadevices.settings-1.apk
./com.yotadevices.yotaphone.wallpapers-1.apk
./com.yotadevices.yotaphone.teachme-1.apk
./com.yotadevices.social-1.apk
./com.yotadevices.framework-1.apk
./com.yotadevices.clocks.main-1.apk
```



# API for E-ink ?

Участие в мероприятии даст вам возможность:

- получить доступ к API YotaPhone за несколько месяцев до официального релиза

<http://www.yotadevices.com/dev/about/>

- Нет в открытом до ступе по сей день



# #Root

- Получаем root на устройстве
  - USB driver
    - <http://4pda.to/forum/index.php?showtopic=408103&st=600>
  - Frameroot (Gandalf exploit)
  - SuperSU



# #Search mode

- Ищем

- adb logcat -c
- adb -d logcat

```
root@android:/ # find . -name "*platinum*"
find . -name "*platinum*"
./system/bin/platinumd
./system/etc/permissions/com.yotadevices.platinum.xml
./system/framework/com.yotadevices.platinum.jar
./system/framework/com.yotadevices.platinum.odex
./system/lib/libyotadevices_platinum_jni.so
```

```
----- beginning of /dev/log/main
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
D/WindowManager< 695>: Gesture: 250, Down: false
----- beginning of /dev/log/system
M/ContextImpl< 2143>: Calling a method in the system process without a qualified user: android.app.C
ontextImpl.sendBroadcast:1058 android.content.ContextWrapper.sendBroadcast:343 com.yotadevices.frame
work.service.bs.BackScreenLayersManager.redrawBSScreen:373 com.yotadevices.framework.service.bs.Back
ScreenLayersManager.handleBsGesture:582 com.yotadevices.framework.service.PlatinumManagerService$2.h
andleMessage:291
D/dalvikvm< 2143>: GC_FOR_ALLOC freed 4313K, 31% free 17142K/24620K, paused 14ms, total 14ms
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 3)
M/PlatinumAPI< 2143>: getPlatinumUtils
D/PlatinumAPI< 274>: BnPlatinumUtils::onTransact 3
D/PlatinumAPI< 274>: enableGestures: 77
D/PlatinumAPI< 274>: enableGestures="752 753 754 756 757 758 ", disableGestures="755 759 760 ", mcu
Bitmask=1b
D/dalvikvm< 2143>: GC_CONCURRENT freed 1299K, 25% free 18553K/24620K, paused 3ms+2ms, total 17ms
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
^C
```

# #Search mode:stage2

- adb -d logcat PlatinumAPI:V \*:S

```

----- beginning of /dev/log/main
----- beginning of /dev/log/system
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 3)
W/PlatinumAPI< 2143>: getPlatinumUtils
D/PlatinumAPI< 274>: BnPlatinumUtils::onTransact 3
D/PlatinumAPI< 274>: enableGestures: 77
D/PlatinumAPI< 274>: enableGestures="752 753 754 756 757 758 ", disableGestures="755 759 760 ", mcu
Bitmask=1b
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 3)
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
W/PlatinumAPI< 2143>: getPlatinumUtils
D/PlatinumAPI< 274>: BnPlatinumUtils::onTransact 3
D/PlatinumAPI< 274>: enableGestures: 77
D/PlatinumAPI< 274>: enableGestures="752 753 754 756 757 758 ", disableGestures="755 759 760 ", mcu
Bitmask=1b
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 3)
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
D/PlatinumAPI< 274>: EInkDevice::drawBitmap(0, 0, 360, 640, 2)
^C

```

- find . -name "\*platinum\*"


```

root@android:/ # find . -name "*platinum*"
find . -name "*platinum*"
./system/bin/platinumd
./system/etc/permissions/com.yotadevices.platinum.xml
./system/framework/com.yotadevices.platinum.jar
./system/framework/com.yotadevices.platinum.odex
./system/lib/libyotadevices_platinum_jni.so

```

# Inf from Apps

- AndroidManifest.xml
  - Permission




```

<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_CALENDAR" />
<uses-permission android:name="android.permission.WRITE_CALENDAR" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="com.yotadevices.framework.permission.ACCESS_BACKSCREEN" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="com.android.email.permission.ACCESS_PROVIDER" />
<uses-permission android:name="android.permission.READ_SYNC_SETTINGS" />
<uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS" />

```

- Library



```

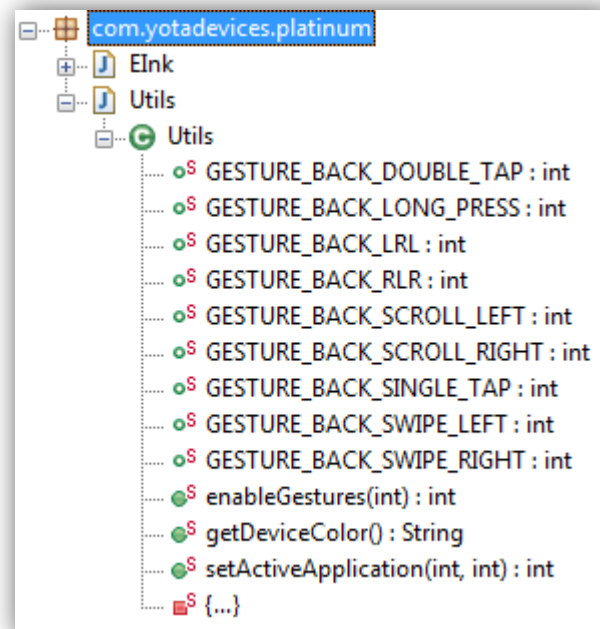
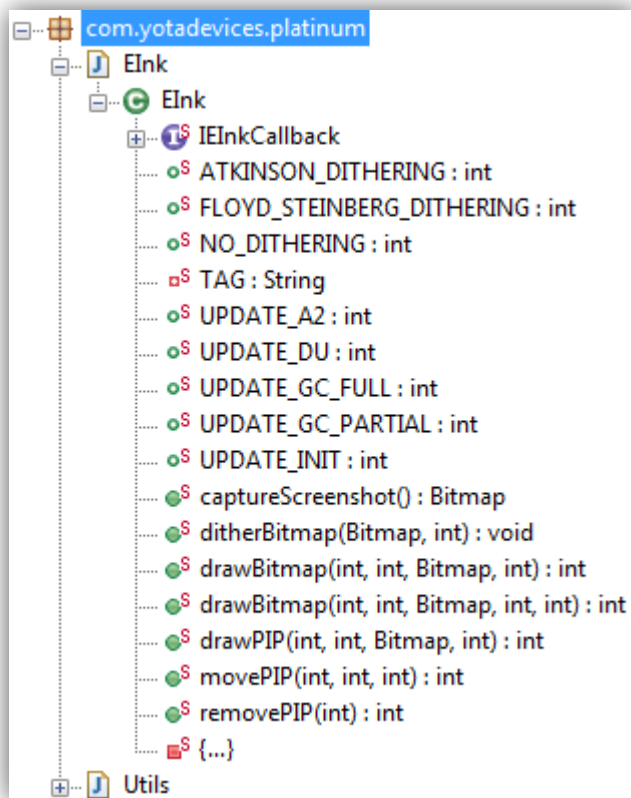
</receiver>
<uses-library android:name="com.yotadevices.platinum" android:required="true" />
</application>

```

# Внутри com.yotadevices.platinum.odex

Decompile odex:

```
java -jar baksmali.jar -d system/framework -x com.yotadevices.platinum.odex
java -jar smali.jar -o classes.dex out
dex2jar.bat classes.dex
```



# Код API

```
public static native Bitmap captureScreenshot();

public static native void ditherBitmap(Bitmap paramBitmap, int paramInt);

public static native int drawBitmap(int paramInt1, int paramInt2, Bitmap paramBitmap, int paramInt3);

public static native int drawBitmap(int paramInt1, int paramInt2, Bitmap paramBitmap, int paramInt3, int paramInt4);

public static native int drawPIP(int paramInt1, int paramInt2, Bitmap paramBitmap, int paramInt3);

public static native int movePIP(int paramInt1, int paramInt2, int paramInt3);

public static native int removePIP(int paramInt);

public static abstract interface IEInkCallback
{
    public abstract void onEinkDrawComplete();

    public abstract void onEinkDrawError(int paramInt);
}
```

```
static
{
    System.loadLibrary("yotadevices_platinum_jni");
}
```

```
public static native int enableGestures(int paramInt);

public static String getDeviceColor()
{
    return SystemProperties.get("service.platinumd.skucolor");
}

public static native int setActiveApplication(int paramInt1, int paramInt2);
```



# Внутри libyotadevices\_platinum\_jni.so

- 2 основных класса
  - PlatinumAPI::BpEInk
  - PlatinumAPI::BpPlatinumUtils

| Function name  | Segment | Start    | Length   | Locals   | Arguments  | R | F | L | S | B | T | = |
|--|---------|----------|----------|----------|------------|---|---|---|---|---|---|---|
| PlatinumAPI::IEInk::getInterfaceDescriptor(void)             | .text   | 00003FD4 | 00000006 |          |            | R | . | . | . | . | . | . |
| virtual thunk to PlatinumAPI::IEInk::~IEInk()                | .text   | 00003FE4 | 0000000C |          |            | R | . | . | . | . | . | . |
| PlatinumAPI::IEInk::~IEInk()                                 | .text   | 00003FF0 | 00000026 | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| virtual thunk to PlatinumAPI::IEInk::~IEInk()                | .text   | 00004020 | 0000000C |          |            | R | . | . | . | . | . | . |
| PlatinumAPI::IEInk::~IEInk()                                 | .text   | 0000402C | 00000012 | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::removePIP(void)                         | .text   | 00004040 | 00000048 | 00000070 | FFFFFFFFC9 | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::movePIP(int,int)                        | .text   | 0000408C | 0000005C | 00000078 | FFFFFFFFC1 | R | . | . | . | . | . | . |
| PlatinumAPI::IEInk::IEInk(void)                              | .text   | 000040EC | 0000001C | 00000010 | FFFFFFFFF0 | R | . | . | . | . | . | . |
| PlatinumAPI::IEInk::IEInk(void)                              | .text   | 00004108 | 00000028 | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| PlatinumAPI::IEInk::~IEInk()                                 | .text   | 00004138 | 0000001C | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::drawPIP(int,int,int,android::sp<...)    | .text   | 0000425C | 00000086 | 00000088 | 00000008   | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::drawBitmap(int,int,int,int,android::... | .text   | 000042E8 | 0000008E | 00000088 | 0000000C   | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::BpEInk(android::sp<android::IBind...    | .text   | 000043AC | 00000034 | 00000010 | FFFFFFFFF0 | R | . | . | . | . | . | . |
| PlatinumAPI::IEInk::asInterface(android::sp<android::IBi...  | .text   | 000043E8 | 0000008E | 00000018 | FFFFFFFFF0 | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::getService(void)                        | .text   | 0000447C | 000000D6 | 00000030 | FFFFFFFFE1 | R | . | . | . | . | . | . |
| PlatinumAPI::BpEInk::BpEInk(android::sp<android::IBind...    | .text   | 0000456C | 00000020 | 00000010 | FFFFFFFFF0 | R | . | . | . | . | . | . |
| PlatinumAPI::PlatinumUtils::getInterfaceDescriptor(void)     | .text   | 000045C4 | 00000006 |          |            | R | . | . | . | . | . | . |
| virtual thunk to PlatinumAPI::PlatinumUtils::~Platinum...    | .text   | 000045D0 | 0000000C |          |            | R | . | . | . | . | . | . |
| PlatinumAPI::PlatinumUtils::~PlatinumUtils()                 | .text   | 000045DC | 00000026 | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| virtual thunk to PlatinumAPI::PlatinumUtils::~Platinum...    | .text   | 0000460C | 0000000C |          |            | R | . | . | . | . | . | . |
| PlatinumAPI::PlatinumUtils::~PlatinumUtils()                 | .text   | 00004618 | 00000012 | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| PlatinumAPI::BpPlatinumUtils::enableGestures(int)            | .text   | 0000462C | 00000052 | 00000078 | FFFFFFFFC1 | R | . | . | . | . | . | . |
| PlatinumAPI::BpPlatinumUtils::setActiveApplication(int,i...  | .text   | 00004684 | 0000005C | 00000078 | FFFFFFFFC1 | R | . | . | . | . | . | . |
| PlatinumAPI::PlatinumUtils::PlatinumUtils(void)              | .text   | 000046E4 | 00000028 | 00000008 | FFFFFFFF8  | R | . | . | . | . | . | . |
| PlatinumAPI::BpPlatinumUtils::captureScreen(android::s...    | .text   | 0000481C | 00000060 | 00000080 | FFFFFFFFC1 | R | . | . | . | . | . | . |
| PlatinumAPI::BpPlatinumUtils::BpPlatinumUtils(android:...    | .text   | 00004880 | 00000034 | 00000010 | FFFFFFFFF0 | R | . | . | . | . | . | . |
| PlatinumAPI::PlatinumUtils::asInterface(android::sp<an...    | .text   | 000048BC | 0000008E | 00000018 | FFFFFFFFF0 | R | . | . | . | . | . | . |
| PlatinumAPI::BpPlatinumUtils::getService(void)               | .text   | 00004950 | 000000C6 | 00000030 | FFFFFFFFE0 | R | . | . | . | . | . | . |

# IDA & Android

## - Добавим динамики

- android\_server from IDA Pro

```
adb push android_server /sdcard/
cp /sdcard/android_server /data/
su
cd /data
chmod 755 android_server
./android_server
```

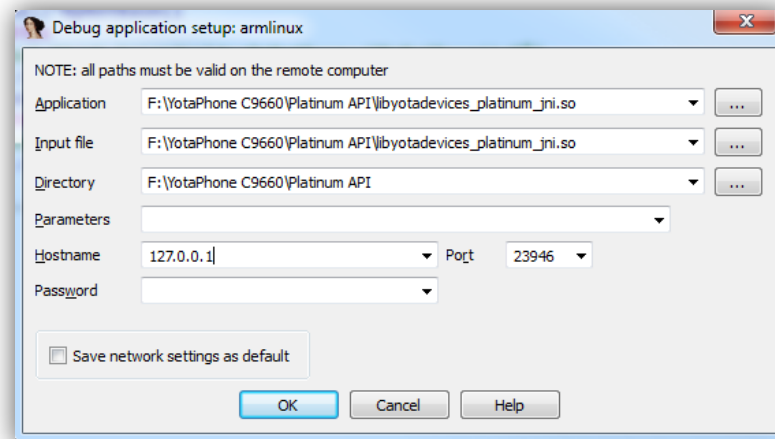
- Перенаправим порты

```
adb forward tcp:23946 tcp:23946
```

- Запускаем

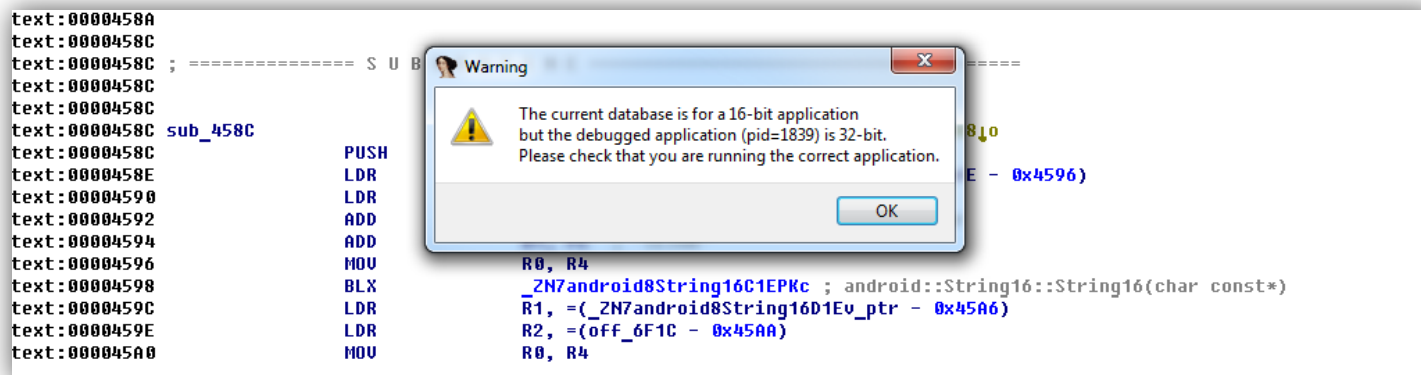
```
root@android:/data # ./android_server
./android_server
IDA Android 32-bit remote debug server(ST) v1.17. Hex-Rays (c) 2004-2013
Listening on port #23946...
=====
[1] Accepting connection from 127.0.0.1...
```

- Соединяемся



# Kill bug in IDA

## - IDA Pro 6.5



- **Ответ Ильфака:** Thank you for the report! Please find the fixed version of the loader attached. It will ensure that newly created databases will have the correct bitness. You can fix the existing databases by executing the following IDC function:

```
SetCharPrm(INF_LFLAGS, GetCharPrm(INF_LFLAGS) | LFLG_PC_FLAT);
```

# Success!

IDA - FA\YotaPhone C9660\Platinum API\platinumd - Running

File Edit Jump Search View Debugger Options Windows Help

Remote ARM Linux/Android debugger

Library function Data Regular function Unexplored Instruction External symbol

Debug View Strings window Structures Enums

IDA View-PC

```
liblog.so:401E5318 ; ===== SUBROUTINE =====
liblog.so:401E5318
liblog.so:401E5318
liblog.so:401E5318 __android_log_print
liblog.so:401E5318
liblog.so:401E5318 var_420= -0x420
liblog.so:401E5318 var_41C= -0x41C
liblog.so:401E5318 var_1C= -0x1C
liblog.so:401E5318 varg_r2= -8
liblog.so:401E5318 varg_r3= -4
liblog.so:401E5318
liblog.so:401E5318 PUSH {R2,R3}
liblog.so:401E531A PUSH {R4-R6,LR}
liblog.so:401E531C SUB.W SP, SP, #0x408
liblog.so:401E5320 LDR R4, -(dword_401E7F50 - 0x401E532E)
liblog.so:401E5322 ADD.W R3, SP, #0x420+varg_r2
liblog.so:401E5326 MOV R5, R1
liblog.so:401E5328 MOV R6, R0
liblog.so:401E532A ADD R4, PC ; dword_401E7F50
liblog.so:401E532C LDR R4, [R4]
liblog.so:401E532E LDR.W R2, [R3], #4
liblog.so:401E5332 ADD R0, SP, #0x420+var_41C
liblog.so:401E5334 LDR R1, [R4]
liblog.so:401E5336 STR R3, [SP, #0x420+var_420]
liblog.so:401E5338 STR.W R1, [SP, #0x420+var_1C]
liblog.so:401E533C MOV.W R1, #0x408
liblog.so:401E5340 BLX unk_401E4DE4
liblog.so:401E5344 ADD R2, SP, #0x420+var_41C
UNKNOWN 401E5318: __android_log_print
```

Hex View-1

```
75 62 6C 69 73 68 65 64 2C 20 77 61 69 74 69 6E ublISHED..waitin
4004C5C1 67 2E 2E 2E 00 55 6E 61 62 6C 65 20 74 6F 20 67 g....Unable to g
4004C5D1 65 74 20 70 72 6F 78 79 20 66 6F 72 20 45 49 6E et.proxy.for:Ein
4004C5E1 68 20 73 65 72 76 69 63 65 00 49 45 49 6E 6B 00 k-service.IEInk.
4004C5F1 6E 50 6C 61 74 69 6E 75 6D 55 74 69 6C 73 3A BnPlatinumUtils:
4004C601 30 6F 6E 54 72 61 6E 73 61 63 74 20 25 64 00 67 :onTransact:4d.g
4004C611 65 74 50 6C 61 74 69 6E 75 6D 55 74 69 6C 73 00 etPlatinumUtils.
4004C621 63 6F 6D 2E 79 6F 74 61 64 65 76 69 63 65 73 2E com.yotadevices.
4004C631 70 6C 61 74 69 6E 75 6D 2E 75 74 69 6C 73 20 6E platinum.utilis:n
4004C641 6F 74 20 70 75 62 6C 69 73 68 65 64 2C 20 77 61 6E ot-published..wa
4004C651 69 74 69 6E 67 2E 2E 2E 00 49 50 6C 61 74 69 6E iting....lPlatin
4004C661 75 6D 55 74 69 6C 73 00 66 61 74 61 6C 20 65 72 umlUtils.Fatal-er
4004C671 72 6F 72 20 6F 70 65 6E 69 6E 67 20 25 73 22 ror-opening:"%s"
4004C681 00 00 2F 73 79 73 2F 70 6F 77 65 72 2F 77 61 6B ../sys/power/wak
4004C691 65 5F 6C 6F 63 68 00 2F 73 79 73 2F 70 6F 77 65 e_lock../sys/powe
4004C6A1
```

UNKNOWN 4004C601: platinumd:4004C601

Output window

```
Caching 'Strings window'... ok
402B9408: thread has started (tid=5535)
Caching 'Strings window'... ok
```

Python

AU: idle Down Disk: 781MB

General registers

|     |          |  |
|-----|----------|--|
| R0  | 00000003 |  |
| R1  | 4004C24C |  |
| R2  | 4004C4F6 |  |
| R3  | BECAE86C |  |
| R4  | BECAE8A0 |  |
| R5  | 00000002 |  |
| R6  | 4004C4F2 |  |
| R7  | 00000040 |  |
| R8  | 4004C838 |  |
| R9  | 401DA228 |  |
| R10 | 401DA228 |  |
| R11 | BECAE8FC |  |
| R12 | 4004FEA8 |  |

Modules

| Path                               | Base     | Size     |
|------------------------------------|----------|----------|
| /system/bin/platinumd              | 40046000 | 00007000 |
| /system/lib/libsysutils.so         | 400B0000 |          |
| /system/lib/libcnefeatureconfig.so | 400D8000 |          |

Line 1 of 20

Threads

| Decimal | Hex  | State   |
|---------|------|---------|
| 4824    | 12D8 | Running |
| 664     | 298  | Running |
| 774     | 112  | Running |

Stack view

```
BECAE858 BECAE8A0 [stack]:BECAE8A0
BECAE85C 00000002
BECAE860 20303637
BECAE864 00007200
BECAE868 401DA228 debug006: __stack_chk_guard
BECAE86C 20383537
BECAE870 BECAE900 [stack]:BECAE900
BECAE874 0000000E
BECAE878 C0000000
BECAE87C 41E020F8 [heap]:41E020F8
BECAE880 00000000
BECAE884 41E02108 [heap]:41E02108
BECAE888 00000304
BECAE88C 401A0833 libc.so:d1free+23
BECAE890 41E020F8 [heap]:41E020F8
UNKNOWN BECAE858: [stack]:BECAE858
```

# To be continue...

- А на этом пока все =)
- Спасибо за внимание!