XCTF easy-dex

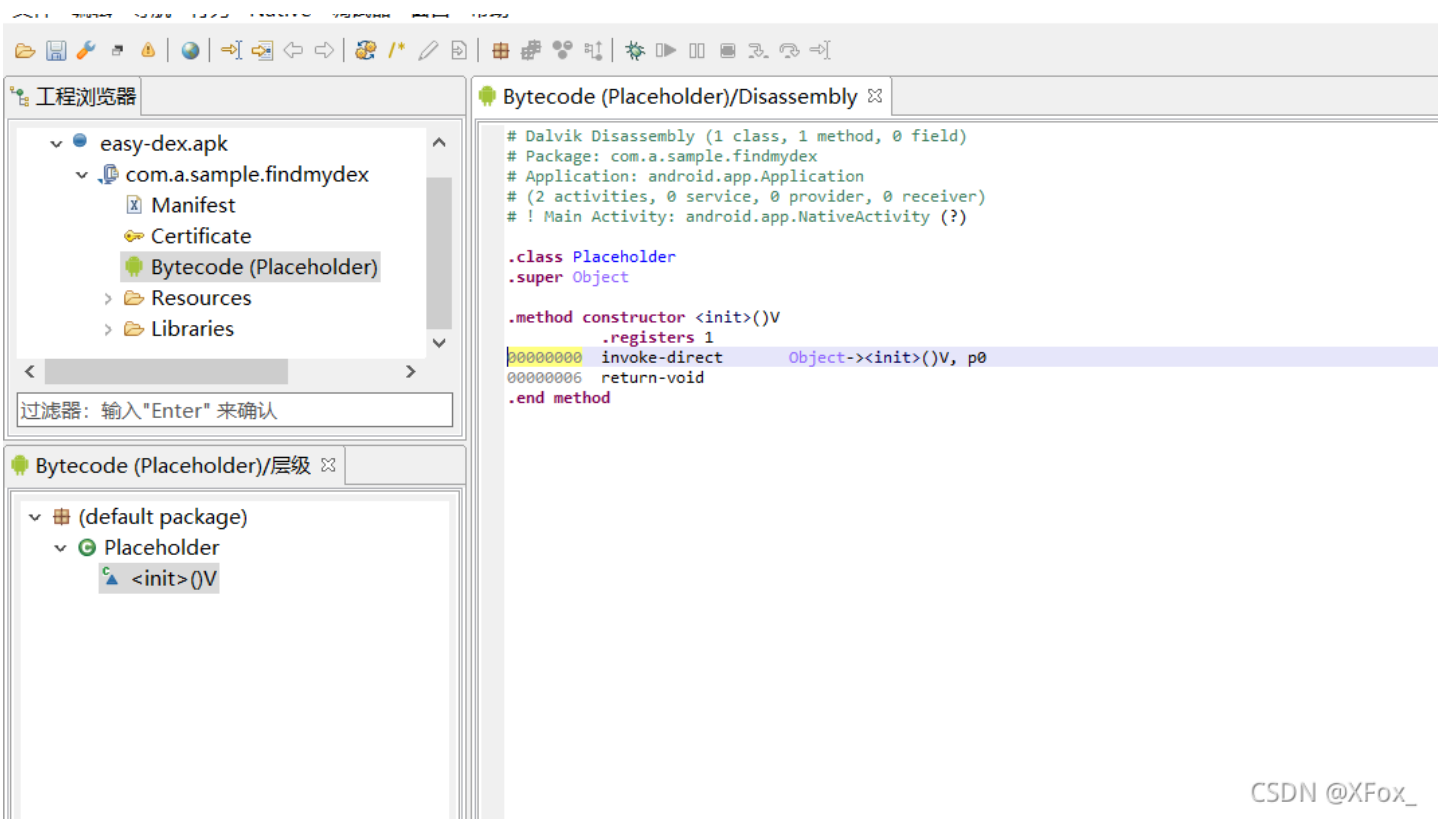
原创

XFox_ 于 2021-11-10 18:28:06 发布 17 收藏

文章标签： android java apache

本文链接：https://blog.csdn.net/XFox_/article/details/121249626

JEB看不出来。。



```
# Dalvik Disassembly (1 class, 1 method, 0 field)
# Package: com.a.sample.findmydex
# Application: android.app.Application
# (2 activities, 0 service, 0 provider, 0 receiver)
# ! Main Activity: android.app.NativeActivity (?)

.class Placeholder
.super Object

.method constructor <init>()V
          .registers 1
00000000  invoke-direct       Object-><init>()V, p0
00000006  return-void
.end method
```

在`ANativeActivity`中有一个新线程：`sub_325C`

```
if ( pipe(&attr.__align + 6) )
  {
    v10 = (int *)_errno();
    v11 = strerror(*v10);
    _android_log_print(6, "threaded_app", "could not create pipe: %s", v11);
    v8 = 0;
  }
  else
  {
    *((_QWORD *)v8 + 9) = *((_QWORD *)&attr.__align + 3);
    pthread_attr_init(&attr);
    pthread_attr_setdetachstate(&attr, 1);
    pthread_create((pthread_t *)v8 + 20, &attr, (void *(*)(void *))sub_325C, v8);
    pthread_mutex_lock((pthread_mutex_t *)(v8 + 64));
    while ( !*((_DWORD *)v8 + 27) )
      pthread_cond_wait((pthread_cond_t *)(v8 + 68), (pthread_mutex_t *)(v8 + 64));
    pthread_mutex_unlock((pthread_mutex_t *)(v8 + 64));
  }
  a1[7] = (int)v8;
  return _stack_chk_guard - *(&attr.__align + 8);
}
```

转进去`sub_325C`查看`j_android_main(a1)`：

```
destLen = 0x100000;
  dest = (Bytef *)malloc(0x100000u);
  v2 = off_43A18;
  v3 = (char *)malloc((size_t)off_43A18);
  qmemcpy(v3, &unk_7004, (size_t)v2);
  *(_DWORD *)filename = -1651995345;
  v45 = -2003974520;
  v46 = -1966700387;
  v47 = -2000190330;
  v48 = -2071422265;
  v49 = -947092071;
  v50 = -1920499569;
  v51 = -1936879484;
  v52 = -2138061167;
  v53 = -962950011;
  v54 = -1702328950;
  v55 = -946172774;
  v56 = -376337267;
  v57 = 0;
  *(_DWORD *)name = -1651995194;
  v32 = -2003974520;
  v33 = -1966700387;
  v34 = -2000190330;
  v35 = -2071422265;
  v36 = -947092071;
  v37 = -1920499569;
  v38 = -1936879484;
  v39 = -2138061167;
  v40 = -962950011;
  v41 = -1853059706;
  v43 = 0;
  v4 = 1;
  v42 = -5690;
  do
    filename[v4++] ^= 0xE9u;
  while ( v4 != 53 );
  while ( v4 != 33 );
  v5 = 1;
  name[0] = 47;
  do
    name[v5++] ^= 0xE9u;
  while ( v5 != 47 );
  j_app_dummy();
  memset(v26, 0, sizeof(v26));
  *a1 = v26;
  a1[1] = sub_29B8;
  a1[2] = sub_2B90;
  v26[0] = (int)a1;
  v26[1] = ASensorManager_getInstance();
  v26[2] = ASensorManager_getDefaultSensor(v26[1], 1);
  v6 = 0;
  v26[3] = ASensorManager_createEventQueue(v26[1], a1[7], 3, 0, 0);
  v7 = (int *)a1[5];
  if ( v7 )
  {
    v8 = v7[1];
    v9 = v7[2];
    v26[10] = *v7;
    v26[11] = v8;
    v26[12] = v9;
  }
  _android_log_print(4, "FindMyDex", "Can you shake your phone 100 times in 10 seconds?");
```

```
data/data/com.a.sample.findmydex/files/classes.dex
data/data/com.a.sample.findmydex/files/classes.dex
/data/data/com.a.sample.findmydex/files/odex/
/data/data/com.a.sample.findmydex/files/odex/
```