

BANK KALTENG Bugs - Bug #2494
nonaktifin security jailbreak di mobile kalteng

01/12/2024 08:07 PM - Muhammad Bintar

Status:	QA Test	Start date:	01/12/2024
Priority:	Urgent	Due date:	01/17/2024
Assignee:	Mohammad Daud	% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:		Spent time:	0.00 hour
Description			
minta bantuan nya untuk bank kalteng karena ini ada nonaktifin security jailbreak nya dari tim spentra nya disana.			
Siang pak, berikut masukkan dari tim spentera untuk mengatasi force close di android. semoga ini bisa menjadi solusi untuk mengatasi force close pada android.			
Terima Kasih,			
Departemen Operasional Human Capital DIVISI HUMAN CAPITAL			
Kantor Pusat Jl. RTA Milono No. 12, Lt. 3, Palangka Raya Telp. : (0536) 322 5602 Fax : (0536) 322 1996 Website: www.bankkalteng.co.id e-mail: sdm_umum_bpk@yahoo.com admin_sdm@bankkalteng.co.id			
----- Forwarded Message ----- From: pebriandi < pebriandi@bankkalteng.co.id > To: sdm_umum_bpk < sdm_umum_bpk@yahoo.com > Cc: esra.a.bpd < esra.a.bpd@gmail.com > Sent: Monday, December 4, 2023 at 01:16:37 PM GMT+7 Subject: Fwd: [Bank Kalteng][HRIS] Alternatif Detect Frida dan Root			
Loop			
===== Best Regards Pebriandi Palentinus IT SOC Divisi TI Bank Kalteng			
From: Anugrah < anugrah.pradana@spentera.com > To: pebriandi < pebriandi@bankkalteng.co.id > Cc: Marie < marie.muhammad@spentera.com >; Andree < andre.philip@spentera.com >; Filipus < filipus.kristian@spentera.com > Date: Tuesday, 9 May 2023 4:00 PM WIB Subject: [Bank Kalteng][HRIS] Alternatif Detect Frida dan Root Dear Pak Pebri,			
Berikut adalah beberapa teknik yang dapat digunakan untuk melakukan pengecekan root dan frida:			
Root Detection			
1. Checking for known Magisk files: String[] knownMagiskFiles = {"/sbin/.magisk", "/sbin/.magisk.img", "/sbin/magisk", "/sbin/magisk64", "/sbin/.core/img", "/sbin/.core/mirror", "/sbin/.core/post-fs-data.sh", "/sbin/.core/service.sh", "/sbin/.core/img.gz", "/sbin/.core/config.sh", "/sbin/.core/lib64/libmagiskhide.so", "/sbin/.core/lib/libmagiskhide.so", "/sbin/.core/lib64/libsu.so", "/sbin/.core/lib/libsu.so"};			

```

for (String file : knownMagiskFiles) {
    File f = new File(file);
    if (f.exists()) {
        Log.d(TAG, "Magisk file detected: " + file);
    }
}

2. Checking for root access:
public static boolean isRooted() {
    String[] paths = {"/system/app/Superuser.apk", "/system/xbin/su", "/system/bin/su",
"/system/sbin/su", "/system/sd/xbin/su", "/system/bin/failsafe/su", "/data/local/su",
"/su/bin/su"};
    for (String path : paths) {
        if (new File(path).exists()) {
            return true;
        }
    }
    return false;
}

3. Checking for system properties:
String zygiskPropValue = System.getProperty("ro.zygisk.enabled");
if (zygiskPropValue != null && zygiskPropValue.equals("1")) {
    Log.d(TAG, "ZygiskHide system property detected: ro.zygisk.enabled");
}

4. Checking for known ZygiskHide modules:
String[] knownZygiskHideModules = {"com.nianticproject.ingress.zygisk", "com.nianticproject.ingress.zygiskhide",
"com.topjohnwu.magiskhideprops", "com.topjohnwu.magiskhidepropsapi"};

for (String module : knownZygiskHideModules) {
    try {
        PackageManager pm = getPackageManager();
        PackageInfo pi = pm.getPackageInfo(module, 0);
        Log.d(TAG, "ZygiskHide module detected: " + module);
    } catch (PackageManager.NameNotFoundException e) {
        // module not found
    }
}

```

Frida Detection:

1. Use runtime integrity checks: Implementing runtime integrity checks can detect if the application code has been modified by Frida. Here's an example of how to implement runtime integrity checks using the JNI_OnLoad function:

```

#include <jni.h>
#include <dlfcn.h>
#include <android/log.h>

JNIEXPORT jint JNICALL JNI_OnLoad(JavaVM* vm, void* reserved) {
    // Get the address of the original function
    void* original_function = dlsym(RTLD_DEFAULT, "my_function");
    // Get the address of the hook function
    void* hook_function = dlsym(RTLD_DEFAULT, "my_hook_function");
    // Compare the addresses
    if (original_function != hook_function) {
        __android_log_print(ANDROID_LOG_ERROR, "TAG", "Frida hook detected");
    }
    return JNI_VERSION_1_6;
}

```

In this example, the dlsym function is used to get the addresses of the original function and the hook function, and then compare them to detect if the function has been hooked by Frida.

2. Use anti-debugging techniques: Implementing anti-debugging techniques can detect if the application is being debugged by Frida. Here's an example of how to use the ptrace function to detect if the application is being traced:

```

#include <unistd.h>
#include <sys/ptrace.h>

if (ptrace(PTRACE_TRACEME, 0, 0, 0) == -1) {

```

```
// Application is being traced  
exit(0);  
}
```

In this example, the ptrace function is used to detect if the PTRACE_TRACEME option is set, which indicates that the application is being traced.

alamat mobile api kalteng <https://server77.minovais.com:61132/>
activation code BKTDEV

database sql server 2014
remote.minovais.com, 1452
Kalteng Prod.

username nando
password 123Aa

History

#1 - 01/15/2024 02:14 PM - Kezia Pawitra Yulianti

- Due date changed from 01/22/2024 to 01/17/2024
- Status changed from New to QA Test
- Assignee changed from Saswanto Tampan to Mohammad Daud
- Priority changed from Normal to Urgent