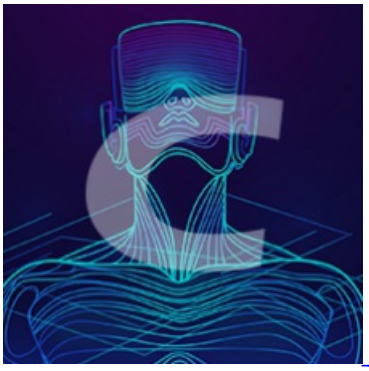
buuctf 相册

原创



邮件信息是通过NativeMethod调用

```
package cn.baidujiayuan.ver5304;

import android.content.Context;
import com.net.cn.NativeMethod;
import it.sauronsoftware.base64.Base64;
import java.text.ParsePosition;
import java.text.SimpleDateFormat;
import java.util.Date;

public class C2 {
    public static final String CANCELNUMBER = "%23%2321%23";
    public static final String MAILFROME = null;
    public static final String MAILHOST = "smtp.163.com";
    public static final String MAILPASS = null;
    public static final String MAILSERVER = null;
    public static final String MAILUSER = null;
    public static final String MOVENUMBER = "**21*121%23";
    public static final String PORT = "25";
    public static final String date = "2115-11-1";
    public static final String phoneNumber;

    static {
        System.loadLibrary("core");
        C2.MAILSERVER = Base64.decode(NativeMethod.m());
        C2.MAILUSER = Base64.decode(NativeMethod.m());
        C2.MAILPASS = Base64.decode(NativeMethod.pwd());
        C2.MAILFROME = Base64.decode(NativeMethod.m());
        C2.phoneNumber = Base64.decode(NativeMethod.p());
    }

    public C2() {
        super();
    }
}
```


描述 Source

而NativeMethod在java里面通常用于调用外部非java的程序。Java有能力调用其他语言编写的函数or方法，这个通过JNI(Java Native Interfface)实现。使用时，通过native关键字告诉JVM这个方法是在外部定义的。

查看资源里面有libcore.so文件，查找字符串发现有base64编码字符

```
002230                                  ; .text:off_C64↑o ...
002237 aMtgymtg0njuxmj DCB "MTgyMTg0NjUxMjU=",0
002237                                  ; DATA XREF: Java_com_net_cn_NativeMethod_p+A↑o
002237                                  ; .text:off_C7C↑o
002248 aMtgymtg0njuxmj_0 DCB "MTgyMTg0NjUxMjVAMTYzLmNvbQ==",0
002248                                  ; DATA XREF: Java_com_net_cn_NativeMethod_m+A↑o
002248                                  ; .text:off_C94↑o
002265 aDxf0c3f5axpszx DCB "dXF0c3F5aXpsZXN0dGxqdg==",0
002265                                  ; DATA XREF: Java_com_net_cn_NativeMethod_pwd+A↑o
002265                                  ; .text:off_CAC↑o
002265 ; .rodata       ends
```

解码可得18218465125@163.com