

# Godfather Android Banking Trojan Technical Analysis

---

 brandefense.io/blog/godfather-android-banking-trojan/

August 17, 2023

This is the open version of **Godfather Android Banking Trojan Technical Analysis**.  
If you want to download it as a PDF [click here](#).

## Executive Summary

---

Godfather stands out among malicious Android software as a significant threat. This malware targets financial and personal information, endangering users' security. Key characteristics of Godfather include:

- **Objective and Threat:** Godfather aims to seize users' financial account information, identity data, and personal details. It can jeopardize users' security, leading to financial losses and identity theft.
- **Operational Mechanism:** Utilizing keylogging, Godfather monitors users' keystrokes, stealing entered data and tracking user interactions.
- **Distribution Methods:** This malware often spreads through fake applications or malicious websites. It increases infection risks by luring users into traps with deceptive content.
- **Data Transmission:** Godfather can transmit captured data to a command and control server.

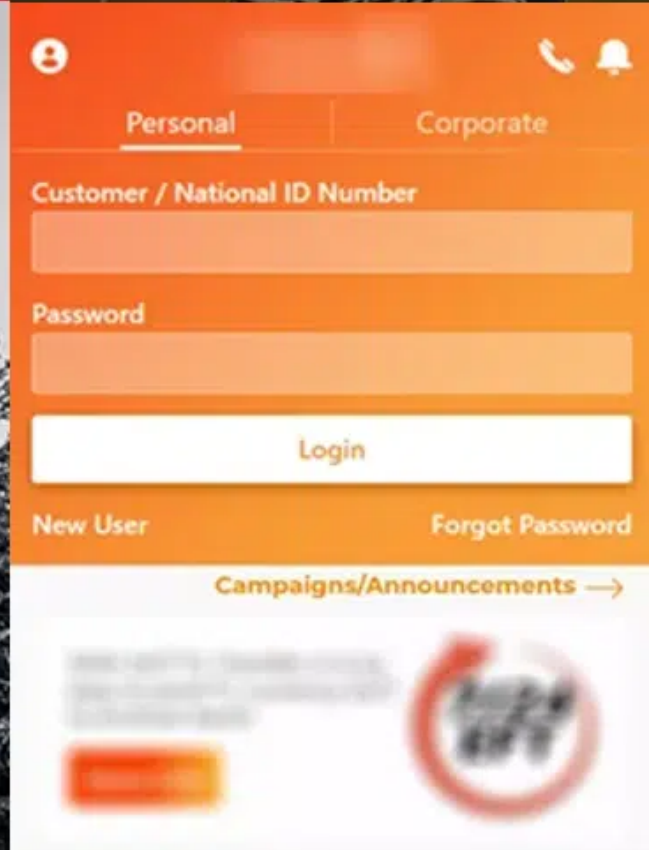
## Before the Analysis

---

### Godfather Trojan Activity Targeting Financial Sector Detected

---

The Group-IB Threat Intelligence team detected that the Godfather Android banking trojan targeted more than 400 international financial companies between June 2021 and October 2022. Half of the targeted financial companies are banks, and the other half are cryptocurrency wallets and exchanges. The Godfather's targets include 49 US-based companies, 31 Turkish-based companies, and 30 Spanish-based companies. Financial service providers in Canada, France, Germany, England, Italy, and Poland are among the hardest-hit companies. [\[Read More\]](#)




Fake Web Pages Imitating Mobile Banking Applications Serving in Turkey  
Some activities that Godfather trojan software performs on infected systems;


- Recording the device's screen

- Creating VNC connections
- Capturing keystrokes (keylogging)
- Leaking push notifications and SMS messages (to bypass 2FA)
- Send SMS messages
- Forward calls
- Execute USSD requests
- Start proxy servers
- Enabling silent mode
- Establishing WebSocket connections


Last 9 months, Godfather Trojan activities have been activated again, especially in Turkey. This time attackers mainly have used music apps to infect the victims of the android trojan, Godfather.



**Müzik**  
com.competitively.untown  
🕒 2023-08-06 5:56:38  
▶ 2023-08-06 5:56:55  
version: 1.2 #12




**Müzik indir**  
com.hltcorp.ches  
🕒 2023-07-04 9:27:09  
▶ 2023-08-03 9:28:15  
version: 1.1 #11




**Elen Müzik**  
com.hithink.scannerhd  
🕒 2023-04-06 7:44:36  
▶ 2023-06-09 11:19:07  
version: 1 #1




**MELO Müzik**  
com.Project100Pi.themusicplayer  
🕒 2023-03-07 12:08:37  
▶ 2023-06-15 15:16:29  
version: 1 #1




**MYT Müzik**  
com.revolut.business  
🕒 2022-12-28 9:38:28  
▶ 2023-03-26 14:44:47  
version: 1.1.0 #1




**Pi Müzik**  
com.style.sticker  
🕒 2023-03-25 11:45:36  
▶ 2023-05-14 16:35:45  
version: 2 #2




**Tubazy**  
com.indiefy.distribution  
🕒 2023-02-09 17:00:23  
▶ 2023-03-01 14:09:27  
version: 1 #1



**Retro Müzik**  
com.frolo.musp  
🕒 2023-03-19 13:43:38  
▶ 2023-05-14 16:34:19  
version: 4.0 #4



**Zuzu**  
com.stitcher.app  
🕒 2023-02-14 11:38:39  
▶ 2023-04-25 20:08:36  
version: 1.5.0 #54



**Mar Müzik**  
com.simplemobiletools.smsmessenger  
🕒 2023-01-19 9:39:38  
▶ 2023-05-16 15:40:37  
version: 1 #1

## Technical Analysis

---

Godfather malware requires the following permissions.

### Permission List

- android.permission.ACCESS\_NETWORK\_STATE
- android.permission.ACCESS\_WIFI\_STATE
- android.permission.BIND\_ACCESSIBILITY\_SERVICE
- android.permission.FOREGROUND\_SERVICE
- android.permission.INTERNET
- android.permission.POST\_NOTIFICATIONS
- android.permission.QUERY\_ALL\_PACKAGES
- android.permission.READ\_PHONE\_STATE
- android.permission.READ\_PRIVILEGED\_PHONE\_STATE
- android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS
- android.permission.WAKE\_LOCK

With the permissions given above, the malware in question is able to perform the following actions:

- Internet access
- Ability to use Accessibility service
- Installing application
- Access notifications
- Running as a foreground service

Upon execution, the malware requests activation of its accessibility service under the name of “Müzik”. It is observed that the malware uses accessibility rights to press buttons on the screen, read user inputs such as user clicks, run applications, and monitor what users have typed in a certain text field.

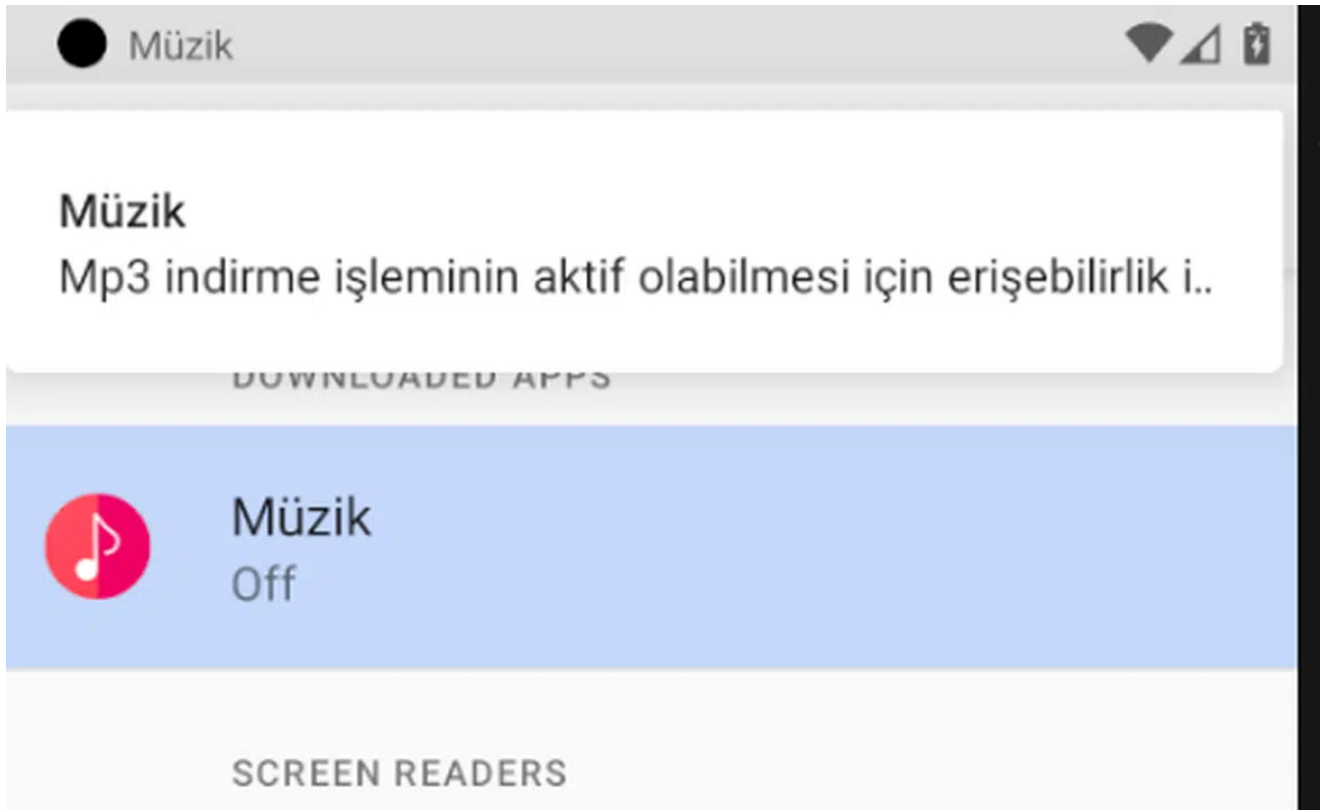


Figure 1: Accessibility service request

## Anti-Analysis Techniques

The malware uses the encrypted strings at runtime by decrypting them using the blowfish algorithm. (secret key: 67d45d2f64)

```

import android.util.Base64;
import java.nio.charset.StandardCharsets;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.SecretKeySpec;

/* compiled from: AnnotationHttp.java */
/* loaded from: classes.dex */
public class foetuses {
    static byte[] b;

    public static String Crypto(String enc) throws NoSuchPaddingException, NoSuchAlgorithmException, InvalidKeyException, IllegalBlockSizeException, BadPaddingException {
        Cipher cip = Cipher.getInstance(new String(Base64.decode("Qmxvd2Zpc2g".getBytes(StandardCharsets.UTF_8), 0)));
        cip.init(2, new SecretKeySpec("67d45d2f64".getBytes(), new String(Base64.decode("Qmxvd2Zpc2g".getBytes(StandardCharsets.UTF_8), 0)));
        return new String(cip.doFinal(Base64.decode(enc, 0)));
    }

    public static String getStr(String string) {
        try {
            return Crypto(string);
        } catch (Exception e) {
            return null;
        }
    }
}

```

Figure 2: Accessibility service request

It gets the command control address with the encrypted string in the description of a telegram account. This method is also often used by other malware.

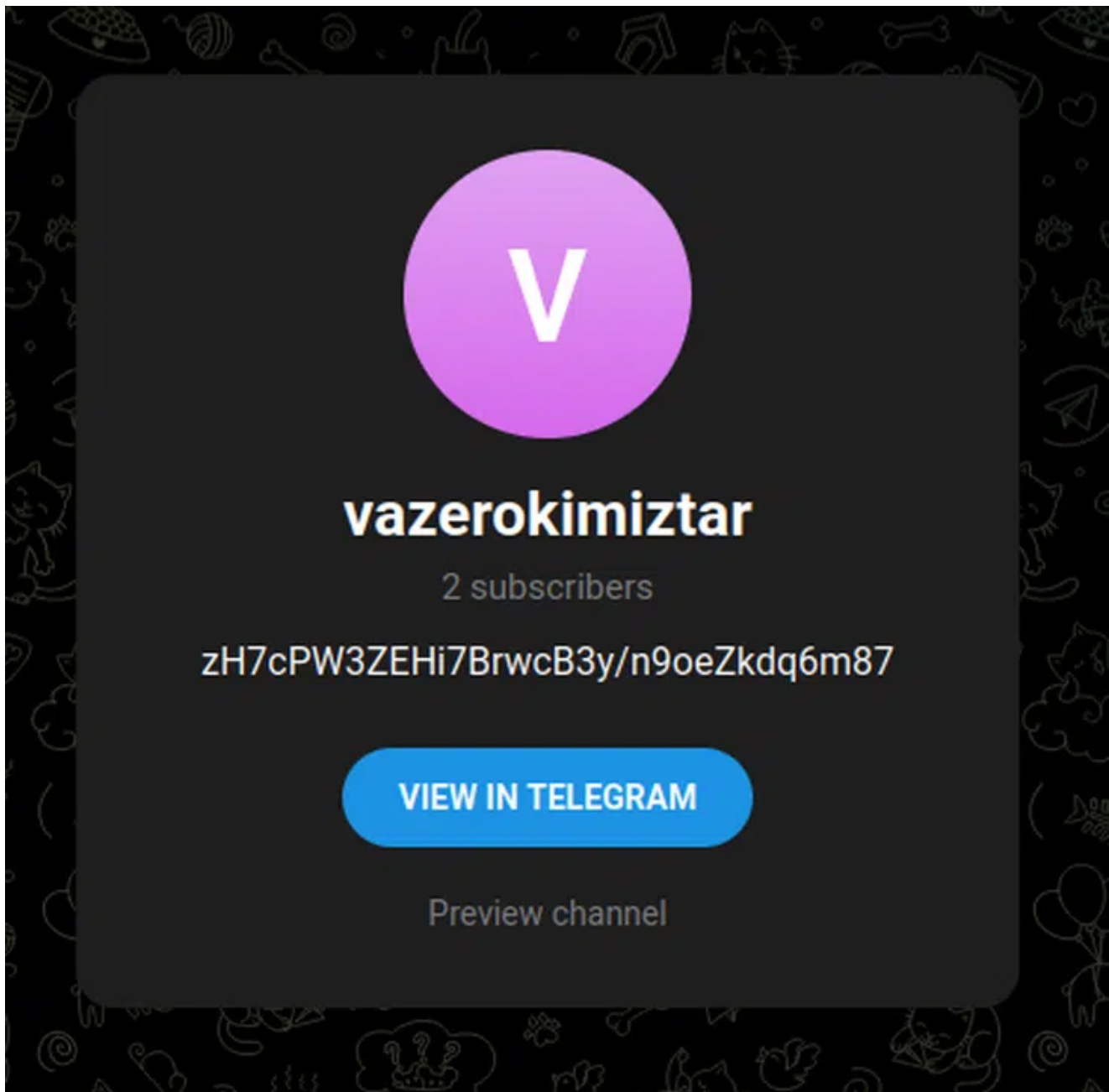


Figure 3: Telegram Description

Again, it uses blowfish to decrypt this encrypted string.(key:ABC, IV:abcdefgh)

```

02D88235 test eax, eax
02D88237 je 2D88285
02D88239 push 40
02D8823B push 1000
02D88240 mov eax, dword ptr ss:[ebp+8]
02D88243 mov eax, dword ptr ds:[eax+4]
02D88246 push dword ptr ds:[eax+9]
02D88249 push 0
02D8824E mov eax, dword ptr ss:[ebp+8]
02D8824F call dword ptr ds:[eax+24]
02D88251 mov dword ptr ss:[ebp-8], eax
02D88254 and dword ptr ss:[ebp-C], 0
02D88258 push 0
02D8825A lea eax, dword ptr ss:[ebp-C]
02D8825D push eax
02D8825E push dword ptr ss:[ebp-8]
02D88261 mov eax, dword ptr ss:[ebp+8]
02D88264 mov eax, dword ptr ds:[eax+4]
02D88267 push dword ptr ds:[eax]
02D88269 push dword ptr ss:[ebp-4]
02D8826C call 2D8828A
02D88271 add esp, 14
02D88274 mov eax, dword ptr ss:[ebp-8]
02D88277 mov dword ptr ss:[ebp-4], eax
02D8827A mov eax, dword ptr ss:[ebp+8]
02D8827D mov eax, dword ptr ds:[eax+4]
02D88280 mov ecx, dword ptr ss:[ebp-C]
02D88283 mov dword ptr ds:[eax], ecx
02D88285 jmp dword ptr ss:[ebp-4]
02D88288 leave
049A0000 jmp 49A0005
049A0002 ret C
049A0005 push ebp
049A0006 mov ebp, esp
049A0008 sub esp, 1000
049A000E mov dword ptr ss:[ebp-40], E2D
049A0015 mov dword ptr ss:[ebp-58], naber.400000
049A001C lea eax, dword ptr ss:[ebp-80]
049A0022 push eax
049A0023 lea eax, dword ptr ss:[ebp-2C]
049A0026 push eax
049A0027 lea eax, dword ptr ss:[ebp-68]
049A002A push eax
049A002B call 49A092B
049A0030 add esp, C
049A0033 call 49A003C
049A0038 add byte ptr ds:[eax], a1
049A003A add byte ptr ds:[eax], a1
049A003C pop eax
049A003D mov dword ptr ss:[ebp-94], eax
049A0043 mov eax, dword ptr ds:[eax]
049A0045 test eax, eax
049A0047 je 49A004C
049A0049 leave
049A004A jmp eax
049A004C call 49A0A3F
049A0051 mov eax, dword ptr ss:[ebp-94]
049A0057 mov ecx, dword ptr ss:[ebp-40]
049A005A lea eax, dword ptr ds:[ecx+eax-38]
049A005E mov dword ptr ss:[ebp-8], eax

```

Figure 3: Jump to the extracted malware payload

## Application Runtime

Godfather malware retrieves the list of target applications from the command and control server.

The screenshot shows a network traffic analysis tool interface. On the left, a request is shown as a POST to /j.php. On the right, the response is shown as HTML content. The response body contains a long list of application package names (APKs) targeted by the malware, including:

- com.paypal.android.p2pmobile
- com.paypal.merchant.client
- com.tideplaf
- com.amazon.mShop.android.shopping
- com.amazon.sellermobile.android
- com.ebay.mobile
- com.netflix.mediaservice
- com.uberab
- com.uberab.eats
- com.whatsapp
- com.facebook.orca
- com.instagram.android
- com.mobilium.papara
- de.indiba.bankingapp
- de.postbank.bestsign
- de.santander.presentation
- com.starfinanz.smob.android.sfinanzstatus
- de.fiducia.smartphone.android.banking.vr
- com.targo\_prod.bad
- com.db.mm.norisbank.eu.unicreditgroup.hvobaplan
- de.comsofinanz.onlinenbanking
- com.vifs.Banking.de.number20.android.de.condirect.android.de.comerbanking.mobil
- de.comsofinanz.onlinenbanking
- com.db.pwcc.dbmobile.de.dkb.portalapp.com.centralway.numbers.de.condirect.app.de.postbank.finanzassistent.com.db.pbc.mabanca.de.sdvzr.ihb.mobile.secureapp.sparda.produktion.de.traktorpoll.cgd.pt.caixadirectparticulares.com.bankinter.empresas.com.bankinter.launcher.com.bbva.bbvacontigo.com.bbva.netcash.com.cajasur.android.com.db.pbc.DBPay.com.imaginbank.app.com.indra.itecban.mobile.novobanco.com.kutxabank.android.com.rsi.com.tecnocom.cajalaboral.es.re.dsys.walletm.app.laboralkutxa.pro.es.ceca.cajalnet.es.avobanco.bancamovil.es.ibercaja.ibercajapp.es.lacaja.mobile.android.newapi.com.es.openbank.mobile.es.bancosantander.app.gt.com.bi.bienlinea.es.bancosantander.empresas.com.grupocajamar.wefferent.com.cajaingenieros.android.bancamovil.com.mediolanum.com.rsi.Colony.com.targoes\_prod.bad.es.caixagalicia.activamovil.es.casxaontinent.casxaontinentapp.es.cecabank.es.lia209lappstore.es.pibank.customers.es.santander.criptoculadora.es.unica.abanco.app.www.indirect.netviewframe.com.boursorama.android.clients.com.caissepargne.android.mobilebanking.com.IndirectAndroid.fr.banquepopulaire.cyberplus.fr.creditagricole.androidapp.mobi.societegenerale.mobile.lappli.net.bnpparibas.mescomptes.com.cn.prod.bad.com.anabaque.fr.com.octo.cdn.activity.creditdunord.fr.lcl.android.customerarea.com.fullsix.android.labanquepostale.accountaccess.com.arkea.android.application.cmb.com.creditcoop.android.mobilebanking.fr.lcl.android.entreprise.fr.hsbc.hsbcfrance.fr.bred.fr.com.mootwin.natixis.fr.bnpparibasentreprise.android.fr.bnpp.digitalbanking.com.cibc.android.mobil.com.td.com.rbc.mobile.android.ca.bnc.android.com.desjardins.mobile.com.scotiabank.banking.com.bmo.mobile.com.bmo.business.mobile.ca.hsbc.hsbcCanada.ca.affinitvcu.mobile.ca.manulife.Mobil

Figure 4: Targeted Apps

Unlike other malware (eg cerberus, hook, ermac), the malware steals information by keylogging instead of using an overlay attack.

```

return;
try {
label_563:
if (novitiate.Annora(((Context)v1), v6).contains(((CharSequence)v5))) {
goto label_589;
}
sorite.Lockering = sorite.Lockering + v7 + arg17.getPackageName().toString() + v4 + sorite.filtrates + foetuses.getStr("j/02K3Y8AC87ndFHpFCKXA==") + ((AccessibilityRecord)arg17).getText().toString() + v2;
return;
} catch (Exception v0_3) {
}
try {
label_589:
if (novitiate.Annora(((Context)v1), v6).contains(((CharSequence)v5))) {
goto label_615;
}
sorite.Lockering = sorite.Lockering + v7 + arg17.getPackageName().toString() + v4 + sorite.filtrates + foetuses.getStr("io/Ydc47dh1BjP0yN8EMLA==") + ((AccessibilityRecord)arg17).getText().toString() + v2;
return;
} catch (Exception v0_3) {
}
try {
label_615:
if (novitiate.Annora(((Context)v1), v6).contains(((CharSequence)v5))) {
goto label_641;
}
sorite.Lockering = sorite.Lockering + v7 + arg17.getPackageName().toString() + v4 + sorite.filtrates + foetuses.getStr("Ncq5nLcQ1/07ndFHpFCKXA==") + ((AccessibilityRecord)arg17).getText().toString() + v2;
return;
} catch (Exception v0_3) {
}
}

```

[[CLICKED]]

[[TEXT]]

[[FOCUSED]]

Figure 5: Keylogger

```

Unuttum{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|
[(TextView)]DEVAM{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|[(TextView)]HEMEN BAÄ•
vUR{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|[(TextView)]MÄÄ•teri
NumaranÄ±z{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|[(TextView)]Ä•
ifreniz{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|[(TextView)]Ä•ifremi
Unuttum{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|[(TextView)]KullanÄ±cÄ±
qdÄ±nÄ±z{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|
[(TextView)]DEVAM{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:02 PM|[(WINDOW)][Ziraat Mobile]
{line}Package:com.android.launcher3|Time: Aug 10, 2023 6:19:02 PM|[(WINDOW)][Recent apps]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:03 PM|[(FOCUSED)][T.C. Kimlik / MÄÄ•teri
NumaranÄ±z]{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:05 PM|[(TEXT)][1]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:05 PM|[(TEXT)][12]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:05 PM|[(TEXT)][123]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:06 PM|[(TEXT)][12312]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:06 PM|[(TEXT)][123124]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:06 PM|[(TEXT)][12312412]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:07 PM|[(TEXT)][123124123]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:07 PM|[(TEXT)][12312412312]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:07 PM|[(FOCUSED)][Ä•ifreniz]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:07 PM|[(TEXT)][1Ä•ç]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:07 PM|[(TEXT)][Ä•ç2Ä•ç]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:07 PM|[(TEXT)][Ä•çÄ•çÄ•ç1Ä•ç]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:08 PM|[(TEXT)][Ä•çÄ•çÄ•çÄ•ç2Ä•ç]
{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:08 PM|[(TextView)]GirdiÄ•iniz bilgiler
hatalÄ±dÄ±r. LÄ±tfen bilgilerinizi kontrol ederek tekrar deneyiniz.{line}Package:com.ziraat.ziraatmobil|Time:
Aug 10, 2023 6:19:08 PM|[(TextView)]TAMAM{line}Package:com.ziraat.ziraatmobil|Time: Aug 10, 2023 6:19:08 PM|
[(WINDOW)][Hata, GirdiÄ•iniz bilgiler hatalÄ±dÄ±r. LÄ±tfen bilgilerinizi kontrol ederek tekrar deneyiniz.,
TAMAM]

```

Figure 6: Keylogger output

## Targeted Applications

- com[.]tmobtech.halkbank
- com[.]vakifbank.mobile
- com[.]ziraat.ziraatmobil
- com[.]akbank.android.apps.akbankdirekt
- com[.]anadolubank.android
- com[.]fibabanka.Fibabanka.mobile
- tr.com[.]sekerbilisim.mbank
- com[.]teb
- com[.]teb.kurumsal
- com[.]pozitron.iscep



- com[.]ykb.android
- tr[.]com[.]abank.dijital
- com[.]a2a.android.burgan
- com[.]denizbank.mobildeniz
- com[.]garanti.cepsubesi
- com[.]ingbanktr.ingmobil
- com[.]magiclick.odeabank
- com[.]finansbank.mobile.cepsube
- finansbank[.]enpara
- finansbank[.]enpara.sirketim
- com[.]kuveytturk.mobil
- com[.]ziraatkatilim.mobilebanking
- com[.]tffb
- com[.]albarakaapp
- com[.]aktifbank.nkolay
- com[.]fibabanka.mobile
- com[.]ininal.wallet
- com[.]intertech.mobilemoneytransfer.activity
- com[.]isbank.isyerim
- com[.]kuveytturk.yourbank
- com[.]mobillium.papara
- com[.]pttfinans
- com[.]turkcell.paycell
- com[.]vakifkatilim.mobil
- paladyum[.]peppara
- tr.com[.]hsbc.hsbcturkey.uk
- tr.com[.]param.android

---

## Conclusion

---

Godfather represents a serious instance of malicious software, carrying risks like financial loss and personal privacy breach. Users need to enhance their cybersecurity awareness and download from reputable sources.

| You can find [the IoCs](#) on our [GitHub repo](#).