



Threat Research Center > Threat Research > Malware

MALWARE

TeleRAT: Another Android Trojan Leveraging Telegram’s Bot API to Target Iranian Users

🕒 9 min read

RELATED PRODUCTS

-  Advanced WildFire
-  Cortex XDR

By: Ruchna Nigam , Kyle Wilhoit
Published: March 20, 2018
Categories: Malware , Threat Research
Tags: Android , Iran , IRRAT , Telegram’s Bot API , TeleRAT

Share 

This post is also available in: [日本語 \(Japanese\)](#)

Summary

Telegram Bots are special accounts that do not require an additional phone number to setup and are generally used to enrich Telegram chats with content from external services or to get customized notifications and news. And while Android malware abusing **Telegram’s Bot API** to target Iranian users is not fresh news (the emergence of a Trojan using this method called IRRAT was discussed in **June** and **July** 2017), we set out to investigate how these Telegram Bots were being abused to command and control malicious Android applications.

This blog details our findings navigating through some Operational Security (OPSEC) fails while sifting through multiple malicious APK variants abusing Telegram’s Bot API; including the discovery of a new Trojan we’ve named “TeleRAT”. TeleRAT not only abuses Telegram’s Bot API for Command and Control (C2), it also abuses it for data exfiltration, unlike IRRAT.

What We Already Know- IRRAT

Based on previous reports, we know Telegram’s Bot API was already being employed by attackers to steal information ranging from SMS and call history to file listings from infected Android devices. The majority of the apps we saw disguise themselves as an app that tells you how many views your Telegram profile received – needless to say, the information provided is inaccurate as Telegram doesn’t allow for populating any such information. We continue to see IRRAT active in the wild to this date. We used the below sample for this analysis.

SHA256	1d0770ac48f8661a5d1595538c60710f886c254205b8cf517e118c94b256137d
--------	--

TeleRAT works by creating and then populating the following files on the phone’s SD Card and sending them to the upload server, after the app’s first launch:

- “[IMEI] numbers.txt”: Contact information
- “[IMEI]acc.txt”: List of Google accounts registered on the phone
- “[IMEI]sms.txt”: SMS history
- 1.jpg: Picture taken with the front-facing camera
- Image.jpg: Picture taken with back-facing camera

RELATED ARTICLES

Beware of BadPack: One Weird Trick Being Used Against Android Devices

Leveraging a Hooking Framework to Expand Malware Detection Coverage on the Android Platform

Android Malware Impersonates ChatGPT-Themed Applications

In the background, the app continues to beacon to the Telegram bot at regular intervals and listens for certain commands, as detailed below.

Command	Action	Communication to Telegram bot
call@[IMEI]@[Number]	Places a call to [Number]	hxxps://api.telegram.org/bot[APIKey]/sendmessage?chat_id=[ChatID]&text=call with <i>[Number]</i>
sms@[IMEI]@[Number]@[Text]	SMS [Text] to [Number]	hxxps://api.telegram.org/bot[APIKey]/sendmessage?chat_id=[ChatID]&text=sent
getapps@[IMEI]	Saves a list of installed apps to SD Card to file named “[IMEI] apps.txt”, uploads to upload server	None
getfiles@[IMEI]@[DirPath]	Retrieves file listing from [DirPath], saves to SD Card as “[IMEI]files.txt”, uploads to server	None
getloc@[IMEI]	Starts a GPS listener that monitors location changes	None
upload@[IMEI]@[FilePath]	Uploads file at [FilePath]	None
removeA@[IMEI]@[FilePath on SDCard]	Deletes file at [FilePath on SDCard]	https://api.telegram.org/bot[APIKey]/sendmessage?chat_id=[ChatID]&text=_____ [FilePath on SDCard]
removeB@[IMEI]@[DirPath on SDCard]	Deletes [DirPath on SDCard]	None
lstmsg@[IMEI]	Saves SMS history to SD Card as “[IMEI]lstmsg.txt”, uploads to server	None
yehoo@[IMEI]	Takes a picture with Front Camera, saves to SD Card as “yahoo.jpg”, uploads to server	None

Table 1: List of IRRAT bot commands

As the table above shows, this IRRAT sample makes use of Telegram's bot API solely to communicate commands to infected devices. The stolen data is uploaded to third party servers, several of which employ a webhosting service. Fortunately for us, these servers had several OPSEC fails. More on that further below.

A New Family- TeleRAT

While sifting through IRRAT samples, using AutoFocus, we came across another family of Android RATs seemingly originating from and/or targeting individuals in Iran that not only makes use of the Telegram API for C2 but also for exfiltrating stolen information.



Figure 1: pivoting in autofocus for applications using the Telegram bot API

We named this new family “TeleRAT” after one of the files it creates on infected devices. We used the below sample for this analysis.

Post-installation TeleRAT creates two files in the app’s internal directory:

- telerat2.txt containing a slew of information about the device - including the System Bootloader version number, total and available Internal and External memory size, and number of cores.
- thisapk_slm.txt mentioning a Telegram channel and a list of commands. We investigate this Telegram channel is greater detail further below.

The RAT announces its successful installation to the attackers by sending a message to a Telegram bot via the Telegram Bot API with the current date and time.
More interestingly, it starts a service that listens for changes made to the Clipboard in the background.

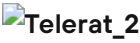


Figure 2: Code snippet that listens for clipboard changes

Finally, the app fetches updates from the Telegram bot API every 4.6 second, listening for the following commands (we used Google Translate for the below Farsi (Persian) translations):

Command	Translation
دریافت مخاطبین	Get contacts
دریافت کلیپ برد	Get the clipboard
Clipboard set:[text]	
دریافت مکان	Get location
دریافت اطلاعات شارژ	Receive charging information
All file list:[/path]	
Root file list:[/path]	
دریافت برنامه ها	Get apps
1Downloadfile:[/filename]	
2Downloadfile:[/filename]	
CreateContact:[/name]/[/number]	
SetWallpaper http[URL]	
دریافت پیام ها	Receive (SMS) messages
Sendsmsfor:[/destination]/[text]	
MessageShow[text]	
گرفتن عکس1	Take photo 1 (front camera)
گرفتن عکس2	Take photo 2 (back camera)
دریافت وضعیت	Get status
دریافت تماس ها	Receive calls
DeleteDir[dirname]	
سایلنت	Silent (set to Vibrate mode)
صدا دار	Loud (set to normal Ringer mode)

ضبط فیلم	Audio recording (saves recorded audio to AUDIO123/MUSIC/rec123.m4a on SD Card)
توقف ضبط فیلم	Stop audio recording
راهنمای دستورات	Instruction manual (Help Menu)
call to [number]	
RESET	(deletes thisapk_slm.txt and sends a new registration message to Telegram bot)
دریافت گالری	Get gallery (sends files from the /Dcim folder on the SD Card to Telegram bot)
Delete app files or دریافت گالری	
Vibrate [x]	(Causes phone to vibrate for x seconds, with a maximum value of 600 secs)
لرزش کم	Low vibration (for a duration of 150 secs)
لرزش متوسط	Medium vibration (350 secs)
لرزش زیاد	Shake too much (600 secs)

Table 2: List of TeleRAT bot commands

Aside from additional commands, this new family’s main differentiator to IRRAT is that it also uploads exfiltrated data using Telegram’s **sendDocument** API method.



Figure 3: Code snippet showing the use of the SendDocument Telegram bot API method

TeleRAT is an upgrade from IRRAT in that it eliminates the possibility of network-based detection that is based on traffic to known upload servers, as all communication (including uploads) is done via the Telegram bot API. However, it still leaves other doors open via Telegram’s bot API, since the API Keys are hardcoded in the APKs. The API allows fetching updates by two means:
1.The **getUpdates** method: Using this exposes a history of all the commands that were sent to the bot, including usernames from which the commands originated. From the bots that were still responding and had an update history (incoming updates are only kept for 24 hours as per Telegram’s policy), we were able to find bot commands originating from four Telegram accounts, shown below.



Figure 4: Telegram usernames revealed from bot command histories

2. Using a **Webhook**: Telegram allows redirecting all bot updates to a URL specified by means of a Webhook. Their policy limits these Webhooks to HTTPS URLs only. While most of the Webhooks we found used certificates issued by Let’s Encrypt with no specific registrar information, some of them led us back to the world of third party webhosting and open directories. Let’s Encrypt has been notified about this activity.

A sample of only a few Webhooks we found are shown below. `hxtps://mr-mehran[.]tk/pot/Bot/` in particular appears to be hosting close to 6500 bots, however, we can’t confirm whether they’re all used for malicious purposes.



Figure 5: Webhooks found associated with some TeleRAT bots

OPSEC Fails, Distribution Channels & Attribution



Figure 6: Image of botmaster testing out the RAT

We were also able to find exfiltrated messages that confirmed our theory about the test run and reveals a thread in Persian Farsi seemingly discussing bot setup.

“صبح ساعت ۶ آنلاین شو تا روباته رو امتحان کنیم”

Google Translation: “Morning 6 hours online to try the robotage”

While investigating attribution for TeleRAT, we noticed the developers made no effort to hide their identities in the code. One username is seen in the screenshot below.



Figure 7: Telegram channel advertised in source code

Looking further into the ‘vahidmail67’ Telegram channel, we found advertisements for applications and builders that ran the entire gamut - from applications that get you likes and followers on Instagram, to ransomware, and even the source code for an unnamed RAT (complete with a video tutorial, shown below).



Figure 8: Screenshot from a Telegram channel advertising & sharing a RAT source code

Aside from the Telegram channel, while looking for references to certain TeleRAT components we stumbled upon **some threads** on an Iranian programmers’ forum advertising the **sale** of a Telegram bot control library. The forum is frequented by some of the developers whose code is heavily reused in a big portion of the TeleRAT samples we came across.



Figure 9: Advertisement for sale of a Telegram bot control library

The forum goes the extra mile to mention all content is in accordance with Iran's laws. However, it's hard to see any non-malicious use for some of the code advertised there or written by developers that frequent it – for instance, a service that runs in the background listening for changes to the Clipboard (pictured in the code snippet in Figure 3 further above).



Figure 10: Forum Disclaimer

Overall, TeleRAT pieces together code written by several developers, however, due to freely available source code via Telegram channels and being sold on forums, we can't point to one single actor commanding either IRRAT or TeleRAT and it appears to be the work of several actors possibly operating inside of Iran.

Victimology

As we investigated these RATs, we also started looking at how victims were getting infected. Further investigating, we witnessed several third-party Android application stores distributing seemingly legitimate applications like "Telegram Finder", which supposedly helps users locate and communicate with other uses with specific interests, like knitting. Also, we've witnessed several samples distributed and shared via both legitimate and nefarious Iranian Telegram channels.

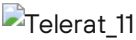


Figure 11: Ielranian third-party application store

Looking closer at the malicious APKs we were able to get an understanding of common application naming conventions and functionality across the board.



Figure 12: 'Telegram finder' application

Based on the samples we analysed, the three most common application names for both IRRATand TeleRAT are:

Native App Name	Translated App Name
پروفایل چکر	Profile Cheer

Additionally, there were several malicious APKs disguised as fake VPN software and/or configuration files, such as "atom vpn" and "vpn for telegram. There appears to be a total identified victim count of 2,293 at the time of writing, based on the infrastructure we analysed. There appears to be a rather small range of geographically dispersed victims, with 82% of having Iranian phone numbers.

Iran	1894
Pakistan	10
India	227
Afghanistan	109
United Kingdom	53

There may also be additional infrastructure or variants we were unaware of at the time of writing. That said, the number of victims likely residing within Iran far exceeds the victim count for any other country.

Conclusion

Part of dissecting and understanding new threats involve looking closer at already established campaigns and malware variants. This is a perfect example of just that; looking closer at a previously established malware family to better understand it's current and possibly changed capabilities. While malware leveraging the Telegram bot API is not necessarily new, we were able to identify a new family, TeleRAT, hiding entirely behind Telegram's API to evade network-based detection and exfiltrate data. Leveraging intelligence from AutoFocus, accessible attacker infrastructure, and other open source intelligence we were able to paint an accurate picture of an ongoing operation leveraging Telegram's API and targeting users via third party application sites and social media channels. Taking some basic precautions can help users protect themselves from malicious applications like TeleRAT, such as:

- Avoid third-party application stores or sources.
- Don't allow application sideloading on your device.
- Ensure the application you are installing is official, regardless of source.
- Closely review and scrutinize application permission requests prior to installation.

Palo Alto Networks customers are protected from this threat by:

- 1 WildFire detects all TeleRAT and IRRAT files with malicious verdicts.
- 2 AutoFocus customers can track these samples with the **IRRAT** and **TeleRAT**
- 3 Traps blocks all of the APK files associated with TeleRAT and IRRAT.

APPENDIX

Telegram usernames found commanding IRRAT or TeleRAT
Ahmad_ghob
My_LiFe_M_a_H_s_A
mmm1230a

Webooks

hxxps://gold.teleagent.ir/bnrdehisaz/index.php
hxxps://shahin-soori.ir/bots/rat/upload_file.php
hxxps://mbosoba.000webhostapp.com/upload_file.php
hxxps://abolking.000webhostapp.com/upload_file.php
hxxps://botmohsan-apk.000webhostapp.com/Bot/bot.php
hxxps://androydiha.ir/bot/Bot/hackelmi_bot/index.php
hxxps://hamidhamid954321.000webhostapp.com/Bot/bot.php
hxxps://mohsan024024.000webhostapp.com/upload_file.php
hxxps://09152104574nazimilad.000webhostapp.com/ربات ساز/CreateBotAll.php
hxxps://darkforceteam.000webhostapp.com/SmartAccounts_Bot/bots/Ratjadidebot/index.php

Back to top

TAGS

- Android
- Iran
- IRRAT
- Telegram's Bot API
- TeleRAT

<

Threat Research Center

Next: Sofacy Uses DealersChoice to Target European Government Agency

>

Related Malware Resources

C THREAT RESEARCH

IC

November 1, 2024

TA Phone Home: EDR Evasion Testing Reveals Extortion Actor's Toolkit

Extortion

Data exfiltration

Read now →

C THREAT RESEARCH

IC

October 9, 2024

Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Inst...

North Korea

Social engineering

Python

C THREAT RESEARCH

IC

October 1, 2024

Detecting Vulnerability Scanning Traffic From Underground Tools Using...

Machine Learning

Read now →

C THREAT ACTOR GROUPS

IC

September 26, 2024

Unraveling Sparkling Pisces’s Tool Set: KLogEXE and FPSpy

MITRE

Keylogger

North Korea

Read now →

Newsletter

Your Email

Subscribe for email updates to all Unit 42 threat research.
By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).



Products and services

Network Security Platform	Code to Cloud Platform
CLOUD DELIVERED SECURITY SERVICES	Prisma Cloud
Advanced Threat Prevention	Cloud-Native Application Protection Platform
DNS Security	
Data Loss Prevention	
IoT Security	
Next-Generation Firewalls	
Hardware Firewalls	
Strata Cloud Manager	
SECURE ACCESS SERVICE EDGE	
Prisma Access	
Prisma SD-WAN	
Autonomous Digital Experience Management	
Cloud Access Security Broker	
Zero Trust Network Access	
AI-Driven Security Operations Platform	Threat Intel and Incident Response Services
Cortex XDR	Proactive Assessments
Cortex XSOAR	Incident Response
Cortex Xpanse	Transform Your Security Strategy
Cortex XSIAM	Discover Threat Intelligence
External Attack Surface Protection	
Security Automation	
Threat Prevention, Detection & Response	

Company

About Us
Careers
Contact Us
Corporate Responsibility
Customers
Investor Relations
Location
Newsroom

Popular links

Blog
Communities
Content Library
Cyberpedia
Event Center
Manage Email Preferences
Products A-Z
Product Certifications
Report a Vulnerability
Sitemap
Tech Docs
Unit 42
Do Not Sell or Share My Personal Information