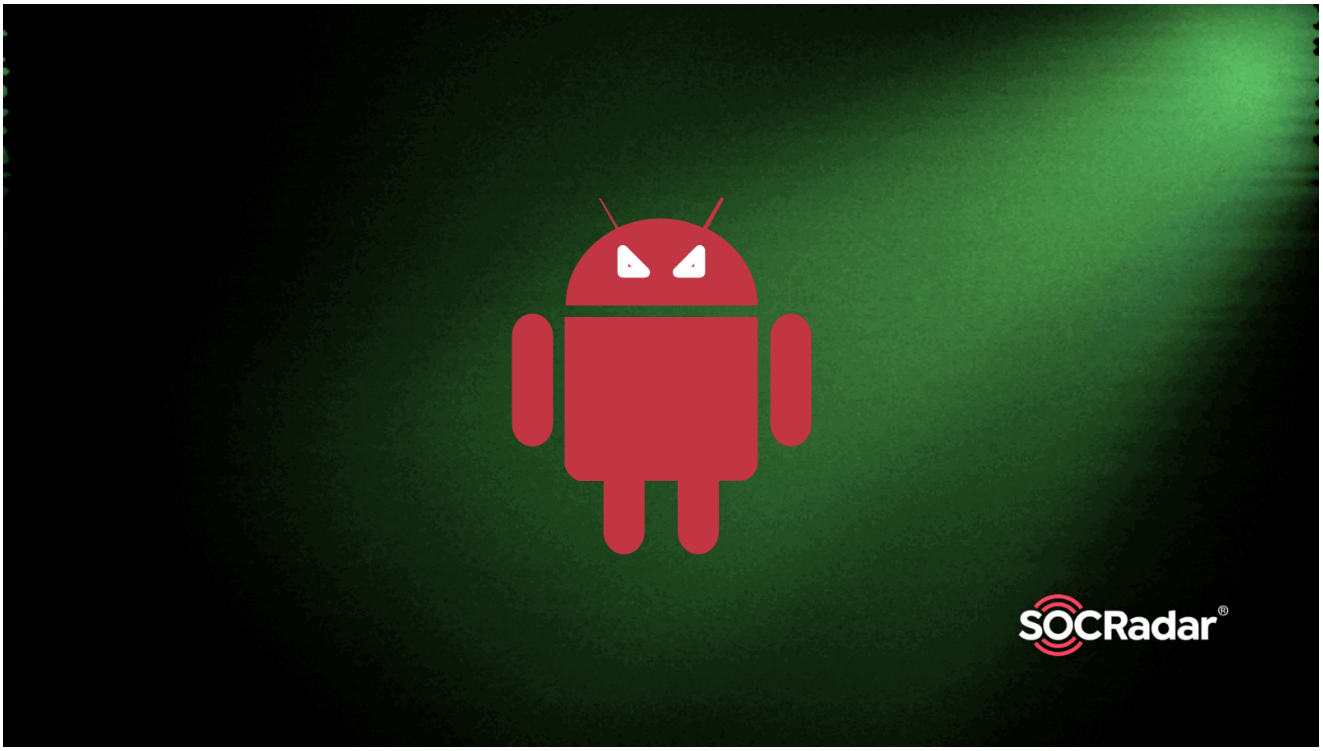
New Spyware RatMilad Targets Middle Eastern Mobile Devices

socradar.io/new-spyware-ratmilad-targets-middle-eastern-mobile-devices

October 6, 2022



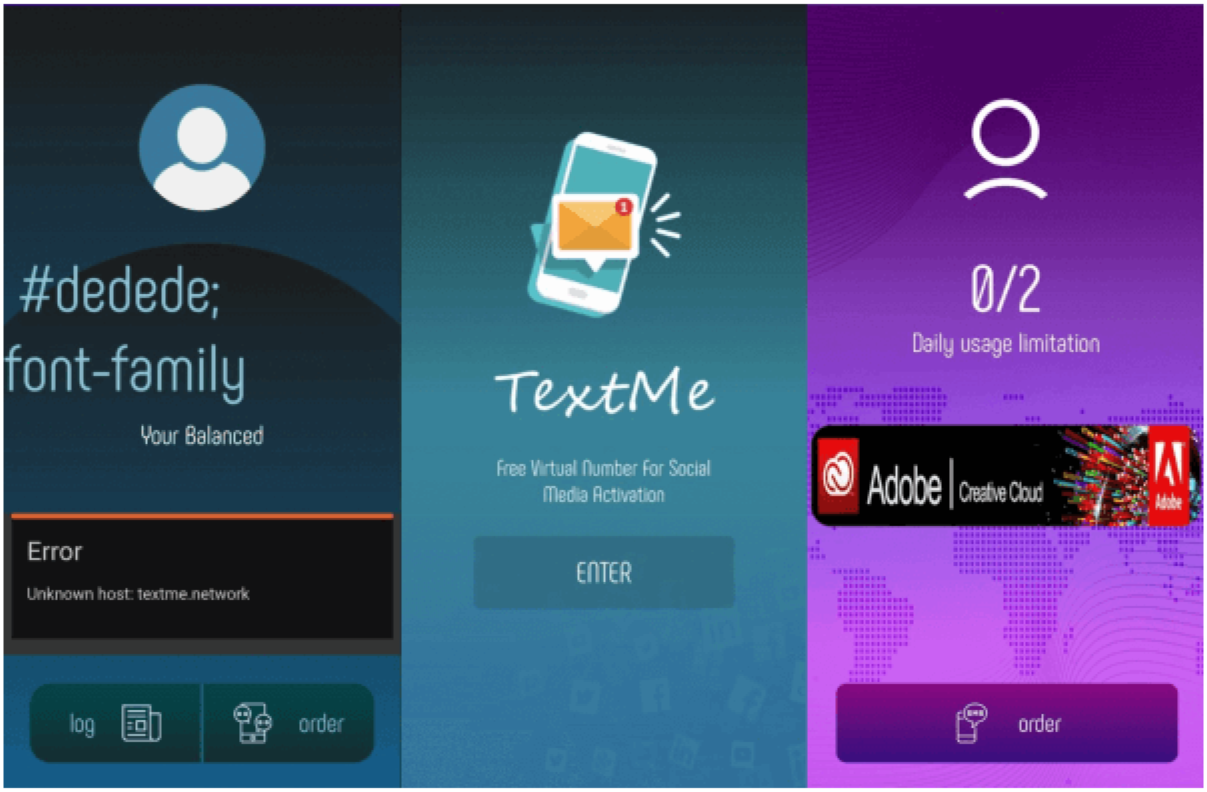
RatMilad, a newly discovered Android spyware, has been stealing data from **mobile devices** in the Middle East.

The malware is spread through links on social media and pretends to be applications for services like **VPN and phone number spoofing**. Unwary users download these trojan applications and grant access to malware.

Loader Applications

Trojan apps named **Text Me and NumRent** were seen sideloading the RatMilad spyware. The two apps claim to help verify social media accounts. They are unavailable on legitimate application stores like Google Play but distributed on Telegram.

With more than **200 external shares**, a post shared on a Telegram channel used to spread the malware sample has received over **4,700 views**.



RatMilad loader apps (Source: Zimperium)

Capabilities of the Malware

RatMilad performs as sophisticated spyware on compromised devices. It can be used for espionage, **extortion**, and victim-eavesdropping, according to mobile security company Zimperium.

The capabilities of spyware include the ability to receive and **execute commands** to gather and exfiltrate data and carry out a wide range of malicious operations, like:

- MAC Address of Device
- Contact List
- SMS List
- Call Logs
- Account Names and Permissions
- Clipboard Data
- GPS Location Data
- Sim Information – Mobile number, Country, IMEI, Sim state
- File list
- Read, write, and Delete Files
- Sound Recording
- File upload to C&C
- List of the installed applications, along with their permissions.
- Set new application permissions.

- Phone info – Model, Brand, buildID, android version, manufacturer

Who is Behind RatMilad?

Zimperium claims that RatMilad's operators obtained the **source code** from the AppMilad hacker group in Iran and combined it with a fraudulent app to trick people into downloading it.

Although it's uncertain how widespread the infections are, the cybersecurity firm claimed it found the spyware during an unsuccessful attempt to infiltrate a **customer's workplace device**.

According to Richard Melick, head of **mobile threat intelligence** at Zimperium, the RatMilad spyware, and the Iranian-based hacking group AppMilad show a changing environment impacting mobile device security.

RatMilad is only one of many mobile spyware options, including Pegasus and PhoneSpy, accessible from both legitimate and illegitimate sources.

Recommendations

Impacts of malicious mobile applications can be prevented with simple security tips:

- Beware of malicious links distributed online.
- Avoid downloading applications from untrusted sources.
- Check for application reviews and concerns on the internet.

RatMilad IoCs

Application Names:

com.example.confirmcode

- com.example.confirmcodf
- com.example.confirmcodg

C&C Servers:

- hxxp://textme[.]network
- api[.]numrent[.]shop

SHA-256 Hashes:

- 31dace8ecb943daa77d71f9a6719cb8008dd4f3026706fb44fab67815546e032
- 3da3d632d5d5dde62b8ca3f6665ab05aadbb4d752a3e6ef8e9fc29e280c5eb07
- 0d0dcc0e2eebf07b902a58665155bd9b035d6b91584bd3cc435f11beca264b1e
- 12f723a19b490d079bea75b72add2a39bb1da07d0f4a24bc30313fc53d6c6e42
- bae6312b00de73eb7a314fc33410a4d59515d56640842c0114bd1a2d2519e387
- 30e5a03da52feff4500c8676776258b98e24b6253bc13fd402f9289ccef27aa8
- c195a9d3e42246242a80250b21beb7aa68c270f7b2c97a9c93b17fbb90fd8194
- 73d04d7906706f90fb81676d4f023fbac75b0047897b289f2eb34f7640ed1e7f