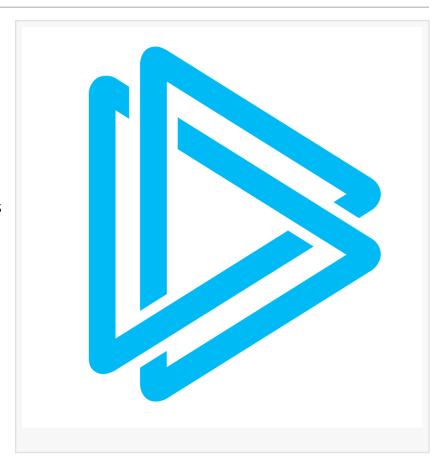


## ANY.RUN Uncovers Salvador Stealer: A New Android Malware Targeting Banking Credentials

DUBAI, DUBAI, UNITED ARAB EMIRATES, April 1, 2025
/EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has uncovered a new Android malware variant, internally naming it Salvador Stealer. Disguised as a legitimate banking application, this malware is designed to steal sensitive personal and financial data, including net banking credentials and OTPs.

## $000\ 00000000\ 0000000\ 00000$

Salvador Stealer follows a two-stage infection chain. It is first delivered as a dropper APK, which silently installs a second-stage payload — the actual banking credential stealer.



Once active, the malware displays a fake banking interface inside the app to trick users into entering their personal and banking details. It also abuses SMS permissions to intercept OTPs and verification codes, allowing attackers to bypass two-factor authentication.

## 

- · 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🖂 Stolen information is sent to a phishing server and Telegram C2.

- · 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🗓 🖂 The malware captures incoming SMS messages to steal OTPs.
- DDDDDDDDDDDDDDDDDDDD: Publicly accessible admin panel and attacker's contact information.

To explore the full technical analysis and see how Salvador Stealer operates in real time, visit the detailed report on the <u>ANY.RUN Blog</u>.

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence solutions. Trusted by over 15,000 companies and more than 500,000 cybersecurity professionals worldwide, ANY.RUN empowers security teams to detect, analyze, and investigate cyber threats in real time across Windows, Linux, and Android environments. Every day, the platform processes more than 20,000 malware samples, helping organizations stay ahead of evolving cyber threats.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:

X LinkedIn YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/799045961

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.