www.isea.gov.in

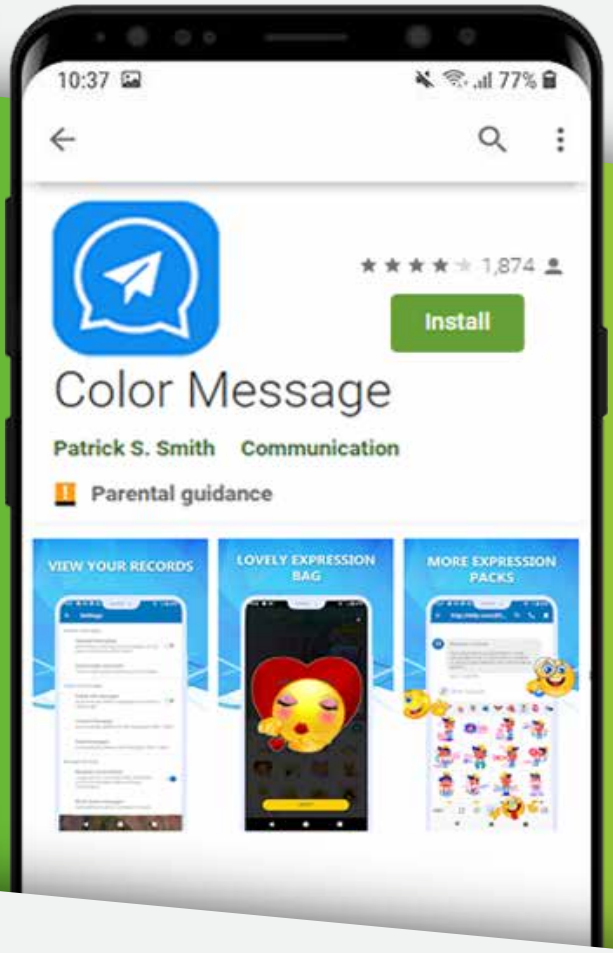
# Advisory On Joker Malware Infected Color Message Application

www.InfoSec awareness.in

An android mobile application named Color Message infected with Joker malware is currently available for download on Google Play store and was installed by more than half a million users across the world .

The application appears to be making connections to Russian servers.

Joker is categorized as Fleeceware, as its main activity is to simulate clicks and intercept SMS to subscribe to unwanted paid premium services without the knowledge to users, Joker malware generates a very discreet footprint that can be tricky to detect.




## Dangers of application

- Accesses users contact list and exfiltrates it over the network.
- The application automatically subscribes to unwanted paid premium services unknown to users.
- The application has the capability to hide its icon once installed.
- Stolen identity (malicious apps might abuse communication apps).

The advisory provides safety measures to safeguard yourself against Android Color Message application.

## Symptoms


Device is running slowly

Dubious applications appear

System settings are modified without users' permission

Data and battery usage is increased significantly

Browsers redirect to rogue websites, intrusive advertisements are delivered

## Advisory

- Uninstall the application from the device
- Scanning your Android device with legitimate anti-malware software to eliminate malware infections on the device
- Update the android devices with latest security updates provided by vendors
- Never click on links received from unknown sources without proper verification/ authentication
- Never share your personal details or login credentials/-passwords/credit or debit card details and other such information online .
- Use a trusted anti-virus software for Mobile Security to stay safe from malware attacks.
- Avoid installing mobile applications which contains advertisements

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

For more details visit the link: https://infosecawareness.in/advisories/color-message-application

http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

For more details / queries on Cyber Security Call us on our Toll free No.

1800 425 6235

Implemented by