

Joker Malware Is Back: Here's What You Need to Know To Stay Protected

Beware!!! Play Store apps found spreading Joker, Face stealer and Coper malware



What is Joker Malware?










A well-known malware family that targets Android mobile devices is Joker. It manages to get into Google's official app store by periodically updating its trail signatures, which also includes updates to the virus's code, execution processes, and payload retrieval techniques. The virus steals the victim's contacts, device data, and SMS messages, as well as signing them up for expensive wireless application protocol (WAP) services.











There are 4 new malicious apps that have been found on Google Play that are infected with the Joker malware that act as droppers, and which disables the Google Play Protect service, installs malicious apps, generates fake reviews, and shows ads. The spyware can steal SMS messages, contact lists, and device information, and to sign victims up for premium service subscriptions. Researchers estimate that over 100,000 users have installed the apps.









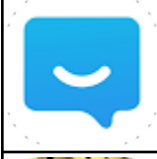

Google has ditched over 50 apps from Play store due to Joker Malware



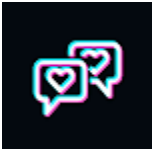



















Over the past two months, ThreatLabz researchers discovered the following malicious Joker downloader apps in the Google Play Store:

	Simple Note Scanner - com.wuhan.pdf scan
	Universal PDF Scanner - com.unpdf.scan.read.docscanuniver
	Private Messenger - com.recollect.linkus
	Premium SMS - com.premium.put.trust sms
	Smart Messages - com.toukyou rsms.time messages
	Text Emoji SMS - messenger.itext.emoji.messenger
	Blood Pressure Checker - com.blood pressure checker.tangjiang
	Funny Keyboard - com.soundly.galaxy keyboard
	Memory Silent Camera - com.silentmary.time camera

	Custom Themed Keyboard - com.custom.keyboard.themes.galaxy
	Light Messages - com.lilysmspro.lighting
	Themes Photo Keyboard - com.themes.bgphotokeyboard
	Send SMS - exact.message.send.text.sms
	Themes Chat Messenger - com.relish.messengers
	Instant Messenger - com.sbdlsms.crazymessenger.mmsrec
	Cool Keyboard - com.collate.gamekeyboard
	Fonts Emoji Keyboard - come.emoji.font.keyboard
	Mini PDF Scanner - com.mnscan.minipdf
	Smart SMS Messages - com.sms.mms.message.ffei.free

	Creative Emoji Keyboard - com.whiteemojis.creativekeyboard.ledsloard
	Fancy SMS - con.sms.fancy
	Fonts Emoji Keyboard - com.symbol.fonts.emoji keyboards
	Personal Message - com.crowne.personal message
	Funny Emoji Message - com.funny.messages
	Magic Photo Editor - com.amagiczy.photo.editor
	Professional Messages - com.adore.attached.message
	All Photo Translator - photocom.allfast translate.translation translator
	Chat SMS - com.maskteslary.messages
	Smile Emoji - com.balap.smile wall.emoji

	Wow Translator - com.imgtop.camtranslator
	All Language Translate - com.exclusivez.alltranslate
	Cool Messages - com.learningz.app.cool.messages
	Blood Pressure Diary - bloodhold.nypressure.mainheart.ratemy.mo.dapulse.app.tracker.diary
	Chat Text SMS - com.chat sms.messages
	Hi Text SMS - ismos.mmsys.message.text itext.bob sms
	Emoji Theme Keyboard - com.go back theme.lovely emoji keyboard
	iMessenger - start.me.messenger
	Text SMS - com.ptx.text sms
	Camera Translator - com.hai goback.outside text.language cameratransla

	Come Messages - com.itext sms.message coming
	Painting Photo Editor - com.painting.pointeditor.photo
	Rich Theme Message - com.getmanytimes.richsmsthememessenge
	Quick Talk Message - messages.sms.messenger
	Advanced SMS - com.from msms.advanced opp
	Professional Messenger - com.akl.sms pro.messenger
	Classic Game Messenger - com.class color.for messenger.sic
	Style Message - com.istyle.messages
	Private Game Messages - com.message.game.india
	Timestamp Camera - already.taken.photo beauty.camera.timestamp



Social Message - com.colorsocial.message

What precautions can be taken?

- ❖ Take the time to research and ensure that the messaging app is well known and reviewed before using it.
- ❖ It's important to take the time to conduct your own research and confirm the app has a well-established and safe reputation before downloading, even when a link comes from a trusted friend asking you to download a messaging app.
- ❖ It is easy for messaging apps to exploit the Read_SMS permission in order to gain information, including a key OTP they can use to further compromise victims.
- ❖ Report malicious apps on the Play Store to Google immediately by using the support options in your Play Store app.
- ❖ In order to limit the spread of malware and inhibit the success of threat actors, we should work together to identify, flag, and remove malicious apps as soon as possible from our preferred app stores.

-Mona Chopra
Birla Vidya Niketan