Malware Goes Mobile: Timeline of Mobile Threats, 2004 – 2015

2004
- Cabir: First worm affecting Symbian Series 60 phones. Spreads from phone to phone by using Bluetooth OBEX push protocol.

2009
- Cabir: Worms affecting jailbroken iPhones using Cydia app distribution system due to a hard-coded password in sshd.

2010
- Ikee and Duh: Worms affecting jailbroken iPhones using Cydia app distribution system due to a hard-coded password in sshd.
- DroidDream: First large attack on Google Play. Over 50 apps containing a root exploit published on the Android market.

2011
- FakePlayer: First malware for Android makes money by sending SMS messages to premium line numbers in Russia.

2012
- Zitmo: Popular Windows bot and banking malware Zeus improved with its Android component designed to steal mobile transaction authentication numbers (mTANs).
- Masterkey: A vulnerability in Android exploiting certificate validation, allowing malware to disguise itself as a legitimate app.

2013
- DownAPK: Windows based malware uses Android debugging bridge to install fake banking app to Android devices connected to the infected PC.

2014
- Gazon: Android virus spams all your contacts via SMS with a link to install a phony Amazon rewards app.

2015
- 2 million cumulative samples of Android malware and potentially unwanted apps.