Mobile malware

Mobile malware• is malicious software that is specifically designed to target mobile device systems such as smartphones and tablets•. Its purpose is to cause the collapse of the system and allow a malicious user to control the device remotely or steal personal information stored on the device itself. It can be divided into three broad categories: malware that can also be found in computer devices, mobile specific malware•• and Bluetooth hacking.

Spyware, Trojan horses, worms and ransomware are the main malware common both in computers and mobile devices.

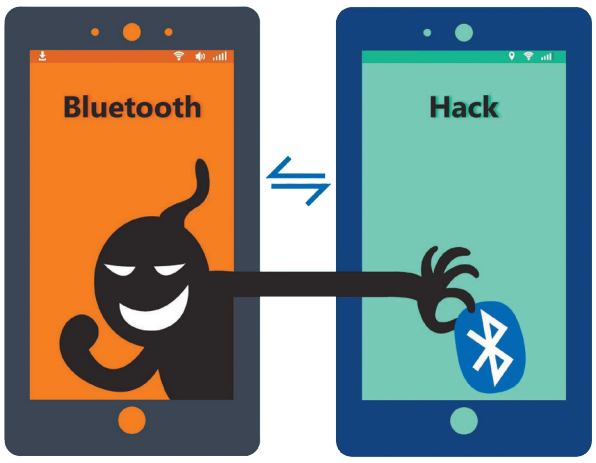
■ Mobile specific malware

There are some types of malware specifically designed for mobile devices, in particular:

- **Expander**: it targets mobile meters, i.e. the amount of expansion that can be added to the signal, for additional phone billing and profits in a way that is similar to the one used by diallers with computers;
- **Ghost push**: it is a kind of malware which infects the Android o/s by automatically gaining root access, i.e. privileged control over various subsystems. The malicious software is downloaded, converted into a system app and at that point root access is lost, which makes it virtually impossible to remove the infection with a factory reset•••.

■ Bluetooth hacking

Some types of malware are connected with attacks through a Bluetooth connection:



- **Blueborne:** it can spread through the air (airborne) and attack devices. The hacker uses the Bluetooth connection to penetrate and take complete control of the targeted device;
- **Bluesnarfing:** it is a type of network attack that occurs when a hacker pairs with a Bluetooth device without the user's knowledge and steals or compromises their personal data;
- **Bluejacking:** a hacker searches for devices in the area and then sends spam in the form of text messages to the device. This form of hacking is rather childish and harmless;
- **Bluebugging:** it uses Bluetooth to establish a backdoor on a victim's device. The attacker can hack the device and also view all the user's data.

The first known mobile malware was a virus called *Timofonica* which originated in Spain and was identified by antivirus labs in Russia and Finland in June 2000.

What do you do protect your smartphone or tablet from malware? Do you have an antivirus program installed?

deployment: *distribuzione*
to drain: *scaricare*
frailty: *fragilità*
to pair with: *accoppiarsi*

The threats associated with mobile malware are expanding. Mobile malware is growing in sophistication, borrowing deployment and obfuscation techniques from conventional PC malware, reflecting the continuous evolution of the cyber threat landscape.

The malware gains control of all system resources making it unresponsive and draining the battery. It steals the user's personal data from the phone.

1 Draw a summary map of the different types of malware.

2 PAIR WORK Take it in turns to describe a type of mobile malware and ask the other student to identify it.

3 Read the text and complete the table.

Notable Mobile Malware

- **Cabir:** this malware infects mobile phones running on Symbian OS, a type of mobile operating system in use between 2012 and 2016, and was first identified in June 2004. When a phone is infected, the message 'Caribe' is displayed on the phone's screen every time the phone is turned on. The worm then attempts to spread to other phones using wireless Bluetooth.
- **Duts:** a file infector virus for the Pocket PC platform. It attempts to infect all EXE files that are larger than 4096 bytes in the current directory.
- **Skulls:** a Trojan horse that targets mainly Symbian OS. Once downloaded, the virus replaces all phone desktop icons with images of a skull. It also renders all phone applications useless. This malware also tends to send text messages containing malicious links to all contacts accessible through the device in order to spread the damage.
- **Commwarrior:** a worm which uses MMS messages and that can spread through Bluetooth as well. It infects devices running under OS Symbian Series 60.
- **Gingermaster**: a Trojan developed for an Android platform that propagates by installing applications that incorporate a hidden malware for installation in the background. It exploits the frailty in the version Gingerbread (2.3) of the operating system and creates a service that steals information from infected terminals.
- **DroidKungFu**: a Trojan content in Android apps, which, when executed, obtains root privileges and installs the file com.google.ssearch.apk, which contains a backdoor.
- **Ikee**: a worm for iOS platforms. It only works on terminals whose private file system has already been corrupted, and spreads by trying to access other devices.
- **Shedun**: adware serving malware able to root Android devices.

Adapted from: *https://en.wikipedia.org/wiki/Mobile_malware*

Name	Type of malware	Platform or o/s affected	Effect produced
Cabir			
Duts			
Skulls			
Commwarrior			
Gingermaster			
DroidKungFu			
Ikee			
Shedun			