# The malware attack against mobile phones is mounting

December 23 2004

The security challenges in the mobile environment are similar to the problems we have encountered in the PC world. Open platforms are becoming popular in smartphones, for example the Symbian operating system is used in more than 20 million mobile phones at the moment.

In spring 2004, a trojanized game called Mosquitos was found. It secretly sent messages to expensive toll numbers, creating invisible costs for the user.

- June 15th: worm was found. Cabir is a worm that replicates over-the-air using bluetooth connections.
- June 16th: Cabir.B is found. This new variant had minor differences compared to the original.

**Cabir**
Cabir (also known as EPOC.cabir and Symbian/Cabir) is the name of a computer worm developed in 2004 that is designed to infect mobile phones running Symbian OS. According to Kaspersky Labs the Cabir worm is the first network worm for mobile phones. When a phone is infected with Cabir, the message "Caribe" is displayed on the phone's display, and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

During the autumn, Cabir.B started spreading in the wild. It has been detected in several countries since, including China, India, Turkey, Philippines and Finland. It continues spreading today, travelling from one country to another as people with infected phones travel.

- November 19th: Skulls.A trojan is found. It replaces icons on the phone with skull images, making the phone almost useless.
- November 29th: Skulls.B is found
- December 9th: Cabir.C is found
- December 9th: Cabir.D is found
- December 9th: Cabir.E is found
- December 21st: Skulls.C is found
- December 21st: Cabir.F is found
- December 21st: Cabir.G is found

This last batch of malware was distributed masked as a pirate version of a popular game for mobile phones; when run, it installs Skulls and Cabir variants and tries to attack security products installed on the phone. It also tries to disable F-Secure Mobile Anti-Virus but fails.

In the future, it is likely that we will also see new kinds of attacks: trojan horses in games, screensavers and other applications – resulting in false billing, unwanted disclosure of stored information, and deleted or stolen user data.The best way to protect a smartphone against harmful content is to install automated antivirus software to the phone. This is also the only way to get full protection against viruses that try to enter the phone for example over Bluetooth or internet connections.

F-Secure Mobile Anti-Virus is the most comprehensive solution available for protecting smartphones against harmful content, from undesired messages to malfunctioning applications. It provides real-time, on-device protection and automatic over-the-air antivirus updates through a patented SMS update mechanism and HTTPS connections.

Citation: The malware attack against mobile phones is mounting (2004, December 23) retrieved 27 April 2024 from https://phys.org/news/2004-12-malware-mobile-mounting.html