Botnets? You're welcome.

Back in December 2010 the specialists reported on the establishment of a botnet out of Android-based devices malware Gemini, which was included in an entirely legitimate applications published in the Chinese shops. In particular, this malicious program has features that allow you to load in the infected device other applications and delete them, send the geographic coordinates of the device, generate a list of installed programs on your device and send them to a malicious server.

Backdoors? Even as. In March of 2012 has spread malware Android.Anzhu, which spread through Chinese websites with free software for Android. The program allows attackers to literally control the infected device remotely. In particular, carry it commands sent from a malicious server, install other applications, as well as change the bookmark in the browser.

Spyware? Well, for mobile devices - is a "sacred thing". In particular, in the summer of 2011, according to the company's CA Technologies, spread malicious software, the functions which allow you to record telephone calls, produced by the device, AMR-files on the memory card. And about the vulnerability of access to information held on removable media, mobile devices running Android, we've already written above. It should be noted that telephone calls to intruders have more value than any text information that is stored on smartphones and tablets.

What about blocking the screen? Information on full-screen pop-up blocker, made in the form of programs for Android has not yet been met. In the course of a forecast that such programs will sooner or later. But at the same time, the attackers went through less tricky, introducing malicious scripts on the site. When opening web pages with similar scripts in the browser opens a dialog box in which the user is asked to send a paid SMS-message and enter the code to make this window disappear. At the same time helps to restart the browser, not in all cases.

Rootkits? Bootkits? Yes, virus writers are ready to take this step in the application to mobile systems. In particular, the Trojan injects itself into startup DKFBootKit system in such a way that is loaded before the initialization of the operating system. This program works only in "rutovannyh" systems, ie users enjoy indulging in the field of information security devices, but at the same time, has the ability built into the system partition and replace a few basic tools, and system services running in the background, as well as a startup script system. The program then waits for receipt of further instructions from the command-and-control server attacks. That is, in fact, this program is a backdoor that has complete control over an infected device.

Do not forget about malware that secretly paid just send SMS-messages. But this is a classic of Android. Thus, in most cases, users do not realize why installed, for example, the game asks for permission to send SMS-messages.

Probably the only type of malware that has not yet been distributed platform for Android - a file viruses, infects executable system. However, for desktop operating systems, the spread of these types of malicious programs is gradually fading away in the form of writing, as well as the complexity of the organization to monetize them.

telefon dinleme