Mobile beasts and where to find them — part four

kaspersky.com/blog/mobile-malware-part-4/24290/

android

We explain the types of malware that can take control of your device, and the dangers of multifunctional infection.

- 
  Ilja Shatilin
- October 22, 2018

- *Mobile beasts and where to find them — part one: Adware, subscribers, flooders, DDoSers.*
- *Mobile beasts and where to find them — part two: Ransomware, wipers, miners.*
- *Mobile beasts and where to find them — part three: Spyware, keyloggers, banking Trojans.*

In part four of our study of mobile threats, we discuss the most complex and dangerous types of malware — the ones that not only exploit Android capabilities, but are also able to tune your system to their taste and combine multiple malicious functions.

RATs — remote access Trojans

RAT by name, rat by nature. Remote administration tools (RATs) can be used to connect to a remote device on the network and not only view the screen contents, but also take full control, issuing commands from remote input devices (keyboard/mouse on a computer; touch screen on a smartphone).

RATs were initially created with good intentions — to help manage various settings and apps, well, remotely. After all, it is far easier for tech support staff to select the right check boxes and settings themselves rather than trying to explain to the user what to do over the phone — and even easier for the user.

But in cybercriminals' hands, RATs are transformed into a formidable weapon: Installing a Trojan on your smartphone that provides someone with remote access to the gadget is like giving the keys to your apartment to a stranger. The malicious use of RATs is so common that the acronym increasingly stands for "remote access Trojan."

Having connected to your device through a RAT, hackers can do as they please, including snooping on all your passwords and PINs, logging into banking apps and transferring your money, and subscribing you to unwanted services that quietly eat up funds on your mobile account or credit card — as well as stealing your mail, social network, and IM accounts to extract money from friends in your name. And that's after copying all your photos to blackmail you later if any of them happen to be of a private nature.

Typically, RATs are used for spying. Such malware allows jealous husbands or wives to spy on their spouses, but more seriously, it can also be used for stealing corporate secrets. For example, AndroRAT (detected in spring this year) sneakily takes pictures with the smartphone camera and records sound (including telephone conversations). It also steals Wi-Fi passwords based on geolocation. This means that no negotiations are ever confidential, and it makes penetrating the office network a piece of cake.

Rooting Trojans

"Root access" in some operating systems, including Android, is another name for superuser rights, which allow changes to system folders and files. For regular user tasks, such access is completely unnecessary and disabled by default. But some advanced enthusiasts like to have it to customize the operating system. See our post Rooting your Android: Advantages, disadvantages, and snags to learn why you should think twice before doing so.

Some malicious programs, called rooting Trojans, can get root privileges using vulnerabilities in the operating system. Having superuser rights allows cybercriminals to configure your smartphone for their purposes. For example, they can force the device to open full-screen ads. Or install malware or adware in the background, without any notifications.

A favorite rooting malware trick is to secretly delete apps installed on the smartphone and replace them with either phishing or malware-augmented software. Moreover, superuser rights can be used to prevent you from removing malware from your device. No wonder that rooting Trojans are considered today's most dangerous type of mobile threat.

Modular Trojans

Jack-of-all-trades modular Trojans can perform several different malicious actions, either simultaneously or selectively according to the situation. One of the most striking examples of such a Trojan is Loapi, detected in late 2017. As soon as it penetrates a victim's device, it immediately ensures its own safety by requesting administrator rights — and it won't take no for an answer; if it is refused, the dialog window pops up again and again, preventing the smartphone from being used. And if access is granted, it becomes impossible to remove Loapi from the device.

The Trojan then launches any one of five modules. It can display ads, subscribe the user to paid content by following links, carry out DDoS attacks on command from a remote server, and forward SMS messages to cybercriminals, concealing them so that the user does not notice malicious transactions.

And in its spare time, when not engaged with these important tasks, the Trojan stealthily mines cryptocurrency, most often when the smartphone is connected to a power outlet or external battery. Mining is a complex computational process that gobbles up energy and resources, so the battery takes a very long time to charge. This can have fatal consequences for phones: Our experts discovered firsthand that a couple of days of Loapi activity is enough to ruin a smartphone battery through overheating.

How to defend against the worst Android malware

As you can see, the dangers posed by RATs, rooting Trojans, and modular malware are serious. But you can guard against them. Here are some simple rules:

- First of all, block app installs from unknown sources. This option is disabled in Android by default, and it should stay that way. It is no panacea, but it does solve most problems associated with mobile Trojans.
- Do not try to skimp by downloading hacked versions of apps. Many of them are infected.

- Do not click on links promising the moon. WhatsApp offers of free airline tickets are usually just an attempt to steal your personal data, and they download malware to your smartphone as a bonus. The same applies to phishing, including texts from friends or strangers containing “Is this your photo?”-type messages.
- Do not ignore updates for Android and apps installed on your device. Updates patch holes through which attackers can sneak into your smartphone.
- Check what rights apps are asking for, and do not be afraid to refuse access to personal information and potentially dangerous functions in Android — in most cases, nothing terrible will happen if such requests are denied.
- Put a good antivirus on your smartphone. For example, Kaspersky Internet Security for Android not only finds and removes Trojans, but also blocks websites with malware and mobile subscriptions.

- android
- AndroRAT
- Loapi
- mobile apps
- modular Trojans
- RAT
- root
- rooting
- smartphones
- threats
- trojans

Share article

Related