



The Threat Menacing Android Smartphones

Got an Android smartphone? Then be careful - it's vulnerable to new malware that can perform a plethora of activities, from mining cryptocurrency and launching DDoS (Distributed Denial of Service) attacks to destroying your phone.

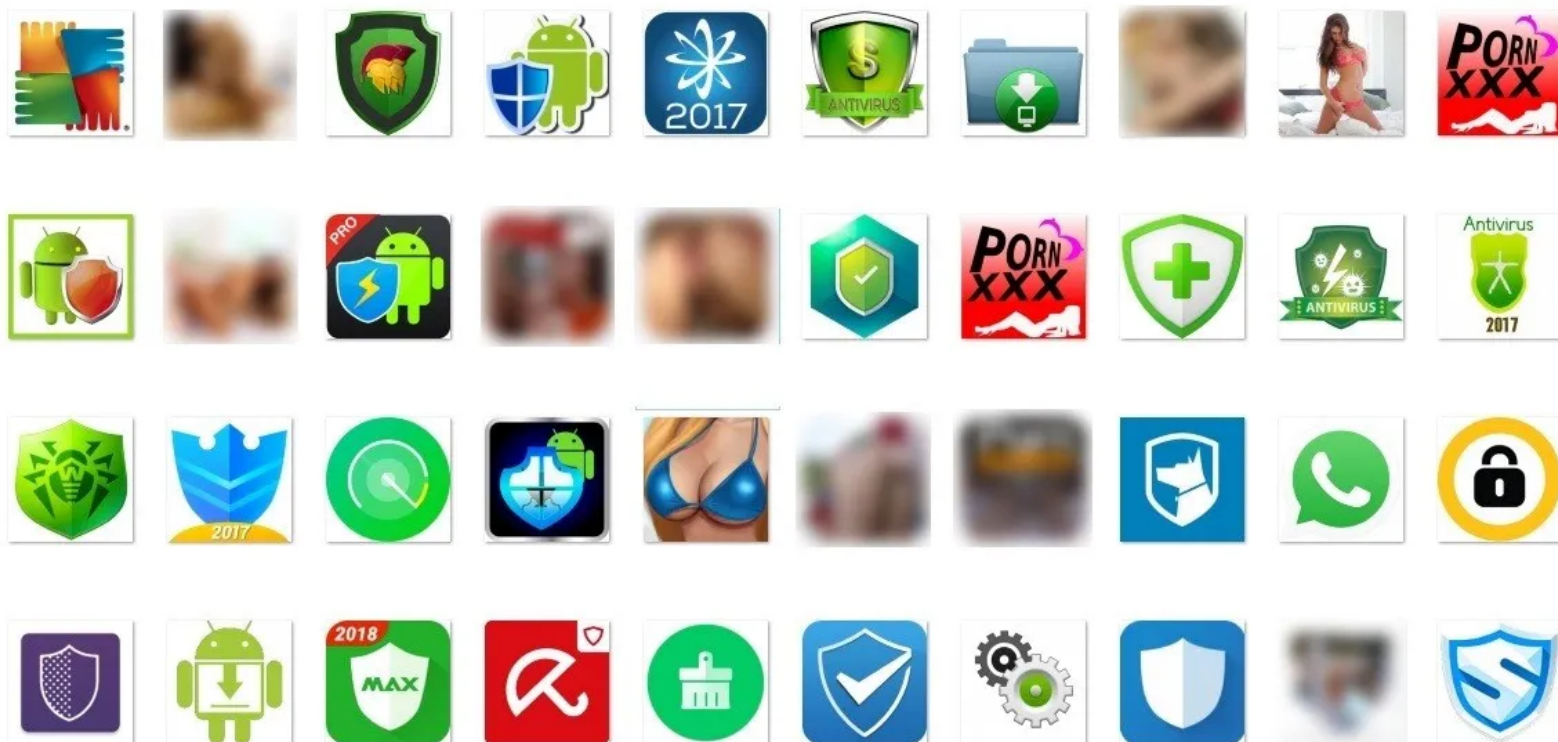
The new virus is called *Loapi*, and more than 45 thousand attempts to infect devices have been recorded to date.

The new malware was [identified](#) by antivirus experts from the Kaspersky Lab cyber security agency, who discovered it is able to sign the user up to paid resources, send SMS messages and even mine cryptocurrency.

- As reported, such multitasking Android-Trojans have never been seen before. Moreover, hackers have now learned how to siphon money in various ways after infecting a device only once.

How virus spreads

Experts warn that the virus spreads through advertising campaigns that redirect users to malicious sites. As a rule, links lead to different antiviral resources or to a site with “adult” content.



After installing the program, Loapi asks for administrative rights and prevents it from opening until the user agrees to give permissions.

Loapi can:

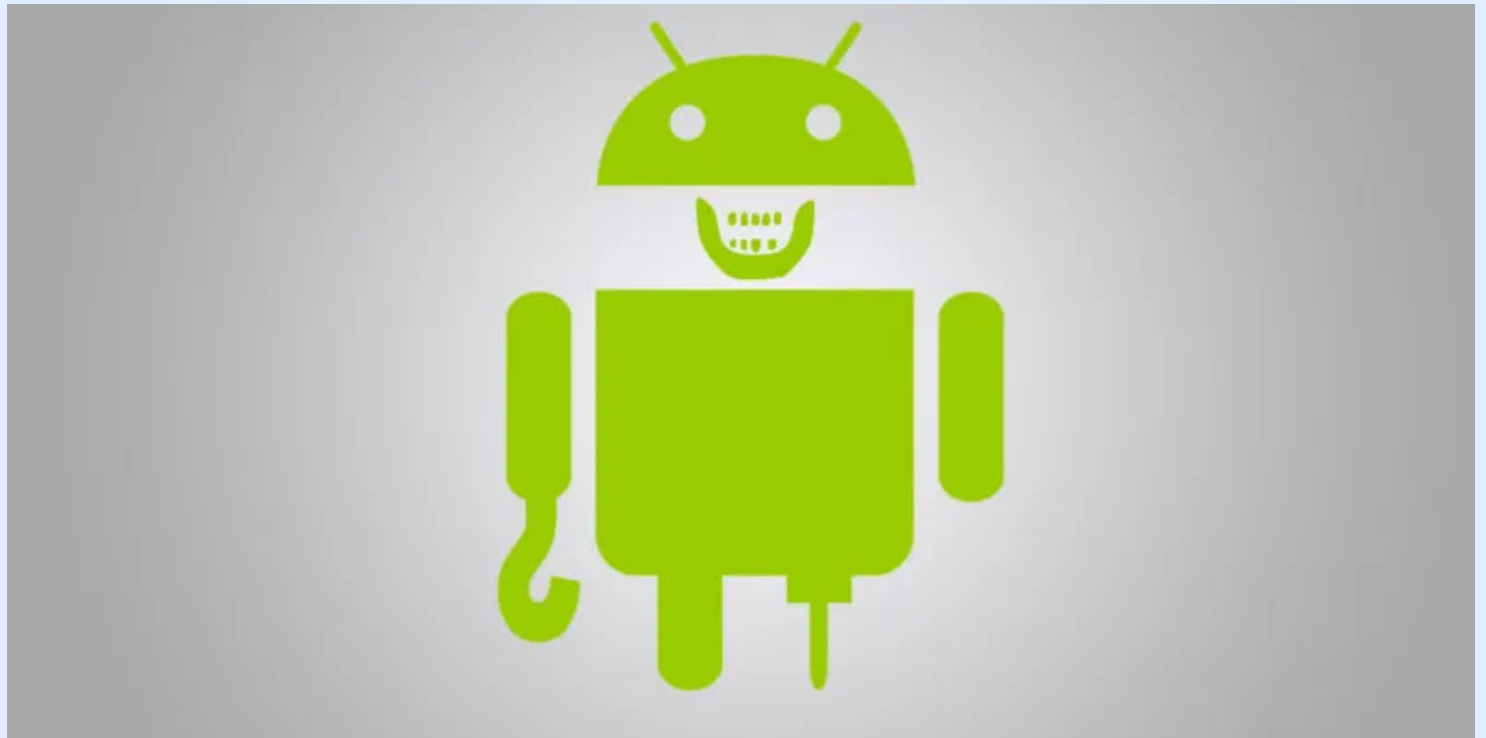
- Show the device owner advertising banners;
- Independently draw up a subscription to paid services;
- Use the device's capacity for massive DDoS attacks.

Users can also suffer damage to their device as hidden mining causes it to overheat.

"Loapi is a very unusual representative of Android malware. The authors embodied in it almost all possible functions of malicious mobile software. For the sake of completeness, the only thing missing is the ability to spy on the user, but thanks to the modular architecture of the Trojan, this "flaw" is quite easy to fix," says Nikita Buchka, antivirus analyst at Kaspersky Lab.

Hard to Conquer

The virus also has a powerful self-defense mechanism. If the smartphone's anti-virus program tries to stop Loapi, the virus closes the settings window and turns off the screen. Malware then issues a warning about the presence of supposedly malicious software and offers to remove it. If the user refuses to uninstall the app, the virus continues to insist and sends regular alerts until the user deletes the program.



In this case, the work of the virus can not only sidestep the device's settings but also cause physical damage to the smartphone, e.g. destroying the battery.

Protect Yourself

Here are some simple tips to follow to protect your smartphone from Loapi:

- Turn off third-party app installation.
- Always keep the operating system up to date.
- Install reliable anti-virus software and make regular updates.

Keep up to date with the most important IT topics of 2018 by following our news feed. If you have any questions about software protection or app development, do not hesitate to contact us.