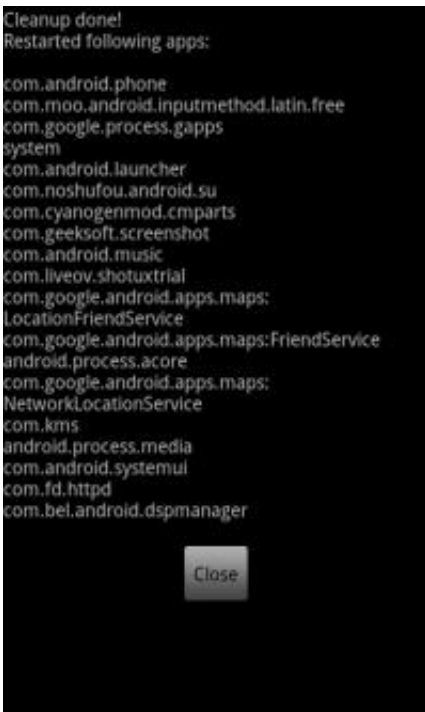


# Kaspersky warns phone users of PC-infecting malware

February 5 2013, by Nancy Owano

---



Credit: Kaspersky Lab

(Phys.org)—Kaspersky Lab has a new warning for smartphone and tablet users. Yes, it's all about Android. No, it's not like anything you've been warned about before. Lab Expert Victor Chebyshev has discovered a new attack vector in the form of nasty apps (DroidCleaner and Superclean) posing as system cleaners for freeing up memory, and boosting performance by cleaning out old data. The apps are malware.

The Superclean and DroidCleaner are the apps that transfer malware. Instead of just infecting the phone they are designed to move across, infecting both the smartphone and PC.

The malware capabilities include stealing data from the victim's [phone](#) and PC as well as eavesdropping on conversations. Kaspersky Lab said the malware was the most extensive feature set it had seen in one [mobile application](#).

After plugging an Android device into a [Windows PC](#), the action starts. *The H* ran a discussion of [how](#) the malware operates: "The app moves on to quietly download three files and save them as "autorun.inf", "folder.ico" and "svchosts.exe" in the root directory of the SD card. Now the phone is ready to infect any PC that it is plugged into when in USB drive emulation mode – if, of course, it still autoruns removable media, and will trigger the running of "svchosts.exe".

The Android version of the bot includes the following features: sending SMS messages; uploading SMS messages; deleting SMS messages; enabling Wi-Fi; opening arbitrary links in a browser; uploading the [SD card](#)'s contents; uploading an arbitrary file (or folder) to the master's server; uploading contacts/photos/coordinates from device to master.

The good news for all this is that current versions of Windows pose no such risk. The attack did depend on the AutoRun feature being enabled in Windows for external drives. The current versions have AutoRun disabled. The attack is only possible against users running older unpatched versions of the OS.

Still, news of the discovery by Kaspersky Lab that the apps were on Google Play, where they are no longer, seemed to have an unsettling effect on most technology sites that carried the news. Though the cleaner-masquerading apps no longer reside in Google Play, the idea that they

were sitting there for any length of time was reminder enough that mobile phone users need to think twice about what they download and install.

**More information:** [www.securelist.com/en/blog/805/Mobile\\_attacks](http://www.securelist.com/en/blog/805/Mobile_attacks)

© 2013 Phys.org

Citation: Kaspersky warns phone users of PC-infecting malware (2013, February 5) retrieved 26 April 2024 from <https://phys.org/news/2013-02-kaspersky-users-pc-infecting-malware.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.