LevelBlue - Open Threat Exchange

By KonstantinJM

Archived: 2026-04-06 02:53:46 UTC

FileHash-SHA256: 9 | **IPv4:** 1 | **Hostname:** 1

PluginPhantom is a new class of Google Android Trojan: it is the first to use updating and to evade static detection. It does this by leveraging the Android plugin technology. It abuses the legitimate and popular open source framework “DroidPlugin”, which allows an app to dynamically launch any apps as plugins without installing them in the system. PluginPhantom implements each element of malicious functionality as a plugin, and utilizes a host app to control the plugins. With the new architecture, PluginPhantom achieves more flexibility to update its modules without reinstalling apps. PluginPhantom also gains the ability to evade the static detection by hiding malicious behaviors in plugins. Since the plugin development pattern is generic and the plugin SDK can be easily embedded, the plugin architecture could be a trend among Android malware in the future.
