Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:48:33 UTC

Tool: PluginPhantom

Names	PluginPhantom
Category	Malware
Type	Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Palo Alto) Recently, we discovered a new Google Android Trojan named "PluginPhantom", which steals many types of user information including: files, location data, contacts and Wi-Fi information. It also takes pictures, captures screenshots, records audios, intercepts and sends SMS messages. In addition, it can log the keyboard input by the Android accessibility service, acting as a keylogger. 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.
Information	<https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:pluginphantom>

Last change to this tool card: 02 July 2020

Download this tool card in JSON format

All groups using tool PluginPhantom

Changed	Name	Country	Observed

APT groups

	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a56b62e0-d456-4098-bfae-a86aeae21b49