Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:14:56 UTC

Tool: PhantomLance

Names	PhantomLance PWNDROID1 Android.Backdoor.736.origin
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader, Exfiltration
Description	(Dr.Web) The backdoor communicates with several command and control servers to receive commands from the attackers and send the collected data. The cybercriminals can also control the trojan via the Firebase Cloud Messaging service. Android.Backdoor.736.origin is capable of: • sending information on contacts from the contact list to the server; • sending information on text messages to the server (the investigated version of the trojan did not have the permissions for this); • sending the phone call history to the server; • sending the device location to the server; • downloading and launching an APK or a DEX file using the DexClassLoader class; • sending the information on the installed software to the server; • downloading and launching a specified executable file; • downloading a file from the server; • uploading a specified file to the server; • transmitting information on files in the specified directory or a memory card to the server; • executing a shell command; • launching the activity specified in a command; • downloading and installing an Android application; • displaying a notification specified in a command; • requesting permission specified in a command; • sending the list of permissions granted to the trojan to the server; • not letting the device go into sleep mode for a specified time period.
Information	<https://news.drweb.com/show/?i=13349&c=0&p=0> <https://securelist.com/apt-phantomlance/96772/>

	<https://threatvector.cylance.com/en_us/home/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.phantomlance>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool PhantomLance

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d6d0a523-fa63-4a7a-a20a-df07a5cb7087