Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:59:01 UTC

Tool: DarkNimbus

Names	DarkNimbus
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(Trend Micro) The main backdoor implanted in XWalk is a comprehensive Android surveillance tool. We managed to find an independent version of the backdoor and discovered that it has been developed and actively updated since 2018. In some versions, we noticed that the backdoor uses the string “DKNS” in their functions. Since then, we named the backdoor as DarkNimbus. DarkNimbus uses the XMPP protocol to communicate with a C&C server. The XMPP communication handlers of the backdoor are implemented with the open-source project “Smack”. In addition, it communicates to another server via HTTPS; this server is used mainly for file transfers. The features supported by DarkNimbus include collecting basic information of the infected device, installed apps, and geolocation (GPS). The backdoor steals personal information including the contact list, phone call records, SMS, clipboard content, browser bookmarks, and conversations from multiple instant messaging apps. It also supports call recording, taking photos, screenshotting, file operations, and command execution.
Information	<https://www.trendmicro.com/en_us/research/24/l/earth-minotaur.html>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool DarkNimbus

Changed	Name	Country	Observed
APT groups			

	Earth Minotaur		2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=30d34631-0151-4a9c-9aa2-ab3cc5cd4b1e