Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:14:24 UTC

Tool: dmsSpy

Names	dmsSpy
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) Another APK link was disguised as a calendar application for checking the schedule of upcoming political events in Hong Kong. Though the link was also down, we managed to find the original file downloaded from it. The calendar application shown above requires manysensitive permissions such as READ_CONTACTS, RECEIVE_SMS, READ_SMS, CALL_PHONE, ACCESS_LOCATION, and WRITE/READ EXTERNAL_STORAGE. When launched, it first collects device information such as device ID, brand, model, OS version, physicallocation, and SDcard file list. It then sends the collected information back to the C&C server. It also steals contact and SMS information stored in the device. Furthermore, it registers a receiver that monitors new incoming SMS messages and syncs messages with the C&C server in real-time. The appcan perform an update by querying the C&C server to fetch the URL of the latest APK file, then download and install it.
Information	<https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf> <https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/> <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.dmsspy>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool dmsSpy

Changed	Name	Country	Observed	
APT groups				
	Operation Poisoned News, TwoSail Junk		2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=94171b88-29ea-4840-8f84-61096123d0b0