Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:47:30 UTC

Tool: GolfSpy

Names	GolfSpy
Category	Malware
Type	Reconnaissance, Info stealer, Exfiltration
Description	(Trend Micro) Given GolfSpy's information-stealing capabilities, this malware can effectively hijack an infected Android device. Here is a list of information that GolfSpy steals: • Device accounts • List of applications installed in the device • Device's current running processes • Battery status • Bookmarks/Histories of the device's default browser • Call logs and records • Clipboard contents • Contacts, including those in VCard format • Mobile operator information • Files stored on SDcard • Device location • List of image, audio, and video files stored on the device • Storage and memory information • Connection information • Sensor information • SMS messages • Pictures GolfSpy also has a function that lets it connect to a remote server to fetch and perform commands, including: searching for, listing, deleting, and renaming files as well as downloading a file into and retrieving a file from the device; taking screenshots; installing other application packages (APK); recording audio and video; and updating the malware.

Information	<https://www.trendmicro.com/en_us/research/19/f/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0421/>

Last change to this tool card: 31 December 2022

Download this tool card in JSON format

All groups using tool GolfSpy

Changed	Name	Country	Observed	
APT groups				
	Domestic Kitten		2016-Oct 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fdd7d92f-6189-40cb-974d-66f655620429