Tempting Cedar Spyware - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:58:19 UTC

Home > List all groups > Tempting Cedar Spyware

APT group: Tempting Cedar Spyware

Names	Tempting Cedar Spyware *(Avast)*
Country	Lebanon
Motivation	Information theft and espionage
First seen	2015
Description	(ZDNet) A hacking campaign used fake Facebook profiles to trick targets into downloading malware capable of stealing vast swathes of information, including messages, photos, audio recordings and even the exact location of victims. The group has been operating since as early as 2015 and is thought to have infected the Android phones of hundreds selected targets across the Middle East. The the highest concentration of infections is in Israel, but victims have also been seen in the US, China, Germany and France. Uncovered by researchers at Avast, the operation has been dubbed 'Tempting Cedar Spyware'. The name combines the main means of attack - by tricking victims using fake social media profiles purporting to be those of a young woman - with the Cedar tree, which features prominently on the flag of Lebanon. The campaign for distributing the malware begins with fake Facebook profiles which are designed to lure in victims - predominantly men - with 'flirty' conversations.
Observed	Countries: China, France, Germany, Israel, USA.
Tools used	Tempting Cedar Spyware.
Information	<https://www.zdnet.com/article/hacking-group-uses-facebook-lures-to-trick-victims-into-downloading-android-spyware/> <https://blog.avast.com/avast-tracks-down-tempting-cedar-spyware>

Last change to this card: 19 April 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=043904a1-321c-421b-86e6-1a8c7b638cbf