

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:25:30 UTC

APT group: Karkadann

Names	Karkadann (<i>Kaspersky</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	<p>(Kaspersky) Karkadann is a threat actor that has been targeting government bodies and news outlets in the Middle East since at least October 2020. The threat actor leverages tailor-made malicious documents with embedded macros that trigger an infection chain, opening a URL in Internet Explorer. The minimal functionality present in the macros and the browser specification suggest that the threat actor might be exploiting a privilege-escalation vulnerability in Internet Explorer. Despite the small amount of evidence available for analysis in the Karkadann case, we were able to find several similarities to the Piwiks case, a watering-hole attack we discovered that targeted multiple prominent websites in the Middle East.</p>
Observed	Sectors: Government , Media . Countries: Middle East.
Tools used	
Information	< https://securelist.com/apt-trends-report-q1-2021/101967/ >

Last change to this card: 16 May 2021

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=d2b2b2d8-739f-4602-98e2-b53dfb24792e>