Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:02:38 UTC

APT group: ZooPark

Names	ZooPark *(Kaspersky)* TG-2884 *(SecureWorks)* Cobalt Juno *(SecureWorks)* APT-C-38 *(Qihoo 360)* Saber Lion *(?)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2015
Description	(Kaspersky) ZooPark is a cyberespionage operation that has been focusing on Middle Eastern targets since at least June 2015. The threat actors behind ZooPark infect Android devices using several generations of malware we label from v1-v4, with v4 being the most recent version deployed in 2017. The preferred infection vector for ZooPark is waterhole attacks. We found several news websites that have been hacked by the attackers to redirect visitors to a downloading site that serves malicious APKs. Some of the themes observed in campaign include “Kurdistan referendum”, “TelegramGroups” and “Alnaharegypt news”, among others. Target profile has evolved during the last years of campaign, focusing on victims in Egypt, Jordan, Morocco, Lebanon and Iran.
Observed	Sectors: Media and United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) in Amman, Jordan. Countries: Egypt, Iraq, Iran, Jordan, Kuwait, Lebanon, Morocco and Kurdistan.
Tools used	ZooPark.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/24122414/ZooPark_for_public_final_edited.pdf>

Last change to this card: 10 August 2021

Download this actor card in PDF or JSON format