Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:39:36 UTC

APT group: DNSpionage

Names	DNSpionage *(Talos)*	
Country	Iran	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
First seen	2019	
Description	(Talos) Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it's clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks. Based on this actor's infrastructure and TTPs, we haven't been able to connect them with any other campaign or actor that's been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling "DNSpionage," supports HTTP and DNS communication with the attackers. Talos found a possible relationship between DNSpionage and OilRig, APT 34, Helix Kitten, Chrysene.	
Observed	Sectors: Aviation, Government, Law enforcement, Telecommunications and Internet infrastructure. Countries: Albania, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Sweden, UAE, USA and North Africa.	
Tools used	DNSpionage, Karkoff.	
Operations performed	Apr 2019	DNSpionage brings out the Karkoff <https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html>

Information	<https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html> <https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html> <https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/> <https://krebsonsecurity.com/tag/dnspionage/>

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
