Sea Turtle - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:59:30 UTC

APT group: Sea Turtle

Names	Sea Turtle *(Talos)* Silicon *(Microsoft)* UNC1326 *(FireEye)* Marbled Dust *(Microsoft)* Teal Kurma *(PwC)* Cosmic Wolf *(CrowdStrike)*
Country	Turkey
Motivation	Information theft and espionage
First seen	2017
Description	(Talos) Cisco Talos has discovered a new cyber threat campaign that we are calling “Sea Turtle,” which is targeting public and private entities, including national security organizations, located primarily in the Middle East and North Africa. The ongoing operation likely began as early as January 2017 and has continued through the first quarter of 2019. Our investigation revealed that at least 40 different organizations across 13 different countries were compromised during this campaign. We assess with high confidence that this activity is being carried out by an advanced, state-sponsored actor that seeks to obtain persistent access to sensitive networks and systems. The actors behind this campaign have focused on using DNS hijacking as a mechanism for achieving their ultimate objectives. DNS hijacking occurs when the actor can illicitly modify DNS name records to point users to actor-controlled servers. The Department of Homeland Security (DHS) issued an alert about this activity on Jan. 24 2019, warning that an attacker could redirect user traffic and obtain valid encryption certificates for an organization’s domain names.
Observed	Sectors: Aerospace, Defense, Energy, Government, NGOs, Telecommunications, Think Tanks and Intelligence agencies. Countries: Albania, Armenia, Cyprus, Egypt, Greece, Iraq, Jordan, Lebanon, Libya, Netherlands, Sudan, Sweden, Switzerland, Syria, Turkey, UAE, USA.
Tools used	Drupalgeddon and DNS hijacking.

Operations performed	Jan 2018	Talos now has moderate confidence that the threat actors behind Sea Turtle have been using another DNS hijacking technique. This new technique has been used very sparingly, and thus far have only identified two entities that were targeted in 2018, though we believe there are likely more.
	Apr 2019	The Institute of Computer Science of the Foundation for Research and Technology – Hellas (ICS-Forth), the ccTLD for Greece, acknowledged on its public website that its network had been compromised on April 19, 2019. Based on Cisco telemetry, we determined that the actors behind the Sea Turtle campaign had access to the ICS-Forth network. <https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html>
	2021	Turkish espionage campaigns in the Netherlands <https://www.huntandhackett.com/blog/turkish-espionage-campaigns>
Information	<https://blog.talosintelligence.com/2019/04/seaturtle.html> <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html> <https://blog.strikeready.com/blog/pivoting-through-a-sea-of-indicators-to-spot-turtles/>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
