Earth Krahang - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:26:05 UTC

APT group: Earth Krahang

Names	Earth Krahang *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(Trend Micro) Since early 2022, we have been monitoring an APT campaign that targets several government entities worldwide, with a strong focus in Southeast Asia, but also seen targeting Europe, America, and Africa. The threat actor exploits public-facing servers and sends spear phishing emails to deliver previously unseen backdoors. Our research allowed us to identify the campaign's multiple connections with a China-nexus threat actor we track as Earth Lusca. However, since the campaign employs independent infrastructure and unique backdoors, we believe it to be a separate intrusion set that we named Earth Krahang.
Observed	Sectors: Defense, Education, Financial, Government, Healthcare, Hospitality, IT, Manufacturing, Media, NGOs, Retail, Shipping and Logistics, Telecommunications. Countries: Argentina, Bangladesh, Bolivia, Brazil, Cambodia, Ecuador, Egypt, Hungary, India, Indonesia, Israel, Jordan, Kazakhstan, Kyrgyzstan, Laos, Malaysia, Mexico, Morocco, Myanmar, Nigeria, Oman, Pakistan, Peru, Romania, Rwanda, Saudi Arabia, South Africa, South Korea, Sri Lanka, Tajikistan, Thailand, Turkey, UAE, UK, USA, Uzbekistan, Vietnam.
Tools used	Cobalt Strike, DinodasRAT, PlugX, Reshell, ShadowPad Winnti.
Information	<https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html>

Last change to this card: 22 April 2024

Download this actor card in PDF or JSON format
