Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:35:59 UTC

APT group: Earth Alux

Names	Earth Alux *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2023
Description	(Trend Micro) The Earth Alux APT group's schemes and tactics have been uncloaked through our relentless monitoring and investigation efforts. The China-linked intrusion set is actively launching cyberespionage attacks against the government, technology, logistics, manufacturing, telecommunications, IT services, and retail sectors. The first sighting of its activity was in the second quarter of 2023; back then, it was predominantly observed in the APAC region. Around the middle of 2024, it was also spotted in Latin America. Earth Alux has also been observed to conduct regular tests for some of its toolsets to ensure stealth and longevity in the target environment.
Observed	Sectors: Government, IT, Manufacturing, Retail, Shipping and Logistics, Technology, Telecommunications. Countries: Brazil, Malaysia, Philippines, Taiwan, Thailand.
Tools used	Cobalt Strike, Godzilla, MASQLOADER, RAILLOAD, RAILSETTER, RSBINJECT, VARGEIT.
Information	<https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html>

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
