Earth Baxia - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:36:57 UTC

APT group: Earth Baxia

Names	Earth Baxia *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2024
Description	(Trend Micro) In July, we observed suspicious activity targeting a government organization in Taiwan, with other APAC countries also likely targeted, attributed to the threat actor Earth Baxia. In these campaigns, Earth Baxia used spear-phishing emails and exploited CVE-2024-36401, a vulnerability in an open-source server for sharing geospatial data called GeoServer, as initial access vectors, deploying customized Cobalt Strike components on compromised machines. Additionally, we identified a new backdoor called EAGLEDOOR that supports multiple protocols. In this report, we will discuss their infection chain and provide a detailed analysis of the malware involved.
Observed	Sectors: Energy, Government. Countries: China, Philippines, South Korea, Taiwan, Thailand, Vietnam.
Tools used	Cobalt Strike, EAGLEDOOR.
Information	<https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html> <https://www.trendmicro.com/en_us/research/25/h/new-ransomware-charon.html>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
