Earth Ammit - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:16:20 UTC

APT group: Earth Ammit

Names	Earth Ammit *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(Trend Micro) Earth Ammit, a threat actor linked to Chinese-speaking APT groups, launched two waves of campaigns from 2023 to 2024. The first wave, VENOM, mainly targeted software service providers, and the second wave, TIDRONE mainly targeted the military industry. In its VENOM campaign, Earth Ammit's approach involved penetrating the upstream segment of the drone supply chain. In the VENOM campaign, the threat actors primarily relied on open-source tools due to low cost and difficult tracking. They shifted to custom-built tools like CXCLNT and CLNTEND in the TIDRONE campaign for cyberespionage purposes. Victims of the TIDRONE and VENOM campaigns primarily originated from Taiwan and South Korea, affecting a range of industries including military, satellite, heavy industry, media, technology, software services, and healthcare sectors. Earth Ammit’s long-term goal is to compromise trusted networks via supply chain attacks, allowing them to target high-value entities downstream and amplify their reach. Organizations that fall prey to these attacks are also at risk of data theft, including exfiltration of credentials and screenshots.
Observed	Countries: Canada, South Korea, Taiwan.
Tools used	
Information	<https://www.trendmicro.com/en_us/research/25/e/earth-ammit.html>

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format