Subgroup: Earth Longzhi - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Earth Longzhi

Names	Earth Longzhi *(Trend Micro)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2020	
Description	A subgroup of APT 41. (Trend Micro) In early 2022, we investigated an incident that compromised a company in Taiwan. The malware used in the incident was a simple but custom Cobalt Strike loader. After further investigation, however, we found incidents targeting multiple regions using a similar Cobalt Strike loader. While analyzing code similarities and tactics, techniques, and procedures (TTPs), we discovered that the actor behind this attack has been active since 2020. After clustering each intrusion, we concluded that the threat actor is a new subgroup of advanced persistent threat (APT) group APT41 that we call Earth Longzhi.	
Observed	Sectors: Aviation, Defense, Education, Financial, Government, Healthcare. Countries: China, Fiji, Indonesia, Malaysia, Pakistan, Philippines, Taiwan, Thailand, Ukraine.	
Tools used	BigpipeLoader, Cobalt Strike, CroxLoader, MultiPipeLoader, OutLoader, Symatic Loader.	
Operations performed	Apr 2023	Attack on Security Titans: Earth Longzhi Returns With New Tricks <https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html>
Information	<https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html>	

Last change to this card: 12 October 2023

Download this actor card in PDF or JSON format
