Earth Kurma - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:15:24 UTC

APT group: Earth Kurma

Names	Earth Kurma *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2020
Description	(Trend Micro) Trend Research uncovered a sophisticated APT campaign targeting government and telecommunications sectors in Southeast Asia. Named Earth Kurma, the attackers use advanced custom malware, rootkits, and cloud storage services for data exfiltration. Earth Kurma demonstrates adaptive malware toolsets, strategic infrastructure abuse, and complex evasion techniques. This campaign poses a high business risk due to targeted espionage, credential theft, persistent foothold established through kernel-level rootkits, and data exfiltration via trusted cloud platforms. Organizations primarily in government and telecommunications sectors in Southeast Asia (particularly the Philippines, Vietnam, Thailand, Malaysia) are affected. Organizations face potential compromise of sensitive government and telecommunications data, with attackers maintaining prolonged, undetected access to their networks. May be related to Operation TunnelSnake or ToddyCat.
Observed	Sectors: Government, Telecommunications. Countries: Malaysia, Philippines, Thailand, Vietnam.
Tools used	Cobalt Strike, DMLOADER, DUNLOADER, KRNRAT, Moriya, ODRIZ, SIMPOBOXSPY, TESDAT.
Information	<https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html>

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format
