

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:47:45 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool DMLOADER


Tool: DMLOADER

Names	DMLOADER
Category	Malware
Type	Loader
Description	(Trend Micro) More recently, we observed a new loader, DMLOADER, was implanted. Instead of loading an additional payload file, it loads the embedded payload and decodes it as an in-memory PE buffer. This loader usually has an export function called “DoMain” or “StartProtect.” In the decoded PE payload, it should have an export function called “MThread.”
Information	< https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html >

Last change to this tool card: 27 June 2025

Download this tool card in [JSON](#) format

All groups using tool DMLOADER

Changed	Name	Country	Observed
APT groups			
	Earth Kurma		2020

1 group listed (1 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5b6875e1-8d92-44bf-89b5-57fd46577729>