

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:21:38 UTC

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


## Tool: MASQLOADER

Names	MASQLOADER
Category	<a href="#">Malware</a>
Type	<a href="#">Loader</a>
Description	<a href="#">(Trend Micro)</a> The first observed loading method used to execute COBEACON payloads is via MASQLOADER, a DLL side-loaded loader. This loader component decrypts its payload using a substitution cipher, where the encrypted payload contains 1-3 character strings that has a hex value equivalent based on MASQLOADER's substitution table.
Information	< <a href="https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html">https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html</a> >

Last change to this tool card: 21 April 2025

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

### All groups using tool MASQLOADER

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Earth Alux</a>		2023

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0b20666a-9fc2-48e9-b52d-96645879c137>