

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:43:44 UTC

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

Tool: Gelsenicine

Names	Gelsenicine
Category	Malware
Type	Loader
Description	(ESET) Gelsenicine is a loader that retrieves Gelsevirine and executes it. There are two different versions of the loader – both of them are DLLs; however, they differ in the context where Gelsemine is executed.
Information	< https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf >
MITRE ATT&CK	< https://attack.mitre.org/software/S0666/ >

Last change to this tool card: 30 December 2022

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

All groups using tool Gelsenicine

Changed	Name	Country	Observed
APT groups			
	Gelsemium		2014-2023

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=88332db7-b2a7-483a-87ce-5d774c9f74dc>