Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:19:26 UTC

Tool: Gelsemine

Names	Gelsemine
Category	Malware
Type	Dropper
Description	(ESET) Gelsemium's first stage is a large dropper written in C++ using the Microsoft Foundation Class library (MFC). This stage contains multiple further stages' binaries. Dropper sizes range from about 400 kB to 700 kB, which is unusual and would be even larger if the eight embedded executables were not compressed. The developers use the zlib library, statically linked, to greatly reduce the overall size.
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 Gelsemine

Changed	Name	Country	Observed	
APT groups				
	Gelsemium		2014-2023	

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