Threat Group Cards: A Threat Actor Encyclopedia

Tool: Gelsevirine

Names	Gelsevirine
Category	Malware
Type	Backdoor
Description	(ESET) Gelsevirine is the last stage of the chain and it is called MainPlugin by its developers, according to the DLL name and also PDB path found in old samples (Z:\z_code\Q1\Client\Win32\Release\MainPlugin.pdb). It's also worth mentioning that if defenders manage to obtain this last stage alone, it won't run flawlessly since it requires its arguments to be set up by Gelsenicine.
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 Gelsevirine

Changed	Name	Country	Observed	
APT groups				
	Gelsemium		2014-2023	

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