Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:46:15 UTC

APT group: Gelsemium

Names	Gelsemium *(ESET)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2014	
Description	(ESET) The Gelsemium group has been active since at least 2014 and was described in the past by a few security compar name comes from one possible translation we found while reading a report from VenusTech who dubbed the group 狼毒 time .It's the name of a genus of flowering plants belonging to the family Gelsemiaceae, Gelsemium elegans is the specie toxic compounds like Gelsemine, Gelsenicine and Gelsevirine, which we chose as names for the three components of this	
Observed	Sectors: Education, Gaming, Government, High-Tech, NGOs and religious organizations. Countries: Argentina, Brunei, China, Djibouti, Egypt, Equatorial Guinea, Hong Kong, Indonesia, Iran, Iraq, Israel, Japan, Laos, Lebanon, Malaysia, Mongolia, Nigeria, North Korea, Oman, Pakistan, Russia, Saudi Arabia, South Korea, Sri Lanl Syria, Taiwan, Thailand, Turkey, UAE, UK, Vietnam, Yemen.	
Tools used	ASPXSpy, BadPotato, China Chopper, Chrommme, EarthWorm, Cobalt Strike, FireWood, Gelsemine, Gelsenicine, Gels JuicyPotato, Owowa, OwlProxy, reGeorg, SessionManager, SpoolFool, SweetPotato, WolfsBane.	
Operations performed	2014	Operation "TooHash" <https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_10
	Jan 2021	Operation "NightScout" A new supply-chain attack compromising the update mechanism of NoxPlayer, an Android emulator for PC part of BigNox's product range with over 150 million users worldwide. <https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia
	Dec 2021	Kaspersky discovers poorly detected backdoor, targeting governments and NGOs around the globe <https://www.kaspersky.com/about/press-releases/2022_kaspersky-discovers-poorly-detected-backdoor-tar governments-and-ngos-around-the-globe>
	Mid 2022	Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Gov <https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/>
	2023	Unveiling WolfsBane: Gelsemium's Linux counterpart to Gelsevirine <https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-g
Information	<https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf> <https://www.venustech.com.cn/uploads/2018/08/231401512426.pdf>	

Last change to this card: 26 December 2024

Download this actor card in PDF or JSON format