Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:03:11 UTC

Tool: Predator

Names	Predator Lycantrox
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Amnesty International) Shocking spyware attacks have been attempted against civil society, journalists, politicians and academics in the European Union (EU), USA and Asia, according to a major new investigation by Amnesty International. Among the targets of Predator spyware are United Nations (UN) officials, a Senator and Congressman in the USA and even the Presidents of the European Parliament and Taiwan. The investigation is part of the 'Predator Files' project, in partnership with the European Investigative Collaborations (EIC) and backed by additional in-depth reporting by Mediapart and Der Spiegel.
Information	<https://securitylab.amnesty.org/latest/2023/10/predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/> <https://eic.network/projects/predator-files.html> <https://citizenlab.ca/2023/10/predator-spyware-targets-us-eu-lawmakers-journalists/> <https://blog.sekoia.io/active-lycantrox-infrastructure-illumination/> <https://www.recordedfuture.com/predator-spyware-operators-rebuild-multi-tier-infrastructure-target-mobile-devices> <https://blog.sekoia.io/the-predator-spyware-ecosystem-is-not-dead/> <https://www.bleepingcomputer.com/news/legal/us-sanctions-predator-spyware-operators-for-spying-on-americans/> <https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions> <https://www.bleepingcomputer.com/news/security/us-cracks-down-on-spyware-vendor-intellexa-with-more-sanctions/> <https://www.recordedfuture.com/research/predator-still-active-new-links-identified>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool Predator

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=410ad12c-49df-4c9e-b318-90082a778aa8