Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:36:12 UTC

APT group: Agrius

Names	Agrius *(SentinelLabs)* DEV-0227 *(Microsoft)* BlackShadow *(Kaspersky)* SharpBoys *(?)* AMERICIUM *(Microsoft)* Pink Sandstorm *(Microsoft)* Agonizing Serpens *(Palo Alto)* Spectral Kitten *(CrowdStrike)*	
Country	Iran	
Motivation	Information theft and espionage, Sabotage and destruction	
First seen	2020	
Description	(SentinelLabs) A new threat actor SentinelLabs track as Agrius was observed operating in Israel beginning in 2020. An analysis of what at first sight appeared to be a ransomware attack revealed new variants of wipers that were deployed in a set of destructive attacks against Israeli targets. The operators behind the attacks intentionally masked their activity as ransomware attacks.	
Observed	Countries: Hong Kong, Israel, South Africa.	
Tools used	Apostle, ASPXSpy, BFG Agonizer Wiper, DEADWOOD, Fantasy, IPsec Helper, Moneybird, MultiLayer Wiper, PartialWasher Wiper, Sqlextractor.	
Operations performed	Feb 2022	Fantasy – a new Agrius wiper deployed through a supply-chain attack <https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/>
	May 2023	Agrius Deploys Moneybird in Targeted Attacks Against Israeli Organizations <https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/>
Information	<https://assets.sentinelone.com/sentinellabs/evol-agrius>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
