Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:06:59 UTC

Tool: SUGARLOADER

Names	SUGARLOADER
Category	Malware
Type	Loader
Description	(Elastic) SUGARLOADER is used for initial access on the machine, and initializing the environment for the final stage. This binary is obfuscated using a binary packer, limiting what can be seen with static analysis.
Information	<https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.sugarloader>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool SUGARLOADER

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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