Threat Group Cards: A Threat Actor Encyclopedia

Tool: KANDYKORN

Names	KANDYKORN
Category	Malware
Type	Backdoor, Exfiltration
Description	(Elastic) KANDYKORN is the final stage of this execution chain and possesses a full-featured set of capabilities to access and exfiltrate data from the victim's computer. Elastic Security Labs was able to retrieve this payload from one C2 server which hadn't been deactivated yet.
Information	<https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.kandykorn>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool KANDYKORN

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

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