Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:19:02 UTC

Tool: Sqlextractor

Names	Sqlextractor
Category	Malware
Type	Info stealer
Description	(Palo Alto) The attackers used a custom tool they named sqlextractor (binary name sql.net4.exe). Its purpose is to query SQL databases and extract sensitive PII data, such as the following: • ID numbers • Passport scans • Emails • Full addresses
Information	<https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/>

Last change to this tool card: 29 November 2023

Download this tool card in JSON format

All groups using tool Sqlextractor

Changed	Name	Country	Observed	
APT groups				
	Agrius		2020-May 2023	

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