Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:50:53 UTC

Tool: SQLRAT

Names	SQLRAT
Category	Malware
Type	Backdoor, Loader
Description	(Flashpoint) The SQLRat script is designed to make a direct SQL connection to a Microsoft database controlled by the attackers and execute the contents of various tables. The script retrieves an item from the bindata table and writes the file to disk. This file appears to primarily be a version of TinyMet—an open source Meterpreter stager—but the actors have the option to store and execute any binary loaded into the table.
Information	<https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0390/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.sqlrat>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool SQLRAT

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	FIN7		2013-Jul 2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=15b99961-7edf-4f39-a9eb-b74bfac2557d