Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:36:29 UTC

Tool: gsecdump

Names	gsecdump
Category	Tools
Type	Credential stealer
Description	gsecdump is a publicly-available credential dumper used to obtain password hashes and LSA secrets from Windows operating systems.
Information	<https://download.openwall.net/pub/projects/john/contrib/win32/pwdump/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0008/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gsecdump>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:GSecDump>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool gsecdump

Changed	Name	Country	Observed	
APT groups				
	Bronze Butler, Tick, RedBaldNight, Stalker Panda		2006-Apr 2021	
	Comment Crew, APT 1		2006-May 2018	
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	Night Dragon		2009	

	PittyTiger, Pitty Panda		2011-2014	
	Suckfly		2014-Late 2015	
	TaskMasters		2010-May 2021	

7 groups listed (7 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=77c08472-aa1f-41ac-aa25-7ee0568b294e