Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:29:32 UTC

Tool: ProcDump

Names	ProcDump
Category	Tools
Type	Credential stealer
Description	ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike. ProcDump also includes hung window monitoring (using the same definition of a window hang that Windows and Task Manager use), unhandled exception monitoring and can generate dumps based on the values of system performance counters. It also can serve as a general process dump utility that you can embed in other scripts. Part of SysInternals.
Information	<https://docs.microsoft.com/en-us/sysinternals/downloads/procdump>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool ProcDump

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Scattered Spider	[Unknown]	2022-Aug 2025	
	Antlion		2011	
	APT 20, Violin Panda		2014-2017	

	Comment Crew, APT 1		2006-May 2018	
	Dalbit		2022	
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	FIN13	[Unknown]	2016	
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	
	Hydrochasma	[Unknown]	2022	
	IAmTheKing		2018	
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	
	Kimsuky, Velvet Chollima		2012-Aug 2025	
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	Operation Harvest		2016	
	Salt Typhoon, GhostEmperor		2020-Feb 2025	
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	
	TaskMasters		2010-May 2021	
	UNC215		2019	

Other groups

	Parinacota	[Unknown]	2018	

19 groups listed (18 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bbc02c6f-31ae-404c-8e7c-75ed7b42600a