Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:26:34 UTC

Tool: certutil

Names	certutil certutil.exe
Category	Tools
Description	certutil is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services.
Information	<https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while-bypassing-av/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0160/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool certutil

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	
	Pinchy Spider, Gold Southfield		2018-Oct 2024	
	Rancor		2017	
	Salt Typhoon, GhostEmperor		2020-Feb 2025	
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

	Stone Panda, APT 10, menuPass		2006-Mar 2025	
	Turla, Waterbug, Venomous Bear		1996-2024	
	UNC215		2019	

9 groups listed (9 APT, 0 other, 0 unknown)
