Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:14:06 UTC

Tool: SpoolFool

Names	SpoolFool
Category	Exploits
Description	(Palo Alto) n addition to using the Potato Suite mentioned above, the attackers also used another local privilege escalation (LPE) proof of concept (PoC) published on GitHub called SpoolFool, as shown in Figure 2 above. This tool exploits CVE-2022-21999 (Windows Print Spooler Elevation of Privilege Vulnerability).
Information	<https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/>

Last change to this tool card: 12 October 2023

Download this tool card in JSON format

All groups using tool SpoolFool

Changed	Name	Country	Observed	
APT groups				
	Gelsemium		2014-2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4a4b1383-1b5e-439f-8929-291e36cd9c58