Threat Group Cards: A Threat Actor Encyclopedia

Tool: THINSPOOL

Names	THINSPOOL
Category	Malware
Type	Dropper
Description	(Mandiant) THINSPOOL is a dropper written in shell script that writes the web shell LIGHTWIRE to a legitimate CS file. THINSPOOL will re-add the malicious web shell code to legitimate files after an update, allowing UNC5221 to persist on the compromised devices. THINSPOOL attempts to evade Ivanti's Integrity Checker but Mandiant observed this attempt failed.
Information	<https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool THINSPOOL

Changed	Name	Country	Observed	
APT groups				
	UNC5221, UTA0178		2022-Mar 2025	

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