Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:35:00 UTC

Tool: DanderSpritz

Names	DanderSpritz
Category	Malware
Type	Control panel
Description	(Check Point) DanderSpritz is a full-featured post-exploitation framework used by the Equation Group. This framework was usually leveraged after exploiting a machine and deploying the PeddleCheap “implant”. DanderSpritz is very modular and contains a wide variety of tools for persistence, reconnaissance, lateral movement, bypassing Antivirus engines, and other such shady activities. It was leaked by The Shadow Brokers on April 14th, 2017 as part of the “Lost in Translation” leak.
Information	<https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/>

Last change to this tool card: 25 January 2022

Download this tool card in JSON format

All groups using tool DanderSpritz

Changed	Name	Country	Observed	
APT groups				
	Equation Group		2001-Aug 2016	

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