Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:23:19 UTC

Tool: PowerStallion

Names	PowerStallion
Category	Malware
Type	Backdoor
Description	(ESET) PowerStallion is a lightweight PowerShell backdoor using Microsoft OneDrive, a storage service in the cloud, as C&C server. The credentials are hardcoded at the beginning of the script.
Information	<https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0393/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool PowerStallion

Changed	Name	Country	Observed	
APT groups				
	Turla, Waterbug, Venomous Bear		1996-2024	

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