Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:10:38 UTC

Tool: PolyglotDuke

Names	PolyglotDuke
Category	Malware
Type	Backdoor
Description	(ESET) Uses Twitter or other websites such as Reddit and Imgur to get its C&C URL. It also relies on steganography in images for its C&C communication.
Information	<https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0518/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.polyglotduke>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool PolyglotDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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