Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:29:16 UTC

Tool: TAMECAT

Names	TAMECAT
Category	Malware
Type	Backdoor
Description	(Mandiant) TAMECAT is a PowerShell toehold that can execute arbitrary PowerShell or C# content. TAMECAT has been observed dropped by malicious macro documents, communicates with its C2 node via HTTP, and expects data from the C2 to be Base64-encoded.
Information	<https://www.mandiant.com/media/17826>
MITRE ATT&CK	<https://attack.mitre.org/software/S1193>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool TAMECAT

Changed	Name	Country	Observed	
APT groups				
	APT 42		2015-Feb 2024	
	GreenCharlie		2020	

2 groups listed (2 APT, 0 other, 0 unknown)
