Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:29:32 UTC

Tool: CHAVECLOAK

Names	CHAVECLOAK
Category	Malware
Type	Banking trojan, Reconnaissance, Backdoor, Info stealer, Credential stealer
Description	(Fortinet) FortiGuard Labs recently uncovered a threat actor employing a malicious PDF file to propagate the banking Trojan CHAVECLOAK. This intricate attack involves the PDF downloading a ZIP file and subsequently utilizing DLL side-loading techniques to execute the final malware. Notably, CHAVECLOAK is specifically designed to target users in Brazil, aiming to steal sensitive information linked to financial activities.
Information	<https://www.fortinet.com/blog/threat-research/banking-trojan-chavecloak-targets-brazil>

Last change to this tool card: 07 March 2024

Download this tool card in JSON format

All groups using tool CHAVECLOAK

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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