Dark Tequila - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:37:49 UTC

Tool: Dark Tequila

Names	Dark Tequila DarkTequila
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer
Description	(Kaspersky) Dark Tequila is a complex malicious campaign targeting Mexican users, with the primary purpose of stealing financial information, as well as login credentials to popular websites that range from code versioning repositories to public file storage accounts and domain registrars. A multi-stage payload is delivered to the victim only when certain conditions are met; avoiding infection when security suites are installed or the sample is being run in an analysis environment. From the target list retrieved from the final payload, this particular campaign targets customers of several Mexican banking institutions and contains some comments embedded in the code written in the Spanish language, using words only spoken in Latin America.
Information	<https://securelist.com/dark-tequila-anejo/87528/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.darktequila>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Dark Tequila

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

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