

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:20:07 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool DarkMe

Tool: DarkMe

Names	DarkMe
Category	Malware
Type	Reconnaissance , Backdoor , Info stealer
Description	(NSFOCUS) DarkMe is a Visual Basic spy Trojan. Its initial version appeared on September 25, 2021. Currently, it supports host information collection, screenshot, file manipulation, registry manipulation, cmd command execution, self-update, persistence and other functions.
Information	< https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/ > < https://nsfocusglobal.com/operation-darkcasino-in-depth-analysis-of-attacks-by-apt-group-evilnum-part-2/ > < https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.darkme >

Last change to this tool card: 06 March 2024

Download this tool card in [JSON](#) format

All groups using tool DarkMe

Changed	Name	Country	Observed
APT groups			
	DarkCasino	[Unknown]	2021

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