Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:16:30 UTC

Tool: VIDAR

Names	VIDAR Vidar Stealer
Category	Malware
Type	Info stealer, Credential stealer
Description	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.
Information	<https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware> <https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d> <https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/> <https://tccontre.blogspot.com/2019/03/infor-stealer-vidar-trojanspy-analysis.html> <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf> <https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/> <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/vidar-malware-launcher-concealed-in-help-file/> <https://asec.ahnlab.com/en/44554/> <https://thehackernews.com/2023/01/raccoon-and-vidar-stealers-spreading.html> <https://www.team-cymru.com/post/darth-vidar-the-aesir-strike-back> <https://www.trendmicro.com/en_us/research/23/i/redline-vidar-first-abuses-ev-certificates.html> <https://asec.ahnlab.com/en/58750/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar>

Last change to this tool card: 29 November 2023

Download this tool card in JSON format

All groups using tool VIDAR

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Scattered Spider	[Unknown]	2022-Aug 2025	
	FIN11	[Unknown]	2016-Mar 2025	
	Pinchy Spider, Gold Southfield		2018-Oct 2024	

3 groups listed (3 APT, 0 other, 0 unknown)

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ebc3d7df-80c6-4979-ae55-1bac4823e315