Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:36:47 UTC

Tool: Snatch

Names	Snatch
Category	Malware
Type	Ransomware
Description	Snatch is a ransomware which infects victims by rebooting the PC into Safe Mode. Most of the existing security protections do not run in Safe Mode so that it the malware can act without expected countermeasures and it can encrypt as many files as it finds. It uses common packers such as UPX to hide its payload.
Information	<https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.snatch>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Snatch

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	
Other groups				
	TA554	[Unknown]	2017	

2 groups listed (1 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a338ae80-2971-4968-b679-0bd59ceb9906