Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:05:40 UTC

Tool: Sardonic

Names	Sardonic Ragnar Loader
Category	Malware
Type	Backdoor
Description	(Bitdefender) As this backdoor has not been documented or referenced before, we named it “Sardonic”, given that artifacts led us to believe the threat actors use this name for an entire project including the backdoor itself, the loader and some additional scripts. We believe this project is still under development, and additional updates will likely follow. Key facts about Sardonic: • Sardonic is a new backdoor in the FIN8 ecosystem • Sardonic is a project still under development and includes several components • The new components were identified in a real-life attack and seems to be compiled just before the attack • Sardonic backdoor is extremely potent and has a wide range of capabilities that help the threat actor leverage new malware on the fly without updating components
Information	<https://www.bitdefender.com/files/News/CaseStudies/study/401/Bitdefender-PR-Whitepaper-FIN8-creat5619-en-EN.pdf> <https://catalyst.prodaft.com/public/report/ragnar-loader/overview>
MITRE ATT&CK	<https://attack.mitre.org/software/S1085>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_103>

Last change to this tool card: 21 April 2025

Download this tool card in JSON format

All groups using tool Sardonic

Changed	Name	Country	Observed	
APT groups				
	FIN7		2013-Jul 2024	
	FIN8	[Unknown]	2016-Dec 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1ef6307c-a55a-42d4-837d-9c7302df751a