Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:05:59 UTC

Tool: Sasfis

Names	Sasfis Oficla
Category	Malware
Type	Downloader
Description	Sasfis acts mostly as a downloader that has been observed to download Asprox and FakeAV. According to a VirusBulletin article from 2012, it is likely authored by the same group as SmokeLoader.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/sasfis-malware-uses-a-new-trick/> <https://blog.trendmicro.com/trendlabs-security-intelligence/sasfis-fizzles-in-the-background/> <https://isc.sans.edu/forums/diary/Sasfis+Propagation/8860/> <https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Sasfis-O/detailed-analysis.aspx> <https://www.virusbulletin.com/virusbulletin/2012/11/tracking-2012-sasfis-campaign>
MITRE ATT&CK	<https://attack.mitre.org/software/S0138>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sasfis>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Sasfis

Changed	Name	Country	Observed	
Other groups				
	Smoky Spider	[Unknown]	2011-Apr 2019	

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

↑
