

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:05:42 UTC

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

↪ Tool: Sisfader

Names	Sisfader Sisfader RAT
Category	Malware
Type	Backdoor , Info stealer
Description	(NCC Group) The payload installed by the WLL file is not a common RAT. We believe it to be either new or custom. Context Information Security, one of the other industry partners on the UK Cyber Incident Response scheme, has named this RAT Sisfader. We have adopted this name for consistency. It maintains persistence installing itself as a system service and has multiple components.
Information	< https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8570-rtf-and-the-sisfader-rat/ > < https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.sisfader >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:Sisfader >

Last change to this tool card: 14 May 2020

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

All groups using tool Sisfader

Changed	Name	Country	Observed
APT groups			
	Goblin Panda , Cycldek , Conimes		2013-Jun 2020
	Naikon , Lotus Panda		2010-Apr 2022

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

Source: <https://apt.etaa.or.th/cgi-bin/listgroups.cgi?u=2f42d87f-40c0-463e-8f89-ee1a9f7c8ea9>