

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:33:53 UTC

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

Tool: Sisron

Names	Sisron
Category	Malware
Type	Banking trojan , Backdoor , Info stealer , Credential stealer , Botnet
Description	(johannesbader) Sisron was part of a financial fraud and identity theft botnet. It was taken down by Microsoft in the anti-botnet operation B106. The malware uses a very simple domain generation algorithm (DGA) that produces sets of similar looking domains.
Information	< https://johannesbader.ch/blog/the-dga-of-sisron/ >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:sisron >

Last change to this tool card: 24 May 2020

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

All groups using tool Sisron

Changed	Name	Country	Observed
Unknown groups			
	_ [Interesting malware not linked to an actor yet] _		

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9579e3cd-0dec-47fc-9e96-bf4bd7968273>