

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:16:59 UTC

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

Tool: Sword

Names	Sword
Category	Malware
Type	Backdoor , Exfiltration , Tunneling
Description	This family of malware provides a backdoor over the network to the attackers. It is configured to connect to a single host and offers file download over HTTP, program execution, and arbitrary execution of commands through a cmd.exe instance.
Information	< https://citizenlab.ca/2013/02/apt1s-glasses-watching-a-human-rights-organization/ > < http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.sword >

Last change to this tool card: 23 April 2020

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

All groups using tool Sword

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cf43eaf3-c6e8-4f75-bae6-4566ac3f5119>