

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:57:19 UTC

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

## Tool: CHAIRSMACK

Names	CHAIRSMACK
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	<a href="#">(Mandiant)</a> CHAIRSMACK is a backdoor written in C++ that communicates using HTTP. CHAIRSMACK's core functionality involves expanding its capabilities by retrieving plugins from a C2 server. Downloaded plugins are cached on disk for future use. Capabilities added via plugins are inferred based on supported backdoor command names. These capabilities include shell command execution, screenshot capture, audio capture, keylogging, file transfer, and file execution.
Information	< <a href="https://www.mandiant.com/media/17826">https://www.mandiant.com/media/17826</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.chairsmack">https://malpedia.caad.fkie.fraunhofer.de/details/win.chairsmack</a> >

Last change to this tool card: 27 December 2022

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

## All groups using tool CHAIRSMACK

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">APT 42</a>		2015-Feb 2024

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f6e9b97e-8e22-43a4-9b5d-8b4d7532ee86>