

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:53:29 UTC

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

## Tool: CloudScout

Names	CloudScout
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	<a href="#">(ESET)</a> In this blogpost, we provide a technical analysis of CloudScout, a post-compromise toolset used by Evasive Panda to target a government entity and a religious organization in Taiwan from 2022 to 2023. The CloudScout toolset is capable of retrieving data from various cloud services by leveraging stolen web session cookies. Through a plugin, CloudScout works seamlessly with MgBot, Evasive Panda's signature malware framework.
Information	< <a href="https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/">https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_scout">https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_scout</a> >

Last change to this tool card: 27 December 2024

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

### All groups using tool CloudScout

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Bronze Highland</a>		2012-Jul 2024

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