

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:58:29 UTC

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

## Tool: Macma

Names	Macma MacMa CDDS OSX.CDDS DazzleSpy
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Info stealer</a> , <a href="#">Credential stealer</a> , <a href="#">Exfiltration</a>
Description	<p>(<a href="#">Symantec</a>) Macma is a macOS backdoor that was first documented by Google in 2021 but appears to have been used since at least 2019. At the time of discovery, it was being distributed in watering hole attacks involving compromised websites in Hong Kong. The watering holes contained exploits for iOS and macOS devices. Users of macOS devices were targeted with a privilege escalation vulnerability (CVE-2021-30869) which allowed the attackers to install Macma on vulnerable systems.</p> <p>Macma is a modular backdoor. Functionality includes:</p> <ul style="list-style-type: none"><li>• Device fingerprinting</li><li>• Executing commands</li><li>• Screen capture</li><li>• Keylogging</li><li>• Audio capture</li><li>• Uploading and downloading files</li></ul>
Information	< <a href="https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset">https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S1016">https://attack.mitre.org/software/S1016</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/osx.cdds">https://malpedia.caad.fkie.fraunhofer.de/details/osx.cdds</a> >

Last change to this tool card: 28 June 2025

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

## All groups using tool Macma

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)

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=069c86ae-99de-4486-a5c4-fa3616d2a2a4>