Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:58:38 UTC

Tool: OceanLotus

Names	OceanLotus OSX_OCEANLOTUS.D Backdoor.MacOS.OCEANLOTUS.F
Category	Malware
Type	Backdoor
Description	OSX_OCEANLOTUS.D is a MacOS backdoor that has been used by APT32.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/> <https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/> <https://researchcenter.paloaltonetworks.com/2017/06/unit42-new-improved-macos-backdoor-oceanlotus/> <https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update>
MITRE ATT&CK	<https://attack.mitre.org/software/S0352/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.oceanlotus>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool OceanLotus

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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

↑