Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:24:05 UTC

Tool: Oceansalt

Names	Oceansalt
Category	Malware
Type	Reconnaissance, Backdoor
Description	(McAfee) Oceansalt reuses a portion of code from the Seasalt implant (circa 2010) that is linked to the Chinese hacking group Comment Crew. Oceansalt appears to be the first stage of an advanced persistent threat. The malware can send system data to a control server and execute commands on infected machines, but we do not yet know its ultimate purpose.
Information	<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0346/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.oceansalt>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Oceansalt

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f3a4d2fb-22d9-4e95-930a-86af8a0df5ce