Ocean - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:12:49 UTC

Tool: Pro-Ocean

Names	Pro-Ocean
Category	Malware
Type	Miner
Description	(Palo Alto) Pro-Ocean uses known vulnerabilities to target cloud applications. In our analysis, we found Pro-Ocean targeting Apache ActiveMQ (CVE-2016-3088), Oracle WebLogic (CVE-2017-10271) and Redis (unsecure instances). In the case that the malware runs in Tencent Cloud or Alibaba Cloud, it will use the exact code of the previous malware to uninstall monitoring agents to avoid detection. Additionally, it attempts to remove other malware and miners including Luoxk, BillGates, XMRig and Hashfish before installation. Once installed, the malware kills any process that uses the CPU heavily, so that it's able to use 100% of the CPU and mine Monero efficiently.
Information	<https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/> <https://seguranca-informatica.pt/new-cryptojacking-malware-called-pro-ocean-is-now-attacking-apache-oracle-and-redis-servers/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.pro_ocean>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Pro-Ocean

Changed	Name	Country	Observed	
Other groups				
	Rocke, Iron Group		2018-Apr 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=794ffbdf-64e6-4f00-911d-a359a08c02a5