Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:46:45 UTC

Tool: OCEANMAP

Names	OCEANMAP
Category	Malware
Type	Backdoor
Description	(BleepingComputer) Another tool used as part of the attack is the 'OCEANMAP,' a C# backdoor used primarily for executing base64-encoded commands via cmd.exe. OCEANMAP establishes persistence on the system by creating a .URL file named 'VMSearch.url' in the Windows Startup folder. OCEANMAP uses the Internet Message Access Protocol (IMAP) as a control channel to receive commands discreetly that are unlikely to raise alarms, storing them as email drafts containing the command, username, and OS version.
Information	<https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-ukraine-with-new-masepie-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.oceanmap>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool OCEANMAP

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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