Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:43:16 UTC

Tool: SeaDuke

Names	SeaDuke SeaDaddy SeaDesk SeaDask
Category	Malware
Type	Backdoor, Exfiltration
Description	(F-Secure) SeaDuke is a simple backdoor that focuses on executing commands retrieved from its C&C server, such as uploading and downloading files, executing system commands and evaluating additional Python code. SeaDuke is made interesting by the fact that it is written in Python and designed to be cross-platform so that it works on both Windows and Linux. The only known infection vector for SeaDuke is via an existing CozyDuke infection, wherein CozyDuke downloads and executes the SeaDuke toolset. Like HammerDuke, SeaDuke appears to be used by the Dukes group primarily as a secondary backdoor left on CozyDuke victims after that toolset has completed the initial infection and stolen any readily available information from them.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf> <https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html> <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0053/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.seadaddy>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:seaduke>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SeaDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8fe4f869-e5d7-4844-ab0b-57d67fd38000