

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:54:41 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool NanHaiShu



Tool: NanHaiShu

Names	NanHaiShu
Category	Malware
Type	Reconnaissance , Backdoor
Description	(F-Secure) Once installed on a machine in the target network, NanHaiShu sends information from the infected machine to a remote command and control (C&C) server.
Information	< https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf > < https://community.spiceworks.com/topic/1028936-stealthy-cyberespionage-campaign-attacks-with-social-engineering > < https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets >
MITRE ATT&CK	< https://attack.mitre.org/software/S0228/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/js.nanhaishu >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:NanHaiShu >

Last change to this tool card: 13 May 2020

Download this tool card in [JSON](#) format

All groups using tool NanHaiShu

Changed	Name	Country	Observed	
APT groups				
	Leviathan , APT 40 , TEMP.Periscope		2013-Jul 2021	

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=3e475211-36fc-4c58-801c-fa3ce5da0879>