

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:50:24 UTC

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

## ↪ Tool: Shipshape

Names	Shipshape
Category	<a href="#">Malware</a>
Type	<a href="#">Worm</a> , <a href="#">Exfiltration</a>
Description	SHIPSHAPE is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.
Information	< <a href="https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/rpt-apt30.pdf">https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/rpt-apt30.pdf</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0028/">https://attack.mitre.org/software/S0028/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.shipshape">https://malpedia.caad.fkie.fraunhofer.de/details/win.shipshape</a> >
AlienVault OTX	< <a href="https://otx.alienvault.com/browse/pulses?q=tag:SHIPSHAPE">https://otx.alienvault.com/browse/pulses?q=tag:SHIPSHAPE</a> >

Last change to this tool card: 23 April 2020

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

## All groups using tool Shipshape

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">APT 30, Override Panda</a>		2005
	<a href="#">Naikon, Lotus Panda</a>		2010-Apr 2022

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=716fb64d-8dc0-4d92-96b6-60604a14aab2>