

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:09:18 UTC

Tool: Wingbird

Names	Wingbird
Category	Malware
Type	Backdoor , Info stealer
Description	Wingbird is a backdoor that appears to be a version of commercial software FinFisher . It is reportedly used to attack individual computers instead of networks. It was used by NEODYMIUM in a May 2016 campaign.
Information	<p><http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf></p> <p><http://www.finfisher.com/FinFisher/index.html></p> <p><https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/></p> <p><https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/></p> <p><https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S0176/ >

Last change to this tool card: 30 December 2022

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

All groups using tool Wingbird

Changed	Name	Country	Observed
APT groups			
	BlackOasis	[Middle East]	2015-Oct 2017
	Neodymium		2016

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

[↑](#)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=de3054dc-0e37-4268-976d-c928ddfaabb5>