


Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:27:05 UTC

APT group: Neodymium

Names	Neodymium (<i>Microsoft</i>) G0055 (<i>MITRE</i>)
Country	 Turkey
Motivation	Information theft and espionage
First seen	2016
Description	<p>Neodymium is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called Promethium, StrongPity due to overlapping victim and campaign characteristics. Neodymium is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.</p> <p>(Microsoft) Neodymium is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.</p>
Observed	Countries: Europe.
Tools used	Wingbird .
Information	< https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/ >
MITRE ATT&CK	< https://attack.mitre.org/groups/G0055/ >

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=05fb2a9c-1ffb-4a2d-87fc-4103c9c62adf>