Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:23:30 UTC

APT group: WindShift

Names	WindShift *(DarkMatter)* Windy Phoenix *(Palo Alto)* G0112 *(MITRE)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2018
Description	(Palo Alto) In August of 2018, DarkMatter released a report entitled “In the Trails of WindShift APT”, which unveiled a threat actor with TTPs very similar to those of Bahamut. Subsequently, two additional articles were released by Objective-See which provide an analysis of some validated WindShift samples targeting OSX systems. Pivoting on specific file attributes and infrastructure indicators, Unit 42 was able to identify and correlate additional attacker activity and can now provide specific details on a targeted WindShift attack as it unfolded at a Middle Eastern government agency.
Observed	Sectors: Government. Countries: Middle East.
Tools used	WindTail.
Information	<https://unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/> <https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0112/>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=windyphoenix>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
