


Subgroup: TA455, Smoke Sandstorm - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:23:11 UTC

[Home](#) > [List all groups](#) > Subgroup: TA455, Smoke Sandstorm

APT group: Subgroup: TA455, Smoke Sandstorm

Names	TA455 (<i>ClearSky</i>) Smoke Sandstorm (<i>Microsoft</i>) Bohrium (<i>Microsoft</i>) DEV-0056 (<i>Microsoft</i>) Yellow Dev 13 (<i>PWC</i>) UNC1549 (<i>Mandiant</i>)		
Country	 Iran		
Motivation	Information theft and espionage		
First seen	2021		
Description	<p>A subgroup of Magic Hound, APT 35, Cobalt Illusion, Charming Kitten.</p> <p>(Microsoft) Smoke Sandstorm (formerly BOHRIUM/DEV-0056) compromised email accounts at a Bahrain-based IT integration company in September 2021. This company works on IT integration with Bahrain Government clients, who were likely Smoke Sandstorm’s ultimate target. Smoke Sandstorm also compromised various accounts at a partially government-owned organization in the Middle East that provides information and communications technology to the defense and transportation sectors, which are targets of interest to the Iranian regime. In May of 2022, Microsoft took legal action to disrupt spear phishing operations linked to Smoke Sandstorm.</p> <p>There seems to be overlap with Tortoiseshell, Imperial Kitten.</p>		
Observed	<p>Sectors: Aerospace, Aviation, Defense.</p> <p>Countries: Albania, India, Israel, Turkey, UAE and Middle East.</p>		
Tools used	LIGHTRAIL , MINIBIKE , MINIBUS , SlugResin , SnailResin .		
Operations performed	<table border="1"> <tr> <td>Jun 2022</td> <td>When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors</td> </tr> </table>	Jun 2022	When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors
Jun 2022	When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors		

		< https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east >
	Sep 2023	Operation “Iranian Dream Job” Iranian “Dream Job” Campaign 11.24 < https://www.clearskysec.com/wp-content/uploads/2024/11/Iranian-Dream-Job-ver1.pdf >
Information		< https://www.microsoft.com/en-us/security/security-insider/smoke-sandstorm >

Last change to this card: 29 December 2024

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

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=1f9277fa-f9e5-4a0b-a2a0-2179ddc62c86>