Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:51:28 UTC

APT group: SandCat

Names	SandCat *(Kaspersky)*
Country	Uzbekistan
Sponsor	State-sponsored, Military Unit 02616
Motivation	Information theft and espionage
First seen	2018
Description	(Kaspersky) SandCat is a relatively new APT group; we first observed them in 2018, although it would appear they have been around for some time," Costin Raiu, director of global research and analysis team at Kaspersky Lab, told Threatpost. "They use both FinFisher/FinSpy [spyware] and the CHAINSHOT framework in attacks, coupled with various zero-days. Targets of SandCat have been mostly observed in Middle East, including but not limited to Saudi Arabia.
Observed	Countries: Saudi Arabia and Middle East.
Tools used	FinFisher, CHAINSHOT and several 0-days.
Information	<https://threatpost.com/sandcat-fruityarmor-exploiting-microsoft-win32k/142751/> <https://www.vice.com/en_us/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format