Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:50:14 UTC

APT group: BlackOasis

Names	BlackOasis *(Kaspersky)* G0063 *(MITRE)*	
Country	[Middle East]	
Motivation	Information theft and espionage	
First seen	2015	
Description	BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. A group known by Microsoft as Neodymium is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.	
Observed	Sectors: Media, Think Tanks and activists and the UN. Countries: Afghanistan, Angola, Bahrain, Iran, Iraq, Jordan, Libya, Netherlands, Nigeria, Russia, Saudi Arabia, Tunisia, UK.	
Tools used	FinFisher, Wingbird and 0-day vulnerabilities in Flash.	
Operations performed	Jun 2015	Leveraging data from Kaspersky Security Network, we identified two other similar exploit chains used by BlackOasis in June 2015 which were zero days at the time. Those include CVE-2015-5119 and CVE-2016-0984, which were patched in July 2015 and February 2016 respectively. These exploit chains also delivered FinSpy installation packages. <https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/>
	May 2016	We first became aware of BlackOasis' activities in May 2016, while investigating another Adobe Flash zero day. On May 10, 2016, Adobe warned of a vulnerability (CVE-2016-4117) affecting Flash Player 21.0.0.226 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. The vulnerability was actively being exploited in the wild.

	Sep 2017	FireEye recently detected a malicious Microsoft Office RTF document that leveraged CVE-2017-8759, a SOAP WSDL parser code injection vulnerability. This vulnerability allows a malicious actor to inject arbitrary code during the parsing of SOAP WSDL definition contents. <https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html>
	Oct 2017	On October 10, 2017, Kaspersky Lab's advanced exploit prevention systems identified a new Adobe Flash zero day exploit used in the wild against our customers. The exploit was delivered through a Microsoft Office document and the final payload was the latest version of FinSpy malware. <https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0063/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
