Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Layover

Names	Operation Layover *(Talos)*
Country	Nigeria
Motivation	Information theft and espionage
First seen	2013
Description	(Talos) Cisco Talos and other security researchers have recently reported on a series of malicious campaigns targeting the aviation industry. These reports mainly center around the crypter that hides the usage of commodity malicious remote access tools. We decided this would be a good starting point to demonstrate how a researcher can pivot from the initial discovery of a RAT and eventually profile a threat actor. This post will show how we discovered previous campaigns targeting the aviation industry, which links back to an actor that's been active for approximately six years. We believe the actor is based out of Nigeria with a high degree of confidence and doesn't seem to be technically sophisticated, using off-the-shelf malware since the beginning of its activities without developing its own malware. The actor also buys the crypters that allow the usage of such malware without being detected, throughout the years it has used several different cryptors, mostly bought on online forums. We also believe with a high degree of confidence that the actor has been active for at least five years. For the last two, they've been targeting the aviation industry, while conducting other campaigns at the same time. Pivoting from an initial discovery is not an exact science — in this process, a researcher must assert a certain level of confidence in these associations.
Observed	
Tools used	AsyncRAT, CyberGate RAT, njRAT.
Information	<https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html>

Last change to this card: 02 November 2021

Download this actor card in PDF or JSON format