Operation Armor Piercer - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Armor Piercer

Names	Operation Armor Piercer *(Talos)*
Country	Pakistan
Motivation	Information theft and espionage
First seen	2020
Description	(Talos) Cisco Talos recently discovered a malicious campaign targeting government employees and military personnel in the Indian sub-continent with two commercial and commodity RAT families known as NetwireRAT (aka NetwireRC) and WarzoneRAT (aka Ave Maria). The attackers delivered a variety of lures to their targets, predominantly posing as guides related to Indian governmental infrastructure and operations such as Kavach and I.T.-related guides in the form of malicious Microsoft Office documents (maldocs) and archives (RARs, ZIPs) containing loaders for the RATs. Some of these lures and tactics utilized by the attackers bear a strong resemblance to the Transparent Tribe, APT 36 and SideCopy APT groups, including the use of compromised websites and fake domains.
Observed	Sectors: Defense, Government. Countries: India.
Tools used	NetWire RC, Warzone RAT.
Information	<https://blog.talosintelligence.com/2021/09/operation-armor-piercer.html>

Last change to this card: 02 November 2021

Download this actor card in PDF or JSON format