Cosmic Leopard, Operation Celestial Force

APT group: Cosmic Leopard, Operation Celestial Force

Names	Cosmic Leopard *(Talos)* Operation Celestial Force *(Talos)*
Country	Pakistan
Motivation	Information theft and espionage
First seen	2018
Description	(Talos) Cisco Talos is disclosing a new malware campaign called “Operation Celestial Force” running since at least 2018. It is still active today, employing the use of GravityRAT, an Android-based malware, along with a Windows-based malware loader we track as “HeavyLift.” All GravityRAT and HeavyLift infections are administered by a standalone tool we are calling “GravityAdmin,” which carries out malicious activities on an infected device. Analysis of the panel binaries reveals that they are meant to administer and run multiple campaigns at the same time, all of which are codenamed and have their own admin panels. Talos attributes this operation with high confidence to a Pakistani nexus of threat actors we’re calling “Cosmic Leopard,” focused on espionage and surveillance of their targets. This multiyear operation continuously targeted Indian entities and individuals likely belonging to defense, government and related technology spaces. Talos initially disclosed the use of the Windows-based GravityRAT malware by suspected Pakistani threat actors in 2018 — also used to target Indian entities. The tactics, techniques, tooling and victimology of Cosmic Leopard contain some overlaps with those of Transparent Tribe, APT 36, another suspected Pakistani APT group, which has a history of targeting high-value individuals from the Indian subcontinent. However, we do not have enough technical evidence to link both the threat actors together for now, therefore we track this cluster of activity under the “Cosmic Leopard” tag.
Observed	Countries: India.
Tools used	GravityAdmin, GravityRAT, HeavyLift.

Information	<https://blog.talosintelligence.com/cosmic-leopard/>

Last change to this card: 19 June 2024

Download this actor card in PDF or JSON format
