Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:38:39 UTC

APT group: Operation Spalax

Names	Operation Spalax *(ESET)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	(ESET) In 2020 ESET saw several attacks targeting Colombian entities exclusively. These attacks are still ongoing at the time of writing and are focused on both government institutions and private companies. For the latter, the most targeted sectors are energy and metallurgical. The attackers rely on the use of remote access trojans, most likely to spy on their victims. They have a large network infrastructure for command and control: ESET observed at least 24 different IP addresses in use in the second half of 2020. These are probably compromised devices that act as proxies for their C&C servers. This, combined with the use of dynamic DNS services, means that their infrastructure never stays still. We have seen at least 70 domain names active in this timeframe and they register new ones on a regular basis.
Observed	Sectors: Energy, Government. Countries: Colombia.
Tools used	AsyncRAT, njRAT, RemcosRAT.
Information	<https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/>

Last change to this card: 20 January 2021

Download this actor card in PDF or JSON format