Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:38:24 UTC

APT group: Packrat

Names	Packrat *(Citizen Lab)*
Country	[Latin America]
Motivation	Information theft and espionage
First seen	2008
Description	(Citizen Lab) This report describes an extensive malware, phishing, and disinformation campaign active in several Latin American countries, including Ecuador, Argentina, Venezuela, and Brazil. The nature and geographic spread of the targets seems to point to a sponsor, or sponsors, with regional, political interests. The attackers, whom we have named Packrat, have shown a keen and systematic interest in the political opposition and the independent press in so-called ALBA countries (Bolivarian Alternative for the Americas), and their recently allied regimes. These countries are linked by a trade agreement as well as a cooperation on a range of non-financial matters. After observing a wave of attacks in Ecuador in 2015, we linked these attacks to a campaign active in Argentina in 2014. The targeting in Argentina was discovered when the attackers attempted to compromise the devices of Alberto Nisman and Jorge Lanata. Building on what we had learned about these two campaigns, we then traced the group's activities back as far as 2008. This report brings together many of the pieces of this campaign, from malware and phishing, to command and control infrastructure spread across Latin America. It also highlights fake online organizations that Packrat has created in Venezuela and Ecuador. Who is responsible? We assess several scenarios, and consider the most likely to be that Packrat is sponsored by a state actor or actors, given their apparent lack of concern about discovery, their targets, and their persistence. However, we do not conclusively attribute Packrat to a particular sponsor.
Observed	Sectors: Government, Media and high profile political figures, journalists, and others. Countries: Argentina, Brazil, Ecuador, Venezuela.
Tools used	Adwind, Adzok, CyberGate RAT, XtremeRAT.
Information	<https://citizenlab.ca/2015/12/packrat-report/>

Last change to this card: 24 April 2021

Download this actor card in PDF or JSON format
