

Report reveals seven-year South American malware campaign

December 10 2015, by Irene Poetranto

A number of journalists, activists, politicians and public figures in Latin America have been targeted by a large-scale hacking campaign since 2008, according to a new report from the University of Toronto's Citizen Lab.

Researchers have named the malicious actor behind the [attacks](#) as "Packrat," to highlight the attacker's preference for Remote Access Trojans (RATs) and for using the same domain names and servers over many years.

The report, written by Citizen Lab Senior Researchers John Scott-Railton, Morgan Marquis-Boire, and Claudio Guarnieri, in collaboration with researcher Marion Marschalek, highlights the threats that [journalists](#) and civil society face from determined adversaries. The study began when Citizen Lab researchers began receiving evidence of malware attacks against public figures and journalists in Ecuador. Their analysis found that these attacks were linked to an unsuccessful malware attack against Alberto Nisman, a high-profile lawyer who was found dead in January 2015 just hours before he was due to release a report condemning the Argentine government.

Building from this discovery, the report uncovers Packrat's extensive activity in Argentina, Ecuador, Brazil, and Venezuela. Citizen Lab researchers, examining almost three dozen attacks, discovered that Packrat creates and maintains websites and social media accounts for fake opposition groups and news organizations, then uses them to

distribute malware and conduct phishing attacks against journalists, political figures, activists, and politicians. The report also documents a fake login page used to target members of Ecuador's National Assembly.

The [report](#) concludes that, while clear attribution to a particular sponsor is not possible, the information collected by Packrat likely makes its way to at least one government. "This case is yet another example of the digital threats confronting civil society, and the role that academic research plays in shedding light on the problem," said Citizen Lab Director Ron Deibert.

More information: Packrat: Seven Years of a South American Threat Actor. citizenlab.org/2015/12/packrat-report/

Provided by University of Toronto

Citation: Report reveals seven-year South American malware campaign (2015, December 10) retrieved 26 April 2024 from <https://phys.org/news/2015-12-reveals-seven-year-south-american-malware.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.