Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:09:51 UTC

APT group: leetMX

Names	leetMX *(ClearSky)*
Country	Mexico
Motivation	Information theft and espionage
First seen	2016
Description	(ClearSky) leetMX is a widespread cyber-attack campaign originating from Mexico and focused on targets in Mexico, El Salvador, and other countries in Latin America, such as Guatemala, Argentina and Costa Rica. It has been operating since November 2016 at least. We are uncertain of its objectives but estimate it is criminally motivated. leetMX infrastructure includes 27 hosts and domains used for malware delivery or for command and control. Hundreds of malware samples have been used, most are Remote Access Trojans and keyloggers. Interestingly, the attackers camouflage one of their delivery domains by redirecting visitors to El Universal, a major Mexican newspaper.
Observed	Countries: Argentina, Costa Rica, El Salvador, Guatemala, Mexico, USA.
Tools used	
Information	<https://www.clearskysec.com/leetmx/>

Last change to this card: 29 April 2020

Download this actor card in PDF or JSON format
