

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:51:27 UTC

[Home](#) > [List all groups](#) > Operation Bandidos

APT group: Operation Bandidos

Names	Operation Bandidos (<i>ESET</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2021
Description	(ESET) In 2021 we detected an ongoing campaign targeting corporate networks in Spanish-speaking countries, with 90% of the detections in Venezuela. When comparing the malware used in this campaign with what was previously documented, we found new functionality and changes to this malware, known as Bandoock. We also found that this campaign targeting Venezuela, despite being active since at least 2015, has somehow remained undocumented. Given the malware used and the targeted locale, we chose to name this campaign Bandidos.
Observed	Countries: Venezuela .
Tools used	Bandoock .
Information	< https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/ >

Last change to this card: 09 August 2021

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=bfea8c04-ab0d-41ac-a997-f5d9cdb740bc>