

El Salvador suffered a massive leak of biometric data

By Pierluigi Paganini

Published: 2024-05-06 · Archived: 2026-04-05 16:32:44 UTC



Resecurity found a massive leak involving the exposure of personally identifiable information (PII) of over five million citizens of El Salvador on the Dark Web.

Resecurity [identified](#) a massive leak of the personally identifiable information (PII) of over five million citizens from El Salvador on the [Dark Web](#), impacting more than 80% of the country's population.

The threat actor, going by the alias 'CiberinteligenciaSV,' posted the 144 GB data dump to Breach Forums, writing that the leak included 5,129,518 high-definition photos, each labeled with the corresponding Salvadorian's document identification (DUI) number. Resecurity assesses that the real intellectual authors of this breach appear to have an interest in obscuring their involvement, using the background specter of the Guacamaya group and its unofficial proxies to form a cloud of uncertainty surrounding the real threat actors and attack chain that caused the data leak.

The data dump includes the following fields:

- ID
- Identification document (DUI)
- Names/Last names
- Date of birth
- Telephone

- Email
- Address
- Photo of the victim

Ultimately, this data leak is significant because it marks one of the first instances in cybercrime history where virtually the entire population of a country has been affected by a compromise of biometric data. A [Federal Trade Commission](#) advisory published last year states, “Biometric information refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person’s body.”

Beyond the massive scale of Salvadorian PII records, threat actors also obtained a headshot of each victim, which represents a crucial biometric data marker – particularly in the golden age of generative AI. Notably, the vast scale of this biometric and PII data breach places most of El Salvador’s population at significant risk for identity theft and fraud. Armed with modern deep fake technology, threat actors can leverage victim headshots and related PII to stage more convincing frauds across a broad universe of digital-first financial, merchant, and government portals.

The detailed report is available [here](#):

<https://www.resecurity.com/blog/article/massive-dump-of-hacked-salvadorean-headshots-and-pii-highlights-growing-threat-actor-interest-in-biometric-data>

Follow me on Twitter: [@securityaffairs](#) and [Facebook](#) and [Mastodon](#)

[Pierluigi Paganini](#)

([SecurityAffairs](#) – hacking, El Salvador)

Source: <https://securityaffairs.com/162790/data-breach/el-salvador-massive-leak-biometric-data.html>