

Hackers threaten to leak a copy of the World-Check database used to assess potential risks associated with entities

By Pierluigi Paganini

Published: 2024-04-22 · Archived: 2026-04-05 15:55:34 UTC



A financially motivated group named GhostR claims the theft of a sensitive database from World-Check and threatens to publish it.

World-Check is a global database utilized by various organizations, including financial institutions, regulatory bodies, and law enforcement agencies, for assessing potential risks associated with individuals and entities. It compiles information from diverse sources like public records, regulatory filings, and proprietary databases to create profiles of entities susceptible to financial crime, terrorism, or corruption. World-Check aids organizations in conducting due diligence and adhering to regulatory standards concerning anti-money laundering (AML) and counter-terrorism financing (CTF).

World-Check is currently owned by LSEG (London Stock Exchange Group).

A financially motivated threat actor, called GhostR, announced the theft of a confidential database containing 5.3 million records from the World-Check.

The threat actor said that he stole the database in March and threatened to publish the data online.

The [hackers told TechCrunch](#) that they stole the database from a Singapore-based company that has access to the sensitive database, however, they did not name the victim organization.

The threat actors shared a portion of the stolen data with TechCrunch as proof of the hack, it includes records on current and former government officials, diplomats, and politically exposed people. The list also includes criminals, suspected terrorists, intelligence operatives and a European spyware firm.

Compromised data vary by individuals and organizations, it includes names, passport numbers, Social Security numbers, online crypto account identifiers and bank account numbers, and more.

World-Check had different owners across the years, it was originally founded as an independent company. Curiously, in 2011, Thomson Reuters acquired World-Check, then in October 2018, Thomson Reuters closed a deal with The Blackstone Group. As a result of this merger, World-Check became part of the new company, Refinitiv. LSEG acquired Refinitiv in 2021.

The disclosure of data in the archive poses a threat to the individuals whose data it contains. This is sensitive information that could lead to discrimination, persecution, or otherwise cause harm to individuals by violating their privacy and exposing them to various types of cyberattacks.

The database was criticized because it includes names of people and organizations that are mistakenly considered terrorists.

In June 2016, security researcher [Chris Vickery](#) [found a copy](#) of the [World-Check](#) database dated 2014 that was accidentally exposed online.

In August 2015, journalists from BBC's Radio 4 [gained 30 minutes of access](#) thanks to the support of a disgruntled customer and demonstrated that the designations in the archive were inaccurate.

The [Vice News](#) also gained access to the World-Check archive in February 2016 arriving at the same conclusion after it analyzed some profiles in the database

[Pierluigi Paganini](#)

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

[\(SecurityAffairs – hacking, GhostR\)](#)
