Database leaks data on most of Ecuador's citizens, including 6.7 million children

Elasticsearch server leaks personal data on Ecuador's citizens, their family trees, and children, but also some users' financial records and car registration information.

By Catalin Cimpanu for Zero Day | September 16, 2019 -- 08:00 GMT (01:00 PDT) | Topic: Security

Quito, Ecuador

Image: Reiseuhu

The personal records of most of Ecuador's population, including children, has been left exposed online due to a misconfigured database, ZDNet has learned.

The database, an Elasticsearch server, was discovered two weeks ago by vpnMentor security researchers Noam Rotem and Ran Locar, who shared their findings exclusively with ZDNet. Together, we worked to analyze the leaking data, verify its authenticity, and contact the server owner.

The leaky server is one of the, if not the biggest, data breaches in Ecuador's history, a small South American country with a population of 16.6 million citizens.

20.8 MILLION USER RECORDS

The Elasticsearch server contained a total of approximately 20.8 million user records, a number larger than the country's total population count. The bigger number comes from duplicate records or older entries, containing the data of deceased persons.

The data was spread across different Elasticsearch indexes. These indexes contained different information, supposedly obtained from different sources. They stored details such as names, information on family members/trees, civil registration data, financial and work information, but also data on car ownership.

Image: ZDNet

Based on the names of these indexes, the entire database could be split in two main categories, based on the data's supposed origin. There's data that appears to have been gathered from a government sources, and data that appears to have been gathered from private databases.

THE DATA FROM GOVERNMENT SOURCES

The most extensive data was the one that appears to have been gathered from the Ecuadorian government's civil registry.

This data contained entries holding citizens' full names, dates of birth, places of birth, home addresses, marital status, cedulas (national ID numbers), work/job information, phone numbers, and education levels.

ZDNet verified the authenticity of this data by contacting some users listed in the database. The database was up to date, containing information as recent as 2019.

We were able to find records for the country's president, and even Julian Assange, who once received political asylum from the small South Americam country, and was issued a national ID number (cedula).

Image: ZDNet

Image: ZDNet

FAMILY AND KIDS DATA

But we only truly understood the extent of this data when we looked at an index named "familia" (family in Spanish), which contained information about every citizen's family members, such as children and parents, allowing anyone to reconstruct family trees for the entire country's population.

Image: ZDNet

However, things didn't stop here. When looking at this index we also realized that there were entries for children, some of whom were born as recent as this spring.

For example, we found 6.77 million entries for children under the age of 18. These entries contained names, cedulas, places of birth, home addresses, and gender.

Image: ZDNet

The table below shows the number of children records we found in the leaky database. With the exception of the past few years, the rest of the database entries are in tune with public reporting on the country's natality rate.

Year	Number of entries
2019	187
2018	231
2017	182
2016	222
2015	145,941
2014	456,687
2013	467,604
2012	501,560
2011	542,050
2010	539,124
2009	546,147
2008	536,624
2007	528,335
2006	521,197
2005	491,148
2004	492,139
2003	498,561
2002	511,235

The leak of childrens' data is without a doubt the biggest privacy concern about this incident. This leak not only exposes children to potential identity theft, but also puts them in physical danger because their home addresses have been left exposed online for anyone to find.

THE DATA FROM PRIVATE SOURCES

But this wasn't all what the database contained. While initially we thought vpnMentor security researchers stumbled upon a database belonging to the Ecuadorian government, this didn't turn out to be true.

At a closer look, the database also contained indexes labeled with the acronyms of private entities, suggesting they were either imported or scraped from those particular sources. Of note, two indexes were named BIESS and AEADE.

The first, BIESS, stands for Banco del Instituto Ecuatoriano de Seguridad Social, and contained financial information for some Ecuadorian citizens, such as account status, account balance, credit type, and information about the account owner, including job details.

The second, AEADE, stands for Asociación de Empresas Automotrices del Ecuador, and contained information on car owners, and their resective cars, including car models and car license plates.

Image: ZDNet

In total, we found 7 million financial records, and 2.5 million records containing car and car owner details.

Just like the Elasticsearch index holding the data of children, these two indexes are also extremely sensitive. The information in both indexes would be as valuable as gold in the hands of criminal gangs.

Crooks would be able to target the country's most wealthy citizens (based on ther financial records) and steal expensive cars (having access to car owners' home addresses and license plate numbers).

Connect the about children and the data about financial records, and criminals would have a list of the most wealthy Ecuadorians, their home addresses, and if they had any children -- making it trivially easy to target and kidnap children from rich families.

THE SOURCE OF THE DATA

When it came time to tracking down the source of this leak, both ZDNet and vpnMentor independently reached the same source, namely a local company named Novaestrat.

According to its website (http://archive.is/K61ZH), the company provides analytics services for the Ecuadorian market. Its website boldy displays the statement "Make financial decisions with updated information of the entire Ecuadorian Financial System" [translated].

However, getting in contact with the company was not as easy as it sounded. The company did not display an email address or phone number where it could be reached. ZDNet reached out to the company via Facebook, and tried contacting employees via LinkedIn, to no success. The company's support forum yielded a PHP error when we tried registering an account.

The database was eventually secured later last week, but only after vpnMentor reached out to the Ecuador CERT (Computer Emergency Response Team) team, which served as an intermediary.

This is the second major leak of user data originating from a South American country in as many months. In August, ZDNet reported about a similar Elasticsearch server that exposed the voter records of 14.3 million Chileans (https://www.zdnet.com/article/voter-records-for-80-of-chiles-population-left-exposed-online/), around 80% of the country's entire population.

Additional coverage of this leak can be found on vpnMentor's blog (https://www.vpnmentor.com/blog/report-ecuador-leak/).

Data leaks: The most common sources (/pictures/data-leaks-the-most-common-sources/)

SEE FULL GALLERY (/pictures/data-leaks-the-most-common-sources/)

(/pictures/data-leaks-the-most-common-sources/6/) (/pictu the-m source

(/pictures/data-leaks- (/pictures/data-leaks- (/pictures/data-leaks- (/pictures/data-leaks- (/pictures/data-leaks-

1 - of 14

NEXT > ()

SECURITY

An inside look at WP-VCD, today's largest WordPress hacking operation (https://www.zdnet.com/article/an-inside-look-at-wp-vcd-todays-largest-wordpress-hacking-operation/)

We must stop smiling our way towards a surveillance state (https://www.zdnet.com/article/we-must-stop-smiling-our-way-towards-a-surveillance-state/)

BlueKeep attacks are happening, but it's not a worm (https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/)

Why you need to think about supply chain security (ZDNet YouTube) (Nervous%20about%20your%20privacy?%20Replace%20Google)

Best home security of 2019: Professional monitoring and DIY (CNET) (https://www.cnet.com/how-to/the-best-home-security-systems-of-2019/?ftag=CMG-01-10aaa1b)

Two steps you should take to protect your network from hackers (TechRepublic) (https://www.zdnet.com/article/two-steps-you-should-take-to-protect-your-network-from-hackers/?ftag=CMG-01-10aaa1b)

RELATED TOPICS: SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

SHOW COMMENTS