Bits 'n Pieces (Trozos y Piezas) - DataBreaches.Net

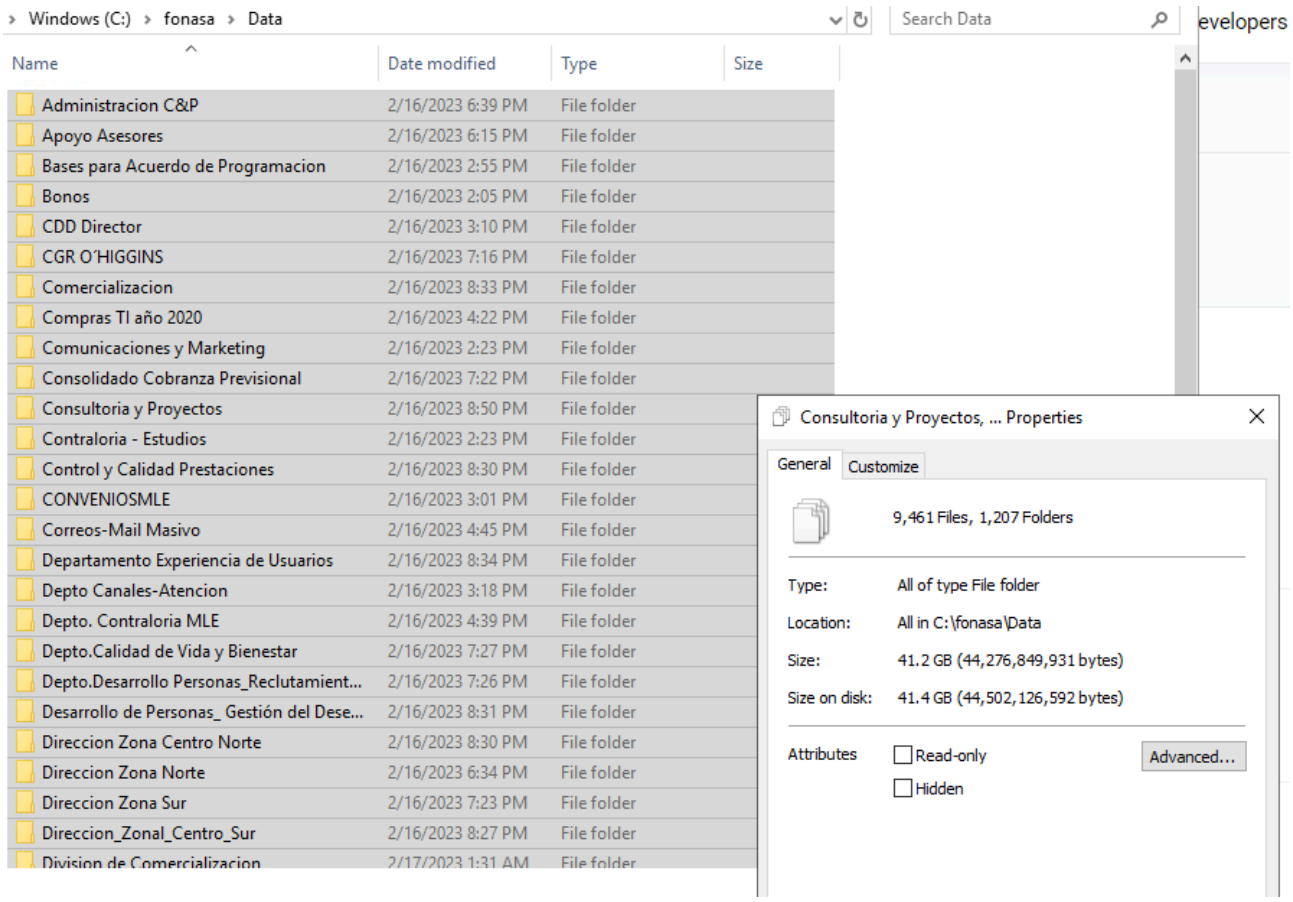
Published: 2023-03-10 · Archived: 2026-04-09 02:00:18 UTC

CL: BlackCat confirms attack on Fonasa

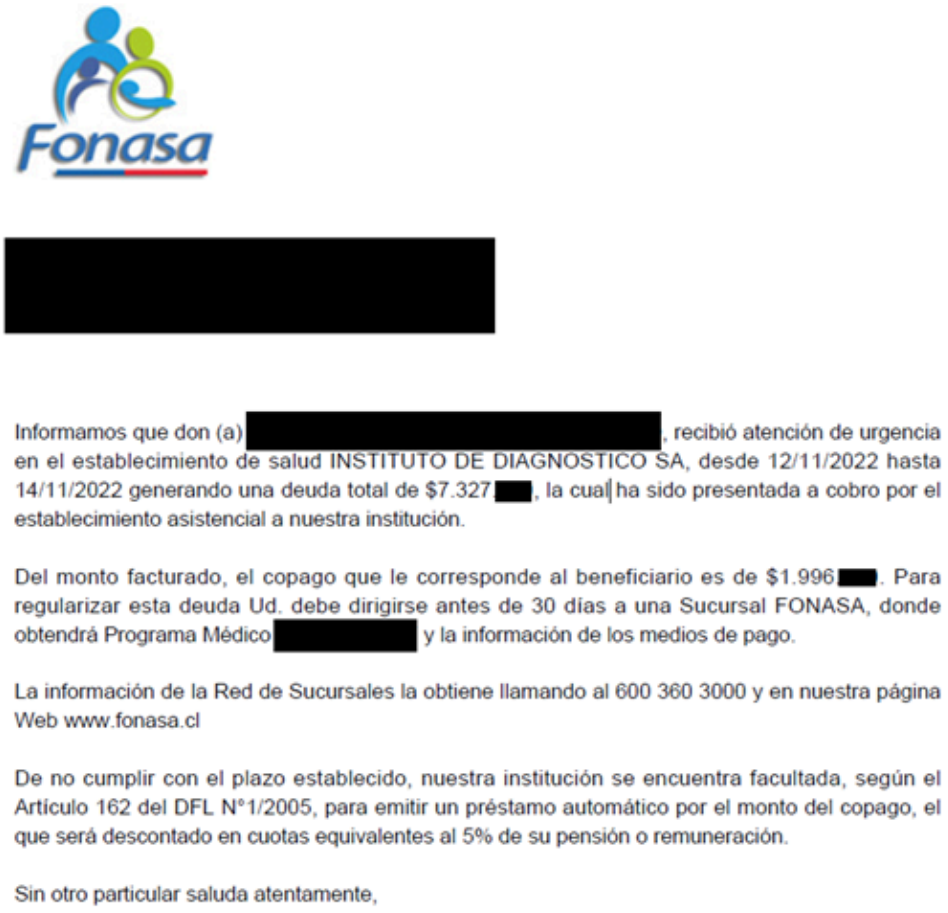
DataBreaches recently reported a malware attack on Chile's National Health Fund (FONASA). There is an update to report:

In a chat on Tox, BlackCat confirmed to DataBreaches that they are responsible for the attack and they say that they will announce it soon on their leaks page. A spokesperson for the group told DataBreaches that they are not giving Fonasa any more time to respond because they have not heard from them at all.

As partial proof of their claims, they provided this site with some files. DataBreaches was shown a screenshot of a directory of files as well as some correspondence with the names, addresses, and city of Fonasa health beneficiaries.



The correspondence below is a letter concerning a co-pay for services for a beneficiary:



[redacted]

Informamos que don (a) [redacted], recibió atención de urgencia en el establecimiento de salud INSTITUTO DE DIAGNOSTICO SA, desde 12/11/2022 hasta 14/11/2022 generando una deuda total de $7.327[redacted], la cual ha sido presentada a cobro por el establecimiento asistencial a nuestra institución.

Del monto facturado, el copago que le corresponde al beneficiario es de $1.996[redacted]. Para regularizar esta deuda Ud. debe dirigirse antes de 30 días a una Sucursal FONASA, donde obtendrá Programa Médico [redacted] y la información de los medios de pago.

La información de la Red de Sucursales la obtiene llamando al 600 360 3000 y en nuestra página Web www.fonasa.cl

De no cumplir con el plazo establecido, nuestra institución se encuentra facultada, según el Artículo 162 del DFL N°1/2005, para emitir un préstamo automático por el monto del copago, el que será descontado en cuotas equivalentes al 5% de su pensión o remuneración.

Sin otro particular saluda atentamente,

File provided by BlackCat, redacted By Databreaches.net.

Other files provided to DataBreaches were from visit reports and included personal data of employees such as names, IDs, and signatures.

Neither Fonasa nor CSIRT have provided any more details about this incident since reporting on the steps and legal action they initiated.

PE: Dark Power claims attack on Peruvian reconstruction agency

Autoridad para la Reconstrucción con Cambios (ARCC) is the Peruvian entity in charge of leading and implementing the Integral Plan for Reconstruction with Changes (PIRCC) of all the physical infrastructure damaged and destroyed by the El Niño Costero phenomenon in 13 regions of the country.

This institution was listed on or about March 9 on a leak site of a new group called Dark Power. Unlike other groups, Dark Power invites people to contact them on Tox to download files, but they were not online whenever DataBreaches attempted to contact them.

On March 9, DataBreaches sent an email to the RCC asking them about this incident. No reply was received. Because there was no notice on their website or social media, DataBreaches also alerted Peru's National Center for Digital Security (CNSD) of the claimed attack and data offer. CNSD thanked DataBreaches for the notification, writing, hey "Thank you for the information provided, we will coordinate with the affected entity, to provide attention to the reported security incident."

EC: Data on vaccinated Ecuadorians offered for sale (Disputed)

A database called Covid-19 allegedly from the Ministry of Public Health in Ecuador has been listed for sale on a popular forum by KelvinSecurity.

The March 5 listing claims the database contains these data fields:

> Year_v Month_v Day V Hour V Vaccination Point Unicode Establishment Zone District Province Canton Surnames Names Type Identification Number Document Sex Year Nac Month Nac Day Nac Nationality Conventional Telephone Cellular Telephone Email Population Vaccinate Vaccination Phase Name Vaccine Lot Dose Applied Was Scheduled Vaccinator Ced Vaccinator Name Enterer ID Enterer Had Covid Ethnic Self-identification Ethnic Nationality Kichwa Peoples Risk Group Exterior Vaccine Exterior Lot Exterior Dose Exterior Vaccine Date Exterior Country.

In a March 6 announcement on Twitter, the Ministry of Public Health of Ecuador appeared to deny any breach (translation):

> MSP confirms that there is no vulnerability to its computer systems
>
> The Ministry of Public Health (MSP) informs that, in relation to the publications generated on social networks about an alleged leak of the institution's database, there is NO violation of its computer systems and, therefore, the information that is hosted on The technological infrastructure is protected in accordance with governmental and international regulations and the industry's own computer protocols.
>
> We urge citizens not to be deceived with the delivery of information. The illegal disclosure of databases is sanctioned by the Comprehensive Organic Penal Code (COIP) as well as by the Organic Law for the Protection of Personal Data that regulates the confidentiality of data and that they are used for the purposes for which they were created.
>
> This State portfolio maintains in force the strategies and mechanisms that guarantee the confidentiality, integrity and availability of information in strict adherence to the law.
>
> Government of Ecuador
>
> Guillermo lasso PRESIDENT

So where does the government believe the data came from? Are they suggesting the data is fake? DataBreaches found real names associated with RUC in the sample data provided by KelvinSecurity but did not contact anyone to ask about their vaccination status.

DataBreaches also reached out to KelvinSecurity to ask for their response to the government's denial or for more information about how they acquired the data. They responded, "it is better that they continue to believe that than if I can negotiate the sale of the files."

CO: Sensitive and exposed data from ICETEX

ICETEX is a Colombian entity that promotes higher education and facilitates access to educational opportunities offered by the international community to improve the quality of life of Colombians.

An Icetex user who discovered a bug that exposes people's data reported it to Icetex, but got no response. The user then reported the bug to muchohacker.lol to call attention to the problem and Icetex's failure to address it. MuchoHacker.lol investigated the claimed vulnerability and reported:

> "MuchoHacker.lol verified that the warning is true and without any kind of technical or 'hacked' knowledge was able to access more than 10 documents with private and sensitive information such as ID, letters of recommendation from a person with the last name Figueroa are online. There You can read your personal data as well as the information of those who confirm that the Icetex user has been doing cultural work in the town of Suba, as well as Datacredito statements, letters from international universities, among others, which are just a click away. "

According to the user who discovered the problem, there are 104,747 documents online without any type of protection. Icetex responded by saying they were going to address the problem. It is not known for how long these data have been improperly secured or whether the data have been accessed by criminals.

Edited by Dissent.
