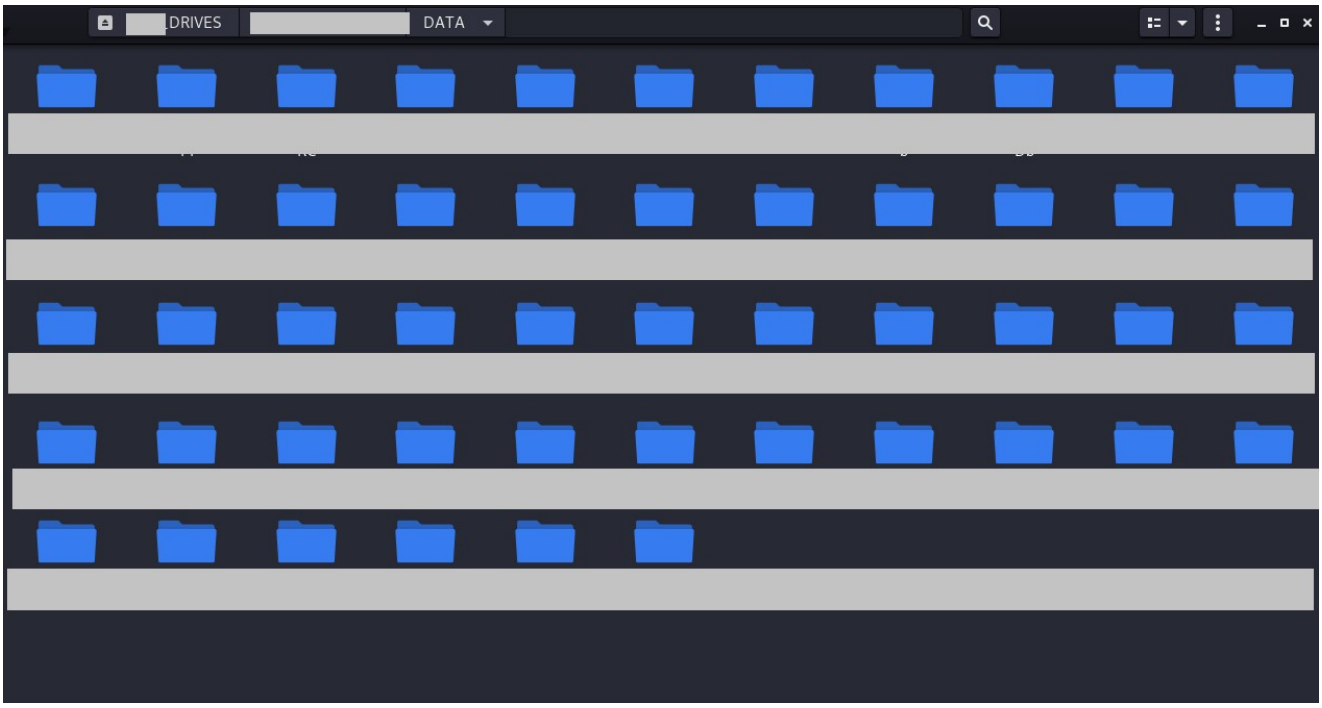
Johnson Fitness and Wellness hit by DESORDEN Group

databreaches.net/johnson-fitness-and-wellness-hit-by-desorden-group/

Dissent October 9, 2022

In what has become a familiar event, DESORDEN Group announced yet another attack on a multinational corporation. This time, their target was **Johnson Fitness and Wellness**, a subsidiary of **Johnson Health Tech. Co., Ltd.** Johnson Health Tech manufactures exercise training equipment and is listed on the Taiwan stock exchange; Johnson Fitness is headquartered in the U.S. and is an exercise equipment retailer.

In their post on a popular hacking forum, DESORDEN stated that the breach involved 71 GB of data and files affecting Johnson Fitness's suppliers, dealers, customers, and employees. Files concerning their internal operations and financial records were also acquired.



A screencap showing folders in one of the drives accessed on JohnsonFitness.com. DataBreaches.net has redacted the folder names.

Most of the sample files did not contain personal information. Other sample data shared exclusively with DataBreaches included customers' personal information such as name, address, phone number, and date of birth.

Of note, a leaked "sysusers" file included employee names, email addresses, usernames, and passwords in plaintext. DESORDEN's spokesperson commented that they were surprised that a big company left their passwords in plaintext, "which is really rare in our attacks against big companies."

> “This Johnson hack took quite a lot of time too,” they added, explaining, “we breached into their [Johnson Health Tech’s] mainframe server, but they had AVs and firewall that prevent outgoing connections — only allowed IPs of those within the network. So we have to find the other servers on the same network, breach in and pray hard that the firewall config is allowed.
>
> At the end of the day, we used another breached server to act as a bridge to the mainframe and stole the data. So it took quite a bit of time.”

DESORDEN’s spokesperson could not recall exactly when they first accessed Johnson but estimated that they were in there for months. They still have access, they claim.

According to their statement to DataBreaches, although Johnson read their emails, downloaded the data samples, and watched the video, they did not reply to any of their communications.

DESORDEN explained that their initial communications to a victim do not specify a specific demand amount. “We will wait for victims to respond, then we will set the sum based on their size,” they tell DataBreaches. So because Johnson did not respond to DESORDEN, they do not know how much DESORDEN might be demanding.

The total lack of response suggests that Johnson has no intention of paying any ransom demand. DESORDEN’s spokesperson told DataBreaches that they are neither surprised nor particularly upset by that because they believe they will be able to quickly sell the corporate information and trade secrets they were able to exfiltrate.

DataBreaches sent an email inquiry to Johnson Fitness about their response to the claimed attack. No reply has been received as of publication time.