https://www.wsj.com/articles/nestles-data-leak-shows-war-related-hacktivism-risks-11649151002

PRO CYBER NEWS

Nestlé's Data Leak Shows War-Related Hacktivism Risks

Food giant denied being hacked, says exposed data was related to information that was unintentionally posted on a business test website

A woman looks at Nescafé coffee packages at a shopping mall in Moscow in this image from March 11. Nestlé later said it would suspend the production of pet food, coffee and confectionery in Russia.

PHOTO: KONSTANTIN ZAVRAZHIN/GETTY IMAGES

By Nicolle Liu

April 5, 2022 5:30 am ET

Companies, already warned to remain alert to potential Russian cyberattacks, are battling operations by online activists aiming to bruise corporate reputations amid the war in Ukraine.

Recent public campaigns by the hacker collective Anonymous against Nestlé SA and other companies continuing to operate in Russia underline the increasing business risks. The high visibility of hacktivists requires extra efforts from companies in internal response and outward crisis communication, cybersecurity and risk experts said.

"The claim of a breach can cause a significant disruption of operations in a business because they need to put resources into investigating it," said Scott Algeier, executive director of the Information Technology Information Sharing and Analysis Center.

In a short period of time, he added, a lot of incident response, including public relations and internal communication between the network security team and legal teams, has to be done.

In the Nestlé incident, KelvinSecurity, which describes itself as a hacker group that "joins the virtual community to transmit important information," obtained the exposed data through a flawed configuration of a cloud server used by the food giant, a representative for the group told the Journal. The original plan was to sell the data, the Kelvin representative said. Instead, the group "decided to release it to collaborate with the hacking operation against Russia," the person said, adding that Kelvin worked with Anonymous to get the word out.

Anonymous said in a tweet on March 22 that it released 10 gigabytes of Nestlé's internal data, including emails, passwords and customer information, in "retaliation for continuing the company's business in Russia."

In a statement to the Journal, a Nestlé representative denied the company was hacked, saying the claim had "no foundation."

Nestlé said the exposed data are related to an incident in February in which information was unintentionally posted online on a business test website.

Ukrainian President Volodymyr Zelensky delivers a video address in Kyiv.

PHOTO: HANDOUT/AGENCE FRANCE-PRESSE/GETTY IMAGES

After the Anonymous tweet, Nestlé deployed resources to investigate the claims, craft a response and communicate with the public and clients.

Nestlé had already been subject to immense pressure from politicians, employees and consumers about its Russian operations. Ukrainian President Volodymyr Zelensky had earlier mentioned Nestlé by name in several speeches calling for Western businesses to pull out of Russia. On March 23, the company said it would scale back its business in Russia, suspending the production of pet food, coffee and confectionery.

A Twitter account linked to Anonymous, @YourAnonTV, has warned a long list of businesses operating in Russia to withdraw and threatened to hack them if they continue operations in the country. "We give you 48 hours to reflect and withdraw from Russia," one tweet from March 20 said, "or else you will be under our target!"

Companies such as Bridgestone Corp. and Dunkin' Brands, promptly replied to the tweet saying they had already withdrawn from Russia.

"We simply wanted to set the record straight," said Steven Kinkade, vice president of communications at Bridgestone Americas Inc.

Dunkin' didn't immediately respond to a request for comment.

Cyberexperts said hacktivists can be harder to deal with than hackers out for financial gain because their primary motive is to draw attention and are often less fearful of prosecution.

The Anonymous collective has participated in hacking operations related to political movements around the world, including the 2011 Syrian uprising, 2019 Hong Kong protests and 2020 Black Lives Matter movement.

Publicity is the goal for hacktivists, said Meredith Griffanti, co-head of the cybersecurity and data privacy communications practice at business advisory firm FTI Consulting Inc. Part of their strategy is to antagonize, she said. "[They] will react in public forums to anything the victimized company says or does."

While hacktivists usually don't have the advanced tooling and techniques of nation-states or financially motivated hackers, they also care less about hiding their online tracks, said Jake Williams, director of cyber threat intelligence at Scythe, a vulnerability assessment company.

"That allows them to be a bit louder, very much louder," he said. "A financially motivated threat actor that gets caught early, is obviously not making any money."

Write to Nicolle Liu at Nicolle.Liu@wsj.com