Australian Beverage Company, Lion, Hit by Successive Cyber Attacks

Mark A. Wells

Initial attack

On Monday, June 8, 2020 Lion Dairy and Drink company in Australia was hit by what they describe as a cyber-attack. The cyber-attack was actually a ransomware attack that halted all IT systems for several days. One unconfirmed report suggests that the hackers demanded $800,000 in crypto-currency from Lion—who seemingly refused to pay (Paganini, 2). Lion IT specialists immediately shut down all IT as an initial precaution and began working through the impact of the attack system by system. By June 10, a few systems were restored, but only one brewery was operational and some of the dairies were operational. The real problem came with customer service and the ability of customers to place orders—normally done electronically. Lion had to begin taking orders manually, over the phone. By June 10 the authorities were notified of the attack and law enforcement joined the effort in discerning the source of the attack. As far as Lion knows, no customer information was accessed. However, they did discover some of their operational data posted on the web a week or so after the attack.

Second Attack

On June 18, following a second attack, the Prime Minister of Australia announced that a state actor from another nation was responsible for several cyber-attacks in the previous two weeks. These attacks were aimed at and disrupted commercial businesses, government services, and political party headquarters in Australia. Just as Lion was recovering from the initial attack, this second cyber-attack set them back again.

By June 19 Lion had all of its breweries operational and most of its dairies and fruit juice operations running, but customer service and filling orders was still lagging. The timing of the attack could not be worse. Just as the hospitality industry was beginning to be allowed to open (pubs, restaurants, hotels) after the initial Covid response, Lion—who supplied beer, wine, and liquors, as well as other drinks—was hit with this attack. Lion had already experienced record low sales because of Covid related closures in that industry and now, just as they could begin selling again, were hit with a debilitating cyber-attack.

Misdirected orders

A humorous, but serious, side effect of the attack occurred when Lion posted several numbers for customer service on their customer portal following the atack. The numbers were new numbers since it was believed that the original numbers may have been compromised in the initial cyber-attack. Lion was employing Cliffside Security as a cybersecurity consultant at the time to help with the forensics on this attack. Lion accidentally posted the Cliffside Security

This Careers Preparation National Center product was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-22-1-0329), which is part of the National Security Agency.

phone number on their list of customer service numbers on the customer portal—clearly a human error. Within an hour Cliffside Security began receiving calls to take milk orders. A Cliffside Security representative reported that they received over 70 calls to place orders, and many more were left on their voicemail. Needless to say, when Lion discovered this issue they quickly deleted the Cliffside Security number from their customer portal.

Sources:

Lion Dairy and Drinks, “Lion Cyber Incident Update: 26 June 2020,” *Lion Dairy and Drinks Website* (June 26, 2020). Accessed on April 6, 2021.

Ry Crozier, “Lion Accidentally Directs Milk Orders to Sydney IT Security Consultancy,” *Next Media* (June 10, 2020). Accessed on April 6, 2021.

Pierluigi Paganini, “Australian Beverages Firm Lion Hit for Second Time in a Few Days by a Cyber Attack,” *Security Affairs* (June 20, 2020). Accessed on April 6, 2021.

*A majority of information for this case was gleaned from Lion Dairy and Drink official website, which posted updates on the attack as it happened over the two weeks of the attacks.