Today's insider threat: Ardyss edition - DataBreaches.Net

Published: 2024-12-24 · Archived: 2026-04-11 02:13:43 UTC

Here's today's reminder of the insider threat. And also the external threat. Consider it a pre-holiday twofer.

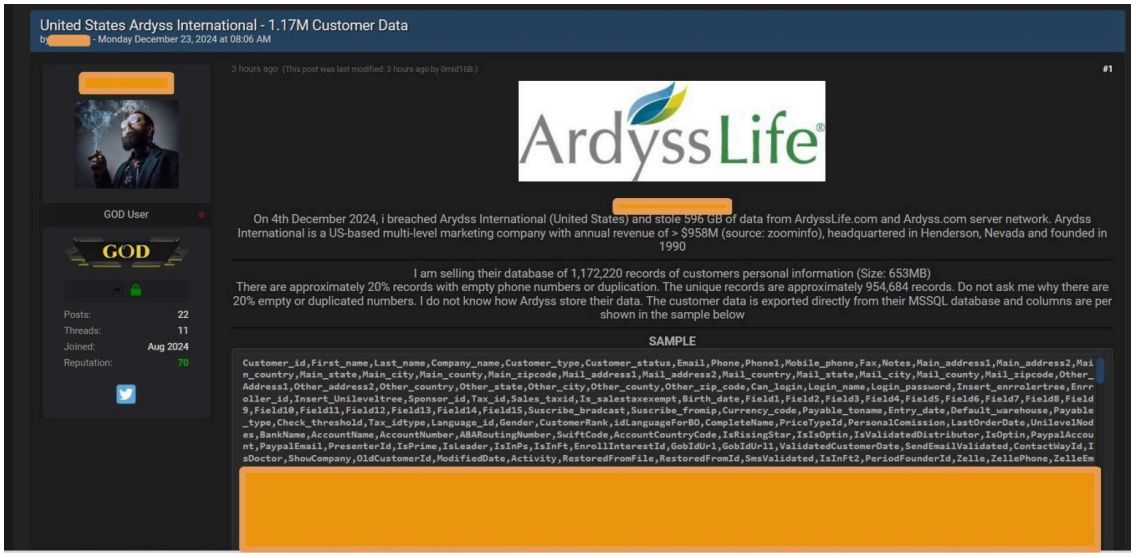
DataBreaches was contacted yesterday by "0mid16B," the same individual who was responsible for previously hacking **The1 Card**, Thailand's most popular loyalty program. In their latest contact, they claim to have successfully attacked Ardyss[.]com and ArdyssLife[.]com, telling DataBreaches, "In December 2024, we breached and stole 596 GB of data from United States ArdyssLife[.]com and Ardyss[.]com server network. Ardyss International is a United States MLM company with annual revenue of > $958M."

As proof of claims, 0mid16B provided DataBreaches with screenshots alleged to be from negotiation chats and a .csv file with basic information on 10,000 customers such as customer's first and last name, the name of their firm, postal address, and phone number. Because fields were not labeled in this sample, it was not clear what some of the data referred to, but a Google search of a few customer records was quickly able to verify that customer names and firms that appeared in the .csv file could be found at the addresses listed in the .csv file.

In follow-up communications with DataBreaches, 0mid16B statedthat although they would not reveal exactly how they gained access to Ardyss, they used two vulnerabilities on their server. The firm's IT staff reportedly detected the intrusion approximately one month after initial access was gained. "They managed to remove persistent access twice," 0mid16B stated. "I waited 2 to 3 days each time to regain access during the time window when they were likely to be asleep."

0mid16B tells DataBreaches that they did not encrypt any files but deleted all files and databases — including the firm's backup server. "But due to permissions issues, I was not able to remove their shadow copies, and they recovered their files and data."

The company's owners and executives reportedly never responded to 0mid16B's demands or attempts to negotiate. As a consequence, their data has been offered for sale, with 0mid16B claiming to have 1,172,220 customer records.

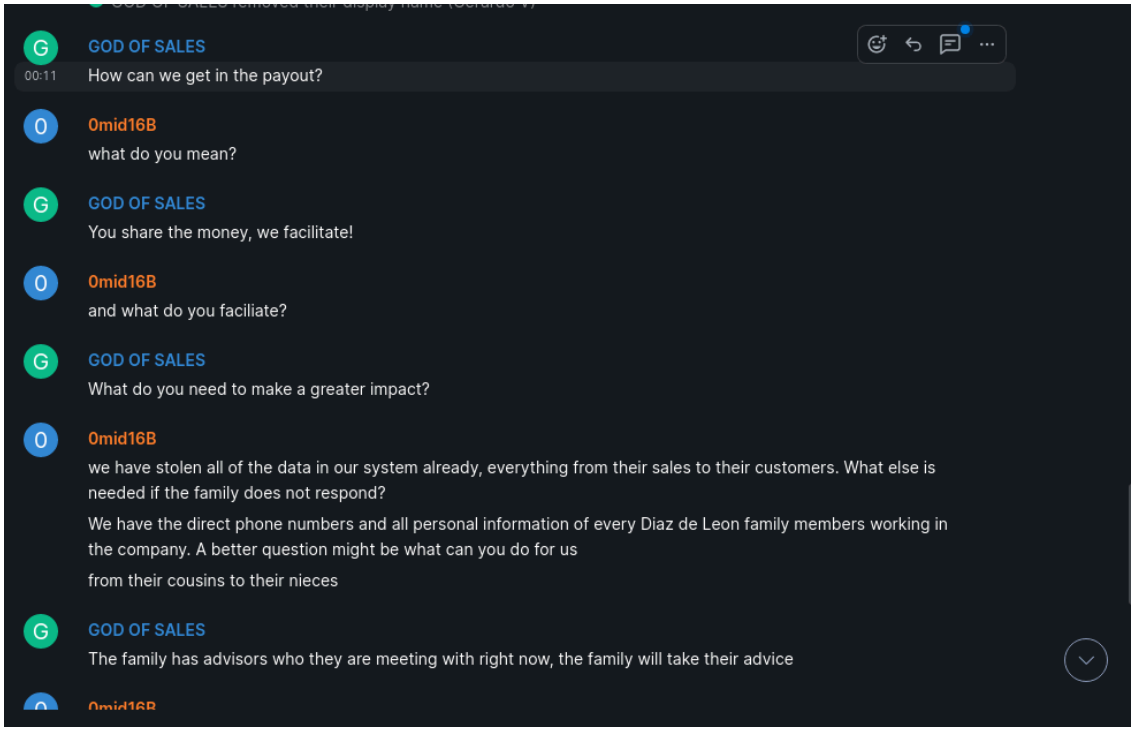


Forum listing describes stolen data and provides sample. Image: DataBreaches.net

While 0mid16B was the external threat actor, Ardyss may have a serious insider threat problem too. According to the chat log screenshots provided to DataBreaches, an employee who logged in to the chat as “Gerardo V” was not an executive or negotiator for Ardyss. By his own statements to 0mid16B, he was an employee in Mexico who had seen 0mid16B’s email to the company executives and wanted to learn what was going on. When asked whether the company knew he was in the chat and whether he was representing them, he stated that the executives did not know he was there, and the family owners of the business were taking advice from their own advisors while IT was busy just setting up another server to replace the one compromised by 0mid16B.

Understandably confused, 0mid16B asked how this chat could possibly help the family owners at all if they had no idea what the hacker’s demands were and they weren’t being informed by Gerardo.

That’s when the chat seems to have taken an unexpected turn. Gerardo declared that he was not trying to help the the family owners at all and that, having googled 0mid16B, he just wanted to know the hacker’s objectives. When 0mid16B stated that the objective was purely financial and that if the owners didn’t respond, they would release the data, notify U.S. regulators, and notify customers, Gerardo declared that they were on the same page, changed his display name in the chat to “GOD OF SALES,” and asked how he and his supervisor (who was reportedly sitting next to him reading the chat) could get in on the payout.

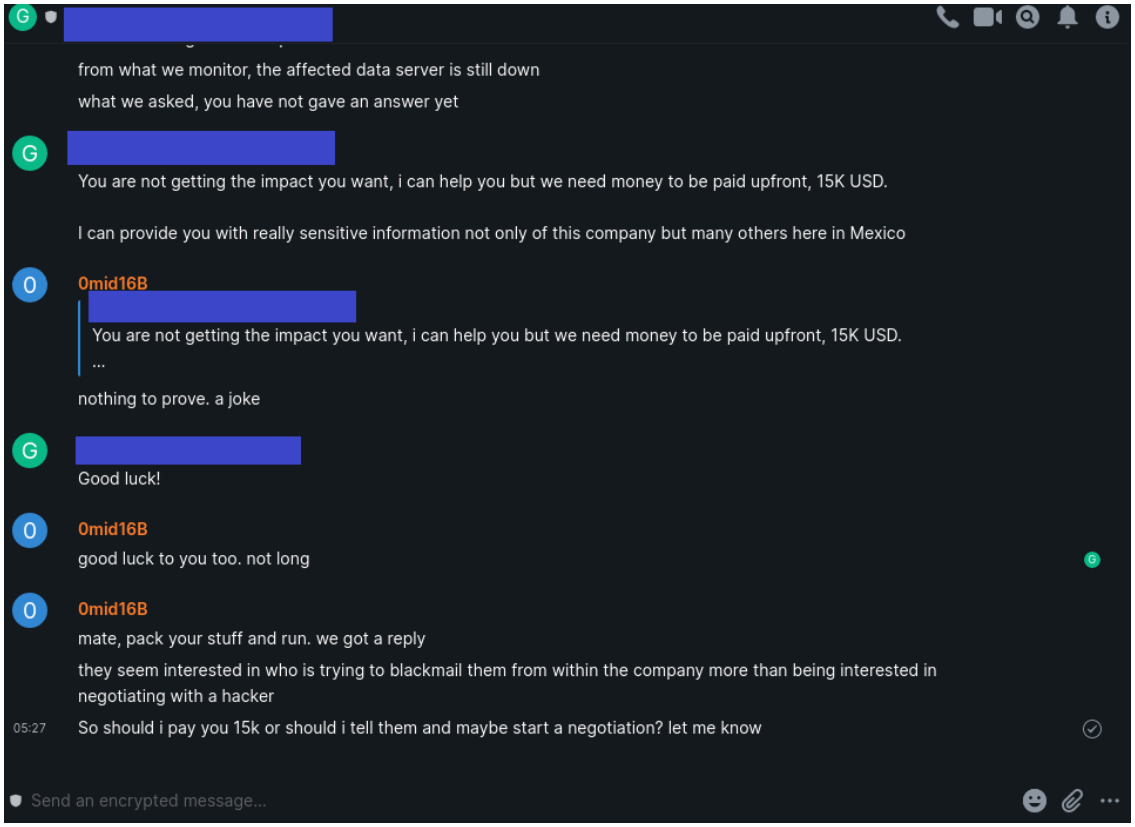


"How can we get in the payout?" employee Gerardo V. aka "GOD OF SALES" asks. Image: Provided.

Om1d16B responded by asking what the self-proclaimed sales representative could do to influence the decision-makers, at which point, "GOD OF SALES" said they could get 0mid16B the impact they needed, but first the hackers would have to pay him $15k USD. For that, he said, he could give the hackers really sensitive information on the company as well as other companies in Mexico.

By now, Gerardo V had changed his display name again, this time to provide a username@matrix.org.

No deal was made between the hacker and GOD OF SALES, with 0mid16B eventually telling him, "mate, pack your stuff and run," because the owners had allegedly responded and wanted to know who in the company was trying to blackmail them. "So should I pay you 15k or should i tell them and maybe start a negotiation? let me know," 0mid16B wrote.



The employee asks the hackers for $15K USD, for which he will provide sensitive info on the company. Image: Provided.

0mid16B tells DataBreaches that he never heard from Gerardo V or his supervisor again.

There are at least two possible explanations, assuming (for now) that the screenshots are real: the employee was trying to cut himself into a deal to extort his employer or he was trying to scam the hackers and had no intention of really helping them or helping the employer.

Either way, this employee appears to be a potentially serious threat to the security of the company and its customers.

The Company's Response

DataBreaches emailed three executives of the firm yesterday to ask about both the breach and the alleged conduct of the employee.

There have been no replies, so there has been no confirmation of the breach by the firm. Neither has there been any confirmation or dispute that an employee engaged in behavior that appears problematic, at best.

This post will be updated if the company responds.

Source: https://databreaches.net/2024/12/24/todays-insider-threat-ardyss-edition/