Exclusive: Advarra hacked, threat actors threatening to leak data (1) - DataBreaches.Net

Published: 2023-11-01 · Archived: 2026-04-09 02:14:40 UTC

Advarra describes itself as providing integrated solutions to safeguard trial participants, empowering clinical sites, ensuring compliance, and optimizing research performance for thousands of sponsors, contract research organizations, institutions, academic medical centers, and research consortia that it services.

On or about October 25, Advarra was hacked and data was exfiltrated. According to one of the people involved in the attack, the executives knew about the breach on October 25 but would not pay or even negotiate with them.

DataBreaches reached out to Advarra via its website to inquire about the attackers' claims. Getting no reply from them at the time, DataBreaches then reached out to one of their clients to try to verify whether some research participant records provided to this site were real. Within minutes of leaving Diablo Clinical Research a voicemail about a possible breach involving their clinical research data, DataBreaches received a call from Lori Vitti, their Director of Finance and Administration. DataBreaches read her a patient's name, diagnoses and medications, the number of records in the database, and the participant's study ID number. Ms Vitti immediately recognized the information and said that the data had to have come from Advarra or one other entity. DataBreaches then told her it had been provided to DataBreaches and described as being exfiltrated from Advarra.

Diablo followed up on their prompt response by reportedly reaching out to Advarra and then contacting DataBreaches again today.

In the interim, hearing about Diablo's quick and forthright incident response, the threat actors turned over the data they had exfiltrated concerning Diablo to DataBreaches, agreed not to leak it publicly, and said they would destroy their own copy of it. DataBreaches transmitted the data to Diablo this morning and the threat actors stated that they had deleted their copy.

Other Advarra clients and Advarra's employees are not faring as well, it seems. Yesterday, the threat actors listed the incident on AlphV.

In their listing, reproduced below with redactions by DataBreaches, they claim to have acquired over 120GB+ of confidential data belonging to customers, patients, and current and former employees.

Image: DataBreaches.net

Of note, the listing, which included a note written in Hebrew, claims that Advarra called the threat actors "digital terrorists" and one of the executives told them to "fuck off." No data was leaked with the posting, but the threat to leak was posted if the company didn't reach out.

The use of the word "terrorists" seemed significant to the threat actors, who informed DataBreaches that they were concerned that the company might wrongly believe that they were on some OFAC-sanctioned list and therefore could not be paid. The Hebrew statement at the end of the listing machine translates to, "A company that has profited greatly from vaccine development. They don't pay digital terrorists.
We are not terrorists, which is why the majority pays us. We are also not tied to any sanctions."

Advarra Responds

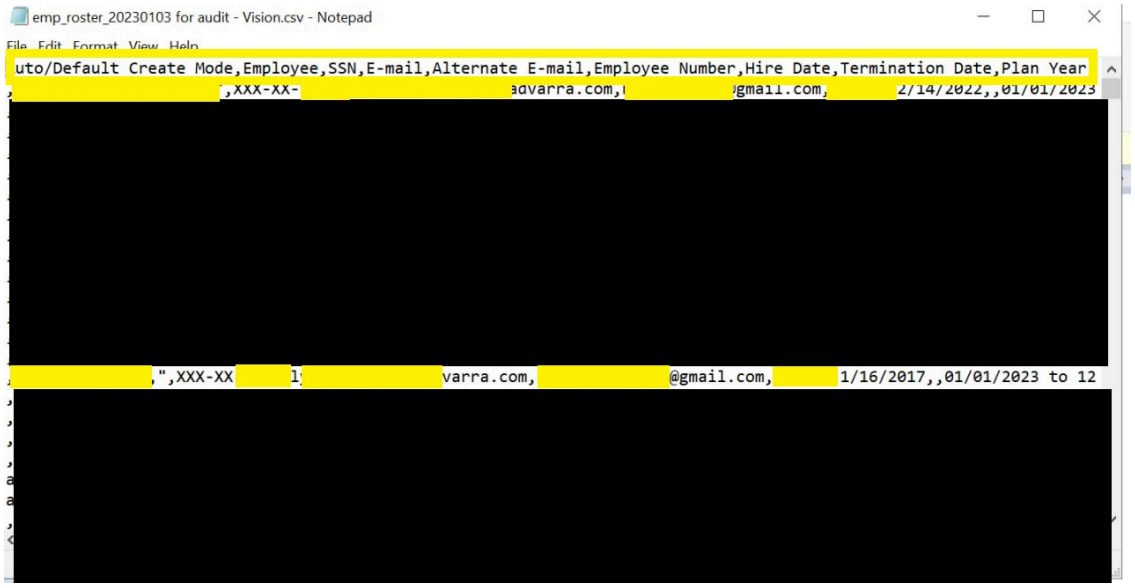
DataBreaches has since been contacted by Advarra and those involved in the investigation. Advarra sent the following statement:

> "An Advarra colleague was the victim of a compromise of their phone number. The intruder used this to access some of the employee's accounts, including LinkedIn, as well as their work account.
>
> We have taken containment actions to prevent further access and are investigating with third-party cyber experts. We also notified federal law enforcement. At this time we believe the matter is contained. We further believe that the intruder never had access to our clients' or partners' systems and it is safe to connect to Advarra's systems. Importantly, we have no evidence that the Advarra systems and products that clients use to interface with us were compromised or accessed. At this time, our business operations have not been disrupted as a result of this activity and we continue to operate as normal. In addition, we continue to take steps to enhance the overall security of our systems in line with industry best practices.
>
> Our investigation remains ongoing, and we will provide additional updates as appropriate."

According to the threat actors, they gained access to Advarra by initially phishing an executive's personal email account. When asked about Advarra's statement to DataBreaches, the threat actors' spokesperson responded:

> We're not sure what the company means by the compromise of a phone number , but we believe this has to do with some spoof calls made to Advarra leadership, prior to the phish taking place. Of course, a wholly inaccurate statement from a company that enriched themselves during the pandemic. As you can see, there is no mention of employee data being taken too, in their statement. To set the record straight, the employee was compromised after her personal email was phished, leading us to placing a cred-stealer in her personal OneDrive. As her PC was actively syncing the contents of the OneDrive, she was infected. Because she had also backed up her Authenticator to the cloud, we were able to bypass MFA. We then leveraged this to access her work account and work files, present on her device. Stay tuned for the leak of this data if no payment is made within 48 hours.

Later, the threat actors would also explain that they also spoofed the employee's phone number when they later sent out messages to family and colleagues.



Part of an employee roster exfiltrated by the threat actors included employee names, last four digits of SSN, their email address at work, their alternate (personal) email address, their employee number, hire date, and termination date. Image redaction: DataBreaches.net

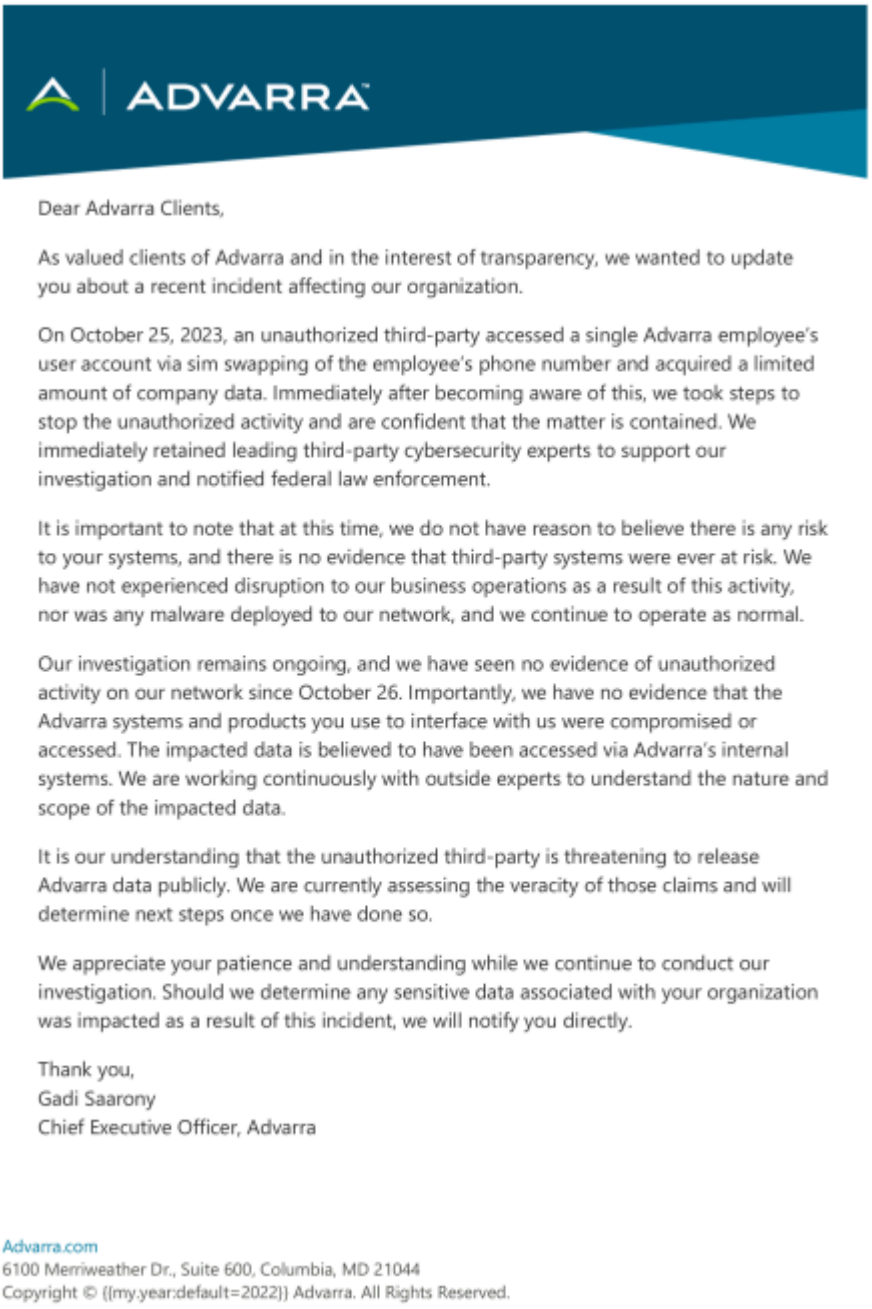
Perhaps one of the most disturbing aspects of this incident is the ugly actions involving one employee whom they allege told them to "go fuck yourself." In response to that, and to the alleged message on the server calling them "digital terrorists" who would never be paid, the threat actors went personal and started contacting the employee's family members, including their child, with sensitive content.

But did an employee really interact with them? An individual close to the matter denied that the messages posted on the dark web by the threat actor came from an Advarra employee. The employee whose phone number was compromised has not communicated with the threat actor responsible for this incident, they told DataBreaches. They also denied that Advarra referred to the threat actor as digital terrorists.

When told of the denials, the threat actors repeated their claim that the employee did communicate with them and reiterated their claim that Advarra's data will be leaked in 48 hours if they are not paid.

Updated November 2: A copy of Advarra's notice to clients appears below. DataBreaches notes that they assert the employee's phone was compromised by sim-swapping, which is a different explanation than the threat actors claimed to DataBreaches.

Diablo Clinical Practice declined to provide any statement for this report. They are reportedly "not concerned" after speaking with Advarra, whatever that means.



ADVARRA

Dear Advarra Clients,

As valued clients of Advarra and in the interest of transparency, we wanted to update you about a recent incident affecting our organization.

On October 25, 2023, an unauthorized third-party accessed a single Advarra employee's user account via sim swapping of the employee's phone number and acquired a limited amount of company data. Immediately after becoming aware of this, we took steps to stop the unauthorized activity and are confident that the matter is contained. We immediately retained leading third-party cybersecurity experts to support our investigation and notified federal law enforcement.

It is important to note that at this time, we do not have reason to believe there is any risk to your systems, and there is no evidence that third-party systems were ever at risk. We have not experienced disruption to our business operations as a result of this activity, nor was any malware deployed to our network, and we continue to operate as normal.

Our investigation remains ongoing, and we have seen no evidence of unauthorized activity on our network since October 26. Importantly, we have no evidence that the Advarra systems and products you use to interface with us were compromised or accessed. The impacted data is believed to have been accessed via Advarra's internal systems. We are working continuously with outside experts to understand the nature and scope of the impacted data.

It is our understanding that the unauthorized third-party is threatening to release Advarra data publicly. We are currently assessing the veracity of those claims and will determine next steps once we have done so.

We appreciate your patience and understanding while we continue to conduct our investigation. Should we determine any sensitive data associated with your organization was impacted as a result of this incident, we will notify you directly.

Thank you,
Gadi Saarony
Chief Executive Officer, Advarra

Advarra.com
6100 Merriweather Dr., Suite 600, Columbia, MD 21044
Copyright © {{my.year:default=2022}} Advarra. All Rights Reserved.

Source: https://www.databreaches.net/exclusive-advarra-hacked-threat-actors-threatening-to-leak-data/