Another small firm suffers a serious ransomware attack: Cadre Services gets mauled by AlphV - DataBreaches.Net

Published: 2023-10-19 · Archived: 2026-04-09 02:13:14 UTC

There are some data leaks that make you shake your head and wonder about how a firm responded to a ransomware attack. This is one of them.

Cadre Services (previously known as Premier Staffing) is a Wisconsin-based company providing employment and staffing services for office professionals. They have been in business since 1994.

In a listing on AlphV's site, the threat actors claim that they acquired 100 GB of files including:

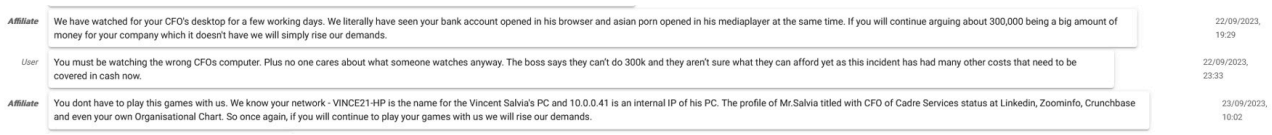
> – job seekers data (contacts, cv's, id's, drug screens, etc)
> – employees data (contracts, ssn, id's, drug screens, contacts, payments, etc)
> – top management data (contracts, ssn, id's, drug screens, contacts, payments, etc)
> – financial data (payments, transfers, etc)
> – ADB Ultrastaff data (all personal files used within this soft)
> – Smartsearch data (all I-9 records which could be find within this software files)
> – collection of pornography we have found at CFO Vincent Salvia PC which were hidden within HR files

AlphV then leaked what they describe as the first part of the data dump because:

> Unfortunately for ordinary people the top management of Cadre Services offered only $35,000 to protect their data. This sum is unacceptable. Since all the time needed for their bosses to make a decision were given and all the evidences were provided, Cadre Services decided to stop at price they have already offered, you can find all the data stolen from Cadre Services for free download now.

In support of that claim, DataBreaches was provided with screenshots of the negotiations between Cadre and the AlphV affiliate. From the screenshots, it appears they first contacted Cadre on or about September 19 and someone from the firm first responded on September 22.

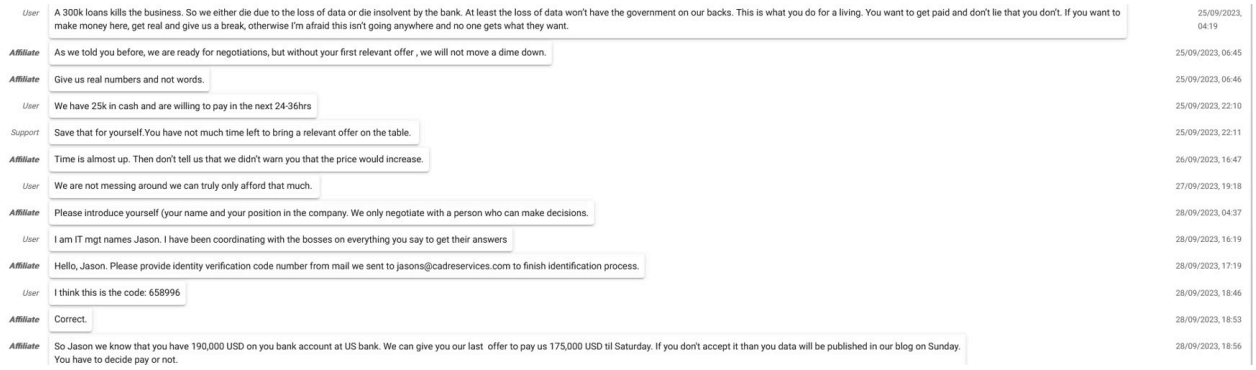
Early interactions did not go well as the firm's negotiator did not seem to really grasp that the affiliate had done their homework researching the firm and could see what the employees were doing — including emails to each other about how to communicate to clients about the breach. The following is a snippet from an early interaction after the negotiator insisted the firm could not afford to pay $300,000. [Note: DataBreaches has no idea if there really was pornography in the files of the CFO and some of the CFO's files have been locked in the data leak.]



The affiliate responded sharply to the negotiator's response:

> "You dont have to play this games with us. We know your network – VINCE21-HP is the name for the Vincent Salvia's PC and 10.0.0.41 is an internal IP of his PC. The profile of Mr.Salvia titled with CFO of Cadre Services status at Linkedin, Zoominfo, Crunchbase, and even your own Organisational Chart. So once again, if you will continue to play your games with us will will rise our demands."

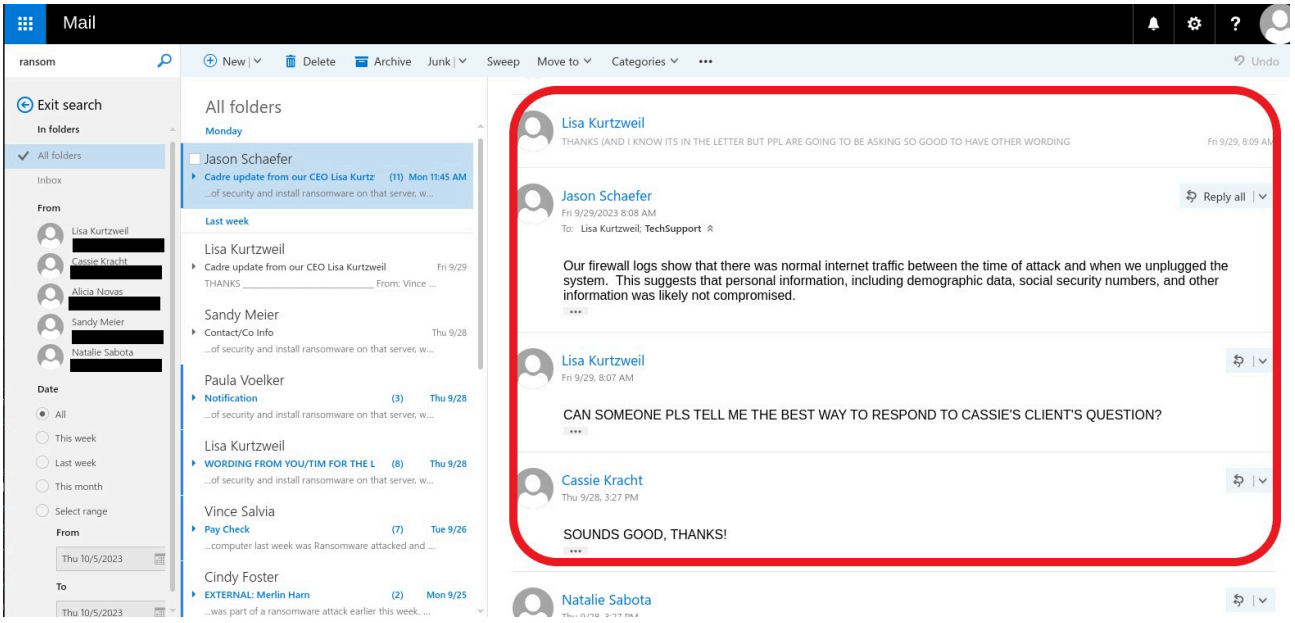
The firm's negotiator, who would later identify himself as the IT manager, "Jason," continued to insist that the company could not afford $300,000 and said the bosses were offering $25,000.00. The affiliate responded by pointing out that they could access the bank account and see that there was $190,000.00 in it.



User	A 300k loans kills the business. So we either die due to the loss of data or die insolvent by the bank. At least the loss of data won't have the government on our backs. This is what you do for a living. You want to get paid and don't lie that you don't. If you want to make money here, get real and give us a break, otherwise I'm afraid this isn't going anywhere and no one gets what they want.	25/09/2023, 04:19
Affiliate	As we told you before, we are ready for negotiations, but without your first relevant offer , we will not move a dime down.	25/09/2023, 06:45
Affiliate	Give us real numbers and not words.	25/09/2023, 06:46
User	We have 25k in cash and are willing to pay in the next 24-36hrs	25/09/2023, 22:10
Support	Save that for yourself.You have not much time left to bring a relevant offer on the table.	25/09/2023, 22:11
Affiliate	Time is almost up. Then don't tell us that we didn't warn you that the price would increase.	26/09/2023, 16:47
User	We are not messing around we can truly only afford that much.	27/09/2023, 19:18
Affiliate	Please introduce yourself (your name and your position in the company. We only negotiate with a person who can make decisions.	28/09/2023, 04:37
User	I am IT mgt names Jason. I have been coordinating with the bosses on everything you say to get their answers	28/09/2023, 16:19
Affiliate	Hello, Jason. Please provide identity verification code number from mail we sent to jasons@cadreservices.com to finish identification process.	28/09/2023, 17:19
User	I think this is the code: 658996	28/09/2023, 18:46
Affiliate	Correct.	28/09/2023, 18:53
Affiliate	So Jason we know that you have 190,000 USD on you bank account at US bank. We can give you our last offer to pay us 175,000 USD til Saturday. If you don't accept it than you data will be published in our blog on Sunday. You have to decide pay or not.	28/09/2023, 18:56

Cadre's subsequent attempts to negotiate fared no better, and their highest offer was $35,000. And that's where things have remained since October 4.

That is, until yesterday when AlphV emailed the firm again and this time included clients and DataBreaches in the distribution list. To show Cadre's clients how serious it was, they included sample files from the data leak that would be made today. One file included a screencap of a .csv file with employees' 401k data with date of birth, date of hire, SSN, name, address, wage information, etc. Another file included an applicant's data in the form of I-9 records. And to make life even more difficult for Cadre, they showed the clients how Cadre attempted to minimize the severity of the situation by saying that their logs did not indicate any SSN were likely to have been accessed:



> "Our firewall logs show that there was normal internet traffic between the time of attack and when we unplugged the system. This suggests that personal information, including demographic data, social security numbers, and other information was likely not compromised," they would tell a client.

"Likely not compromised? By September 29, when that email exchange took place, Cadre had already had one week to figure out that AlphV had acquired a lot of files with personal information.

Yesterday, DataBreaches emailed Cadre some questions after looking at a preview of the upcoming data leak and noting a lot of concerning files. The questions asked whether the firm had any cyberinsurance or insurance to help them recover from this attack. The second question was whether Cadre had any usable backups for the data AlphV had locked. The third question asked how many employees and applicants had their personal information accessed or acquired. The fourth question asked whether they had contacted law enforcement and whether they had notified anyone whose personal information was stolen.

No response was received, even though DataBreaches noted that if they were concerned that AlphV was still in their system, they could call this site from a personal mobile number.

So today AlphV uploaded what they say is the first part of the data leak. In one folder alone, there were almost 4,400 files with detailed personal and identity information on people seeking work. Most of these records used the Department of Homeland Security e-verify system. The forms included name, address, date of birth, Social Security number, and other identity information such as driver's license or passport, etc. Some of the information may now be inaccurate because many of these 4,400 files are more than a decade old. Why these files were not encrypted or stored offline is unknown to DataBreaches, but that was just one folder. Many other folders and files also appear to contain varying amounts of personal information.

Cadre appears to have somewhat of an incident response nightmare on their hands. Hopefully, they have usable backups, but they will still have a slew of individual notifications to make to people whose durable personal identity information has not only been compromised but has now been made freely available. And hopefully, they

also have cyberinsurance or some policy that may help pay the recovery and incident response costs that will mount up.

Note: DataBreaches notes that it's always possible that Cadre never intended to pay at all and was just stalling for time by appearing to negotiate.
