MUFON Data Base Hacked, YES .....

On Feb. 7th, 2024: I began getting emails, phone calls, and social media messages telling me the MUFON C.M.S. data base was compromised and no one in MUFON could access the C.M.S. system. My own concern was more than warranted as my own information, casework, witness information and other data was now in the hands of an unknown actor. Pertaining to the cases, in each case I had told witnesses that their information was secure, as this was what we all (MUFON functioning members) were told by MUFON.

On Feb. 7th, I contacted by phone Steve Hudgeons, the current MUFON Director of Investigations, and inquired about this recent news that was circulating on social media sites. Mr. Hudgeons was very forth coming about the events surrounding this data breech and shared with me relevant information. During the conversation, actually several conversation's that day, we discussed possible players that could be responsible for this data breech along with other actions or inactions MUFON was contemplating.

Mr. Hudgeons shared with me the following information.

As of Feb.5th, 2024, the MUFON data base had been hacked. This resulted in the total loss of control or use of the system by all MUFON members including upper MUFON management. The data base known as the C.M.S. (Case Management System) currently contains over 160,000 case reports.

The MUFON website was still operational. I did advise Mr. Hudgeons to consider securing some areas of the website until it was known if the cyber-attack was only targeted against the C.M.S. system.

We discussed the C.M.S. data base (created in 2005) and the event and witness information it contained. Information that was compromised includes names, addresses, telephone numbers, and in most case reports it contains the longitude and latitude locations of witnesses and event sites, along with other data surrounding the specifics of the event. This gives very exact data as to where the witness lives, and in many cases the witness's profession and other personal data.

..... On a side note, as it pertains to Close Encounter cases where a witness has an encounter with an entity: This could be of great concern if this information is also compromised as it contains very personal testimony from the witness. The last I knew these cases were kept on a dedicated server and not saved in the C.M.S. system. But I do recall a conversation with Mr. Hudgeons in the past where he stated there was an issue with the E.R.T. team (Experiencer Research Team) and it was decided Close Encounter cases were to be put in the C.M.S. system as is any other case reported to MUFON. Now, if this did actually play out as Mr. Hudgeons stated to me, I would recommend someone contact MUFON. If you were one of those who had an experience and reported it to MUFON, I would recommend you get a direct answer.

During my conversation on Feb. 7th, 2024, with Mr. Hudgeons, he informed me of specific information such as the I.P. address associated with the cyber-attack along with exactly how it has shut down MUFON's ability to function as an investigative body at the moment. Mr. Hudgeons also shared some current thoughts among MUFON personnel; below are the discussions that we had on Feb. 7th, 2024.

Mr. Hudgeons advised me that the C.M.S. system had been "backed up" and the data could be retrieved, with the exception of the last two weeks of activity. I have no reason to doubt this statement. I did advise Mr. Hudgeons that a definitive answer should be obtained; in cyber security attacks in the past on various other organizations/businesses it is common for those involved in this type of activity to not only access the system but to also take control of any backup systems in place.

During my discussions with Mr. Hudgeons on Feb.7th, 2024, there was discussion as to what steps were being taken to retrieve the data base back, if any. Mr. Hudgeons stated, as to steps to be taken, "None." He stated that they were "sitting behind the curtain and watching and waiting." I asked Mr. Hudgeons if law enforcement was involved. He stated that "law enforcement" had contacted MUFON and MUFON did not want any such help.

Mr. Hudgeons advised me that the I.P. number possibly returned to a specific ufology-related group. There was a lengthy conversation around this possibility. I was unaware of this newer ufology-related group's activities, or its current standing in the ufology field. Mr. Hudgeons advised me that I should conduct a Google search to see this particular group and I could see that their website was now appearing before MUFON's website in Google search returns when it came to reporting a U.A.P. / UFO. I ran some independent research. And it seems Mr. Hudgeons' statement was correct.

To clear up any misconception, this was one possibility that presented itself with the current information of which Mr. Hudgeons was aware and shared with me. As to not interfere with any ongoing or future investigation by law enforcement, I have not directly named the group in question.

I asked Mr. Hudgeons how they would proceed if this was a cyberattack of the sort where those who committed the crime requested a cash payment to get the data returned to MUFON. Mr. Hudgeons advised me it was doubtful MUFON would pay a ransom amount as it was discussed within MUFON that the direction they would take would be to start over with a new program system for C.M.S.

During my conversation with Mr. Hudgeons, he stated that it would take six months to one year to get things started back up. He believed they had the data backed up and they would use that for startup programming. Over the years Mr. Hudgeons and I have discussed data in the C.M.S.

system and he always kept the same train of thought that there was “nothing of value" in the C.M.S. system.

This data breech not only affects the witnesses but all of the past and present MUFON members. The C.M.S. system contains case work, witness data (which includes phone numbers, addresses etc.), with many cases containing very specific witness information. The C.M.S. system also contains Field Investigator contact information and passwords - over all, very sensitive information that goes back to at least 2005. This could include my own personal information.

Because of any ongoing or future investigations, I am not going to publish the I.P. address provided to me by email by Mr. Hudgeons on Feb. 7th, 2024.

To my knowledge MUFON has not made a statement concerning this issue nor has MUFON heard from the person(s) responsible for the cyberattack crime. Being reluctant to work with law enforcement, as is Mr. Hudgeons, makes this that much more of an important issue for all involved. MUFON has always stated that witness information and sensitive data would be protected, of which witnesses were made aware when reporting a U.A.P./U.F.O.

I am not releasing this information in an attempt to degrade MUFON or any other group. It is nothing more than the truth as I was told., allowing the reader to make up their own minds about its content.

To expand on this data breech: I would recommend those affected take the needed steps to ensure your safety, your information’s integrity, along with the safety of any other pertinent data you might have shared during the investigation. This recommendation is typical of any known data breech that has compromised any company or organization where it affects large amounts of public user information.

MUFON has many dedicated members with a true desire to solve the ufology mystery. This unfortunate event has changed the playing field for now. It is my hope MUFON gets ahead of this security breech and takes the needed steps to ensure this type of issue does not occur in the future if sensitive information is obtained by an unknown source. As stated, MUFON has the data backed up. I do hope MUFON reaches out to those who may be affected by this security breech as any other organization or business would do, and advise them of their options to protect their private information.

Phil Leech
February 8, 2024