AlphV responds to MGM incident and sloppy reporting - DataBreaches.Net

Published: 2023-09-15 · Archived: 2026-04-09 02:18:25 UTC

AlphV has posted a statement about their attack on MGM Resorts. They also post some scathing criticisms of journalists and news outlets for reporting inaccurately and not verifying sources. Of note, their statement also asserts, "The ALPHV ransomware group has not before privately or publicly claimed responsibility for an attack before this point. Rumors were leaked from MGM Resorts International by unhappy employees or outside cybersecurity experts prior to this disclosure. Based on unverified disclosures, news outlets made the decision to falsely claim that we had claimed responsibility for the attack before we had."

So no one from AlphV ever contacted vx-underground and talked about LinkedIn or social engineering on September 12? vx-underground has not retracted his claim about that, although DataBreaches reported at the time that there was no confirmation for his claims. DataBreaches has reached out to AlphV on Tox to ask them whether the report that LinkedIn was used, etc. was accurate or not, especially since it later seemed that the contact vx-underground heard from was someone AlphV says was pranking Reuters. Unfortunately, AlphV has not yet responded to this site's request for clarification so reports of social engineering using LinkedIn remain unconfirmed and possibly refuted.

Here is AlphV's full statement:

Statement of ALPHV group on MGM Resorts International: Setting the record straight

9/14/2023, 7:46:49 PM

We have made multiple attempts to reach out to MGM Resorts International, "MGM". As reported, MGM shutdown computers inside their network as a response to us. We intend to set the record straight.

No ransomware was deployed prior to the initial take down of their infrastructure by their internal teams.

MGM made the hasty decision to shut down each and every one of their Okta Sync servers after learning that we had been lurking on their Okta Agent servers sniffing passwords of people whose passwords couldn't be cracked from their domain controller hash dumps. Resulting in their Okta being completely locked out. Meanwhile we continued having super administrator privileges to their Okta, along with Global Administrator privileges to their Azure tenant. They made an attempt to evict us after discovering that we had access to their Okta environment, but things did not go according to plan.

On Sunday night, MGM implemented conditional restrictions that barred all access to their Okta (MGMResorts.okta.com) environment due to inadequate administrative capabilities and weak incident response playbooks. Their network has been infiltrated since Friday. Due to their network engineers' lack of understanding of how the network functions, network access was problematic on Saturday. They then made the decision to "take offline" seemingly important components of their infrastructure on Sunday.

After waiting a day, we successfully launched ransomware attacks against more than 100 ESXi hypervisors in their environment on September 11th after trying to get in touch but failing. This was after they brought in external firms for assistance in containing the incident.

In our MGM victim chat, a user suddenly surfaced a few hours after the ransomware was deployed. As they were not responding to our emails with the special link provided (In order to prevent other IT Personnel from reading the chats) we could not actively identify if the user in the victim chat was authorized by MGM Leadership to be present.

We posted a link to download any and all exfiltrated materials up until September 12th, on September 13th in the same discussion. Since the individual in the conversation did not originate from the email but rather from the hypervisor note, as was already indicated, we were unable to confirm whether they had permission to be there.

To guard against any unneeded data leaking, we added a password to the data link we provided them. Two passwords belonging to senior executives were combined to create the password. Which was clearly hinted to them with asterisks on the bulk of the password characters so that the authorized individuals would be able to view the files. The employee ids were also provided for the two users for identification purposes.

The user has consistently been coming into the chat room every several hours, remaining for a few hours, and then leaving. About seven hours ago, we informed the chat user that if they do not respond by 11:59 PM Eastern Standard Time, we will post a statement. Even after the deadline passed, they continued to visit without responding. We are unsure if this activity is automated but would likely assume it is a human checking it.

We are unable to reveal if PII information has been exfiltrated at this time. If we are unable to reach an agreement with MGM and we are able to establish that there is PII information contained in the exfiltrated data, we will take the first steps of notifying Troy Hunt from HaveIBeenPwned.com. He is free to disclose it in a responsible manner if he so chooses.

We believe MGM will not agree to a deal with us. Simply observe their insider trading behavior. You believe that this company is concerned for your privacy and well-being while visiting one of their resorts?

We are not sure about anyone else, but it is evident from this that no insiders have purchased any stock in the past 12 months, while 7 insiders have sold shares for a combined 33 MILLION dollars. (https://www.marketbeat.com/stocks/NYSE/MGM/insider-trades/). This corporation is riddled with greed, incompetence, and corruption.

We recognize that MGM is mistreating the hotel’s customers and really regret that it has taken them five years to get their act together. Other lodging options, including casinos, are undoubtedly open and happy to assist you.

At this point, we have no choice but to criticize outlets such as The Financial Times for falsely reporting events that never happened. We did not attempt to tamper with MGM’s slot machines to spit out money because doing so would not be to our benefit and would decrease the chances of any sort of deal.

The rumors about teenagers from the US and UK breaking into this organization are still just that—rumors. We are waiting for these ostensibly respected cybersecurity firms who continue to make this claim to start providing solid evidence to support it. Starting to the actors’ identities as they are so well-versed in them.

The truth is that these specialists find it difficult to delineate between the actions of various threat groupings, therefore they have grouped them together. Two wrongs do not make a right, thus they chose to make false attribution claims and then leak them to the press when they are still unable to confirm attribution with high degrees of certainty after doing this. The Tactics, Techniques, and Procedures (TTPs) used by the people they blame for the attacks are known to the public and are relatively easy for anyone to imitate.

The ALPHV ransomware group has not before privately or publicly claimed responsibility for an attack before this point. Rumors were leaked from MGM Resorts International by unhappy employees or outside cybersecurity experts prior to this disclosure. Based on unverified disclosures, news outlets made the decision to falsely claim that we had claimed responsibility for the attack before we had.

We still continue to have access to some of MGM's infrastructure. If a deal is not reached, we shall carry out additional attacks. We continue to wait for MGM to grow a pair and reach out as they have clearly demonstrated that they know where to contact us.

———————————————-

Updates:

Tech Crunch & others: neither you nor anybody else was contacted by the hacker who took control of MGM. Next time, verify your sources more thoroughly, or at the very least, give some hint that you do.

Additional Edits:

Previously incorrect attribution for slot machine report has been changed to correctly identify The Financial Times as the source of the utterly false information.

https://www.ft.com/content/a25d2897-b0ce-4ba7-92ed-ff5df09d1b47

More Updates on Fake News:

Zeba Siddiqui (Reuters) fails to confirm the credibility of sources before publishing items on Reuters that contain fake news, funnily enough naive individuals like this are the direct targets of social engineering schemes because they are so gullible. Find a new profession.

You were actually made fun of by a random Telegram user. You idiot. But hey, anything for a story, right?

https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14/

———————————————

As of September 15, 2023, we have not spoken with any journalists, news organizations, Twitter/X users, or anyone else. Any official updates are only available on this blog. You would think that after the tweet below, people would know better than to believe anything unreliable they would hear about this incident. If we talk to a reporter, we will share it here. We did not and most likely won't.

https://twitter.com/VitalVegas/status/1702017681963237410/photo/1
