

# "Almost everything you have posted in your news article about this incident is a total crap" -- BlackCat to Bangladeshi news outlets - DataBreaches.Net

Published: 2023-07-07 · Archived: 2026-04-11 02:21:07 UTC

On June 23, using the greeting that Hive ransomware always used in emailing victims, AlphV wrote to the Bangladesh Krishi Bank (BKB). Typos, grammar, and spelling as in the original:

Hello,Ladies and Gentlemen! This is ALPHV Ransomware Team.  
We are here to inform you about data breach which took place at the "Bangladesh Krishi Bank" network on June 21th 2023. As a result of this breach our team had downloaded over 170Gb of sensitive data from this network. Also we have encrypted all servers and data stored there. We have infiltrated your network and stayed there for 12 days, it was enough to study your documentation and download everything was needed.

Here is a quick scope of data we have downloaded:

- financial data (accounts, statements, payments, taxes, etc)
- employees data (emails, passports, labor papers, contracts, etc)
- sql backups dated 6/19/2023

You should contact us as soon as possible if you want to keep this incident confidential, protect your data and negate aftermath. We are ready to help you with data recovery and also we can show you how to protect your network and store data properly, for a fee.

You can find our contacts at the "RECOVER-a5pyfnp-FILES.txt" file which we left on every pc or contact us through this email.

Our organisation is kindly offering you to start negotiation with us. Sooner we will get message from you – less will be the price for your data!

We should inform you that if you will refuse to answer to us we will be forced to publish your data for free download through our special website.

Have a good day!

!!! DO NOT TRY TO DECRYPT OR CHANGE ENCRYPTED FILES ON YOUR COMPUTERS, IT WILL COMPLETELY DESTROY THEM !!!

On July 6, they wrote to BKB again, with a large distribution list of executives at BKB included. The July 6 email repeated a lot of the earlier communication but added:

http://[redacted by DataBreaches]

don't waste your time and stop the leak, contact us asap

and:

Unfortunately, for “Bangladesh Krishi Bank” top management, they decided not to negotiate recovery of stolen data's.

We have placed a strong backdoor tools within Krishi Bank's network, so we can always return there and do whatever we want.

IT-management of this bank does not have enough qualification and skills to protect their data.

“All the contributors and investors who used to store their money at the Bangladesh Krishi Bank should withdraw their money within 7 days after this message being send, in case if they don't want to lost all their money.” – this message will be send to all contacts and emails we will found in “Bangladesh Krishi Bank” documents, in case if “Bangladesh Krishi Bank” top-management will not contact us within 72 hours starting July 8th 2023.

An AlphV spokesperson confirmed to DataBreaches that BKB hadn't contacted AlphV at all since their first June 23 communication. But while the bank didn't contact AlphV, they were giving statements to local media. A June 25 news story reported that the Bangladesh Agricultural Bank was [in the hands of hackers](#). And on June 26, another news story provided an update claiming that the [server was recovered after 72 hours](#), but

The staff of the bank could not identify who is responsible for this hacking. It could not be confirmed whether any information was leaked or not.

That seems a bit odd since AlphV's very first email even announced who they were, but reporting in a [Barta24](#) article went beyond “odd” to downright inaccurate:

The [Managing Director] of the bank gave this information to the media on Sunday (June 25) night.

Shawkat Ali Khan claimed that some hackers had taken control of the bank's servers but could do no harm. All documents are intact. I have already taken full control.

[...]

When asked who hacked, he said, I have formed a committee to investigate the matter. When the committee's inquiry report comes in hand, it will be clear who did it and how.

Bangladesh Bank Executive Director and Acting Spokesperson Zakir Hossain Chowdhury said, “There was no hacking, I heard about Krishi Bank's server being down.” But now it is normal. No problem.

No hacking? Are they serious? DataBreaches is not criticizing the news outlet, but it sounds like they were given inaccurate info by a bank spokesperson. Perhaps after they read AlphV's site or this reporting, they will understand the discrepancy between what the bank has stated and what the attackers claim and have shown with proof of claims.

In any event, the local media coverage appears to have ticked off AlphV, who sent out another email today, but this time to press:

Hello, Ladies and Gentlemen!

This is ALPHV Ransomware Team.

We want to share with you some information relating to Bangladesh Krishi Bank hack attack.

Almost everything you have posted in your news article about this incident is a total crap.

The email then continues with a repetition of AlphV's claims about what they did and what they acquired and that they have already started leaking some of the data.

Finding no notice on its website or press release indexed in Google, DataBreaches reached out to the bank via email with three primary questions:

Does Krishi Bank acknowledge that some personal/financial information of customers was accessed and exfiltrated in the attack?

Is Krishi Bank notifying any customers or employees whose data has been accessed or exfiltrated?

How many customers had their personal information accessed or acquired?

No reply has been received as yet.

---

Source: <https://www.databreaches.net/almost-everything-you-have-posted-in-your-news-article-about-this-incident-is-a-total-crap-blackcat-to-bangladeshi-news-outlets/>