# Hackers claim to have attacked major Bangladeshi conglomerate - DataBreaches.Net

Published: 2021-01-19 · Archived: 2026-04-09 02:09:06 UTC

Hackers claim to have successfully attacked a multinational  conglomerate that is described as having the largest market capitalization on Bangladesh's stock market.


*Beximco's mission is "Taking Bangladesh to the World."*

**Background on BEXIMCO**

The Bangladesh Export Import Company Limited ("BEXIMCO") was founded in the 1970s and has approximately 70,000 employees worldwide.  It has operations and investments across a wide range of industries including textiles, pharmaceuticals, PPE, ceramics, real estate development, construction, trading, marine food, information and communication technologies, media, Direct to Home (DTH) services, financial services, and energy.

"The Group" (as it is called) consists of four publicly traded and seventeen privately held companies. The publicly traded companies are Bangladesh Export Import Company Limited, Beximco Pharmaceuticals Limited, Shinepukur Ceramics Limited and Beximco Synthetics Limited.

BEXIMCO's newest vertical is its PPE Division. In May, 2020, BEXIMCO began shipping millions of PPE gowns, masks, and coveralls to the U.S., and its pharmaceutical division became the world's first company to start supplying the generic version of the antiviral medication Remdevisir for COVID-19 treatment after the drug was approved by the U.S. Food and Drug Administration for emergency use.

The total revenue of the BEXIMO group stands in excess of $1 billion USD each year. And that made it an attractive target for hackers.

**ALTDOS Claims**

This week, ALTDOS hackers contacted DataBreaches.net to report that they had hacked BEXIMCO in December, but BEXIMCO had not responded to their demands.

*[Note: DataBreaches.net refers to ALTDOS in the plural because a spokesperson claims that ALTDOS has multiple members, but DataBreaches.net really has no proof as to whether ALTDOS is one person, a few, or many.*

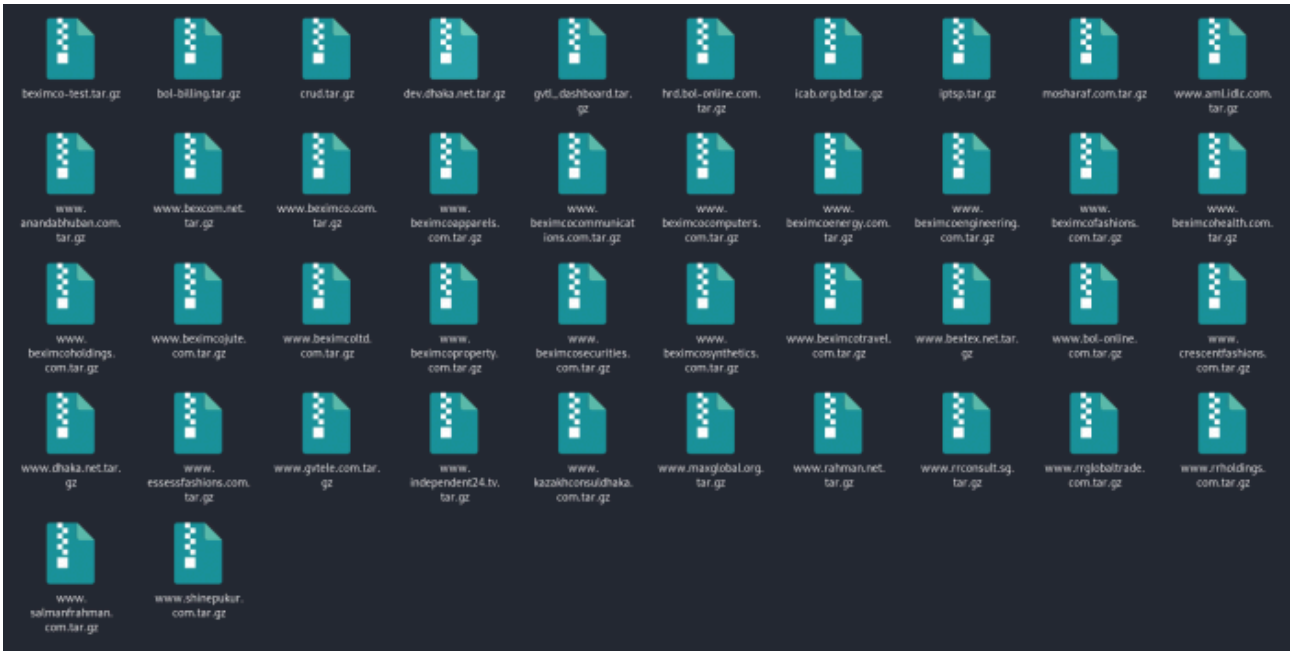
*Previous coverage of ALTDOS's claimed hacks are linked from [here](here).]*

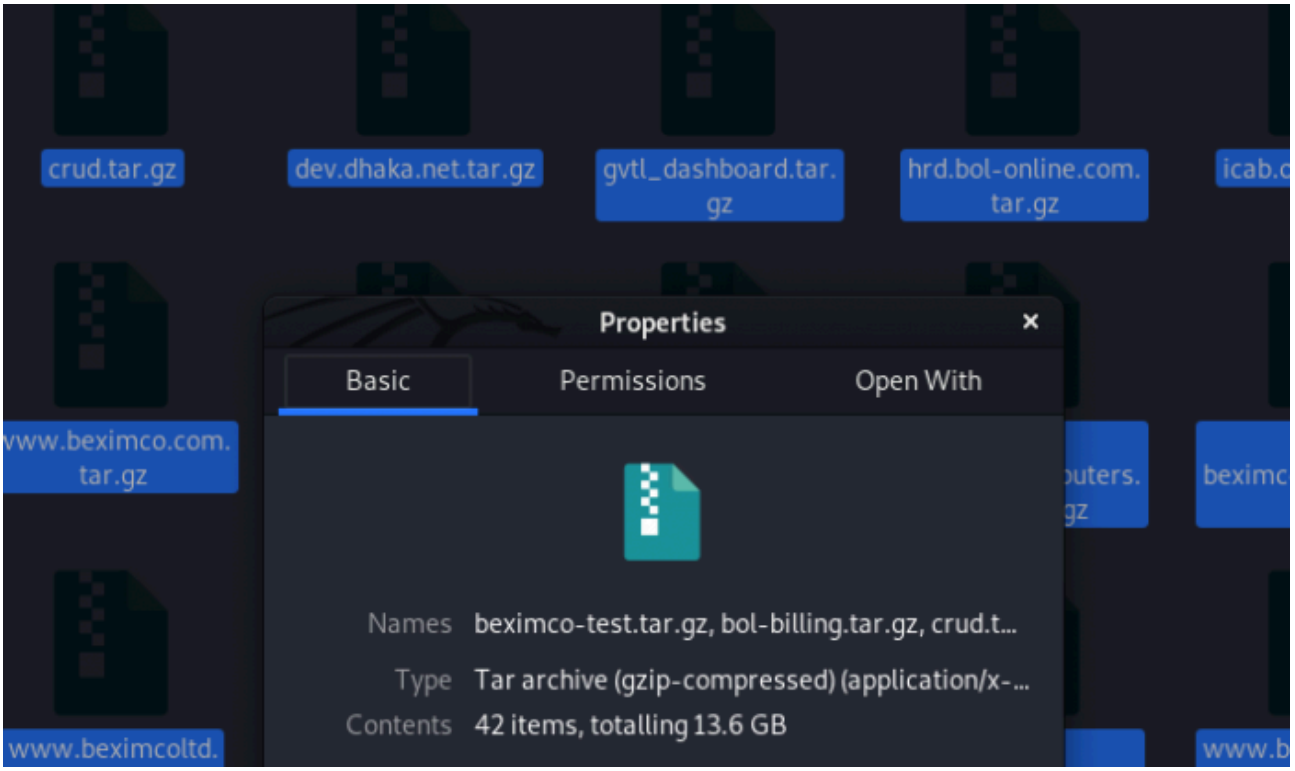
"In total, ALTDOS has stolen hundreds of gigabytes of files, source coding and databases from 34 of Beximco websites, including its telecom subsidiary – BOL-ONLINE.COM," a spokesperson wrote to DataBreaches.net.

As they have done with other hacks they have claimed, ALTDOS provided a small sample of data and screencaps as proof. Nothing in the data sample appeared super-sensitive, although one of the files contained some employee attendance information for a time period from September 24, 2018 to May 17, 2019. That file had 56,088 rows each with an employee ID number, their department, their name, and their email address. More than 23,450 of the email addresses were from the bol-online.com domain. More than 19,000 of the email addresses were from the beximco.net domain. Approximately 4800 were from gvtele.com. The remainder were from assorted non-corporate domains such as gmail.com, yahoo.com, and hotmail.com.

DataBreaches.net sent email inquiries to a few of the email addresses in the file listed as being involved in security or network. A few bounced back. Others were seemingly delivered, but DataBreaches.net received no reply. Nor did the conglomerate's corporate media department reply to an inquiry sent 24 hours ago.

ALTDOS provided screencaps showing the names of folders in various directories, and the amount of data being downloaded (or in this case, 13.6 GB compressed size for 42 compressed web site folders, one of which is likely just a test folder).






Another file called “payment_info” contained what appeared to be more than 65,000 rows with payment records, but there was nothing in there that would be problematic in terms of bank account numbers, credit account numbers, or parties’ names, etc.

Of note, DataBreaches.net did not see any evidence that ALTDOS had obtained any corporate IP, trade secrets, or confidential communications from any of the conglomerate’s divisions. When asked about other proof or types of files, an ALTDOS spokesperson said they were currently going through all the sql databases they had exfiltrated to evaluate the information they had obtained and would be providing more proof and details in the future.

This story will be updated if more information is obtained or a response is received from the conglomerate. While Bangladeshi law provides for criminal consequences to hackers, if caught and convicted, it is not clear that the conglomerate would have any breach notification obligations under Bangladeshi law if the hackers acquired personal information of employees and/or customers. There appear to be obligations about reasonable security, but there does not seem to be any obligation to notify employees or customers in the event of a data breach involving personal information. A review of Bangladeshi data protection laws can be found here. If this site has mis-stated the country’s breach notification laws, please let us know.

---