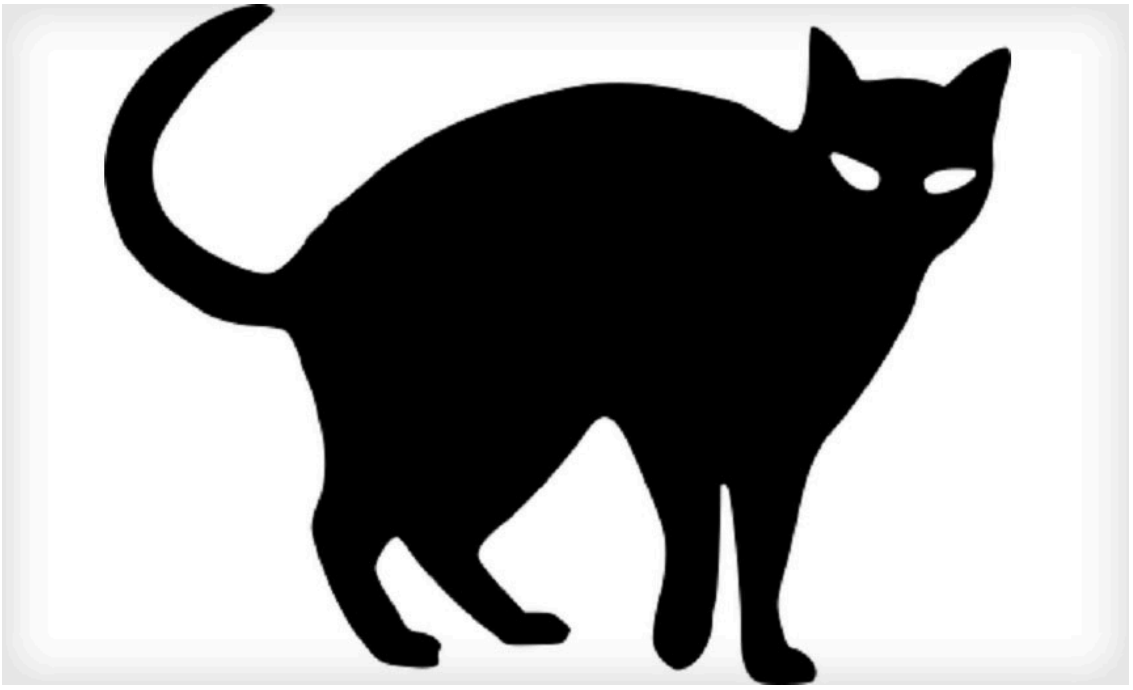
Update: What's BlackCat Ransomware Been Up to Recently?

By Mihir Bagwe

Archived: 2026-04-05 19:59:45 UTC

Business Continuity Management / Disaster Recovery , Cybercrime , Cybercrime as-a-service

1 Betting Platform, 3 Universities and 1 Natural Gas Supplier Allegedly Compromised (MihirBagwe) • April 11, 2022



The BlackCat ransomware group is possibly a rebrand of BlackMatter and DarkSide. (Source: Pixabay)

BlackCat, believed to be a rebranded version of the BlackMatter or DarkSide ransomware group, has claimed to have successfully targeted several organizations including a popular Nigerian betting platform Bet9ja, three universities - FIU, NCAT State University, AIT-Thailand, and the largest natural gas supplier in Latin America - TGS, in the past few days.

Bet9ja, FIU, and NCAT State University have confirmed to ISMG that they were subjected to ransomware attacks, however, they say that no data losses have been found yet.

Bet9ja Bets All Data is Secured

Nigerian betting platform Bet9ja suffered a ransomware attack perpetrated by the BlackCat ransomware group on April 6, which the company confirmed on Sunday - two days after the attack.

The attack disrupted Bet9ja's regular operations, and many users complained of not being able to log into their accounts, but CEO Ayo Ojuroye maintains that "all accounts, data and funds" are "safe."

On Wednesday, Bet9ja tweeted that its website was experiencing a technical issue and restricted its users from logging in to their accounts. The company promised customers that its IT team was working on the issue as a priority, but the platform continued to face downtime. According to recent reports, however, services have finally been restored.

On Sunday, the company issued a statement on the "criminal cyberattack."

In the announcement, Bet9ja says it has hired independent cyber forensics and cybercrime experts to investigate and resolve the situation.

Ojuroye also tweeted a confirmation of the "unprovoked and unjustified" attack on Wednesday, adding that the company continued to be in control of the situation and that all customer accounts, data and funds were secure.

Ojuroye says that the company has "taken steps to reduce and mitigate any risk to our network systems and operations. We have deployed international cybersecurity and [cyber] forensic experts to help us analyze and improve our network security and strengthen our operations to be more resilient and secure."

He did not, however, detail what measures were taken. The company did not respond to Information Security Media Group's request for comment.

Acknowledging the attack, the National Lottery Regulatory Commission of Nigeria says that it condemns the attack on "one of Nigeria's leading sports betting companies" - KC Gaming Networks Limited, which is Bet9ja's parent company.

"As the apex regulator of lotteries and gaming in Nigeria, we entirely condemn such a nefarious act that has adversely affected the company's operations, albeit temporarily," it says.

The NLRC adds that it was satisfied with Bet9ja's response to the incident and assured the public that its business operations would soon return to normal.

BlackCat Lists Bet9ja

While Bet9ja did not respond to ISMG's queries on whether the company would pay a ransom, BlackCat has upped the pressure by publishing details of the attack on its darknet website.

Soufiane Tahiri, an independent cybersecurity researcher, tweeted screenshots of the website, which shows the attackers claiming that they "have about 2TB confidential data of all clients, financial reports, software source code, etc."

The screenshot also contains redacted images of what appear to be copies of customer passports, credit/debit card, and other personally identifiable information, including banking details.

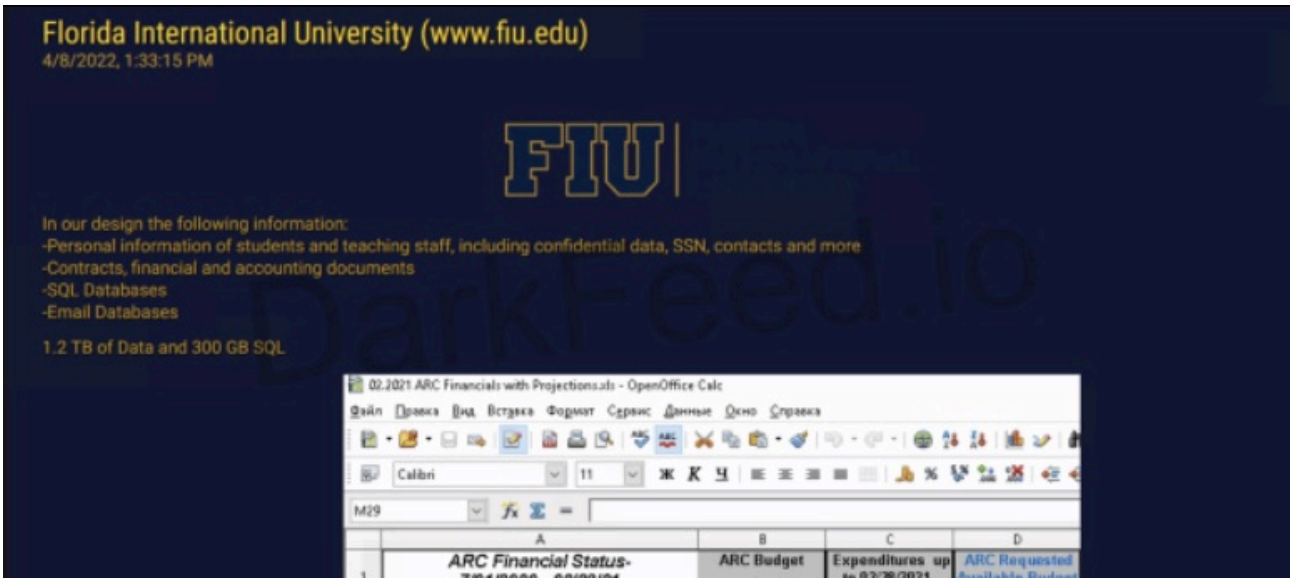
BlackCat's Other Victims

It appears that BlackCat has been busy elsewhere in the world.

In the past four days, it has reportedly published details of leaks following an attack on several educational institutions, including Florida International University, North Carolina Agricultural and Technical State University, the Asian Institute of Technology, and Argentina's largest natural gas extractor company, Transportadora de Gas del Sur - or TGS.

Florida International University

Darkfeed, a darknet monitoring platform, on Friday shared that BlackCat has claimed to have stolen nearly 1.2 TB of data and 300 GB of SQL databases from Florida International University.



BlackCat's FIU data leak post on its darknet website. (Source: Darkfeed.io)

The stolen data allegedly contains PII of students and staff members, including their Social Security numbers and contacts. The threat actor has also stolen the university's contracts, financial and accounting documents, SQL and email databases, according to Darkfeed.

The university shared with ISMG the statement it sent to its employees and students. So far, there is no indication of the compromise, FIU says.

FIU | FLORIDA INTERNATIONAL UNIVERSITY

April 8, 2022

Dear members of the university community,

Today, a ransomware group posted that sensitive FIU data had been exfiltrated. We have been investigating and there is no indication thus far that sensitive information has been compromised. At this time, no further information is available.

Statement shared with ISMG

In an update shared with ISMG on April 12, FIU confirms that it recently became aware of a security incident involving ransomware that affected some of its systems at the university. "We immediately started an investigation, informed law enforcement and engaged third party professionals to assist in the investigation of the incident. On Friday, April 8, 2022 [as seen above], we made our university community aware of a ransomware group's claims that sensitive FIU data was exfiltrated and our efforts to investigate," FIU says.

This investigation is ongoing, and with the help of its partners, FIU says, it is trying to gain a complete understanding of the incident – "including what type of data was stored on the server and may be at risk."

Currently FIU tells ISMG that the organization does not believe that any financial information, social security numbers, or information on student performance was stored on the impacted server.

FIU adds that the "incident has not impacted the education process – students and researchers are continuing their work, uninterrupted." Updates about any new findings will be shared soon, the FIU concluded.

North Carolina Agricultural and Technical State University

The ransomware operators did not specify how much data they exfiltrated from the NCAT State University, but posted that the details were similar to those leaked in the FIU case.

A spokesperson for NCAT State University tells ISMG, "We recently experienced a cybersecurity incident to which our IT Services Department responded immediately, shutting down various systems to contain the incident. After exhaustive review, multiple investigating agencies have found no current faculty, staff or student data were affected."

"While we have restored access to the majority of our systems, work continues to be done to enhance and strengthen our IT infrastructure, while ensuring that systems needed by faculty, staff and students are available."

Citing the ongoing investigation, the spokesperson declined to comment on further specifics of the attack.

Noting the ransomware attacks on FIU and NCAT State University, Brett Callow, a threat analyst at Emsisoft, says BlackCat, or Alphv, has increased its targeting of educational institutions. Callow says this is the third time this year that the group has targeted a U.S.-based university or college, and the first such attack in 2022 was on Phillips Community College in February.

According to Callow, at least 10 U.S. universities or colleges and eight school districts, for a total of 214 schools, have been affected by ransomware so far this year. He says data was stolen in at least 11 of the 18 incidents.

Asian Institute of Technology

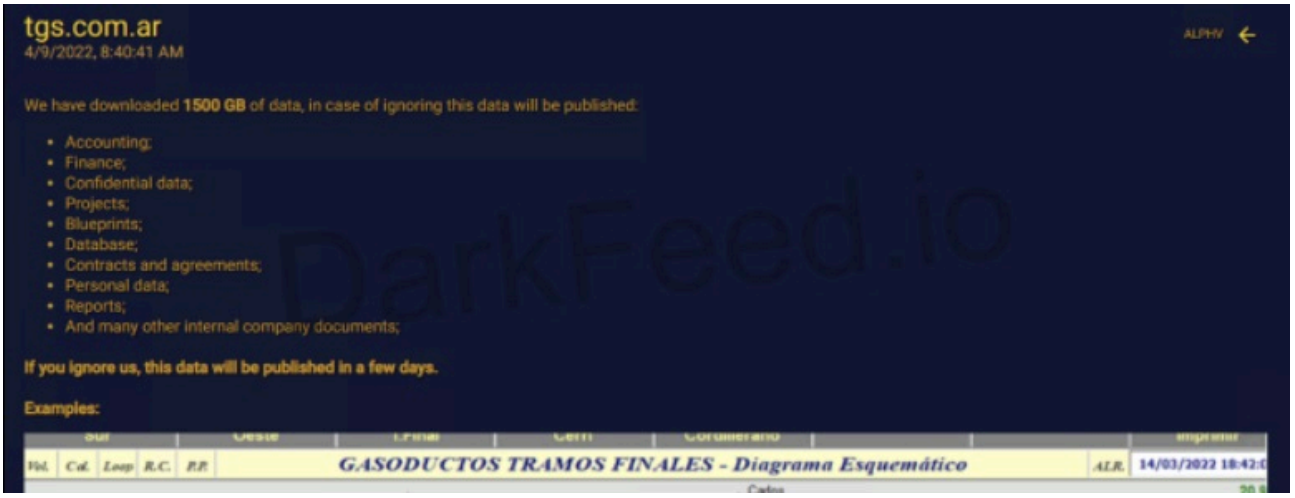
BlackCat has allegedly said that it stole 2TB worth of data, including employee PII data, client documentation and network map, including credentials for local and remote services, from Bangkok-based Asian Institute of Technology.

No other details about the leak could be confirmed or verified by the institute.

An independent Indian security practitioner who uses the alias Kulkarni Defence on Twitter, shared unredacted grabs of the alleged data leak post. The images show investment and financial records, along with associated files starting in 2017.

Transportadora de Gas del Sur

Of all the alleged ransomware attacks and claimed leaks, the claimed breach of Transportadora de Gas del Sur is likely to have the biggest impact, if proven. TGS is the biggest pipeline system in Latin America, transporting 60% of the total natural gas consumed in the region, and it supplies directly to distributors, electric generators and industries.



BlackCat's TGS data leak post on its darknet website (Source: Darkfeed.io)

There is no independent confirmation, but BlackCat says it has exfiltrated around 1,500GB or 1.5TB worth of data, including accounting, finance, contracts and agreements, PII, project blue prints, reports and several other internal company documents of TGS.

BlackCat has reportedly warned all victims that the stolen data will be published on their sites if the ransom amount is not paid.

AIT and TGS did not immediately respond to ISMG's request for further details on the veracity of the threat group's claims and the ransom demands.

Connection with BlackMatter

BlackCat is said to be a rebrand of ransomware groups BlackMatter and DarkSide, following international scrutiny last year. Some security practitioners have debated these claims, but a new study from cybersecurity researchers at Kaspersky has uncovered further links between BlackCat and BlackMatter ransomware families.

"At least some members of the new BlackCat group have links to the BlackMatter group, because they modified and reused a custom exfiltration tool which has only been observed in BlackMatter activity," the Kaspersky researchers say.

The tool, dubbed Fendr, has been upgraded to include more file types and has been used extensively to steal data from corporate networks. "This use of a modified Fendr, also known as ExMatter, represents a new data point connecting BlackCat with past BlackMatter activity," the researchers say.
