Ransomware attack on Accenture

Global IT consultancy giant Accenture confirmed that LockBit ransomware operators stole data from its systems during an attack that hit the company's systems in August 2021.

This was revealed in the company's financial report for the fourth quarter and full fiscal year, which ended on August 31, 2021.

Accenture stated that the affected systems had been recovered from a backup. A spokesperson in a statement provided to CNN implied that the attack was discovered through monitoring and that it had no impact on the company's operations or its clients' systems. Cybel, a dark web and cyber crime monitoring firm tweeted that the $50 million ransom was for 6 TB of stolen data which was stolen with the help of a company insider. In fact, LockBit 2.0 is actively recruiting insiders and promising to pay them millions.

Meanwhile, some of the data was exposed for a limited time after the first payment deadline of four hours passed. However, Tor was down at the time. LockBit then set another deadline which has also passed.

LockBit 2.0 is the latest version of the ransomware. Felipe Duarte, a security researcher at Appgate said that the new version is capable of encrypting entire Windows domains through group policies. Then it spreads to devices connected to the network and disables antivirus software and execute ransomware. It also sets the wallpaper to a ransom note which is an ad attempting to recruit insiders willing to aid and abet a LockBit ransomware attack for a promise of millions.

Crime intelligence firm Hudson Rock said that 2,500 employee and partner computers were affected. Sources familiar with the attack also told BleepingComputer that Accenture confirmed the ransomware attack to at least one cyber threat intelligence vendor.

Even though Accenture has now confirmed that the attackers stole information from its systems and leaked it online, the company has not yet publicly acknowledged the data breach outside SEC filings or filed data breach notification letters with relevant authorities.

This likely means that the stolen data didn't contain any personally identifiable information (PII) or protected health information (PHI) data which would've triggered regulatory notification requirements.

Accenture did not reply to a CRN inquiry about why no mention was made of the ransomware attack.

However, an Accenture spokesperson at the time of the attack told CRN via email that, “Through our security controls and protocols, we identified irregular activity in on of our environments. We immediately contained the matter and isolated the affected servers. We fully restored our affected servers from back up. There was no impact on Accenture’s operations, or on our clients’ systems.”

Accenture on September 1, in response to reports that the LockBit gang took advantage of credentials accessed during the Accenture cyberattack to go after the consulting giant’s customers, disputed that claim in a statement.€€

“We have completed a thorough forensic review of documents on the attacked Accenture systems. This claim is false. As we have stated, there was no impact on Accenture’s operations, or on our client’s systems. As soon as we detected the presence of this threat actor, we isolated the affected servers,” the company said in that statement.

Reference:

1. <https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/>
2. <https://www.zdnet.com/article/accenture-says-lockbit-ransomware-attack-caused-no-impact-on-operations-or-clients/>
3. <https://www.cshub.com/executive-decisions/articles/accenture-faces-50-million-ransom-demand>