Ransomware Case Study

Blackbaud

Khadijat Yussuff, 2022

Cybercriminal Ransomware Attack on Blackbaud

- Ransomware is a type of malware that is designed to deny a user or organization access to their own files.
- In 2021, the average number of cyberattacks and data breaches increased by 15.1% from the previous year.
- Data breaches and ransomware attacks last year alone specifically cost the healthcare industry an estimated $4 billion. As experts note, it has more to do with the value of healthcare data than the state of security in the industry.
- At least 10 of Blackbaud’s clients were healthcare providers, and over 1.7 million individual’s information was potentially accessed.

Blackbaud Inc. is a publicly-traded company based in South Carolina, and provides cloud-based CMS for a variety of organizations including charitable foundations, educational and health institutions, religious organizations and non-profit groups in the U.S. and abroad.

“Blackbaud became victim to a ransomware attack beginning in February 2020, which remained undetected until May 2020. Blackbaud paid the ransom and received confirmation the data had been destroyed. Before deleting the data, the cybercriminals copied sensitive data from over 6 million donors, potential donors, patients and community members including names, emails, phone numbers, dates of birth, genders, provider names, dates of service, department visited and philanthropic giving history. A recent SEC filing in September 2020 reveals hackers gained access to more unencrypted data than originally reported, including Social Security numbers, financial accounts, and payment information. Hundreds of Blackbaud’s impacted clients continue to disclose the data incident.”

Timeline

Blackbaud Attack

1 7 Feb 2020 - Hackers gain entry into Blackbaud’s servers & install ransomware.

2 20 May 2020 - Blackbaud detects the attack, and stops it - after paying $350k to the hackers to delete, decrypt, and refrain from leaking all acquired data in the breach.

3 16 Jul 2020 - Blackbaud informs clients of the attack, and makes a statement claiming "The cybercriminal did not access credit card information, bank account information, or social security numbers."

4 29 Sept 2020 - Blackbaud reneges in an SEC filing, admitting that “the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords.”

5 Apr 2021 - 15 lawsuits by 34 plaintiffs across 20 US states are consolidated and filed as a class-action lawsuit against Blackbaud.

6 2022 - Lawsuit proceedings continue.

Vulnerabilities

While the Blackbaud data breach was unfortunate in itself, the true mistake was in the way the company mishandled the situation upon detection in May. From not alerting its clients for 2 months to not following best practices for containment of hacker attacks, it saw over a dozen lawsuits leveraged against it claiming deception, and went down as one of the largest data breaches, especially in the healthcare sector, this decade.

Vulnerability #1

We do not know how the hacker gained access to Blackbaud's servers, but that process would reveal a security vulnerability.

Vulnerability #2

The then-current security protocols being unable to detect an intruder, before the ransomware installation.

Vulnerability #3

Having no action plan and recourse but to pay the hacker the requested amount for data deletion.

Vulnerability #4

Being intentionally dishonest about the scope of the attack with its clients, leading to further financial loss in the form of legislative fees.

Costs

- $350k to Hackers for Decryption & Deletion
- $25 - 35M in legal fees related to lawsuits
- Blackbaud has not recorded a loss contingency related to the data breach "as it is unable to reasonably estimate the possible amount or range of such loss."

Prevention

- Tokenize & encrypt ALL data on its servers, not just bank data or SSNs, and back up data in a timely manner.
- Ensure consistent penetration testing and monitoring for potential attacks, as well as implementing monthly patches.
- Create an action plan in the case of a potential breach, including how and when to alert their clients.

Bibliography

- “2020 Data Breaches - the Most Significant Breaches of the Year: IdentityForce®.” *We Aren't Just Protecting You From Identity Theft. We Protect Who You Are.*, 4 Feb. 2022, https://www.identityforce.com/blog/2020-data-breaches.

- Admin. “5 Key Industries Most Vulnerable to Cyber Attacks in 2020.” *SecurIT*, 13 July 2021, https://www.securit.biz/en/blog/key-industries-most-vulnerable-to-cyber-attacks.

- Brooks, Chuck. “Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know.” *Forbes*, Forbes Magazine, 6 June 2022, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=24fab17c7864.

- Cimpanu, Catalin. “Cloud Provider Stopped Ransomware Attack but Had to Pay Ransom Demand Anyway.” *ZDNet*, 17 July 2020, https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/.

- “FORM 8-K Blackbaud, Inc.” *BLKB-20200929*, UNITED STATES SECURITIES AND EXCHANGE COMMISSION, 29 Sept. 2020, https://www.sec.gov/Archives/edgar/data/1280058/000128005820000044/blkb-20200929.htm.

- Hrywna, Mark. “Blackbaud Projects $1B in Revenue, Millions in Breach Costs.” *The NonProfit Times*, 23 Feb. 2022, https://www.thenonprofittimes.com/finance/blackbaud-projects-1b-in-revenue-millions-in-breach-costs/.

- Karabus, Jude. “Blackbaud – Firm That Paid off Crooks after 2020 Ransomware Attack – Fails to Get California Privacy Law Claim Dropped.” *The Register® - Biting the Hand That Feeds IT*, The Register, 17 Aug. 2021, https://www.theregister.com/2021/08/17/ccpa_blackbaud/.