UK Labour Party discloses data breach after ransomware attack

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** November 3, 2021 01:22 PM **0**

The U.K. Labour Party notified members that some of their information was impacted in a data breach after a ransomware attack hit a supplier managing the party's data.

The data breach was announced in a data breach notification published on the party's website after informing relevant authorities about the incident.

"On 29 October 2021, we were informed of the cyber incident by the third party. The third party told us that the incident had resulted in a significant quantity of Party data being rendered inaccessible on their systems," the breach notice reads (https://labour.org.uk/about-your-data/).

"As soon as the Party was notified of these matters, we engaged third-party experts and the incident was immediately reported to the relevant authorities, including the National Crime Agency (NCA), National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO)."

Breach caused by ransomware attack

Data involved in the incident includes information provided by members, registered and affiliated supporters, and others who have provided their info to the Party.

The incident is still being investigated, and the full scope and impact of the data breach are yet unknown.

The Labour Party advises members potentially affected by this incident

While the U.K. party did not disclose the nature of the incident, sources close to the investigation told Sky News (https://news.sky.com/story/labour-party-supporters-details-affected-by-cyber-security-breach-12458935https://news.sky.com/story/labour-party-supporters-details-affected-by-cyber-security-breach-12458935) that the attack involved ransomware being deployed on the third-party supplier's systems containing Labour Party data.

> *The Party takes the security of all personal information for which it is responsible very seriously. It is doing everything within its power to investigate and address this incident in close liaison with law enforcement, the Information Commissioner's Office, and the affected third party. - Labour Party*

Members' financial info, credentials exposed in 2020 breach

The Labour Party disclosed another data breach (https://labour.org.uk/privacy-policy/blackbaud-data-breach/) following a similar incident last year, in July, after leading cloud software provider Blackbaud and of the party's suppliers was hit by a ransomware attack in May 2020 and disclosed on July 16 (https://www.blackbaud.com/newsroom/article/2020/07/16/learn-more-about-the-ransomware-attack-we-recently-stopped).

As the party revealed at the time, the breach included members' names, email addresses, phone numbers, and amounts donated.

While the party said immediately after the breach that no sensitive data like bank account information, passwords, or usernames were exposed, Blackbaud's forensic investigation revealed (https://www.bleepingcomputer.com/news/security/blackbaud-ransomware-gang-had-access-to-banking-info-and-passwords/) that the threat actors had access to unencrypted banking info, credentials, and SSNs.

security numbers, usernames and/or passwords," Blackbaud said in an 8-K filing (https://www.documentcloud.org/documents/7220021-BLACKBAUD-BC-8K.html) with the U.S. Securities and Exchange Commission (SEC).

Other organizations impacted by the Blackbaud ransomware attack (http://www.prnewswire.com/search/news/?keyword=Blackbaud&page=1&pagesize=100www.prnewswire.com/search/news/?keyword=Blackbaud&page=1&pagesize=100) include charities, non-profits, foundations, and universities from the United States, Canada, the United Kingdom, and the Netherlands.

Related Articles:

Accenture confirms data breach after August ransomware attack (https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/)

Trucking giant Forward Air reports ransomware data breach (https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-reports-ransomware-data-breach/)

BlackMatter ransomware moves victims to LockBit after shutdown (https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/)

BlackMatter ransomware claims to be shutting down due to police pressure (https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-claims-to-be-shutting-down-due-to-police-pressure/)

BlackByte ransomware decryptor released to recover files for free (https://www.bleepingcomputer.com/news/security/blackbyte-ransomware-decryptor-released-to-recover-files-for-free/)

DATA BREACH (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DATA-BREACH/)

LABOUR PARTY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LABOUR-PARTY/)

RANSOMWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/)

UK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/UK/)