Rail giant Wabtec discloses data breach after Lockbit ransomware attack

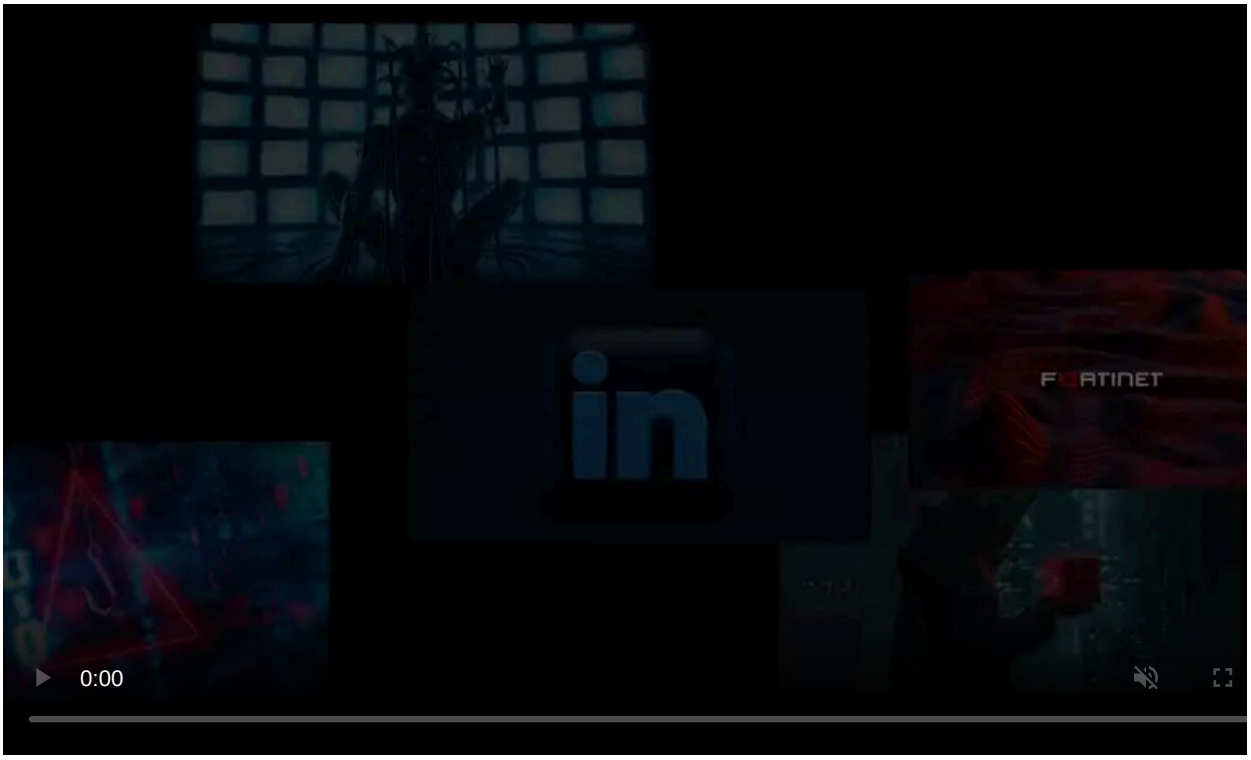
By Bill Toulas

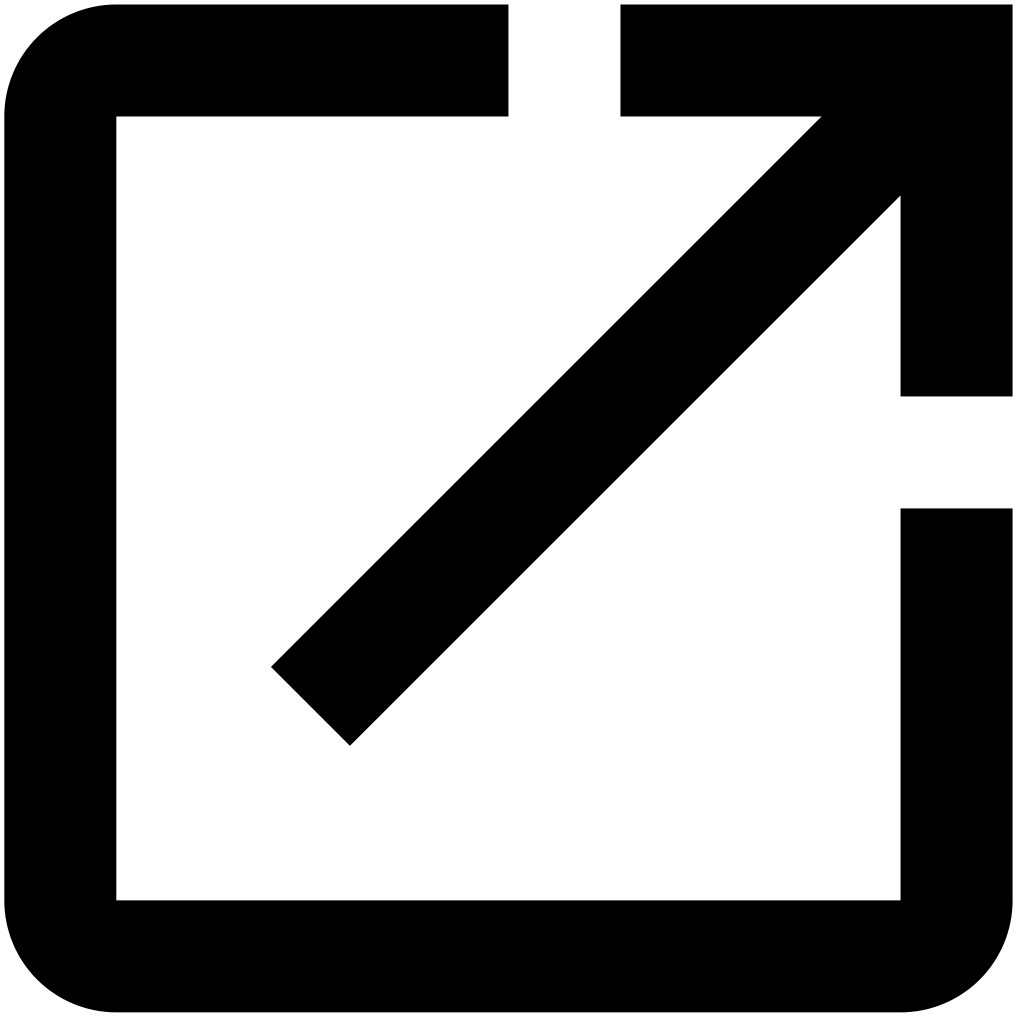
Published: 2023-01-03 · Archived: 2026-04-05 19:13:22 UTC

U.S. rail and locomotive company Wabtec Corporation has disclosed a data breach that exposed personal and sensitive information.

Wabtec is a U.S.-based public company producing state-of-the-art locomotives and rail systems. The company employs approximately 25,000 people and has a presence in 50 countries, being the world's market leader in freight locomotives and a major player in the transit segment.

The firm's 2021 financial results give a revenue figure of $7.8 billion, reporting a staggering 20% of the world's freight being moved by the 23,000 of Wabtec's locomotives in global operation.


0:00



Visit Advertiser websiteGO TO PAGE

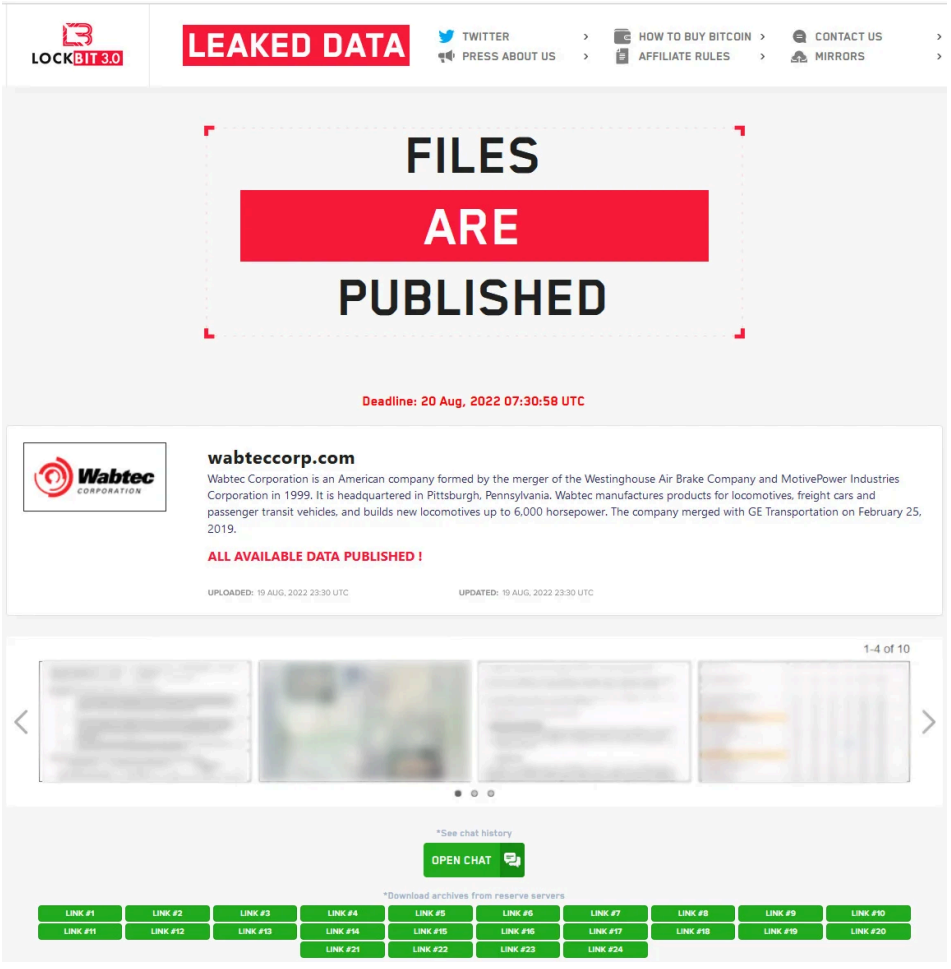
Wabtec discloses a data breach

In an announcement published at the end of the year, Wabtec says hackers breached their network and installed malware on specific systems as early as March 15th, 2022.

On June 26th, Wabtec said they detected unusual activity on their network leading to an investigation of the attack and whether the hackers had stolen data.

On the next day, news outlets reported that sources at one of Wabtec's plants indicated that it was a ransomware attack impacting the rail giant. However, the company did not officially respond to the rumors.

A couple of weeks later, LockBit published samples of data stolen from Wabtec and eventually leaked all stolen data on August 20th, 2022, presumably after a ransom was not paid.



LockBit published all files stolen from Wabtec *(BleepingComputer)*

As Wabtec explains now, its investigation of the incident was concluded on November 23rd, 2022, when data review specialists confirmed that LockBit had stolen files containing sensitive personal information.

This stolen data exposed a wide variety of sensitive information, including:

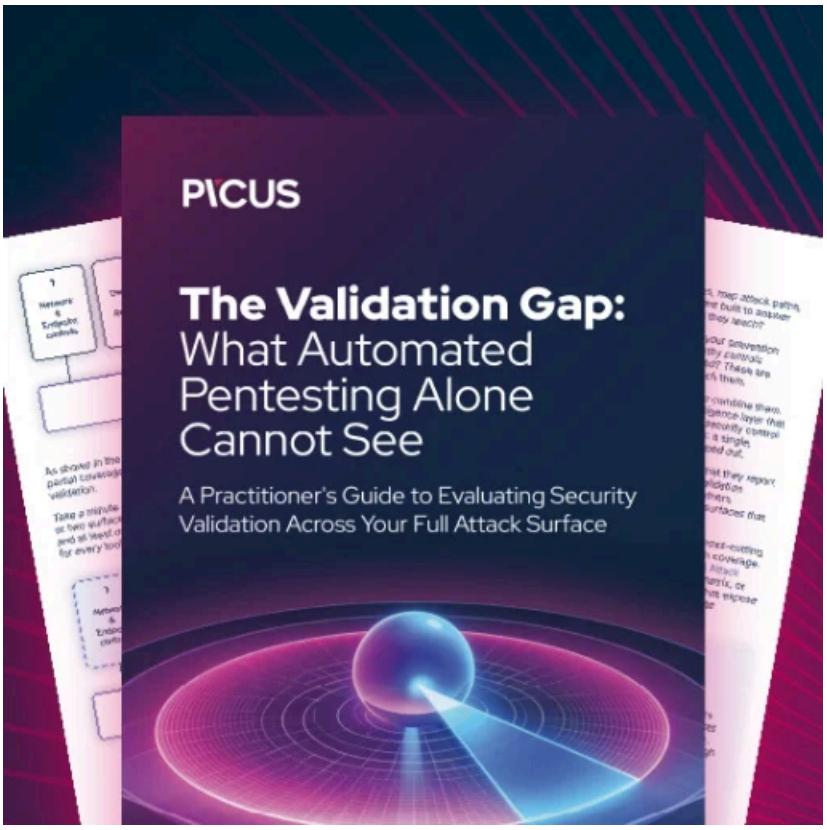
- Full Name,
- Date of Birth,
- Non-US National ID Number,
- Non-US Social Insurance Number or Fiscal Code,
- Passport Number,
- IP Address,

- Employer Identification Number (EIN),
- USCIS or Alien Registration Number,
- NHS (National Health Service) Number (UK),
- Medical Record/Health Insurance Information,
- Photograph, Gender/Gender Identity,
- Salary, Social Security Number (US),
- Financial Account Information,
- Payment Card Information,
- Account Username and Password,
- Biometric Information,
- Race/Ethnicity,
- Criminal Conviction or Offense,
- Sexual Orientation/Life,
- Religious Beliefs,
- Union Affiliation

"While there is no indication that any specific information was or will be misused, considering the nature of the incident and of the affected personal data, we cannot rule out that there may be attempts to carry out fraudulent activity." - Wabtec.

"For this reason, Wabtec encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their financial account statements and credit reports for any anomalies."

The company started sending notices of a data breach to all impacted individuals on December 30th, 2022, but the exact number of people affected by the incident remains undisclosed.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/rail-giant-wabtec-discloses-data-breach-after-lockbit-ransomware-attack/