Engineering firm Parker discloses data breach after ransomware attack

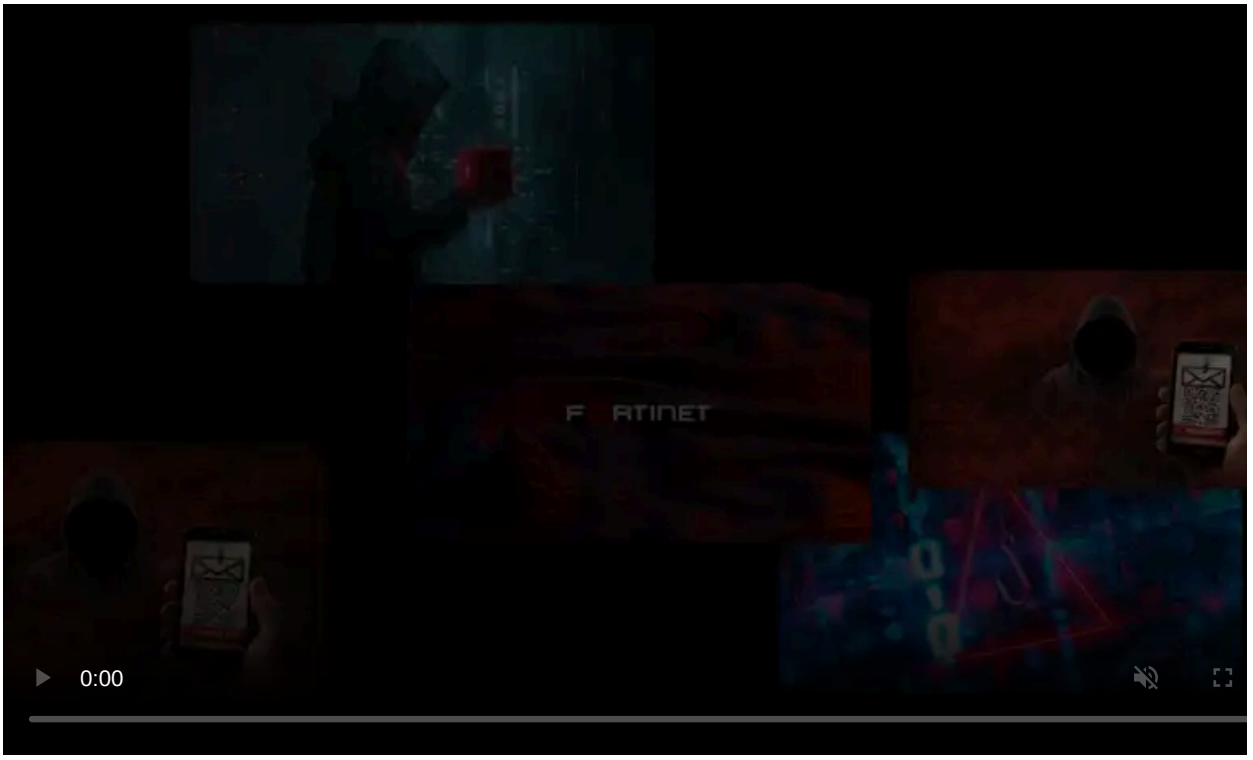
By Bill Toulas

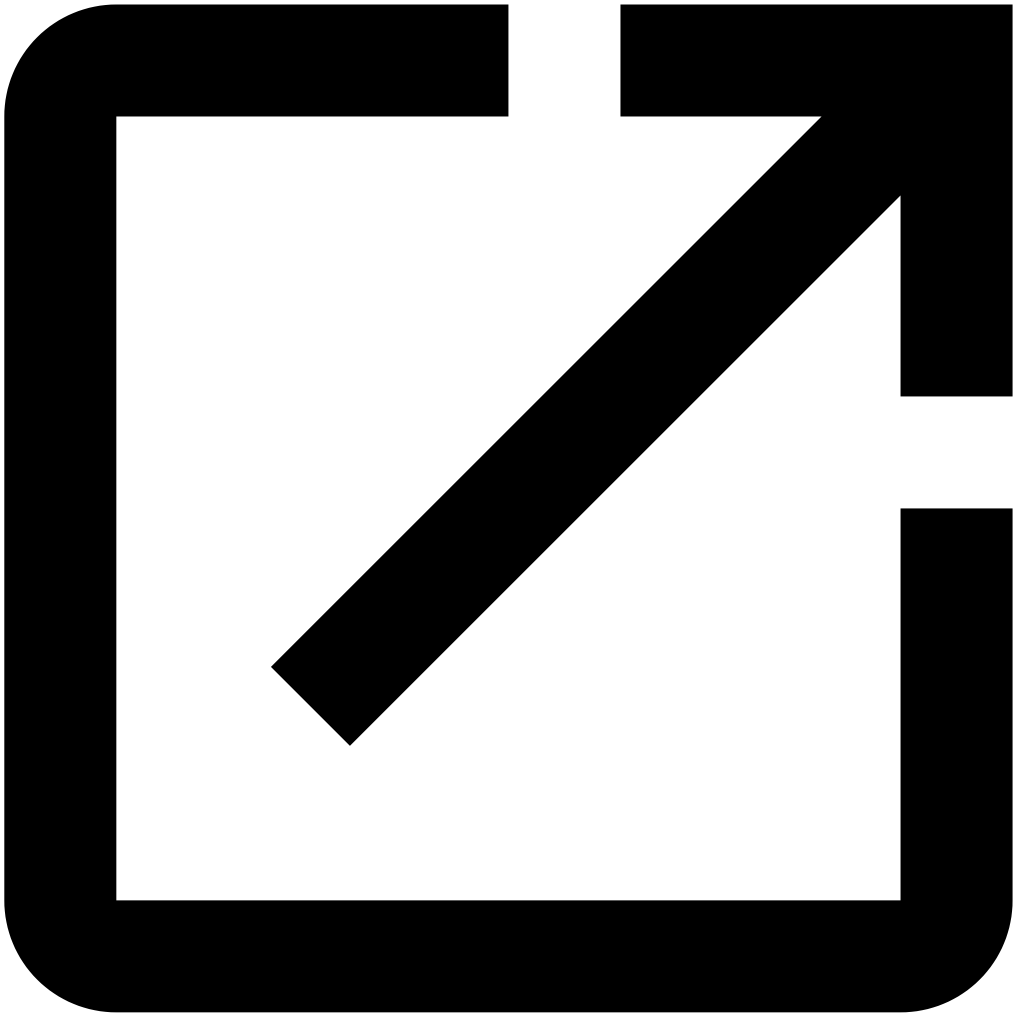
Published: 2022-05-16 · Archived: 2026-04-06 00:34:11 UTC

The Parker-Hannifin Corporation announced a data breach exposing employees' personal information after the Conti ransomware gang began publishing allegedly stolen data last month.

Parker is an Ohio-based corporation specializing in advanced motion and control technologies, with a strong focus in aerospace hydraulic equipment. It has a revenue of $15.6 billion and employs over 58,000 people.

Parker-Hannifin says a security incident occurred between March 11 and March 14, 2022, and that it involved a third party who gained unauthorized access to Parker's computer systems.


F RTINET
0:00



"Upon learning of this incident, Parker's IT team immediately activated its incident response protocols, which included shutting down certain systems," reads the firm's notice.

"Parker then launched an investigation with the assistance of a forensic investigation firm and other third-party cyber security and incident response professionals."

The subsequent investigation determined that threat actors had exfiltrated specific files from the firm's computers, so Parker immediately informed the law enforcement authorities of the data breach.

Employee data exposed

Upon reviewing the stolen files, Parker determined that stolen data included information related to current and former employees enrolled in Parker's Group Health Plans and their dependents.

The information that was compromised includes the following details:

- Full name
- Social Security Number (SSN)
- Date of birth
- Home address
- Driver's license number
- U.S. passport number
- Financial account information (bank account and routing numbers)
- Online account username and password
- Health insurance plan member ID number
- Health insurance dates of coverage

The exposed information includes dates of service, health provider info, claims data, and clinical treatment details for a small subset of employees.

The above details would make it possible for malicious actors to carry out phishing attacks, social engineering, or even identity theft and bank fraud.

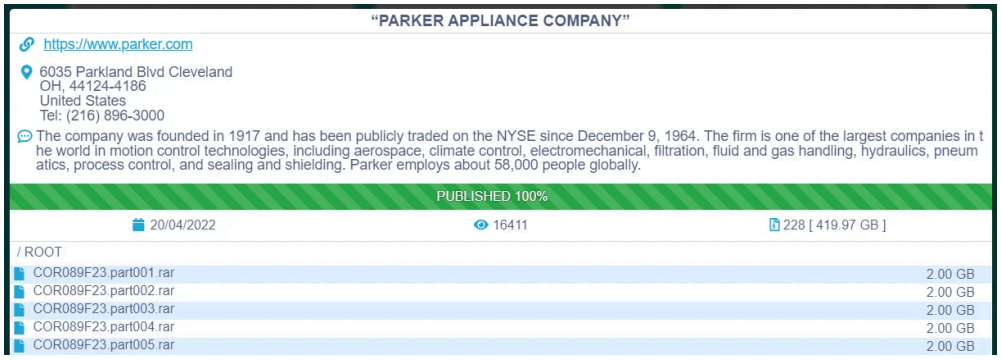
For this reason, Parker is also covering all impacted employees and beneficiaries with a two-year membership in identity protection services via Experian.

Considering that the incident impacts current and former employees, their dependents, and employees and beneficiaries of subsidiaries, the number of the affected individuals could be far more significant than the company's current workforce.

Conti claimed the attack

While Parker-Hannifin did not disclose who attacked them in April, the Conti ransomware group claimed responsibility on April 1, 2022, when the notorious gang published 3% of the data that they allegedly stole during their attack.

Full publication of the entire 419GB data set followed on April 20, which likely means that negotiations for the payment of a ransom had failed or never occurred.



Parker listing on Conti's extortion site *(Bleeping Computer)*

Parker-Hannifin designs and manufactures aerospace components, including hydraulic assemblies and fuel systems for Airbus, Boeing, Sikorsky, Rolls-Royce, Lockheed Martin, and the Commercial Aircraft Corporation of China.

As such, a data breach on the firm's systems might have compromised technical details and schematics that are worth a lot in engineering circles and could help competitors leap forward using stolen R&D.

At this time, we don't know if Conti accessed technical data or if the breach was limited to employee details, but similar data has been stolen in previous attacks.

Bleeping Computer has emailed Parker-Hannifin to determine the number of impacted individuals and clarify if technical data was also stolen in the incident, but a spokesperson of the firm declined to comment.
