UK Car Retailer Arnold Clark Hit by Ransomware

UK-based car retailer Arnold Clark is informing customers that their personal information may have been stolen as a result of a cyberattack. A ransomware group has taken credit for the attack, claiming to have obtained gigabytes of sensitive information.

Arnold Clark has more than 200 dealerships in England and Scotland, selling vehicles from over 25 manufacturers, and claiming to be the biggest car company of its kind in Europe. According to its Wikipedia page, the firm has 11,000 employees.

The company told customers that it was targeted in a cyberattack on December 23, 2022. An investigation revealed that the hackers may have obtained personal data such as names, contact details, dates of birth, vehicle information, passports or driver's licenses, national insurance numbers, and bank account details.

The investigation is ongoing, with Arnold Clark trying to determine the precise extent and nature of the compromised data, but impacted individuals are already being offered two years of free credit and web monitoring services through Experian.

The ransomware group named Play has taken credit for the attack on its Tor-based leak website.

The hackers have published a significant amount of information allegedly stolen from Arnold Clark and they claim more will be made public if the company refuses to pay up. Currently, they released 31 archive files of 500 Mb each, totaling roughly 15 Gb.

They claim to have stolen “private and personal data”, including passport and ID copies, confidential contracts, agreements, leasing contracts, and finance-related documents.

Arnold Clark targeted by Play ransomware

The Play ransomware (also known as PlayCrypt) emerged in June 2022 and it has been one of the most active ransomware operations. The cybercriminals are deploying file-encrypting malware and stealing data from victims in an effort to increase their chances of getting paid.

Play is best known for the recent attack on cloud company Rackspace. In that attack, the hackers used a new exploitation method for targeting Microsoft Exchange servers.

Related: Hacker Selling Data Allegedly Stolen From Volvo Cars Following Ransomware Attack

Related: Ransomware Group Threatens to Leak Data Stolen From Car Parts Giant Continental

UK Car Retailer Arnold Clark Hit by Ransomware