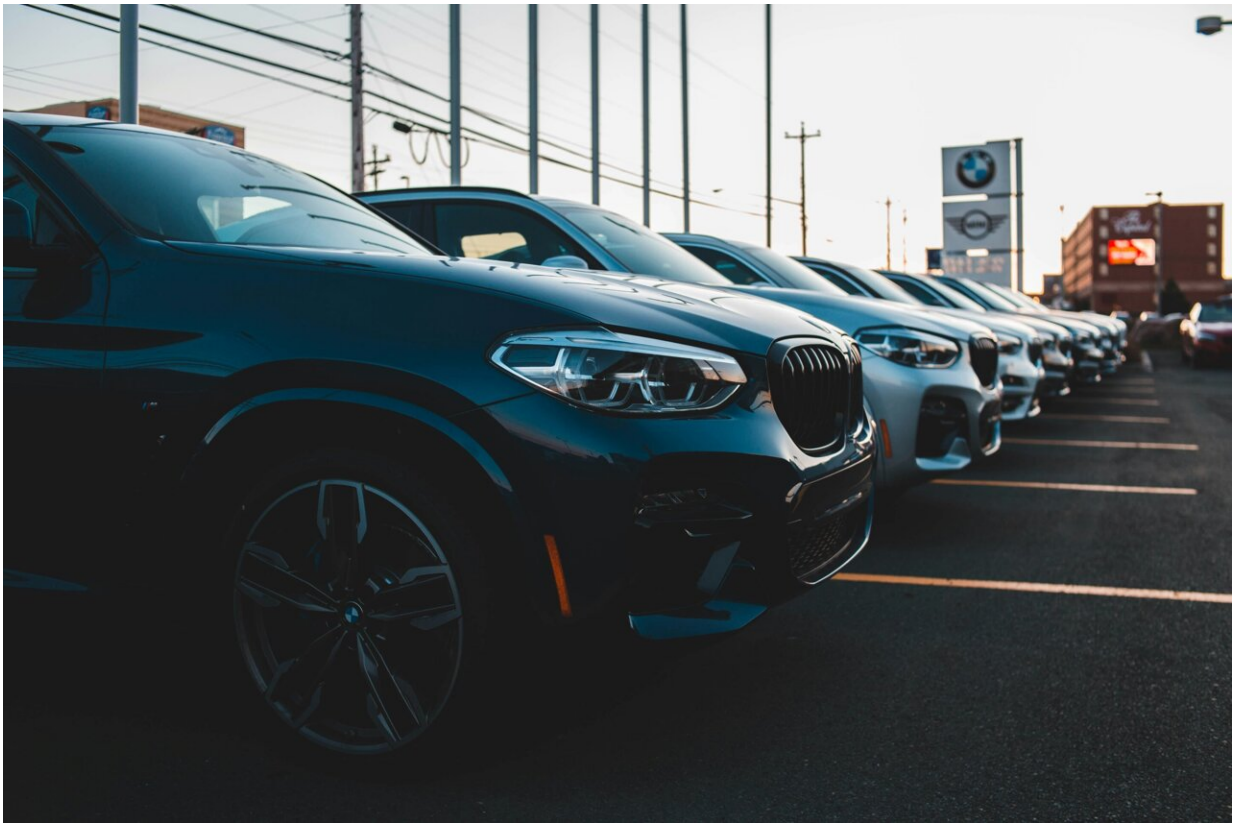
CDK hackers want millions in ransom to end car dealership outage

June 24 2024, by Craig Trudell, Bloomberg News



Credit: Unsplash/CC0 Public Domain

A group that claims to have hacked CDK Global, the software provider to thousands of car dealerships in North America, has demanded tens of millions of dollars in ransom, according to a person familiar with the

matter.

CDK is planning to make the payment, said the person, who asked not to be identified because the information is private. The hacking group behind the attack is believed to be based in eastern Europe, the person said. In the early days of any ransomware attack, discussions are fluid, and the situation could change.

CDK didn't respond to multiple requests for comment on June 21.

Since CDK discovered the breach and shut off systems on June 19, chaos has ensued at many of the roughly 15,000 car dealerships that it counts as clients. CDK's core product—a suite of software tools referred to as a dealership management system, or DMS—underpins virtually every element of auto retailers' day-to-day business. So the outage hampered sales, interrupted repairs and delayed deliveries across an industry that topped $1.2 trillion in U.S. sales last year. The disruptions also are hitting amid an end-of-quarter sales push.

"It's just mass chaos at this point," Diana Lee, the chief executive officer of Constellation, a marketing agency that works with auto dealerships across the U.S., said on Bloomberg Television. "The dealer's required to actually run a DMS for sales, service, parts, for every single functionality—even stocking a vehicle, you can't do it without the DMS system. So it is a disaster."

CDK had briefly restored some services for a few hours on June 19, but was forced to deactivate them following a second cyberattack. On Thursday, the company warned dealers that their systems likely will not be available for several days.

A demand in the tens of millions of dollars comes after hackers sought $50 million from a lab services company at the center of an ongoing

ransomware attack that's caused outages in London hospitals. UnitedHealth Group Inc., the largest medical insurer in the U.S., acknowledged earlier this year it paid hackers a $22 million extortion fee.

CDK hasn't said who or which entity is behind the intrusion, but it issued a warning to customers Thursday evening, saying that outside parties are reaching out to customers, attempting to capitalize on the confusion.

"We are aware that bad actors are contacting our customers, posing as members or affiliates of CDK, trying to obtain system access," the company said. "CDK associates are not contacting customers for access to their environment or systems. Please only respond to known CDK employees and communications."

There are only a handful of DMS companies for dealers to choose from after decades of consolidation within this corner of the car-retailing industry. As a result, thousands of stores are highly reliant on CDK's services to line up financing and insurance, manage inventory of vehicles and parts, and complete sales and repairs.

The car dealer Sonic Automotive Inc., which uses CDK to support critical dealership operations, said disruptions caused by the cyberattack are likely to have a "negative impact" on its operations until its systems have recovered, according to a Friday filing. Sonic hasn't determined if the attack will have a material impact on its finances, and it has reopened all of its dealerships with workaround solutions to limit disruption, the company said.

CDK's parent, Brookfield Business Partners LP, had its worst trading day since October—plunging 5.7% on Thursday—and extended its decline Friday. Shares in dealer groups AutoNation Inc., Group 1 Automotive Inc. and Sonic Automotive Inc. also slumped.