CDK Global outage caused by BlackSuit ransomware attack

By **Lawrence Abrams**

June 22, 2024 03:08 PM 6

The BlackSuit ransomware gang is behind CDK Global's massive IT outage and disruption to car dealerships across North America, according to multiple sources familiar with the matter.

The same sources, who provided information on condition of anonymity, told BleepingComputer that CDK is currently negotiating with the ransomware gang to receive a decryptor and not leak stolen data.

The negotiations come after the BlackSuit ransomware attack forced CDK to shut down its IT systems and data centers to prevent the attack's spread, including its car dealership platform. The company tried restoring services on Wednesday but suffered a second cybersecurity incident, causing it to shut down all IT systems again.

CDK is a software-as-a-service (SaaS) provider whose platform is used by car dealerships to run all aspects of its operation, including sales, financing, inventory, service, and back office functions.

As the platform is now shut down, car dealerships have had to switch to pen and paper to conduct their operations, with BleepingComputer told by car buyers that they could not purchase a car due to the outage or receive service for existing cars.

Two of the largest public car dealership companies, Penske Automotive Group and Sonic Automotive, disclosed yesterday that they, too, were impacted by the outages.

"Our Premier Truck Group business utilizes CDK's dealer management system which has been disrupted," Penske shared in an SEC filing.

"We immediately took precautionary containment steps to protect our systems and commenced an investigation of the incident, which efforts are ongoing. Premier Truck Group has implemented its business continuity response plans and continues to operate at all locations through manual or alternate processes developed to respond to such incidents."

"As a result, the Company experienced disruptions to its dealer management system ("DMS") hosted by CDK, which supports critical dealership operations including those supporting sales, inventory and accounting functions and its customer relationship management ("CRM") system," reported Sonic Automotive in an SEC filing.

"All of the Company's dealerships are open and operating utilizing workaround solutions to minimize the disruption caused by this CDK outage."

CDK also warns that threat actors are calling dealerships posing as CDK agents or affiliates to gain unauthorized systems access.

While BleepingComputer is the first to report that BlackSuit is behind the attack, the news that CDK is negotiating with threat actors was revealed by Bloomberg yesterday.

BleepingComputer contacted CDK to learn more about the ransomware attack but has not received a response yet.

The BlackSuit ransomware gang

BlackSuit launched in May 2023 and is believed to be a rebrand of the Royal ransomware operation.

Royal Ransomware, and thus BlackSuit, is believed to be the direct successor of the notorious Conti cybercrime syndicate, an organized cybercrime gang comprised of

Russian and Eastern European threat actors.

In June 2023, the Royal Ransomware operation began testing a new encryptor called BlackSuit amid rumors that they planned to rebrand under a new name after they attacked the City of Dallas, Texas.

Since then, attacks under the Royal name have disappeared, with the threat actors now working under the BlackSuit name.

In November 2023, the FBI and CISA revealed in a joint advisory that Royal and BlackSuit share similar tactics and coding overlaps in their encryptors.

The advisory also linked the Royal ransomware gang to attacks on at least 350 organizations worldwide since September 2022 and more than $275 million in ransom demands.

BLACKSUIT CDK GLOBAL CONTI CYBERATTACK RANSOMWARE

LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE NEXT ARTICLE

Comments

AMANNENC - 2 days ago

May the odds be always and ever in your favor... The games have begun!

Elastoer - 2 days ago

I guess these hackers can't think of anything constructive to do? I wonder how many of them still live in their mother's basements?

SDGOL - 1 day ago

At the ransom they are getting I doubt anyone is living in their parents basement.

bygrob - 1 day ago

Time for CDK to invest in zScaler and drop the VPN crap!

def1014 - 23 hours ago

Guessing HyperV and virtual disks got encrypted too. No snapshots?

bygrob - 21 hours ago

lol