www.wsj.com /articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6

Exclusive | Hackers Broke Into Change Healthcare’s Systems Days Before Cyberattack

James Rundle ⁝ 4-5 minutes

The hackers who attacked UnitedHealth Group’s Change Healthcare unit were in the company’s networks for more than a week before they launched a ransomware strike that has crippled vital parts of the U.S. healthcare system since February.

The attackers, who represented themselves as the ALPHV ransomware gang or one of its affiliates, gained entry into Change’s network on Feb. 12, a person familiar with the cyber investigation said. They used compromised credentials on an application that allows staff to remotely access systems, the person said.

Multifactor authentication protocols are typically used to guard against such breaches, including the use of text-message codes or access tokens keyed to individual users. MFA wasn’t enabled on this particular application, the person said.

The cyberattack on Change, which operates the largest U.S. clearinghouse for medical payments in the U.S., sent healthcare providers scrambling to find ways to bill insurers in the weeks and months following the Feb. 21 attack.

Change’s parent, insurer UnitedHealth Group, eventually paid a ransom to the attackers, the person said, declining to say how much, or if the company has paid a second ransom since another group of hackers began leaking data in recent days. Wired magazine reported on March 4 that UnitedHealth likely paid around $22 million in bitcoin to the attackers, citing darknet forum posts and analysis of the public blockchain.

Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change’s network, the person said. The length of time the attackers were in the network suggests they might have been able to steal significant amounts of data from Change’s systems.

Change processes around 15 billion transactions a year, and touches one in three medical records. It shut down more than 100 of its systems in the wake of the attack, and the effects of that outage have left many smaller providers reliant on loans and personal funds to stay afloat while they are unable to take in revenue. Some have contemplated closing.

UnitedHealth said last week the attack has so far cost it $870 million.

The company has been steadily restoring systems since March, including its pharmacy software, claims management and other platforms. It has also launched financial assistance programs, although some providers have complained of low amounts offered. Some providers have said they have been pressured by UnitedHealth staff to make positive public comments about the loans.

Lawmakers have raised questions about the cyber risks associated with a handful of healthcare companies holding dominant positions. The U.S. Department of Health and Human Services has also launched a probe into the potential compromise of sensitive patient information.

UnitedHealth said late Monday that an investigation and review of the data compromised by a recent cyberattack includes protected health or personally identifiable information.

The healthcare and insurance company said “a substantial proportion of people in America” could be affected by the incident, but that it hasn’t seen evidence of any removal of materials such as doctors’ charts or full medical histories among the data.

The company also warned it will most likely take months to identify and notify the customers and individuals affected.

“We know this attack has caused concern and been disruptive for consumers and providers, and we are committed to doing everything possible to help and provide support to anyone who may need it,” Chief Executive Andrew Witty said.

Witty is expected to testify about the incident before the House on May 1.

Sabela Ojea contributed to this article.

Write to James Rundle at james.rundle@wsj.com