Tech & Telecom Law News
Sept. 18, 2024, 1:48 PM EDT

Hackers Got Record Ransom of $75 Million for Cencora Breach (2)

By Katrina Manson

- Payment made through three Bitcoin installments in March
- Dark Angels hacking gang pursues high prices and low profile

Bloomberg Law News 2024-11-13T14:30:49752475388-05:00

Hackers Got Record Ransom of $75 Million for Cencora Breach (2)

By Katrina Manson2024-09-18T13:48:48742-04:00

- Payment made through three Bitcoin installments in March
- Dark Angels hacking gang pursues high prices and low profile

The hackers behind a cyberattack against the drug distributor Cencora Inc. received a total of $75 million, the largest known cyber extortion payment ever made, according to people familiar with the matter.

The payment made for the Cencora hack occurred in three installments in Bitcoin in March, according to people familiar with the matter who declined to be named in order to discuss sensitive details. The initial ransom demand was $150 million, according to two of the people. Cencora learned that data was stolen from its systems in February, according to a regulatory filing.

A representative for Cencora said the company doesn't comment on rumor or speculation. The representative added that the company stands by publicly available information, pointing to a July quarterly report that included expenses incurred by a cybersecurity event.

Shares of Cencora fell as much as 3.1% to a session low of $227.20 following Bloomberg's report on the ransom payment.

Cencora, a Conshohocken, Pennsylvania-based company, has a market capitalization of about $46 billion and generated $262 billion in revenue in the last fiscal year. It was formerly known as AmerisourceBergen.

Reports of a $75 million ransom first surfaced in July, when the cybersecurity firm Zscaler Inc. and the blockchain analytics company Chainalysis Inc. said the hacking gang Dark Angels received the massive payment, without identifying the victim. Bloomberg's reporting marks the first confirmation that the drug distributor was the victim of the hack.

Brett Callow, a managing director at FTI Consulting, an advisory services company with a large cybersecurity practice, said paying $75 million was previously “unthinkable.” The highest known cyber extortion before that was $40 million, paid in 2021 by insurance company CNA Financial Corp., Bloomberg reported that year.

“Lottery jackpot-level payouts like this make the health and medical sector a more attractive target than it already is,” Callow said. “We’re not talking about buy-a-Ferrari amounts here. It’s build-your-own-army amounts.”

Charles Carmakal, chief technology officer at Mandiant Consulting, Google’s cybersecurity unit that helps customers deal with cyber incidents, said the $75 million payout is on the top end of the spectrum he’s seen previously. He added that there have been payments higher than $40 million.

“It happens, but it’s not common,” he said.

Two months after disclosing the incident, Cencora started notifying individuals and state authorities that personal data including names, addresses, dates of birth, diagnoses, prescriptions and medications had been taken. The company’s July quarterly report says the majority of $31.4 million in “other” expenses, for the nine months ending June 30, were incurred as a result of a cybersecurity event in which data was exfiltrated. It’s not clear what that money covered related to the cyberattack.

Read More: CNA Financial Paid $40 Million in Ransom After March Cyberattack

Cybercriminals often demand money after major hacking incidents in which they deploy ransomware to lock up computer systems, steal sensitive data they threaten to reveal, or both.

Hospitals and health-care organizations have become a regular target for hacking gangs. In February, a cyberattack against Change Healthcare, a unit of insurer UnitedHealth Group Inc., roiled the country’s health-care systems and exposed patient medical data. UnitedHealth paid a $22 million ransom payment.

The $75 million extortion payment comes after years of efforts by the Biden administration to try to curb criminal hacking. For instance, the administration has been pushing some critical sectorsto meet minimum cybersecurity practices to make them harder to hack but has met with some resistance. The US Securities and Exchange Commission now requires public companies to report material cybersecurity incidents, while law enforcement has tried to disrupt hacking gangs’ efforts through indictments, sanctions and other methods.

Read More: White House to Push Cybersecurity Standards on Hospitals

The value of total ransom payouts is rising, according to Chainalysis. The median ransom payment made for the most severe ransomware strains stood at $1.5 million in June, up from just under $200,000 early last year, according to an August report from Chainalysis. The company predicts total ransom payments in 2024 will eclipse the record $1 billion it says was paid last year.

Paul Nakasone, a retired four-star army general who led the National Security Agency for nearly six years until February, said the US is failing to tackle ransomware. “We’re not making the progress that we need. In fact, we’re not even keeping up,” he told Bloomberg in an interview when asked about the high payout. He watched both the number of ransom hacks — and their damaging impact — grow during his tenure, he added.

Cencora told the SEC the incident will impact neither the company’s financial condition nor its operations in any material way. Cencora has said there is no evidence that any of the information stolen “has been or will be publicly disclosed.”

Paying ransoms cannot guarantee what a hacker will do with stolen data in the future, Callow said. “They certainly have no way of knowing whether the payment of a demand will result in the criminals deleting their copy of the data. It’s a bit like wiring money to a burglar in the hope he’ll return your belongings,” he said.

(Updates with stock movements in fourth paragraph.)

To contact the reporter on this story:
Katrina Manson in New York at kmanson4@bloomberg.net

To contact the editors responsible for this story:
Andrew Martin at amartin146@bloomberg.net

Lynn Doan