CYBERSAFE CASE STUDY **FINANCIAL INDUSTRY**

Ransomware Hits Major Financial Firm

A major financial institution with multiple offices across the country was hit by ransomware. The company reached out to Cybersafe, which helped it resume business operations.

FACTS OF THE CASE

TYPE OF ATTACK
Ransomware

TARGET
Major financial instutition

DEMAND
$2 million

THE BREACH

Just moments after the closing bell rang on a Friday afternoon at the New York Stock Exchange, a multi-million-dollar financial institution with hundreds of employees had all of its systems frozen and encrypted by a ransomware attack.

The ransom request was for more than $2 million to be paid in bitcoin. In return, the cybercriminals would decrypt the data. During the first few hours after the incident, our incident response team was able to determine very quickly which systems were infected. The team then identified the tools the attackers had used to laterally move and spread their malware across the company's network.

All of the victim's systems were encrypted, and the ransom request was for **more than $2 million** paid in bitcoin.

As soon as we began the investigation, our incident response team saw the creation of multiple administrative accounts. This allowed the bad actors to disable the existing security controls that were in place, including the company's antivirus software. Having turned off multiple-security controls, they were able to search and discover where the firm's back-up data was located and deleted it.

This was a sophisticated attack designed to prevent our client from recovering its data and resuming operations. The company had no other option: it paid the ransom to receive the decryption key to unlock its files.

OUR SOLUTION

Our incident response team rapidly deployed a software agent to every endpoint to investigate and determine the type of malware that had infiltrated the network.

This particular malware strain was designed to reinfect the system through the creation of a scheduled task. We found and removed the scheduled task. By early Monday morning, our incident response team had effectively eradicated the threat.

When the New York Stock Exchange opening bell rang on Monday morning, our client resumed operations as if nothing had happened.

ASSESSMENT & RESULTS

After completing the incident response engagement, we identified that these bad actors were in our client's network for more than two years, observing all the users' activities. They penetrated the network through a phishing email sent to the firm's administrative assistant.

The fast response to the ransomware was essential for our client to resume normal business operations.

If the business was unable to trade on Monday, it would have lost a significant amount of money.

Companies that invest in a 24/7/365 security operations center, SOC-as-a-Service, with detection, response, and containment capabilities will be better prepared to defend against future attacks.

CYBERSAFE SOLUTIONS®