Corporate Ransomware: 3 Infamous Incidents

They rarely, if ever, become public, but multimillion-dollar demands from organized hackers with colorful names are surprisingly common.

WHERE'S THE BEEF?

What was stolen:

REvil, one of the most notorious ransomware groups, took down the processing plants of a meat producer.

Ransom demanded:

$22.5 million

(in Bitcoin)

Resolution:

Following negotiations, the company agreed to pay an $11 million ransom, still one of the largest payouts ever.

GROUNDED

What was stolen:

In 2020, the Ragnar Locker ransomware gang infiltrated a global travel-services company, corrupting 30,000 computers and obtaining financial, security, and employee data.

Ransom demanded:

$10 million

(in Bitcoin)

Resolution:

Citing the impact of COVID-19 on its business, the company negotiated the payment down to $4.5 million.

OUT OF GAS

What was stolen:

In 2021, the DarkSide hacker group gained access to the network of a major oil and gas company, infecting billing, tracking, and other files, and forcing operations to shut down for two days.

Ransom demanded:

$5 million

(in Bitcoin)

Resolution:

The company ultimately paid $4.4 million.