CASE STUDY

Nonprofit reports cryptojacking event after noticing higher utility bills

INDUSTRY

Nonprofit

EMPLOYEES

251-1,000

COVERAGES

Service Fraud

After noticing the invoices for utilities seemed much higher than usual, a UK nonprofit realized they were the victims of cryptojacking. These events are often underreported because companies don't immediately realize their utility costs are rising until the damage has been done.

A threat actor spent nearly two months mining cryptocurrencies on the nonprofit's dime. By the time they contacted Coalition Claims[1] to report the event, the organization's internal IT team had already eliminated the threat actor from their environment and shut down the fraudulent activity.

Coalition Claims calculated the loss based on typical utility usage across multiple billing cycles. Because the event occurred at the nonprofit's subsidiary in Denver, CO, we had to decide whether it should be calculated in pounds or dollars. Ultimately, the loss amount was determined to be $48,084. After the nonprofit's self-insured retention of $25,000, they received nearly $24,000 under their Service Fraud coverage to cover the losses.

Coalition brings together active monitoring, incident response, and comprehensive cyber insurance designed to help mitigate your organization's cyber risk. To learn more, visit coalitioninc.com.

[1] The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.