CASE STUDY

Business interruption coverage mitigates downtime from repeated DDoS attacks

INDUSTRY
Specialty Retail

EMPLOYEES
1—25

COVERAGES
- Business interruption
- Breach response

A specialty toy retailer received an email threatening continued DDoS attacks unless they conceded to the attacker's demands. The policyholder had experienced once-daily attacks which took their store offline for four to five minutes at the time they received the email, which was passed from the customer support team to the CEO. The CEO reached out to Coalition, using our standard communication channel, approaching 9 p.m. California time. We responded within 20 minutes, and within an hour, we were on the phone with the CEO.

After a brief explanation, the CEO looped in the company's IT team which runs their custom e-commerce infrastructure. We started a multi-time zone call to dive in, combing through logs, reviewing DNS settings, and digging into firewall configurations. During the conversation, the company updated its security groups, proxied (protected) more traffic, and changed their server's public IP address. After some more back-and-forth, we uncovered a firewall rule put in place long ago which allowed all traffic from the United States through, regardless of other protections.

Once this rule was removed, all was well. The attackers returned in the following days, but their throttled attempts were not disruptive, and the attack activity stuck out like the proverbial sore thumb — easy to mitigate.

Business interruption is the key coverage in play. If a security failure such as a DDoS attack disrupts your business, you may qualify for lost income and expenses under your insurance policy. Unlike many other cyber insurers, Coalition's waiting period does not act as a deductible, just a trigger for the time period that a business interruption must satisfy prior to coverage being available. Several services qualify for Coalition's enhanced waiting period, which means less interruption (only one hour) before coverage kicks in.

Coalition brings together active monitoring, incident response, and comprehensive insurance to solve cyber risk. To learn more, visit coalitioninc.com/uk-cyber.

I spoke to the insured this morning regarding the renewal and he shared how satisfied he had been with his interaction with your staff in regards to the recent DDoS incident. He found your staff to be very knowledgeable and helpful.