CASE STUDY

# Active monitoring and forensic investigation uncovers a ransomware attack

**INDUSTRY**
Chemical Manufacturing

**EMPLOYEES**
251—1,000

**COVERAGES**
- Ransomware
- Breach response
- Digital asset restoration

Coalition's teams are agile; we skip the red tape and have people across across the globe who are ready to help around the clock. Our Claims and Security Incident Response teams respond immediately to keep our policyholders safe after an incident.

Early on a September morning at roughly 5 a.m., an IT professional at a large manufacturing company booted up their computer and logged in. They immediately noticed a series of mass file changes on their network — a clear sign of a ransomware attack. The policyholder contacted Coalition, and within 90 minutes, we were discussing the steps we needed to take next to diagnose the issue, eradicate the threat, remediate the systems, and get their business up and running again.

We deployed an endpoint detection and response (EDR) tool, Carbon Black, to collect and visualise comprehensive information about endpoint events to see how widespread the infection was. Next, we preserved all the data we could, changed all passwords, and got a copy of the ransomware note: a request for $2 million. The ransomware variant, known as Mount Locker, was fairly new at the time. Finally, we took a forensic image, including all files, folders, and unallocated space.

The attacker had likely utilised TrickBot, a modular banking trojan that acts as a dropper for other malware. This policyholder had a previous infection in 2018 with powerful ransomware that they didn't fully remediate. While combing through the system data, we noted a TrickBot banking trojan that appeared to be on a handful of systems from 2018. Thus, the connection to the bad actor was persistent and most likely aided the new Mount Locker infection.

We negotiated the ransom down from $2 million to $200,000. That's a difference of $1.8 million dollars — an amount that could cripple any business.

Ultimately, we worked tirelessly over five days to image various systems, move them to a new, clean network, give legal advice, provide security recommendations going forward, and work with counsel to negotiate the ransom. While they did end up paying the ransom, we negotiated it down from $2 million to $200,000. That's a difference of $1.8 million dollars — an amount that could cripple many businesses.

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