CYLANCE

CASE STUDY ENERGY

Bapco Takes on Cybersecurity

INDUSTRY

Oil Exploration
and Refining

ENVIRONMENT

- 1,900 endpoints protected by CylancePROTECT,® including Windows desktops and servers

CHALLENGES

- A recent ransomware attack bypassed antivirus (AV) security controls
- A system-wide cleanup required additional expertise and headcount

SOLUTION

- Deploy CylancePROTECT endpoint security to protect against ransomware and zero-day threats
- Utilize a Cylance Compromise Assessment to conclusively determine if the network has been compromised
- Retain ThreatZERO™ services to optimize and operationalize CylancePROTECT

Bapco

The Company

Wholly owned by the Government of Bahrain, Bahrain Petroleum Company, or Bapco, is primarily engaged with oil exploration, refining, storage, production, marketing, training and development, and environmental initiatives in the kingdom. The company owns a 264,000 barrel-a-day refinery, storage facilities for more than 14 million barrels, and a marine terminal for its petroleum products. 95% of the company's refined products are exported. Bapco's primary customers for crude oil and refined products are based in the Middle East, India, the Far East, South East Asia, and Africa. Bapco is the largest contributor to the Bahrain economy.

The Situation

Kevin Lovegrove leads Bapco's security organization known as the Computer Security Management and Response Team or CSMART. Made up of staff from all disciplines across IT security, the team is responsible for strategy, policies, and procedures. Members include security admins, application developers, a network team, infrastructure, industrial computing, governance, and help desk support.

1,900
ENDPOINTS
PROTECTED

700
PIECES OF
MALWARE
REMEDIATED

Bapco ramped up its security defenses after the Saudi Aramco breach. Today, CSMART oversees a comprehensive security program that uses the CIS Critical Security Controls Version 6.1 as a model for IT security, and requires SANS security awareness training for employees. “We wanted to put in place a security strategy that goes beyond incident response,” Kevin told Cylance®.

Nevertheless, the company recently sustained a ransomware attack launched via email that bypassed its AV security controls. According to Kevin, “Quite a few people opened the attachment, and it caused a rash of alerts.” The malware required a callback to get the payload. Fortunately, it was caught in a sandbox, and unable to execute. CSMART immediately shut down the network and cleaned out the Microsoft Exchange folders. “After that attack, we determined signature-based AV wasn’t going to do it — not on its own. We need something more sophisticated for the endpoint.”

The Process

During a security seminar Kevin attended in Dubai, presented by a former CISO of the CIA, someone posed the question, “What do you recommend for AV?” The former CISO recommended two vendors, including Cylance.

Kevin reached out to both vendors. What ultimately convinced him to go with Cylance was the explanation of how Cylance works and the scope of activity it detects. “At the end of the day, malware — even the most sophisticated malware — is all somewhat similar. We want to know that our endpoint security has covered the bases for all these behaviors. Cylance is as good as it gets.”

Due to Bapco’s ransomware attack, Cylance began the engagement with a Compromise Assessment. The assessment allowed Bapco to determine if the environment had been the victim of a security breach, if sensitive data had been exfiltrated, and whether credentials had been stolen or misused. Using dissolvable scripts, consultants were able to collect data for analysis by Cylance, while avoiding detection by the attacker.

The Results

The Cylance assessment uncovered over 700 pieces of malware and 1,000 potentially unwanted programs (PUPs). Consultants then deployed CylancePROTECT with ThreatZERO Services to remediate the threats. The ThreatZERO consultants helped optimize and operationalize CylancePROTECT, including handling all their malware and PUPs, moving the environment into full auto-quarantine mode, fully enabling script and application control, and addressing memory protection blocking exclusions. ThreatZERO enabled Bapco to achieve a state of prevention from further attacks in just four weeks. Throughout the process, Bapco’s team was educated on best practices. Kevin said, “We dumped it on the ThreatZERO team and let them sort it out, and that is what happened.”

According to Kevin, “ThreatZERO found some intriguing connections that were likely legitimate between employees and certain countries that would normally raise suspicion — perhaps someone just calling their mom. Going forward, we want to make sure there aren’t communications to other places that we should be concerned about.”

CSMART is rolling out new network equipment and anticipates finding additional endpoints that do not have Cylance. Those endpoints will require cleanup. Kevin said, “No computers are allowed to connect to the network unless they have CylancePROTECT installed first.”

Kevin added, “We asked Cylance to take the lead. They provided a low impact, fast, and easy implementation. CylancePROTECT gives us peace of mind — it is there to stop malware on the desktop. If it finds malware, it blocks it. We’ve had no issues since it was installed, and because it is cloud-based, CylancePROTECT saves us from doing updates.”

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™