Success Stories

Preventing a Targeted Cyber
Ransomware Attack

Challenge

A financial services company was the target of a ransomware attack via phishing email. The employee thought it was coming from an authentic source and opened a malicious link. When the link was opened, a download of ransomware was attempted.

Approach

Quess GTS prevented malicious files from being downloaded due to the proactive actions of our Security Operation Center (SOC). By fine tuning CylancePROTECT®, part of our Quess Guard Cyber solutions, the tool was able to identify the malicious code and stop the attack. The Quess GTS solution did this by preventing java script from installing malicious files after detecting fileless malware. The file was locked, the malicious process was stopped, and then it was investigated through Quess GTS's SOC. They were able to take the data from the prevented attack to hunt for identical threats using CylanceOPTICS®.

Using the CylancePROTECT® component, we identified that the ransomware file could have cost the firm tens of thousands of dollars in ransomware payments through bitcoin and lost revenue from reputational risk. Our NEXTGEN antivirus looks at the behavior of files and the agents on each endpoint and makes the final decision on level of risk.

Benefits

Quess GTS did not have to remediate anything because the Artificial Intelligence (AI) was programmed proactively by the security team to react instantly to these types of threats 24/7. Before the file executes, the CylancePROTECT® agent determines if the file is safe. Because this was a Managed Services customer, our SOC team monitors these incidents. Our Quess Guard Cyber suite is part of our offering. As a BlackBerry managed security services provider (MSSP) partner, their CylancePROTECT® and CylanceOPTICS® components are among the solutions deployed by Quess GTS to clients, either as individual managed services or integrated into a SOC-as-a-service offering.

Our customer benefited from the investment in managed services and the real threat of ransomware, phishing, and other intrusion attempts. The ROI on this investment is compelling on that one incident alone. These attempts are mitigated daily at various levels of sophistication.