CASE STUDY

A MALAYSIAN DEBT RECOVERY OPERATIONS COMPANY PROTECTED FROM PITOU RANSOMWARE

COMPANY BACKGROUND

Queby Recovery Management Sdn Bhd ("**Queby**") is a Kuala Lumpur, Malaysian based enterprise that operates in the credit intermediation financial services industry. Queby provides services to major institutions including RHB Bank, Maybank and other financial institutions. Its' daily operation involves handling and processing large volume of highly confidential data for both corporates and consumers.

"It is really amazing to witness how Invisiron had saved the company from the hackers' ransomware. I can't image how severe the consequences could have been should the threats had gotten their way into our network. This proactive automated solution not only protected my entire network, it has certainly boosted up our confidence in protecting our customers' confidential data."

Dato Sri Dr LS Kalaiselvam, Executive Director, Queby

BUSINESS IMPACT

Invisiron allows Queby to implement a productive and effective cyber defence solution without the need of an in-house cyber security team.

Queby has seen significant benefits from safeguarding its network from critical cyber threats for example Pitou ransomware on a daily basis.

THE CHALLENGE

Strict cybersecurity compliance to the Banking and Financial Institutions Act 1989 and the Personal Data Protection Act 2010 is a mandate in Malaysia. Hence, it is imperative for financial institutions to incorporate a robust cyber security platform, capable of safeguarding against any potential data exfiltration that may lead to significant reputation and monetary loss.

Being a medium sized enterprise, the cost to have an in-house cybersecurity team is not justifiable. Furthermore, there is a huge shortage of cyber security talent in the country. Queby required a modern, automated cyber defense technology that can proactively detect and mitigate threats automatically round the clock.

THE SOLUTION

Taking Cyber Defense to the next level at affordable costs

After an extensive search in finding the right solution, the management chose to deploy the Invisiron solution at its main office to protect it's main network. Upon deployment, Invisiron proactively monitored Queby's network 24/7 and leveraged on its updated cyber threat intelligence feeds to inspect and mitigate any malicious packets that go in and out of the network, with full activity logs provided to the IT team. This proactive cyber defense solution provided by Invisiron allowed Queby's IT team to better focus on other day to day IT related tasks.

THE RESULT

Protected from malicious ransomware

In one incident, a 3rd party software was used to do a version update on one of the employee's computer connected to Queby's network, resulting in the computer getting infected with Pitou ransomware.

The ransomware's external host tried various attempts to establish communications with the infected computer and was detected and identified by the Invisiron Cyber Defense as a critical event.

Upon detection of the Pitou ransomware attempts to communicate with its external host, Invisiron successfully blocked the malicious traffic from the infected computer and automatically notified the system administrators on these critical events through the Invisiron alert system. The user was immediately informed, and timely actions were taken to remove the infected computer from Queby's network.

This event has demonstrated Invisiron's capability to detect and mitigate cyber threats, protecting users from incurring potential hefty damages resulting from ransomware or other malicious attacks.