CUSTOMER STORY

FireEye Secures Thailand's Largest Shipyard from Data Breaches

Unithai Shipyard and Engineering Limited is critical to the country's supply chain operations

FACTS AT A GLANCE

INDUSTRY

Transportation

CUSTOMER PROFILE

Located in the deep-sea port of Laem Chabang on the eastern seaboard of the Gulf of Thailand, the largest shipyard in Thailand — a 688,000 square meter facility — is owned and operated by Unithai Shipyard and Engineering Limited (Unithai). Incorporated in 1990, the company is at the heart of Thailand's chemical and oil tanker, container, dry bulk, car and offshore trade. It provides a wide range of services, including ship building, repair, modification and conversion; oil and gas platforms; and heavy engineering fabrication for power plants.

Business challenge

As a key element in the country's distribution and logistics operations, Unithai is an obvious target for malware and cyber attacks. Teams of engineers and draftsmen create and store data — such as detailed design, shop and "as-built" CAD drawings — to enable them to provide efficient ship repair, conversion and new building activities.

Nuttasit Wongprecha, MIS Manager for Unithai Shipyard and Engineering Limited and the Unithai Group of Companies, projected, "The impact of a breach could be huge: Lost intellectual property, hijacked customer information, destruction of our brand reputation but worse still, it would severely impact the entire Thai logistic and warehouse supply chain."

> "The heightened level of defense along with the labor and cost savings from not having to deal with a breach, makes FireEye a mission-critical partner in our security portfolio."
>
> — **Nuttasit Wongprecha**, MIS Manager, Unithai Shipyard and Engineering Ltd. and the Unithai Group of Companies

Unithai had traditionally relied on standard malware protection from firewalls, antivirus software, and the use of proxy servers but the escalating levels of zero-day and advanced persistent threats, as well as news of shipyards elsewhere in the world being crippled by such attacks made Wongprecha and his staff look for additional protection. He commented, "We kept hearing about cyber threats directed towards companies with many similarities to Unithai, including attacks on power plant control systems and a shipbuilding operation in Poland. It became imperative to maximize protection and mitigate any potential risks to our customers."

Solution

The company chose to do a proof of value with the FireEye® Network Threat Prevention Platform, using it in parallel with traffic from the production environment to evaluate the state of the infrastructure and determine its ability to catch malware that the existing security defenses missed. The test revealed that undetected threats already resided within Unithai's network, and Wongprecha recommended the immediate purchase of the FireEye solution because of this compelling demonstration, and its broad functionality and ease-of-use.

Deployment proved to be very straightforward, taking just half a day for preparation followed by a 15 minute cut-over exercise where the FireEye Network Threat Prevention Platform was configured inline to enable instantaneous blocking of malware. Wongprecha's staff then received four hours of on-the-job training.

Wongprecha observed, "FireEye has really shown the difference between traditional defenses and the next-generation, signature-less security solutions. With the expertise and the in-depth knowledge of advanced malware delivered by FireEye, we are able to understand more about these attacks and can better prepare ourselves for the battles against those threats in the future."

Business benefits

Wongprecha observed, "The FireEye Network Threat Prevention Platform has become an excellent source of intelligence about zero-day attacks and has enabled us to proactively issue quarterly threat reports to our own customers to keep them better informed and protected.

"Receiving information about the number, type, and severity of the malware caught; the number of incidents prevented; the identification of attackers; and the data theft that's been prevented, makes us feel so much better about the level of protection we now have in place for our customers' information. The heightened level of defense along with the labor and cost savings from not having to deal with a breach, makes FireEye a mission-critical partner in our security portfolio."

Wongprecha reflected, "The only truly secure system is the one that is not powered on — everything else needs help! FireEye allows us to continually harden our defenses."

Vision

"FireEye helped us realize our existing security infrastructure was not enough to protect us from modern malware," summarized Wongprecha. "When you consider the lifecycle of an attack and ways that FireEye identifies the initial exploit, discovers callback communication, detects or prevents the dropping of additional attacker utilities, thwarts data theft, and prevents a repeat attack, we wouldn't consider being without it today!"

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®