Notpetya ransomware attack on Maersk - key learnings

The shipping sector has traditionally stood apart from the developments in cybersecurity over the past decade. With the majority of critical functions and assets physically isolated by miles of ocean, the need to secure these resources against cyber threats has seemed similarly remote.

However, in recent years, this hands-off approach to cybersecurity and assurance has become riskier and ultimately, costlier. In the modern cyber threat landscape, less capable adversaries such as hacktivists and teenage virus writers take a back seat to organised criminals and even nation state-sponsored threat actors. The cyber-crime economy is now mature, well-established, and well-developed.

Below we will take a look at the key learnings for ship owners and operators which can be taken from previous research and attacks, most notably the NotPetya attack in 2017 which caused major implications for global shipping giant Maersk.

What was the NotPetya ransomware attack?

NotPetya is a type of ransomware that surfaced in 2017, in which it rapidly made global news and caused a major outage for global shipping giant Maersk. The untargeted infection of 'ransomware' impacted the majority of their key systems, disrupting every function critical to the organisation's survival.

How does a ransomware attack work?

Ransomware is a form of 'malware', maliciously-created computer software designed to stealthily infiltrate PCs, mobile devices, and even Industrial Control Systems. The variant known as 'NotPetya' represented a particularly aggressive and damaging strain of ransomware, utilising highly advanced infiltration and lateral movement techniques to infect systems and gain persistence in a target's network once that access is established.

Once the malicious programme has control of the device, it locks down access to the device and its functionality before demanding payment in the form of cryptocurrency, the untraceable digital currency upon which the black-market economy now runs.

The impact of the NotPetya attack

- Estimated Financial Impact: 300 million USD
- Infected Systems: 45,000 PCs and 4,000 servers
- Affected Facilities: 76 global port terminals shut down

The response to the NotPetya Attack

Maersk's response to this crisis was admirable, rapidly switching from an IT-enabled process model to a manual, paper-driven model to bypass disabled systems. This approach enabled the organisation to restore an estimated 80% of critical functionality and throughput while systems were intensively cleared and restored to their working state.

Two days after the attack, Maersk Line was able to accept bookings from customers with existing accounts and 6-12 days after Maersk Line, Damco and APM Terminals gradually progressed to more normalised operations, during which Maersk's internal technical staff and resources were tested to the limit.

Jim Hagemann, Chairman of Maersk commented:

"We were basically average when it came to cybersecurity, like many companies. This was a wake-up call not just to become good, but to have cybersecurity as a competitive advantage."

The source of Maersk's troubles has been attributed to cyber-warfare in the region of Ukraine, likely backscatter from the ongoing conflict there between Russia, Ukraine, and NATO interests. The infection of NotPetya was traced back to a local accounting software package, which rapidly spread globally through Maersk's interconnected infrastructure.

What can we learn from Maersk?

What we can learn from Maersk's ordeal is that shipping interests are caught in the crossfire between nation-states, organised criminals and their economic targets. Even if not directly targeted themselves, shipping company assets can rapidly fall victim to enhanced cyber-weaponry that is being developed at an accelerating pace.

It is a fair assessment that incidents like that suffered by Maersk can be vastly mitigated in their ultimate cost and level of disruption, with proper forward-thinking and forward-planning. Cyber response planning, assurance testing and accurate threat intelligence are the cornerstones of an effective risk mitigation strategy, and as the rate of global cyber incidents continues to rise, we will begin to see a stark separation between those businesses prepared for cyber incidents and those which are not.

What platforms need to be protected?

The global shipping demand continues to increase year on year. If you are a shipowner, manager or charterer how do you determine if an older, proven, established ship is more or less secure than a modern, connected and potentially more automated vessel? The answer is not as obvious as it may seem. Older ships may have more dated equipment, less securely designed networks and almost certainly unpatched and/ or unsupported software and components.

Platforms for consideration

- **Modern ships -** Modern ships will be more connected have a more diverse set of components, and a more varied and complex supply chain. This means increased complexity around system integration and interfaces. This requires more knowledge and expertise in assurance and verification. More modern ships often require fewer people to manage and oversee as automation plays a higher role.

- **Older Ships -** From a cybersecurity perspective, older ships are far more likely to contain security vulnerabilities than those constructed in a post-cybersecurity technical environment. A shipping vessel presents a very tempting attack surface to a potential threat actor, and critical functions like Industrial Control Systems, automated navigation and onboard inventory and bay management software are frequently overlooked as potential attack vectors. So, an older ship may have more vulnerabilities and weaknesses, but the likelihood of a cyber-attack would be potentially less as the opportunity and ability to exploit these vulnerabilities is more limited.
- **Supply Chains -** Supply chains are an increasing challenge as the importance of developing appropriate Type Approvals and enforcing these on the increasing complexity of manufacturers, IoT devices, sensors and automation technology in use can be hard.
- **Big Data -** Ships are a wealth of data points that are increasingly being used to manage the functions, navigation, positioning, logistics, cargo and safety of vessels. Ports and shore-based operations increasingly rely on communication systems to keep processes running smoothly, and any IT glitches can create major disruptions for complex logistic supply chains.

The bottom line

The future needs us all to have clear visibility into the cyber threat surface presented by ships, builders, supply chains and operational managed services, both to comply with regulatory requirements to manage cyber risks and to minimise the risk of business interruption.

To find out more about the strategic steps to take toward cyber assurance, please see our full research report on the topic.