MARITIME CYBERSECURITY'S CHOPPY WATERS

Adam Brown, Manager, Security Solutions,
Synopsys, London, UK

The nefarious hacker has been around for a long time, despite popular culture painting a picture of the hacker as a uniquely modern phenomenon.

In 1903, the first possible instance of a hack took place during Alexander Fleming's demonstration of his boss Guglielmo Marconi's technological wonder of the age: a long-range secure wireless communication system, resulting in the display being disrupted at the Royal Institute in London.

Just prior to the demonstration, the Morse code receiver started spitting out insulting messages, initially repeating the word "rats" and then a limerick - "There was a young fellow of Italy, who diddled the public quite prettily", which places this hack as more mischievous than malicious – but a hack all the same.

Whilst these days we imagine a hacker as a hooded individual who wears a Guy Fawkes mask and is hunched over a computer, the perpetrator in this case was a mustachioed music hall magician called Nevil Maskelyne.

We know this thanks to a triumphant confession letter he sent to The Times newspaper.

LESSONS FROM THE PAST

But what does all this have to do with the security of shipping? Well, there are parallels that are important to consider.

Although Marconi was using a specific frequency to transmit and receive messages, his hacker breached, with relative ease, what was supposedly a secure channel.

In 1903, the technology was new, so no one had thought to probe its security, but there was no reason to, and this mistake may be the same one the maritime industry is making by using overshared networks and insecure devices visible on the public internet for its intercommunications.

Industries can also be tiered; financial services tend to lead (they have always been an obvious target, and therefore need to be at the top of their game when it comes to protection), followed by software vendors and cloud providers, then by healthcare.

Each vertical has its own specific motivation for advancement based on the unique threat situation.

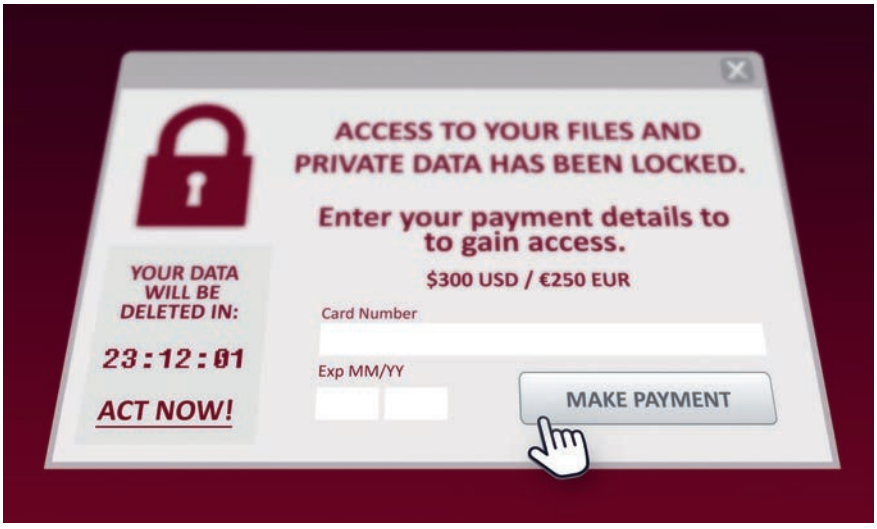
Synopsys has identified many clear trends after running a study of software security initiatives (SSIs) for more than a decade.

So far, we have not seen any maritime SSIs that would indicate a lag in cyber maturity, but the last year has shown us that exploits were relatively easy to deploy — a stark contrast to the cyber-defence-embracing financial service companies who pre-empt breaches even though there is a much larger attack surface.

The associated supply chain issues that arise from a major cyberattack on a

container shipping company, the cogs in an economic machine that transports food and commodities worldwide, threatens the security of the businesses who rely on the goods being shipped.

This is without even considering the potential issues associated with compromising the ships themselves, as the nature of internet-connected shipping today means that a cybersecurity incident at sea could lead to loss of life.



VICTIMS

A real-world shipping industry breach at the end of July came in the form of a ransomware attack on the US network of global shipping giant COSCO (China Ocean Shipping Company), resulting in it being unable to use local email and network telephone.

This comes just a year after the NotPetya ransomware attack on the world's largest shipping company, Maersk, which cost the ocean carrier up to nearly $400 million in operational downtime and disruption after the attack infected its systems as it spread from Ukrainian utilities to major international companies across the world.

However, Maersk's significant financial losses are a drop in the ocean when it comes to the damaging factors that could play out in future attacks.

VULNERABILITIES

Due to cybersecurity issues relating to network configuration, security configuration (default and hardcoded passwords), and application security vulnerabilities, it is possible to use hacking to misdirect or control a ship through these systems:

- Satellite communications data or devices with network vulnerabilities due to public internet connection weaknesses and issues regarding physical security
- Electronic Chart Display and Information Systems (ECDISs) with underlying old and insecure operating systems
- Serial communications/IP convertors that control the ships industrial control systems.

Financial crimes or disruption to logistics can also happen by United Nations/Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) tampering.

EDIFACT has some security measures in place, but an easy bypass could lead to stolen cargo or the mishandling of cargo, which could affect ballast or result in dangerous hazardous cargo situations.

Who would do such a thing? Marconi had a situation where someone wanted to defame him and his machine by hijacking the demonstration, and each industry has its own unique threats and threat actors with their own motivations.

HAPPY HACKING

Recently, I found myself talking to an activist who was proud of his disruptive activities, which had caused delays and resulted in additional port fees and breaches of service levels.

He did this by locating vessels that had turned off their automatic identification system (AIS); not by using highly skilled hacking techniques, but by using some easily obtainable open source intelligence by way of the crew beaming out location data via GPS on social media updates from their phones. Each industry and sub-industry has its own unique threat actors, however, while the threats are different, the techniques are the same.

CLOSING THE BACKDOOR

The shipping industry can learn from the last two decades of security experience from other industries and apply mitigation techniques, whether that is process, people, training or technology.

Those responsible for the cybersecurity of ships should pay attention to the practices already established, and identify threats through threat modelling, assessment of risk exposure and then mitigation, but there are no silver bullets; any vendor-supplied security needs independent checks.

Avoid becoming a victim, as Marconi did, and always assume a system has weak points.

The BIMCO guidelines on cybersecurity for ships has emerged as a great reference for the industry, however, it must be used as advice and not a checklist, as this simply doesn't work.

Vendors of devices for ship control, navigation and communication should consider a software security initiative – a good measurement tool for such a thing is the free document at BSIMM.com.

Finally, a last parallel is that Marconi's hacker was self-proclaimed.

As with many breaches today, the breached organisation only becomes aware through outside notification.

Would you know if there was a breach of confidentiality, integrity or availability of sensitive data or control messages on your ship?

ABOUT THE AUTHOR

Adam Brown is a security solutions manager at Synopsys. He has over 20 years' experience working directly with customers, helping them to resolve application challenges they're seeing within their business. Starting as a consultant, automating repeatable quality tests, Adam moved into application performance to ensure applications can withstand spikes in demand. Today, he helps enterprises evaluate the security and quality of the software and technology they build and buy.

ABOUT THE ORGANIZATION

Synopsys helps development teams build secure, high-quality software, minimising risks while maximizing speed and productivity.

ENQUIRIES

Synopsys Northern Europe Ltd.
6th Floor
3 Harbour Exchange Square
London E14 9GE
United Kingdom
Tel: +44-207-510-9020