Preventing the ghost in the machine

By JIM WILSON

It was a relatively newly-built ship. It had a power management system that could be connected to the internet for software updates.

And it was riddled with malicious software.

The system was thoroughly compromised with a "worm", which is computer jargon for self-replicating malicious software ('malware').

It could create its own files. It could create its own folders. It was actively trying to connect to the internet.

Why? It was trying to communicate with a "command and control" computer somewhere in the world so that it could get its next set of instructions.

The only reason it did not actually connect to the internet was because it actually could not connect to the internet – that facility had been disabled by design.

The ship operator's IT department decided one day to visit the ship to test for vulnerabilities and to find out if it was safe to connect the power management system to the internet.

That's when they found the worm.

Malicious actors

In the literature, there are several different categories of malicious actor, all of which pose a grave threat given that they could compromise safety of life at sea, the preservation of the marine environment and the protection of valuable property.

Firstly, there's the disgruntled or rogue employee who wants to get revenge or otherwise cause trouble for the employer or its suppliers/customers.

Then there's the hacker for fun-and-glory, who is doing it for the amusement and the test of their abilities. Dangerous though they are, there are worse malicious actors lurking in cyber and physical-space.

Another threat is from government intelligence agents or government-sponsored hackers. Knowledgeable and well-resourced, they seek to infiltrate systems, gather data and intelligence, and potentially render assets vulnerable to attack at a later date.

Criminal gangs also pose a threat. They seek to infiltrate systems and collect data, but they have the aim of collecting money through some kind of extortion. They could, for instance, seek to lock-up data or prevent the operation of assets, pending payment.

Finally, there are those who seek to advance their political cause, whatever that may be. These could be a so-called "hacktivist" (a portmanteau of the words "hacker" and "activist") or, worse, they could be terrorists.

Back to the ship and its dormant worm

It was discovered that the worm had been installed into the power management service by a portable USB-connecting device that had been used during a software installation. A cyber-security firm discovered that the worm had compromised all servers associated with the system, and that the dormant-worm had been in the system for 875 days.

Further details of this incident have not been provided in the document "Guidelines on cyber security onboard ships", which has been jointly provided by industry bodies BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and the World Shipping Council.

Caring for our **Clients** and their **Cargo**

When you combine Newcastle's hugely diverse range of facilities with our levels of service, competence and experience, we believe you will find a genuinely competitive option for all your imports and exports through the Eastern Sea Board.

130 Young Street, Carrington NSW 2294 I PO BOX 190, CARRINGTON NSW 2294
Ph Main: +61 2 4978 7100 I Mobile: +61 412 680 001 I Email: geoff@newcastlestevedores.com.au

A chilling incident

The dormant-worm incident is chilling for a host of reasons. Only two decisions prevented the situation from being much worse. Firstly, there was the original, deliberate, decision not to connect the system to the internet and, secondly, there was a decision to carry out an IT audit before connecting the system to the internet.

Then there's the question of why the attack took place. Was it simply malware that had somehow randomly found its way onto a device that a technician just happened to pick up and use that day? Or was it a situation involving an intelligence agent? A criminal gang member? A terrorist?

The incident also shows that the so called "air-gap" (that is, not being internet-connected) offers little protection. Then there's the fact that a portable storage device could be plugged into the ship's systems at all. As any seafarer will tell you, plenty of people come aboard ships brandishing laptops, portable devices, USB sticks. Customs agents, on-signing seafarers, ship agents, inspectors of all kinds. Any of them – and others too – could well be looking for a slot to plug in their devices.

Is that an innocent act? Or the beginning of something more sinister?

Unfortunately, the dormant-worm incident is no mere isolated event. The industry wide guidelines give plenty of examples of computer malware causing potentially catastrophic problems. For instance, there was the technician who discovered computer viruses lurking in a new-build ship's electronic charting display system. And there were ship agents who accidentally infected a maritime company's computer networks with ransomware (software that encrypts data until money is paid to a criminal organisation) by sending infected emails to the company.

Cyber security – international regulation

It is because of such threats that, from 1 January 2021, the International Maritime Organization's Resolution MSC.428(98) took effect. The resolution affirms that an approved safety management system should consider cyber risk management in accordance with the objectives and functional requirements of the International Ship Management Code. Secondly, it encourages maritime administrations to ensure that cyber risks are appropriately addressed in safety management systems.

This resolution has been given legal effect by maritime administrations around the world, which have translated it into national law. So, for instance, in Australia, the Australian Maritime Safety Authority has given it legal effect in Marine Order 58 by requiring owners of Australian and foreign-flagged vessels to comply with, among other things, the ISM Code. Ship operating companies, and their safety management systems, must be audited by a maritime administration or recognised organisation, for compliance with the ISM Code.

IMO guidance

Back in July 2017, the International Maritime Organization set out its guidelines on Cyber Risk Management in MSC-FAL.1/Circ.3.

It defined "maritime cyber risk" as a "measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised". The same document added that the goal of cyber risk management is to 'support safe and secure shipping, which is operationally resilient to cyber risks'.

As computer and information technology has advanced, bringing huge benefits along the way, there has been somewhat of a merger of information technology (technology that manages data) and operational technology (technology that uses data to monitor, control and operate physical processes and devices). Add in remote connectivity and networking of companies and ship-based assets, and it is clear that ongoing automation and digitalisation has increased the cyber-risk to ships and the maritime industries.

Academic study: an urgent need

Dr Vera Zhang and Dr Wendy Shi of the Australian Maritime College, along with researchers Changki Park, Christos Kontovas and Chia-Hsun Chang of Liverpool John Moores University in the UK, recently carried out a study to evaluate maritime cybersecurity.

They were interested in the area, as there appeared to be a dearth of published studies and literature on the topic but there were plenty of media reports of maritime cyber security incidents.

What the academics found does not make for pleasant reading.

"Risk management is fundamental to safe and secure shipping operations… it has traditionally been focused on operations in the physical domain, but greater reliance on digitisation, integration, automation and network-based systems has created an increasing need for cyber risk management in the maritime industry. Compared to other industries such as military, financing, airlines, cybersecurity related studies in the maritime industry are sitting at the backseat (for example, ten to twenty years behind other computer-based industries)… cybersecurity in the maritime industry needs to be addressed in urgency," they write.

To err is… ?

Readers may be wholly unsurprised to learn that the root cause of a lot of compromised systems was nothing more than extraordinarily basic failures in computer security management. These included the use of outdated IT systems and password-related failures.

Companies need to have a layered defence. There are some cheap and easy tactics that can be adopted, such as requiring longer and more complex passwords. Updating software in computers and systems is vital, as is having good anti-malware software on networks.

But the biggest exploitable vulnerability is posed by the people that staff companies and who crew ships.

"We found that the most fierce kind of threat comes from phishing and human error. These include impersonation emails, downloading of files. Phishing was the highest threat," Dr Vera Zhang told Shipping Australia.

"An attack may happen because one person clicked one link or downloaded one attachment. It's about awareness of cyber-security. In very large companies, employees may receive an email from top management, and they may not have their awareness in place and they just click," Dr Zhang says.

"Based on our research, we found that respondents were aware of these cyber-security attacks and issues. They just don't realise that it is so serious. It has not happened in their companies before. Many just don't have an awareness of the critical nature of attacks."

So, a vitally important step for any company is to create a culture of cyber-security. That's going to take education and training.

"Our message would be to boost cyber-security awareness among all levels of staff, and boost cyber-security culture. We have to enhance cyber security awareness. If everyone could have such cyber security awareness then IT can [do such things as] install malware protection," Dr Zhang explains.

A friend in the business. Hamburg Süd.

In business, it helps to have a friend you can turn to for good advice and strong support. Someone who knows your needs and takes the personal care needed to meet them, always working in your best interests. Product excellence and service reliability are indispensable, but what creates that kind of commitment is a spirit of cooperation, continuity, and trust – in other words, friendship. And that's the ship you can count on to carry everything forward.

No matter what.

HAMBURG SÜD

www.hamburgsud-line.com

Globelink AUSTRALIA

"The Forwarder's Choice"

Over 1400 Ports
Covering 31 Countries
More than 100 Offices Worldwide
Shipping to & from Melbourne, Brisbane
Sydney, Fremantle & Adelaide

LINKING AUSTRALIA TO THE WORLD AND THE WORLD TO AUSTRALIA

INTRODUCING AIRSHIP A NEW DIMENSION TO OUR SERVICES OFFERING DYNAMIC INTERNATIONAL SOLUTIONS

When seafreight is too slow & airfreight too expensive.
Airship is the key to your continued business success.

Simplified Tariff
Door-to-port service
Substantially reduced transit times
Priority transfer from plane to vessel
Prompt vessel connection in Singapore

DCN DAILY CARGO NEWS

THE 2019 DCN AUSTRALIAN Shipping & Maritime INDUSTRY AWARDS HIGHLY COMMENDED

Contact us for your most competitive rates & service

WWW.GLOBELINK.COM.AU