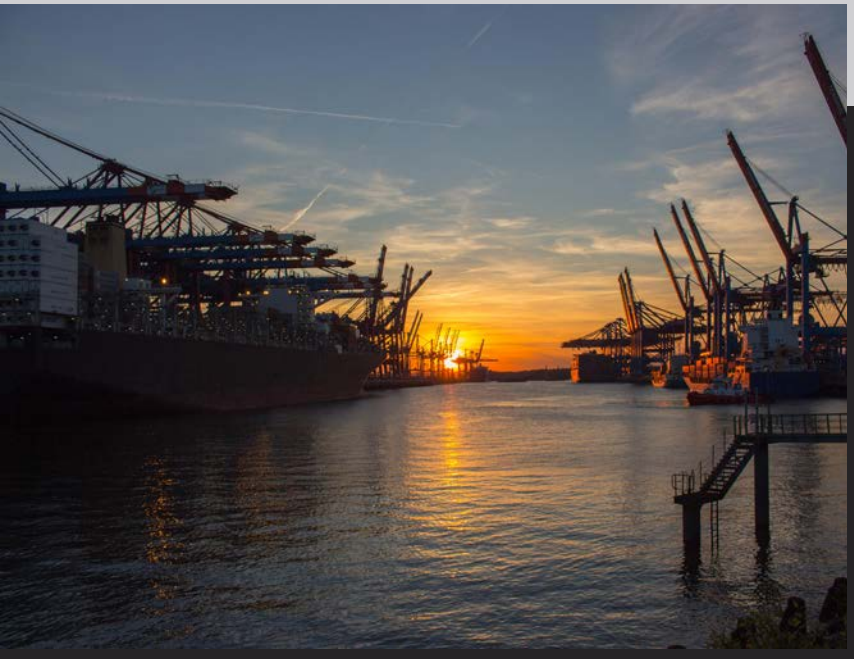
#8

JULY:2017

PHISH & SHIPS



Kindly sponsored by

CSO ALLIANCE
MARITIME

MAJOR COMPANIES HIT BY ATTACK

Welcome to issue 8 of "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the maritime and offshore industry initiative, "Be Cyber Aware At Sea".

In the previous issue we looked at the fallout of the "wannacry" ransomware attack; this time round it is "Petya" which has been making the headlines.

This most recent ransomware attack crippled a wide range of global businesses, from airports, banks and even the government of Ukraine. For us though, the fact that shipping giant Maersk was caught out serves as clear, unequivocal proof that shipping companies are in the cyber firing line.

The virus is believed to be ransomware - a piece of malicious software that shuts down a computer system and then demands an often extortionate sum of money to "fix the problem".

As the news of the attack spread, Maersk announced that "multiple sites and business units" had been shut down.

Ports were affected too, with Maersk's APM Terminals also hit. The media reported that 17 shipping container terminals run by APM Terminals had been hacked, including two in Rotterdam and 15 in other parts of the world.

So, finally it seems that shipping will be forced to face the fact that attacks are not only probable, but that they are real, and the industry is vulnerable to them.

Some have been eager to stress that this was not a maritime issue, and that it was the offices ashore which have been affected. While seemingly true, the fact remains that no-one in the industry can ignore the effect that such an attack can have. The risks are real, and the responses need to be adequate.

The full facts of the case will no doubt emerge as time goes on. For now, there is shock at the scale and spread of the attack. Even more so that such major multinational companies were caught out.

While it is not yet clear as to how the likes of Maersk or APM Terminals were compromised, we should spare a thought for likeliest route for the virus to have entered the system. Someone, quietly sat at their desk, thoughtlessly opening an infected attachment.

Employees going about their daily work, can, with one click, suddenly change everything, so that by the end of the day the news headlines around the world have lit up with their company's name. Not a good day.

Just one click is all it takes - and so people need to be trained, aware and able to react properly. Without that awareness, the risks turn to reality, and that is what we are seeing today.

IMO ACTION

The International Maritime Organization (IMO) has given shipowners and managers until 2021 to incorporate cyber risk management and security into their safety management systems.

The implementation, and indeed the new focus on cyber risks and responses, will not be an easy or comfortable task for shipping. However, there should be some comfort in the fact that both owners and officers understand the processes of managing safety through the existing ISM Code structure.

Overall, considering the interconnectedness of the issues, interweaving cyber safety into regular safety management systems is the most sensible route, not least by making compliance an important business decision too.

Not conforming to the new rules means shipowners run the risk of their vessels being detained. Detained vessels, or those found to be unseaworthy in commercial disputes are a major threat to any business so there is a financial pressure for shipping companies to react promptly.

Shipowners and managers need to get onboard with the new risks and work to address the cyber needs of their people, clients, vessels and shore management effectively. The clock is ticking...

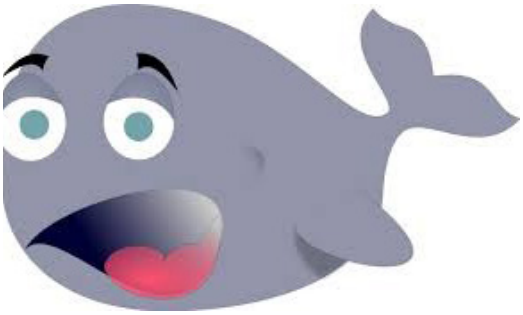
BROKER SCAM

According to a report from specialist advisory and consulting group Gray Page, a maritime bunker company in Malaysia claims to have been the victim of a phishing scam.

The owner of the company has told police that it has been defrauded of US$ 1 million, having been deceived into making two transactions to a bank in the United States. Malaysian police believe Spyware was embedded in the victim's computer allowing the perpetrators of the fraud to read email exchanges between the bunker company and its fuel supplier, picking up the key convincing details.

Police have urged companies to check with their counterparties before making payments to accounts that differ from the usual numbers. Reports said police were still investigating the incident and would cooperate with the International Police Organisation (INTERPOL).

So beware and DO NOT FEED THE PHISH!



BEWARE THE WHALERS

You've heard all about phishing, but what about whaling? This is where criminals take it up a level and send out a highly targeted phishing attack: one usually aimed at senior executives, and which masquerades as a legitimate email. Victims are encouraged to perform secondary actions, such as initiating a wire transfer of funds.

Whaling does not require extensive technical knowledge yet can deliver huge returns. As such, it is one of the biggest risks facing businesses. In their choice of target, senior management and chief executives, whaling emails tend to look more sophisticated than generic phishing emails. They usually contain:

- **Personalised information**
- **Convey a sense of urgency**
- **Have a solid understanding of business language and tone**

https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it

PROTECT YOURSELF FROM THE INSIDE OUT

Viral infections in onboard IT networks and computers are all too common. NCC Group senior advisor Tim Rawlins claims his investigators are yet to find a ship that does not have malware on board.

In the light of this, and given the impending 2021 deadline to provision for cyber issues in safety management systems, shipowners are urged to install "kernel level" filter technology at the core of all processes, such as the popular system "Abatis".

This protects networks from all types of malware by blocking virus executable files. The name stems from the ancient use of trees and spears to block the paths of attackers, and it works in much the same way today, sitting as gatekeeper inside the operation system software. Everything has to go through this code to reach the permanent storage and in this way it prevents any malware from writing to this storage.

Of particular note for shipowners is the fact the technology works on any Windows or Linux operating systems including legacy ones. It even provides an audit mode which records all the input and output devices on a system, producing a log for forensic analysis.

As the new operational environment sees cyber issues sitting within safety management, the issues of auditing, recording and reporting will take on new significance.

MAYFLOWER LEADS THE UNMANNED WAY

If all goes according to plan, the unmanned Mayflower Autonomous Research Ship (MARS) aims to cross the Atlantic in 2020. The project, developed in partnership with Plymouth University, the research and exploration charity Promare, and autonomous craft specialists MSubs, will push the boundaries of autonomous vessels at sea.

The Mayflower is a 100-foot trimaran which will use renewable wind and solar energy for propulsion to cross the Atlantic on the 400th anniversary of the original Mayflower's voyage. Along the way, the revolutionary vessel will conduct experiments using a variety of drones and subsea gliders carried on board.

According to the project partners, the Mayflower will confront current regulations governing autonomous craft at sea. Confronting rules is one thing, but there remains concern as to how safe such vessels are. There is criticism that the civilian maritime world has, as yet, been unable to harness the autonomous technology that has been used so effectively elsewhere.

See www.mayflowerautoship.com to follow progress.

ELIZABETH SOFTWARE

It is not just commercial shipping in the cyber spotlight, Britain's largest ever warship could seemingly be vulnerable to cyber attack too.

As HMS Queen Elizabeth embarked on sea trials, it was revealed the £3.5billion aircraft carrier is apparently using the same outdated and unsupported software that has frequently been exposed by hackers.

According to media reports, screens inside a control room on the ship, which is the largest vessel ever built for the Royal Navy, reportedly displayed "Microsoft Windows XP - copyright 1985 to 2001".

It was subsequently stated that the ship's systems were safe because the aircraft carrier is "properly protected". Time will tell, but with the scale and frequency of major attacks on the rise, the time to act is now.

SHIPPING'S DIGITAL FOG SLOWLY STARTS TO CLEAR

Professor Paul Dorey Ph.D. CISM F.Inst.ISP, Director, CSO Confidential & Visiting Professor in Information Security, Royal Holloway, University of London, has been writing for Inmarsat on the ways in which the digital fog is clearing, allowing us to finally see through the complexity of maritime cybersecurity

According to Professor Dorey, where digitisation appears, cybersecurity is never far behind. While this has been driven by banks and retailers trying to tackle criminals, it has finally reached shipping and the maritime industry.

Ships, ports and maritime support activities continue to adopt digital systems to handle commercial, cargo and personal information, and even control the ships or port facilities themselves. cruel irony at play as Professor Dorey states: "The more we digitise, the more interesting the systems become to cyber attackers and the more significant the potential impact could be when they do attack."

There is no one-size-fits-all solution, because there is no singular problem. So, from Professor Dorey, the message remains that cybersecurity investment needs to be appropriate to the risk, as nobody has the luxury of bottomless digital budgets.

The growing importance of cybersecurity in maritime has been recognised, but with this urgent enthusiasm there has been a risk of an information "fog" appearing, as so many have rushed to provide their own interpretations and guidance on dealing with maritime cyber threats.

The awakening to cyber problems is leading to action and a wide range of groups are producing their own cybersecurity guidelines, including now, the Classification Societies who are now working on a draft set of recommendations.

In the rush to provide solutions there are dangers. While it is far better to have too much guidance than have none at all, there is the potential for real problems and confusion if every association, nation, region or even ports start to set different expectations and solutions

The maritime industry needs to work together to see a way through the fog and it may be that they are doing just that. A joint working group has been established under Chair George Reilly of ABS, picking up on the direction set by the IMO cybersecurity guidelines, and hoping to find a common way to describe maritime cybersecurity risk. Under one universal language, we hope there will be one clear understanding of cyber risks and solutions. Access the full blog here https://goo.gl/n7GC2B

CYBER SECURITY & UK PORTS

Lawrie Abercrombie Director and co-founder of Arcanum Cyber Security has worked on various projects for UK Central Government Departments and commercial clients in the UK, Nato and Middle East and has a particular interest in the development of Cyber Defence Capability in multinational and joint cyber operations.

Much has been said about cybersecurity in today's geo-political climate. Shipping is on high alert and has received recent attention but focus has not yet been placed on Ports and port infrastructure. But it should be.

Transport - including roads, airports, ports and railways - is one of the 9 Critical National Infrastructure sectors in UK. It's easy to see why when, according to DEFRA, almost half our food is imported by sea, port security is paramount.

So it's quite worrying when the UK's Security Authorities, having listed cyber as a major threat to the Critical National Infrastructure, have said that "Transport continues to face enduringly high levels of threat" and that "Hostile actors can use malicious software to manipulate industrial process command and control systems."

Arcanum Information Security Ltd has spent considerable time over the last four years looking at cyber threats to the Port & Maritime sector, including working with very sophisticated threat modelling tools in the US, and it's evident that a relatively simple Cyber-attack on industrial control systems (ICS) could cause exponential levels of damage to a Port and bring 'just in time' supply chains to a grinding halt in just a couple of days.

Arcanum
CYBER SECURITY

Increasing numbers of new ICS are being introduced and connected to Port networks and existing ICS, at least partly due to the ever-present demand to cut costs. In many ports, these systems now control pumping of fuel, use RFID and optical recognition to track, load and unload containers whilst the same systems are used to control entry and exit to the port itself.

It's evident that many of these ICS systems are not suitably protected. An attack here could potentially cause injury or loss of life and damage equipment. It would certainly lead to extensive financial costs both to the port operators through cargo disruption, loss of confidence and subsequent loss of customers, and to the country as a whole through the economic chaos that could ensue from disruption across the transportation system.

With an extensive background in cybersecurity for critical Defence and Government projects, Arcanum is perfectly positioned to deliver security solutions to protect your assets and ensure business continuity. Talk to our experts today to discover how you can protect your critical data and infrastructure.

http://arcanum-cyber.com/

TALKING CYBER SENSE: ASSESSING SHIPPING RISKS

Novae
LOOKING FORWARD

Sharif Gardner Cyber Unit Training Manager at Novae Group talks about the importance of assessing cyber risks in shipping.

There has been a high focus in shipping on assessing cyber risks at sea and rightly so. A vessel that is unable to operate or leave port because its systems are down is an asset not earning money for the business. And it is the business impact arising from this that should grab the attention of ship owners.

Not all risks are presented equal and as such, not all security controls are equal in measure. Evaluating the effectiveness of critical security controls is different dependent on industry. What is consistent, however, is that every organisation should map out its risk with a risk assessment across its entire business environment. For example, security by design is ideal, but retro fitting every vessel with custom built anti-malware solutions for its operating technology is not necessarily proportionate to the risks currently faced. So, a way to truly understand this is to ask:

WHO IS A THREAT TO YOU AND WHY?

Criminal syndicates primary motivation is financial gain. The best way to make money out of shipping for a criminal in today's climate is still most likely through its supply chain with a simple business email compromise, leading to transactional e-theft or fraud.

WHERE ARE YOU MOST VULNERABLE?

Most shipboard systems are inherently insecure and by nature are vulnerable to human error and indiscriminate malware introduction. However, data damage to the integrity of critical cargo management and operating systems could lead to widespread business interruption. The human factor is presented a lot in shipping because business owners can relate to it – humans have a tendency to cut corners.

Talking to equipment suppliers will help in understanding critical vulnerabilities within software systems. Whilst patching is considered a critical control, it may not always be feasible, and in such cases, extra controls to ensure these systems are segregated.

HOW DO YOU REDUCE RISK?

Each company is different. There are technical and procedural responses for reducing risk. Technical controls in today's environment will require getting the basics right where possible, such as software and system updates, reducing privileged access and where possible, technically restricting automatic downloads of unauthorised software. Procedural controls will take longer because it is a behavioural challenge and one that enforced policies alone will not fix – training is the key to improving procedural security.

https://www.novae.com/

HOW ARE YOUR PA55W0RDS DISCOVERED?

Attackers use a variety of techniques to discover passwords. Many of these techniques are freely available and documented on the Internet, and use powerful, automated tools.

Approaches to discovering passwords include:

- Social engineering eg phishing; coercion
- Manual password guessing, perhaps using personal information 'cribs' such as name, date of birth, or pet names
- Intercepting a password as it is transmitted over a network
- 'Shoulder surfing', observing someone typing in their password at their desk
- Installing a keylogger to intercept passwords when they are entered into a device
- Searching an enterprise's IT infrastructure for electronically stored password information
- Brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found

Source: UK National Cyber Security Centre (NCSC)

INSURERS TOUGHEN CYBER STANCE

The International Union of Marine Insurance (IUMI) has announced its support for the efforts of the International Maritime Organization (IMO), classification societies and shipowner associations when it comes to cyber threats.

Cyber security has been high on its agenda of late, and IUMI has cooperated with international shipowner associations, such as BIMCO, the International Chamber of Shipping (ICS), Intertanko, Intercargo and Cruise Lines International Association (CLIA), for the second edition of the "Shipowners Guidelines on Cyber Security Onboard Ships"- intended to be launched in the late summer of 2017.

IUMI has also supported proposals to make cyber risk management onboard ships mandatory as part of the ISM Code and accordingly part of the ship's mandatory Safety Management System.

IUMI currently relies on shipowners' voluntary efforts to perform a proper risk assessment, and it seems this is no longer enough. With the move of cyber into safety, and as class recommendations beckon there will be a flurry of activity to assess and react to cyber risks.

Sponsored by:

CSO ALLIANCE MARITIME

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....