2017
N. 3 - 11th YEAR
Xmas Edition

news

MAGAZINE OF MEDITERRANEA DI NAVIGAZIONE SPA

THE FUTURE CAN BE BRIGHT

www.mediterraneanav.it

PAOLO CAGNONI
Chairman & CEO

Editorial

2017 is turning out to be a year with a sharp reduction in freight which started in the spring. Many geopolitical events have affected the potential recovery and the new units ordered in recent years have been delivered in large quantities. This reduction in freight, especially in large ships, is mainly due to excess available tonnage rather than a reduction in traffic.
On the contrary, there has been an increase in trade in chemicals and volumes in individual transport. Our highly diversified company has been able to benefit from specialized trades and consolidate the bond with its customers.
We are improving border/land interaction by trying to share more and more choices and ways of improvement.
We look forward to continuing to improve our encouraging statistics with the help of all of you, while maintaining high attention and motivation for achieving the goals that, together, we have set for ourselves.
Have a great day at work!

Il 2017 sta risultando un anno con una forte riduzione dei noli iniziata nella primavera. Molti eventi geopolitici hanno inciso sulla potenziale ripresa e le nuove unità ordinate negli anni scorsi sono state consegnate in grande quantità. Questa riduzione dei noli, specialmente nelle navi di grande portata, è dovuta principalmente ad un eccesso di tonnellaggio disponibile più che ad una riduzione dei traffici.
Si nota contrariamente un aumento dei traffici nella chimica e dei volumi nei singoli trasporti. La nostra società, molto diversificata, ha potuto beneficiare dei traffici specialistici e consolidare il legame con i propri clienti.
Stiamo migliorando l'interazione bordo/terra cercando di condividere sempre più le scelte e le vie di miglioramento.
Contiamo di continuare a migliorare le nostre incoraggianti statistiche con l'aiuto di tutti voi, mantenendo alta l'attenzione e la motivazione per il raggiungimento degli obiettivi che assieme ci siamo dati.
Buon lavoro

The challenge for the best advice on the safety matter is closed. Congratulations to Chief Officer Musumeci Giuseppe, awarded with a special price as our Best Safety Councellor!

La sfida per il miglior consiglio sulla safety si è conclusa, congratulazioni al Primo Ufficiale Musumeci Giuseppe! Riceverà un premio speciale.

news

Magazine of Mediterranea di Navigazione Spa

2017 – Nr. 3 / 11th Year

Table of Contents / *Sommario*:

Contributors: Paolo Cagnoni
Riccardo Franchini
Alberto Chiappe
Francesco Costa
Nicola Camorali
Davide Servidei

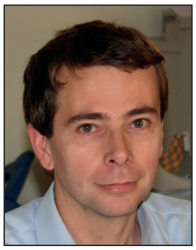
Master: Cosmo Vellucci
Chief Engineer: Baurda Chiril Amen

Printing: Samorani - Forlì
Illustrator: C.E. Mariano Borghero
Editorial coordinator: Chiara Amadori

Mediterranea's **latest news**

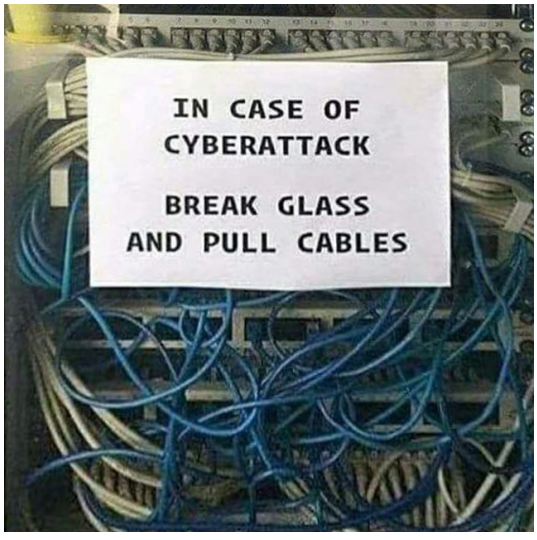
Mr. Cagnoni during visit on board MT Cosmo

Meeting for resilience programme on board MT Cosmo



RICCARDO FRANCHINI
Safety and Quality Dept.

Cyber Security



The topic "Cyber Security" has now become so vast and important that it would be extremely reductive to exhaust it with just one article. For this reason, beginning with this issue of the company magazine, we will start with a series of articles on the subject. In recent years, the growing introduction of IT systems in the workplace has paved the way for new issues related to machine and information security. Recently, the awareness of cyber risk has consolidated in the society to such an extent that national and global institutions have had to issue directives about it. At European level, reference can be made to Directive 2016/1148 of 6 July 2016 laying down measures for a high common level of network and information security in the Union and Regulation 2016/679 of 27 April 2016 on the protection of individuals regarding the processing of personal data. In IMO, the MSC.1 / Circ. 1526 of 1 June 2016 cyber risk management guide in marine environment can be highlighted. One of the first definitions of cyber security can be found in the Presidential Directive on National Security (NSPD-54 / HSPD-23) issued in January 2008, which defines the term "Prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communications services, wire communication and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and nonrepudiation." The document also outlines the definition of cyberspace or "The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." In Italy, five years later, by decree of the President of the Council of Ministers of 24 January 2013, cybernetic security is defined as "the condition for which cybernetic space is protected by the adoption of appropriate physical, logical and procedural security measures with respect to events of a voluntary or accidental nature, consisting of the acquisition and the transfer of undue data, their alteration or illegal destruction or the damage, destruction or blocking of the proper functioning of networks and information systems or their constituent elements." In the same decree, cyber space is defined as "the set of interconnected IT infrastructures, including hardware, software, data and users as well as logical relationships, however established, among them." As one can see, these definitions can be considered analogous and it is proven by the fact that in recent years the definition of Cyber security and Cyberspace has become unambiguous. Cybernetic threats can be divided into four types: Cybercrime: complex criminal activities such as fraud or telematic fraud, identity theft, misappropriation of information or creations and of intellectual property; Hacktivism: pursuit of social and political goals through computer piracy, term deriving from the union of words hacking and activism; Espionage: Undeclared acquisition of sensitive, proprietary or classified data/information; Cyber Warfare: A set of activities and military operations planned and conducted to achieve effects in this context. From the Clusit 2017 report prepared by the Italian Association for Computer Security on ICT Security in Italy, it is stated that 2016 can be considered the annus horribilis of cyber security. In fact, in 2016, there was a growth of 117% for the "information war"; a 1162% increase in attacks with Phishing/Social Engineering techniques; healthcare was the most affected sector (+ 102%) followed by the large organized distribution (+ 70%) and "only" third the Finance/Banks sector (+ 64%). Critical Infrastructure attacks that had picked up sharply in 2015 grew even though with a lower rate (+ 15%). The attacks on Europe and Asia are increasing. In absolute terms, the highest value of Cybercrime and Cyber Warfare attacks is recorded there. Cybercrime is the cause of 72% of the attacks in 2016 globally, demonstrating that money is always the prevalent cause of the attacks and the ultimate motivation of the attackers. However, this trend appears to be constant since 2011, when this type of attack and crime amounted to 36% of the total. Slightly lowered are the attacks for "Cyber Espionage" (-8%) and Hacktivism (-23%). In 2016, the most striking attacks are indiscriminately against public institutions and private companies. For example, attacks on hospitals such as the Hollywood Presbyterian Medical Center could be reported, which, due to a ransomware, center executives were forced to pay a $ 17,000 ransom to obtain the compromised file deciphering key from the criminals. In addition, the attack on Bangladesh Bank with the introduction of fraudulent transactions in the SWIFT system for a

total of $ 1 billion that, just for a trivial mistake of criminals, have only been successful for 81 million. From a technical point of view it impresses the attack suffered by ADUPS Technology by editing the firmware for Android devices marketed in different countries around the world. The change created a backdoor that allowed criminals to acquire various phone information, including SMS and phone lists. Moreover, the attack on DynDNS is very important especially in view of the access path used. In fact, the company that manages DNS services (DNS is the acronym of the Domain Name System and is the Internet node names resolution system for IP addresses and vice versa) was hit by using IoT devices (on the merits of cameras security) and was remotely compromised. Last but not least, from a socio-political point of view, was the attack suffered by the Democratic National Committee of the US Democratic Party with 19252 e-mail thefts. The subsequent policy controversy may have influenced the presidential election. The leading US intelligence agencies support the presence of Russian intervention behind the scenes, though officially responsible is a hacker with the nickname Guccifer 2.0. Even the attack on the Italian Foreign Ministry at the beginning of 2017 could have been "sponsored" by Russia. Clusit's report shows the following trend of cybernetic attacks from public sources (see table A) While the distribution of attacks is distributed as follows: (see table B). The distribution of victims by geographical area shows that the majority of attacks, though slightly diminishing, focus on the American area. In Europe, the trend is rising (see table C). The distribution of attack sources undermines some common places. The statistics presented by AKAMAI Technologies on Distributed Denial of Service DDos on their network is very interesting (see table D). The root causes of serious 2016 attacks show an increase in the use of "Common Malware" (+ 116%), of Distributed Denial of Service (DDoS) attacks, or targeting a target by flooding traffic to generate a block exploiting a large number of infected computers, with a 13% increase, and operating system vulnerabilities (+ 333%), of which an example is the recent Wannacry attack. Above all, the significant increase in the category "Phishing/Social Engineering" (+ 1166%) has to be recorded. Improved defenses in recent years have been demonstrated by the fall in the "Known Vulnerabilities/Misconfigurations" category, but it also highlights a change in the strategy of criminals by increasingly relying on "common malware", especially on Ransomware both for attacks to small businesses and for attacks to bigger targets and/or with significant impacts (see table E).The current world is increasingly based on computer technology. In the maritime field, just climb up the control bridge to realize the increased dependence of navigation on the IoT devices (just think about the connection between ECDIS / radars and GPS). Communications (such as e-mail, voip, access to certain institutional internet platforms, etc.) are becoming more and more important to the operation of ships. Hardware and software systems are evolving very quickly to cope with computer criminals, but if they are not assisted by good user preparation, they will never be able to completely overcome the increasingly sophisticated attacks. In the next articles, we will talk about topics that are more common to both work and private spheres, to make computer criminals' lives more and more difficult.

5

(A) ATTACKERS BY TYPE — VARIATIONS 2016 OVER 2015

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2016
Cybercrime	170	633	609	526	684	751	9,80%	↑
Hacktivism	114	368	451	236	209	161	-22,97%	↓
Espionage / Sabotage	23	29	67	69	96	88	-8,33%	↘
Cyber warfare	14	43	25	42	23	50	117,39%	↑
TOTALE	469	1.183	1.152	873	1.012	1.050	+3,75%	↗

(B)