



Introduction to main Cybersecurity Terms

Serena Ramovecchi
IT Security Operations



Lisbon / 6 March 2019

Table of Contents



1

What's going on in the cyber space

2

IT Security at EMSA

3

Cybersecurity Terminology

4

MaKCs e-Learning Portal

5

Have you been pwned?

Live Cyber Attack Threat Map

Cyber attacks are socially or politically motivated attacks carried out primarily through the **spread of malicious programs**, unauthorized web access and manipulation of electronic devices or computer systems causing **far-reaching damage**.

Powered by ThreatCloud Intelligence

THREATCLOUD

LIVE CYBER ATTACK THREAT

Check Point
SOFTWARE TECHNOLOGIES, INC.

ATTACKS TODAY

(since 12AM PST)

10,619,763

ATTACKS YESTERDAY

71,942,793

TOP TARGETS BY COUNTRY

France

THREAT STATS

Last Week Last Month

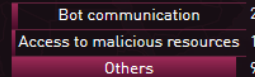
Average Infection Rate



Most Frequent Attack Source

FRANCE

Infecting Malware Types



Belgium

THREAT STATS

Last Week Last Month

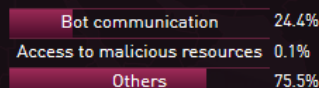
Average Infection Rate



Most Frequent Attack Source

USA

Infecting Malware Types



Germany

THREAT STATS

Last Week Last Month

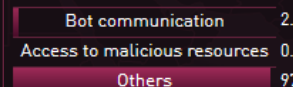
Average Infection Rate



Most Frequent Attack Source

GERMANY

Infecting Malware Types



Spain

THREAT STATS

Last Week Last Month

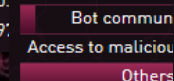
Average Infection Rate



Most Frequent Attack Source

GERMANY

Infecting Malware Types



Portugal

THREAT STATS

Last Week Last Month

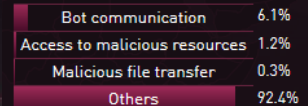
Average Infection Rate



Most Frequent Attack Source

USA

Infecting Malware Types



TIME

ATTACK

SOURCE

TARGET

Table of Contents



1

What's going on in the cyber space

2

IT Security at EMSA

3

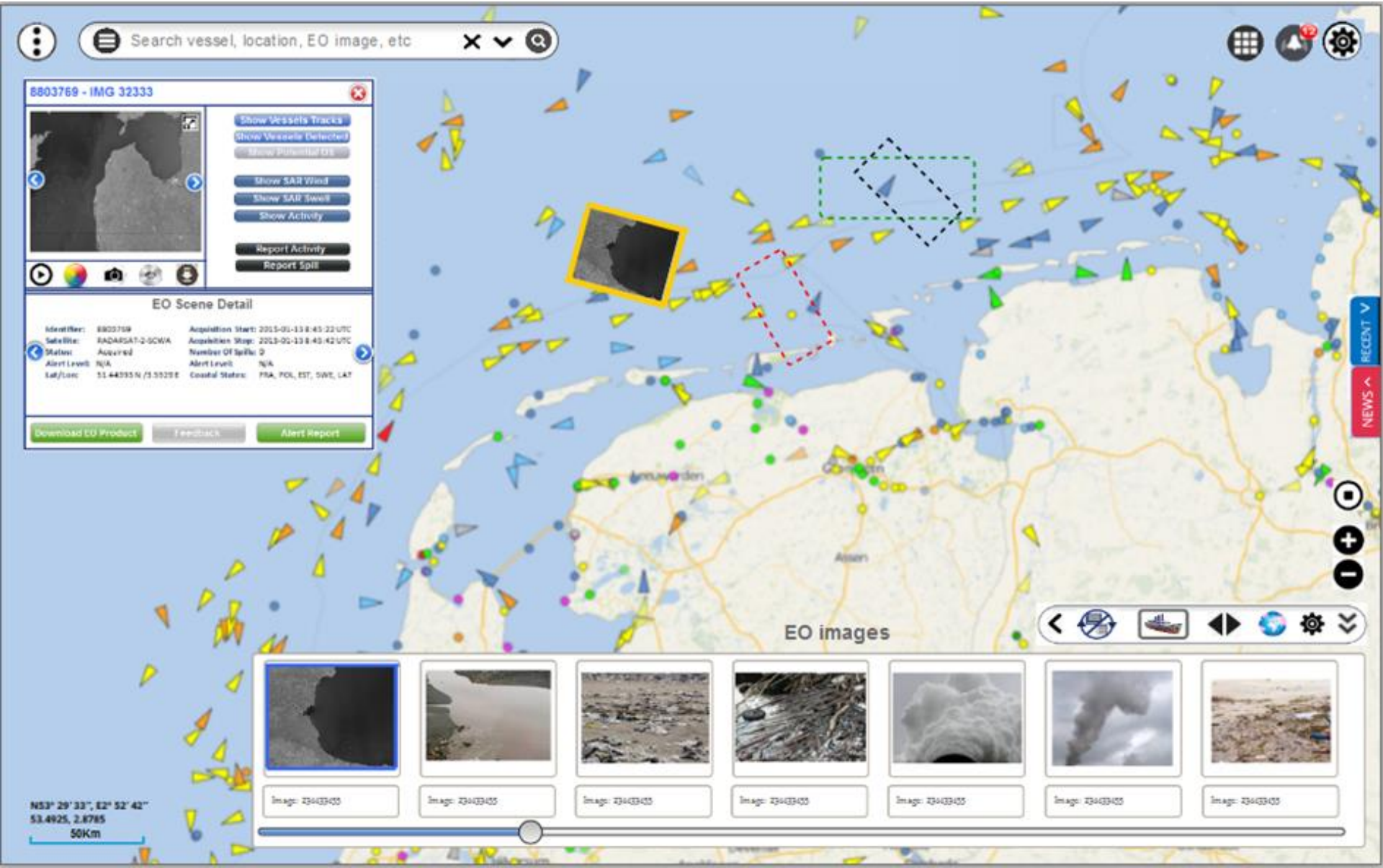
Cybersecurity Terminology

4

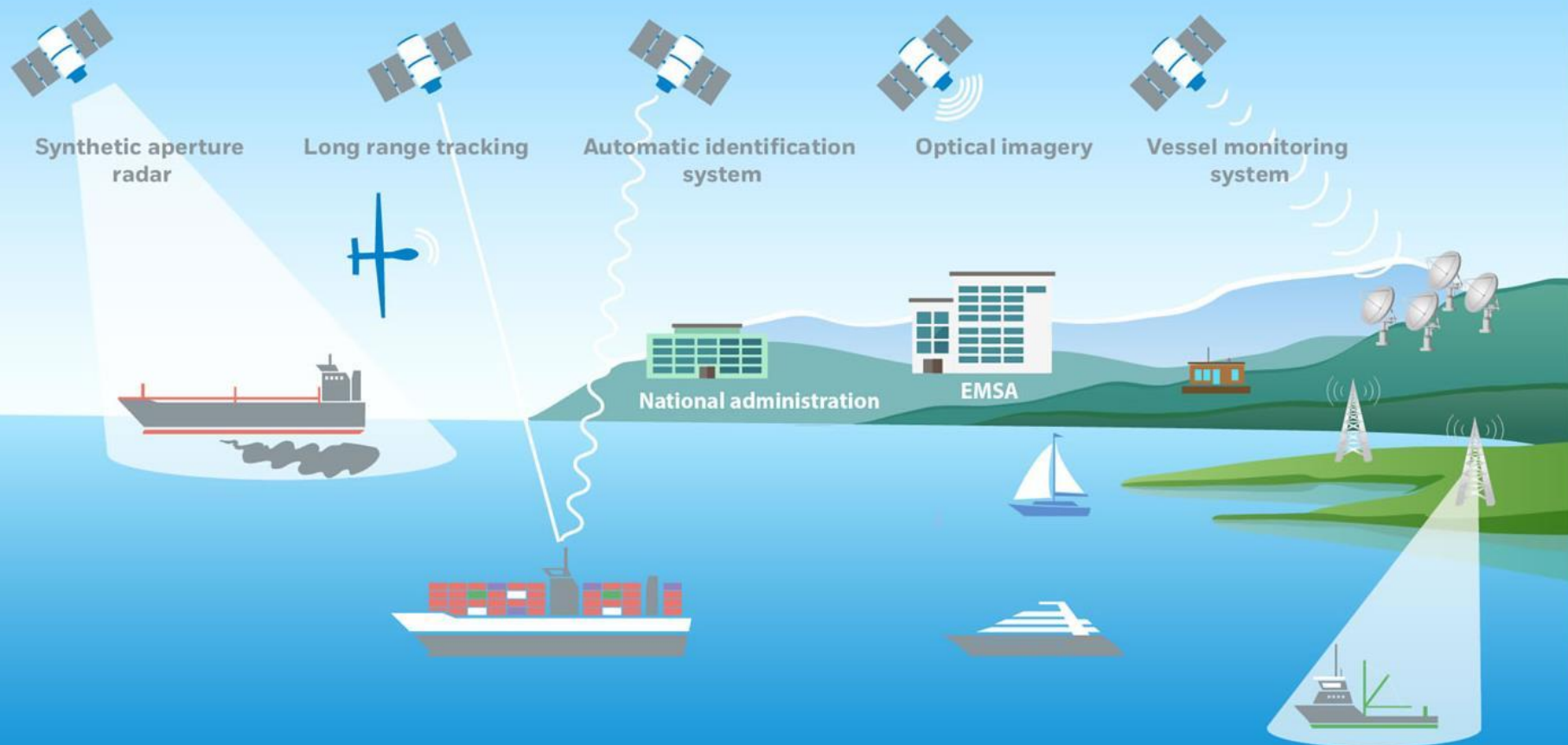
MaKCs e-Learning Portal

5

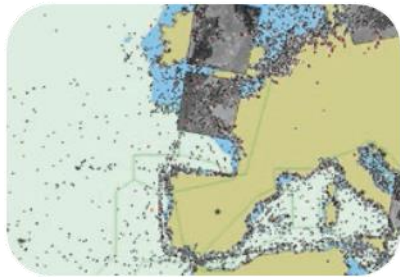
Have you been pwned?



EMSA maritime integrated ecosystem/2



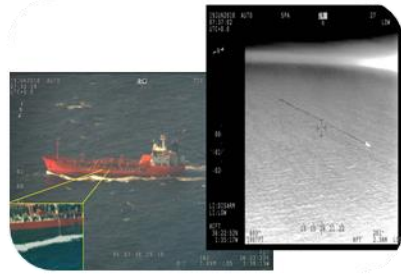
User communities



MARITIME SAFETY & VESSEL
TRAFFIC MANAGEMENT



Member States



MARITIME ENVIRONMENTAL
PROTECTION & RESPONSE



Member States



MARITIME
SEARCH & RESCUE



Member States



MARITIME
BORDER CONTROL



Frontex



ANTI-PIRACY &
MARITIME MIGRATION



EU Navfor



FISHERIES INSPECTION
& CONTROL



EFCA



MARITIME
CUSTOMS ACTIVITIES



OLAF



PREVENTION & SUPPRESSION OF
TRAFFICKING & SMUGGLING
& RELATED MARITIME
LAW ENFORCEMENT



MAOC-N 7



A layered Security approach



Enterprise Architecture protection:

- ✓ Identity & Access Management
- ✓ 2-way SSL with internal Certification Authority for maritime services

Perimeter protection:

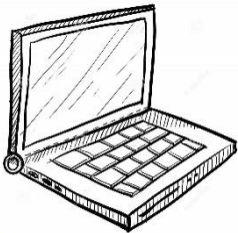
- ✓ **IPS** Intrusion Prevention System
- ✓ **WAF** Web Application Firewall
- ✓ **Firewall** Threat Prevention + Antibot + Application & URL filtering

End-point protection:

- ✓ Windows Defender ATP – Advanced Threat Prevention
- ✓ AppLocker files execution administration
- ✓ BitLocker Drive Encryption

Security processes:

- ✓ Security Information and Event Management (Splunk) => CERT-EU
- ✓ Incident response support & forensics => CERT-EU
- ✓ Penetration testing => CERT-EU



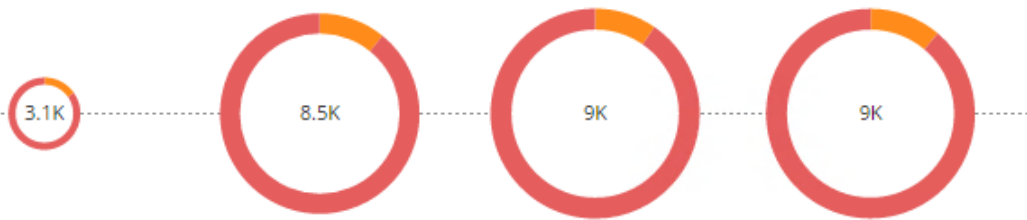
EMSA Layered IT security/2

Firewall

A **firewall** is a security device that monitors network traffic and allows or blocks it based on a defined set of security rules.

Security Incidents (by Logs)

● High ● Critical



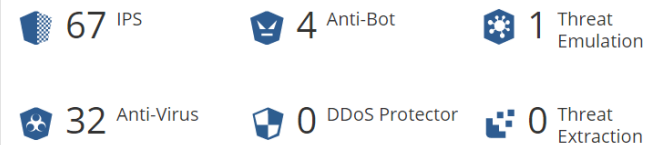
Jan 24, 2019

Jan 31, 2019

Feb 7, 2019

Feb 14, 2019

Attack Types by Blades



Infected hosts



Top Attacks

Protection Name	Severity	Blade	Logs
SQL Injection	Critical	IPS	4.9K
LDAP Injection	Critical	IPS	1.2K
Non Compliant HTTP	Critical	Firewall	454
Non Compliant DNS	Critical	Firewall	333
Command Injection	Critical	IPS	114
Microsoft IIS WebDAV ScSto...	Critical	IPS	48
Havij Automated SQL Injecti...	Critical	IPS	37
Cross-Site Scripting	Critical	IPS	33
China Chopper Web Shell Re...	Critical	IPS	22
Suspicious Executable Mail ...	Critical	IPS	16
SQL Servers UNION Query-b...	Critical	IPS	15
DNS Data Overflow	Critical	IPS	13

Top Sources

Source	Severity	Blade	Logs
130.193.52.69	Critical	IPS	1.6K
185.183.104.139	Critical	IPS	607
host87-120-40-89...	Critical	IPS	561
55.232.187.35.bc...	Critical	IPS	224
42.113.90.35	Critical	IPS	220
H_DMZ-1_LTM_VI...	Critical	IPS	179
10.120.0.157	Critical	Firewall	171
128.96.151.27.bro...	Critical	IPS	149
209.79.231.35.bc...	Critical	IPS	148
94-237-60-17.uk-L...	Critical	IPS	148
178-37-18-205.ad...	Critical	IPS	148
05409082 skubro...	Critical	IPS	148

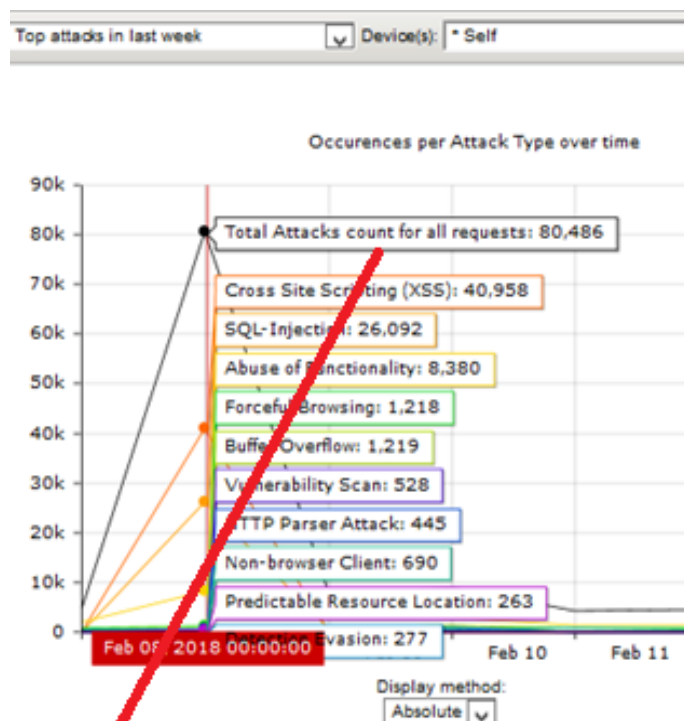
Top Destinations

Destination	Severity	Blade	Logs
EMSA_PL_91.231.2...	Critical	Multiple Blades	7.0K
no-mans-land.m2...	Critical	Firewall	89
EMSA_PL_91.231.2...	Critical	Multiple Blades	71
82.102.17.242	Critical	Firewall	44
EMSA_PL_91.231.2...	Critical	Multiple Blades	39
FW_EXT_2 (91.231...	Critical	Multiple Blades	37
FW_EXT_1 (91.231...	Critical	Multiple Blades	37
vpn-gw-prod-001...	Critical	Firewall	36
vpn-gw-prod-002...	Critical	Firewall	36
H_DMZ-1_PWGT1 ...	Critical	IPS	31
H_DMZ-1_QVLAN_...	Critical	IPS	29
FMSA_PL_91.231.2...	Critical	Multiple Blades	28

EMSA IT security measures/3

Web Application Firewall (WAF)

A **WAF** is a security device that monitors and filters HTTP traffic to and from an WEB application.



80 000 security incidents per week

Top attacks:

#	Attack Type	Occurrences
1	Abuse of Functionality	16382
2	Buffer Overflow	9513
3	Forceful Browsing	8870
4	Non-browser Client	5131
5	SQL-Injection	3213
6	Detection Evasion	2712
7	HTTP Parser Attack	1701
8	Predictable Resource Location	327

Top violations:

#	Violation	Occurrences
1	Illegal meta character in URL	14179
2	Attack signature detected	9325
3	Illegal request length	8872
4	Illegal file type	8872
5	Illegal URL length	8750
6	Illegal meta character in parameter name	2210
7	HTTP protocol compliance failed	1701
8	Illegal query string length	1033

EMSA IT security measures/6

Security information and event management (SIEM)

EMSA adopted Splunk SIEM and built an integrated dashboard

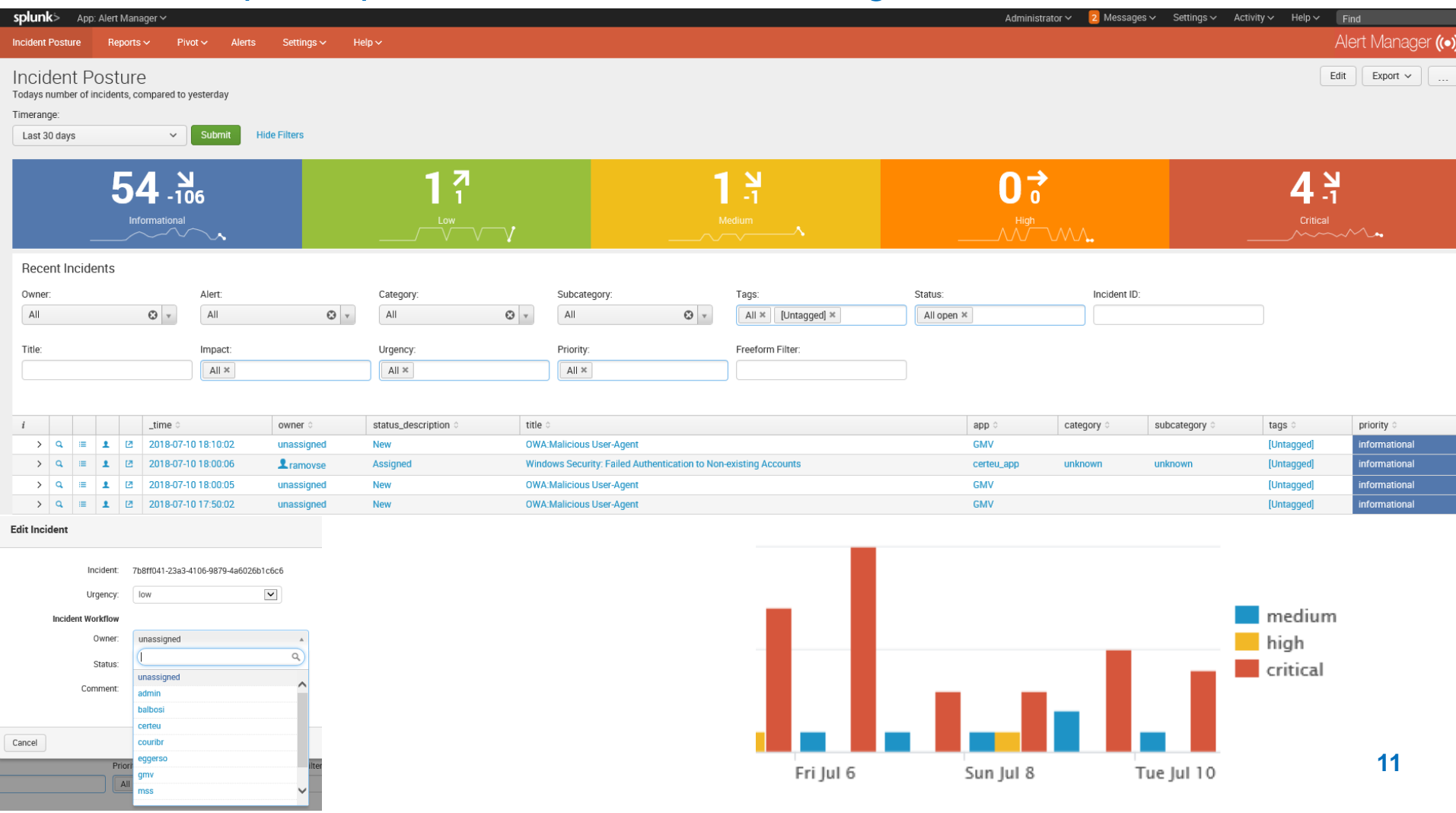


Table of Contents



1

What's going on in the cyber space

2

IT Security at EMSA

3

Cybersecurity Terminology

4

MaKCs e-Learning Portal

5

Have you been pwned?

Terminology - Exploit & Vulnerabilities



A **vulnerability** is a **weakness** an adversary could take advantage of to **compromise** the confidentiality, availability, or integrity of a resource.

An **exploitation technique** is a technique used by the adversary to use victim's resources unfairly for its own advantage.

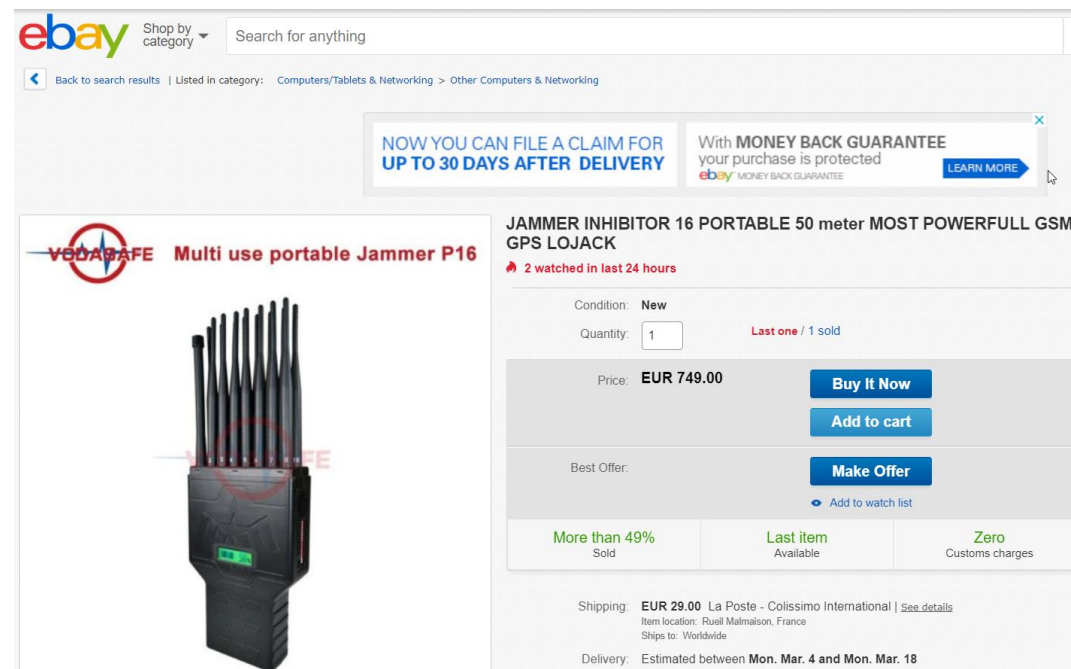
An **exploit** can be a piece of software or a sequence of commands that takes advantage of a software vulnerability to cause unintended behavior on computer software, hardware, or electronic devices.

This unintended behavior can be gaining control of a system, allow privilege escalation, or compromise a resource/service.

Terminology – JAMMING

Radio jamming is the deliberate jamming, disrupt, interference or blocking of radio signal with authorized wireless communications.

Radio jamming devices are called "jammers".



The screenshot shows an eBay product listing for a "JAMMER INHIBITOR 16 PORTABLE 50 meter MOST POWERFULL GSM GPS LOJACK". The item is a "Multi use portable Jammer P16" by "VODAFONE". The listing includes a search bar at the top, a "NOW YOU CAN FILE A CLAIM FOR UP TO 30 DAYS AFTER DELIVERY" banner, and a "With MONEY BACK GUARANTEE" banner. The item is listed for EUR 749.00, is in "New" condition, and has a quantity of 1. It is marked as "Last one / 1 sold". The listing also shows a "Best Offer" section with a "Make Offer" button. Shipping is EUR 29.00 via La Poste - Colissimo International, and delivery is estimated between Mon. Mar. 4 and Mon. Mar. 18. The item is described as "More than 49% Sold", "Last item Available", and "Zero Customs charges".

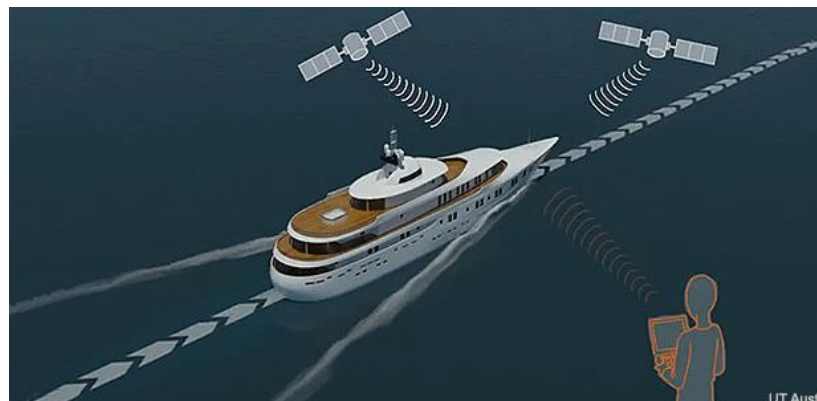
Terminology – SPOOFING

Spoofing is the act of *camouflage* so that an unknown source appears to be a trusted source.

A **Spoofing attack** is a situation in which a person or program successfully *masquerades* as another by falsifying data.

A **GPS spoofing attack** attempts to deceive a GPS receiver by broadcasting incorrect GPS signals, structured to resemble a set of normal GPS signals or genuine signals captured elsewhere or at a different time.

These spoofed signals may be modified in such a way as to cause the receiver to estimate its position to be somewhere other than where it actually is..



Terminology - SPEAR PHISHING

Phishing attacks persuade potential victims to divulge sensitive information (credentials, credit card details).

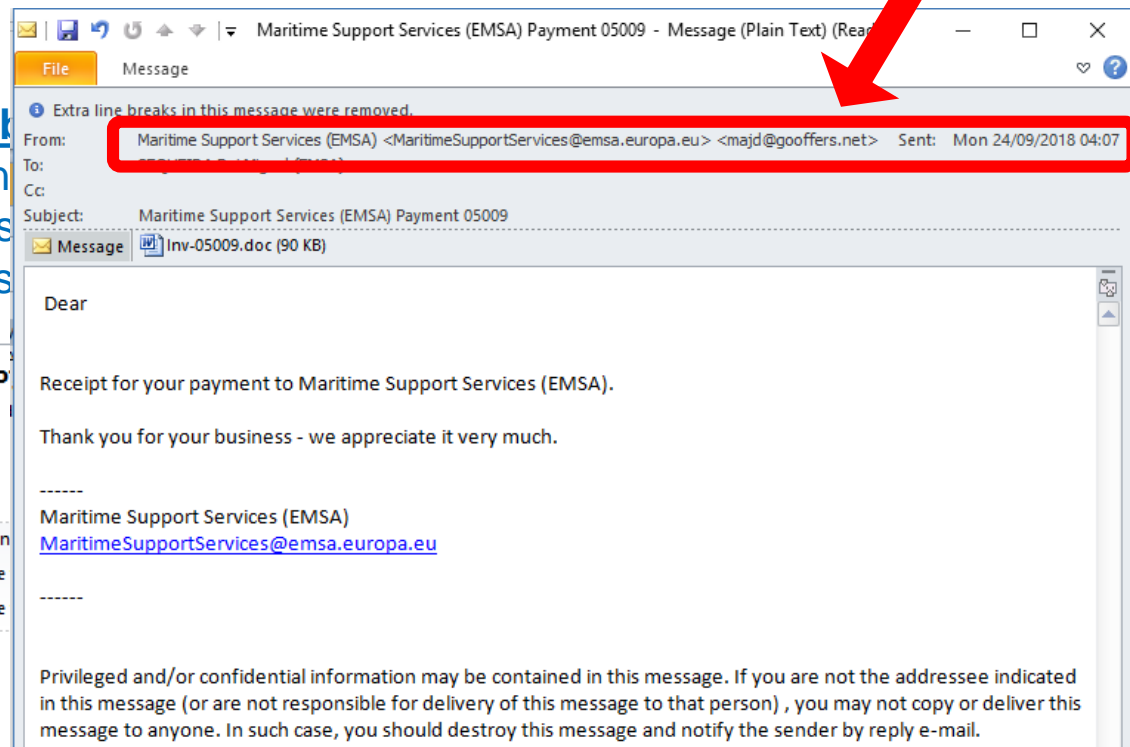
They take the form of SPAM mail, malicious Web sites, email messages **appearing to be from a legitimate source**.

Spear phishing is a more sophisticated version of phishing in which the attack is **personalised to the specific victim**.

Spear Phishing email

With Spoofed sender

EMSA receives on a daily basis emails quite often impersonating service providers (workshops, operators, freight forwarders)



Samples of SPAM messages entering in food

EMSA)

You forwarded this message on 12/11/2018 10:53.

Sent: Wed 07/11/2018 09:39

To: ICT Security (EMSA)

Message

- Issue Updated - Sea Sentinels Joins as a Sponsor
- Issue Updated - ALERT: Email with executable
- Issue Updated - ALERT: Email with executable

Terminology - Malware

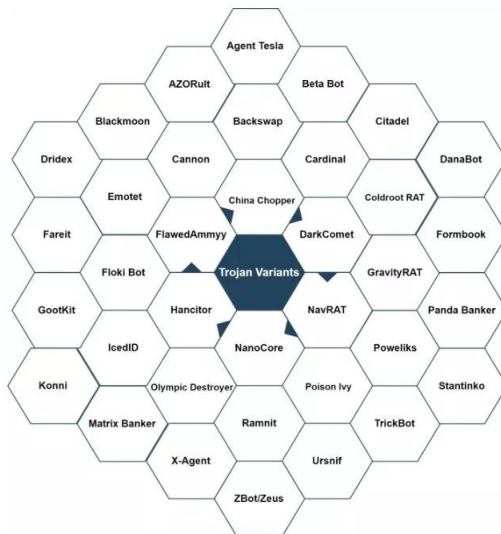
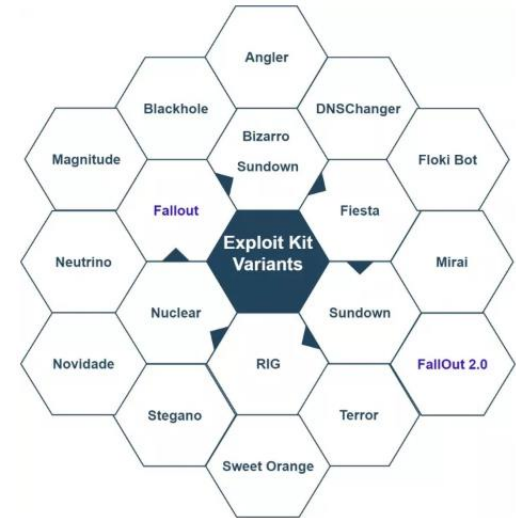
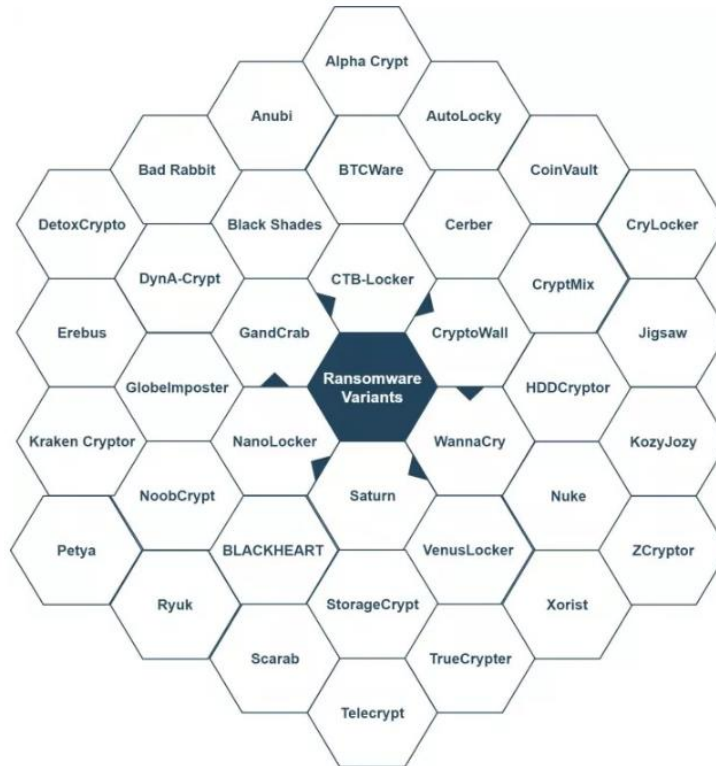
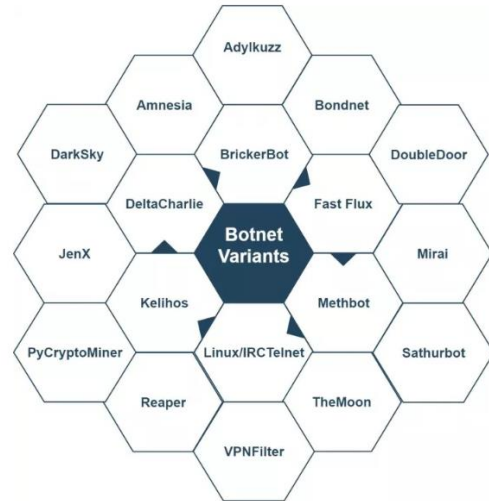


Malware is derived from the term '**Malicious Software**'.

Any piece of software that performs undesirable operations such as Trojans, Viruses, Worms, and Spyware.

Malware families

Variants of malware families



Patch Management/1



Meltdown and Spectre

Reference: CITAR-Flash-2018-001 - Date: 05/01/2018 – Version: 1.0

ASSESSMENT

THREAT	TARGETS / VICTIMS	THREAT ACTOR
Type: Vulnerability	Domains: All	Profile: none
Level: Medium	Sectors: All	Motive: none
Information-Confidence: A1	Victims: None reported	Historical activity: none

COURSE OF ACTIONS

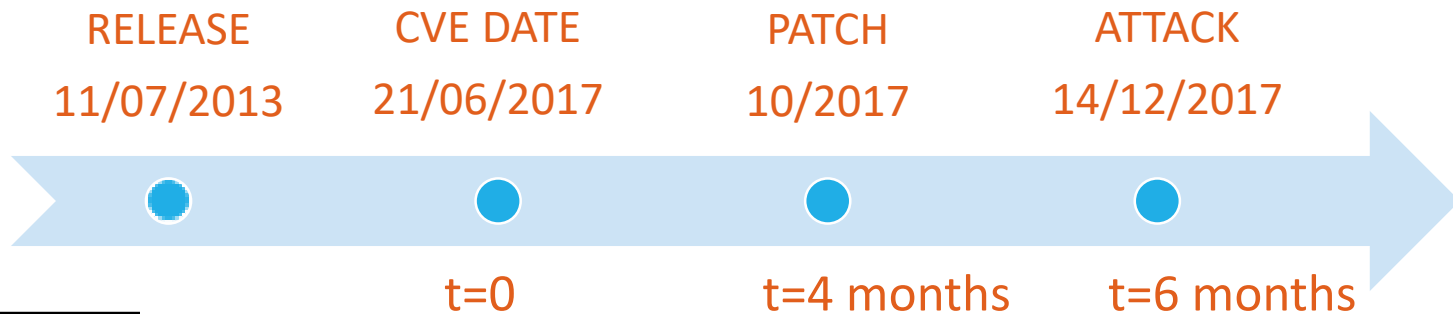
ACTOR	ACTIONS
CERT-EU	✓ Monitor reporting about the vulnerabilities and alert customers as needed
EU institutions, bodies and agencies	<div>✓ Apply software patches as they become available</div> <div>✓ Implement Microsoft recommended configuration changes as described here: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution-s</div> <div>✓ Identify and consider replacing any systems that cannot be updated</div>

Software Patch

A software patch is a set of changes to the software designed to add new features or resolve functionality and security issues.

Vulnerability Lifecycle

Patching delay, Patching deployment process....a real life scenario



CVE-ID	Common Vulnerabilities and Exposures (CVE) Published
CVE-2017-10271	
Description	
Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	



**Maersk case show us the need of a multilayer,
integrated approach to security**

**that includes all actors in the supply chain:assets,
people, processes and technology**



A **supply chain attack** is a cyber-attack that seeks to damage an organization by targeting **less-secure elements** in the supply network (suppliers of components, software, telco services, contractors etc..).

A chain is as strong as its weakest link!

Have you assessed what is the strength of your contractors and suppliers in term of IT security?

Table of Contents



1

What's going on in the cyber space

2

IT Security at EMSA

3

Cybersecurity Terminology

4

MaKCs e-Learning Portal

5

Have you been pwned?

MaKCs Learning Portal

<https://portal.emsa.europa.eu>

EMSA

Welcome **Serena RAMOVECCHI**

My Pages Portals Reset Logout


IMS MaKCs RuleCheck SEG THETIS

WUP MaKCs Home RuleCheck Home SEG HomePage Homepage

MY TASKS MY DOCUMENTS MY COURSES USERS

EMSA - EU

My courses

Title	
	Awareness in Maritime Cybersecurity

EMSA © 2014 [Personal data protection clause](#)

Awareness in Maritime Cybersecurity



Info Details

Description

This course has been designed to raise awareness in maritime cybersecurity.

The course will be divided into six sections, covering from basic concepts in cybersecurity, to International and European legal aspects applying to the maritime world. Also, we will introduce the latest International Maritime Organization (IMO) recommendations and guidelines on cyber risk management for shipping. At the end of the course, there will be a test of ten graded questions just to check if you understood the topic.

Availability

From: 7/30/2018

Duration (Min)

120

Learning Materials

 	Welcome and Introduction		To be started	▼ Results	▼ Info	Launch
 	Basic Concepts in Maritime Cybersecurity		Incomplete	▼ Results	▼ Info	Launch
 	International legal framework applicable to the maritime domain		To be started	▼ Results	▼ Info	Launch
 	European legal framework applicable to the maritime domain		To be started	▼ Results	▼ Info	Launch
 	Challenges		To be started	▼ Results	▼ Info	Launch
 	Final Test		To be started	▼ Results	▼ Info	Launch

MaKCs Learning Portal

<https://portal.emsa.europa.eu>

Menu Attachments Glossary Audio text

Awareness in Maritime Cybersecurity



Basic concepts in maritime cybersecurity


Menu Attachments Glossary Audio text

Menu Attachments Glossary Audio text

Basic concepts in maritime cybersecurity

Examples of maritime assets

Please, click on the active areas of the ship to see examples of maritime assets.



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

2 Bridge systems:

Because some parts of these systems are usually found on the bridge of a ship, they are also commonly referred to as "bridge systems". In this group, we would include the systems designed to help the ship navigate (in broad terms), like Global Positioning System (or GPS) receivers; Automatic Identification System (or AIS); Electronic Chart Display and Information System (or ECDIS), systems which help to keep the course of the ship (like autopilots), RADAR, non-magnetic compass (or gyro compass), dynamic positioning system (or DP) and Voyage Data Recorder (or VDR).

Menu Attachments Glossary Audio text

Menu Attachments Glossary Audio text

Basic concepts in maritime cybersecurity

Terms used in cybersecurity – Malware

Click on each term to see the definition.

Malware					
Malware	Ransomware	Adware	Virus	Scareware	
Blended Malware	Worms	Spyware	Zero Day Malware	Trojans	Cryptocurrency Miners

A computer worm is a standalone piece of malware that replicates itself without the need for any host in order to spread. Worms often propagate over networks by exploiting security vulnerabilities on target computers and networks. Because they normally consume network bandwidth, worms can inflict harm even without modifying systems or stealing data.

Menu Attachments Glossary Audio text

Menu Attachments Glossary Audio text

Exploitation techniques

Cyber-attack	Spoofing	Botnet	Spam	Jamming
Faking the sending address of a transmission to gain illegal entry into a secure system (for example, a computer) is known as spoofing. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. For example, if computer A sends a message to server B, and somehow computer C sends a message to server B saying that it is computer A.				

Menu Attachments Glossary Audio text

Table of Contents



1

What's going on in the cyber space

2

IT Security at EMSA

3

Cybersecurity Terminology

4

MaKCs e-Learning Portal

5

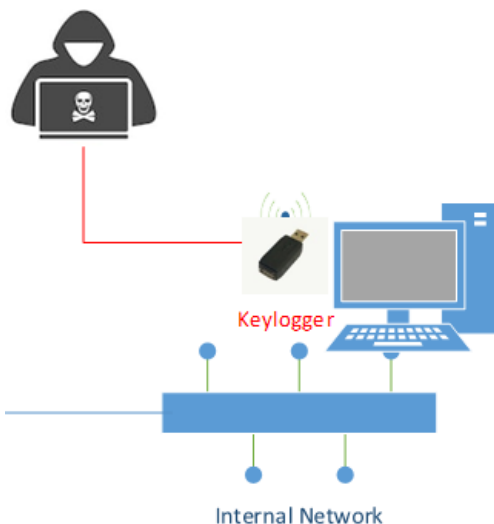
Have you been pwned?

Stealing Login Credentials is Key to Cyber criminals!

Brute Force attack

```
[http-brute 127.0.0.1:80] Trying admin/<empty> against 1
[http-brute 127.0.0.1:80] Trying admin/123456 against 12
[http-brute 127.0.0.1:80] Trying admin/12345 against 127
[http-brute 127.0.0.1:80] Trying admin/123456789 against
[http-brute 127.0.0.1:80] Trying admin/password against
[http-brute 127.0.0.1:80] Trying admin/iloveyou against
[http-brute 127.0.0.1:80] Trying admin/princess against
```

Keylogging



Dictionary attacks

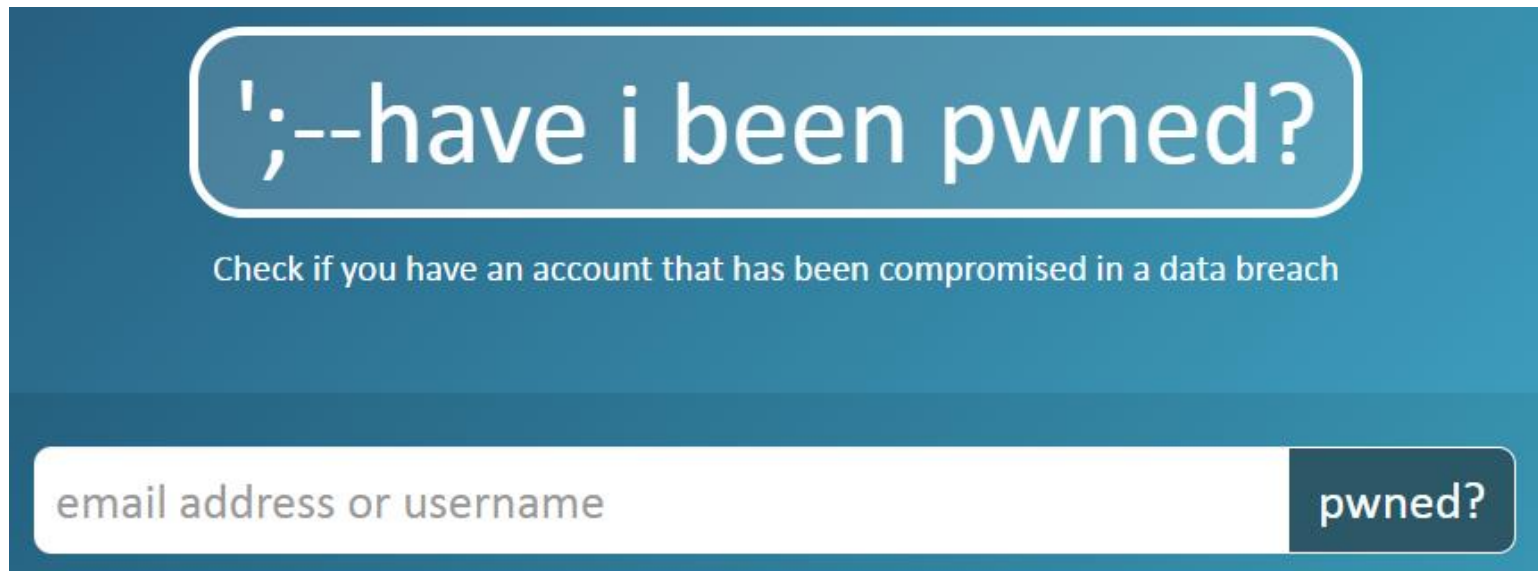
Password Reuse
is a Significant
Risk Factor for Security Breaches!

Helpful Tip



Website which checks if your email account has been compromised.

<https://haveibeenpwned.com/>

A screenshot of the 'have i been pwned?' website. The background is a dark teal color. At the top, the text '';--have i been pwned?' is displayed in a white, rounded rectangular box. Below this, in smaller white text, it says 'Check if you have an account that has been compromised in a data breach'. At the bottom, there is a white input field with the placeholder text 'email address or username' and a dark teal button with the text 'pwned?' in white.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

pwned?



 twitter.com/emsa_lisbon
 facebook.com/emsa.lisbon

