Introduction to main Cybersecurity Terms

Serena Ramovecchi
IT Security Operations

EMSA
European Maritime Safety Agency

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**.

Table of Contents

1 What's going on in the cyber space

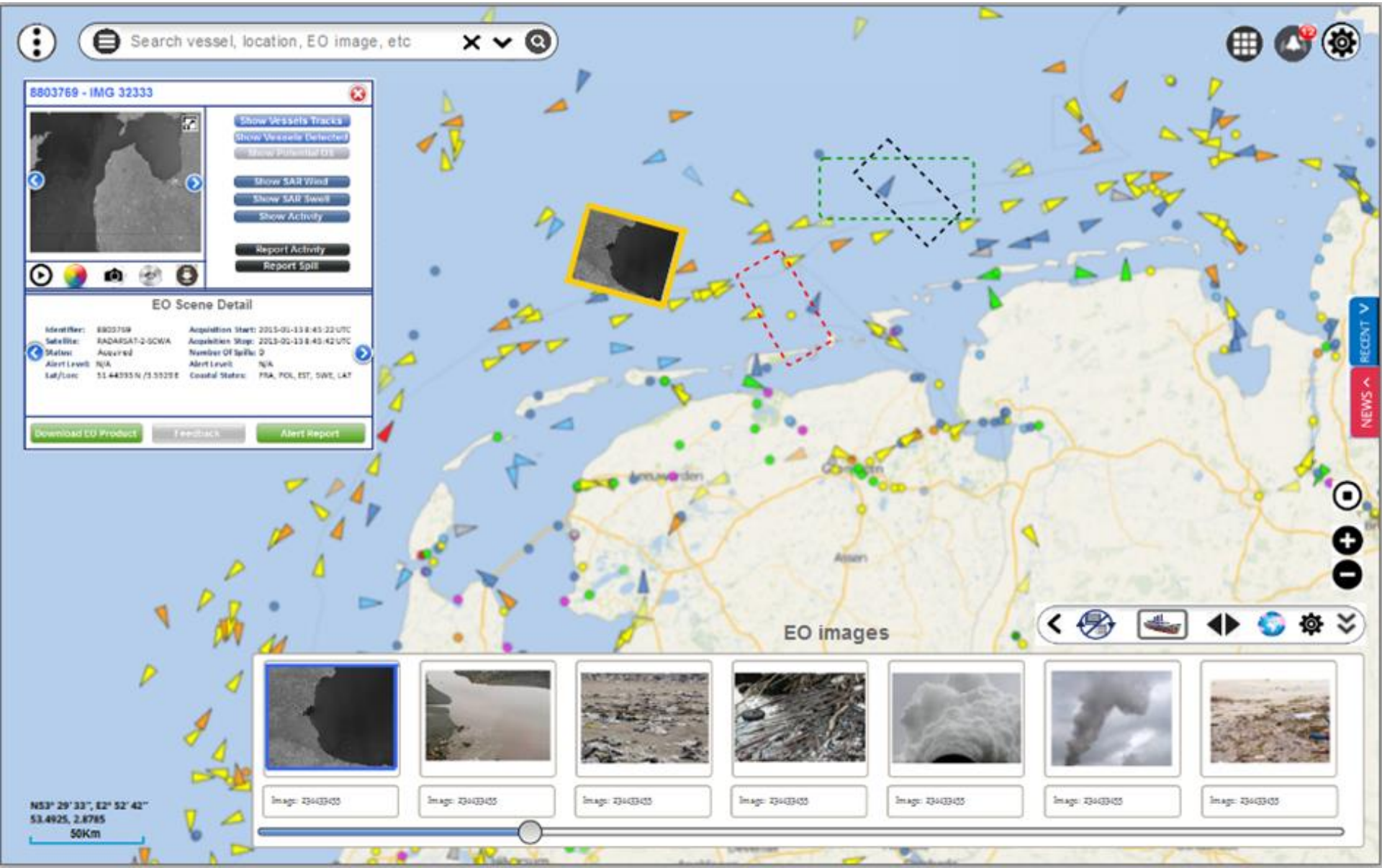
2 IT Security at EMSA

3 Cybersecurity Terminology

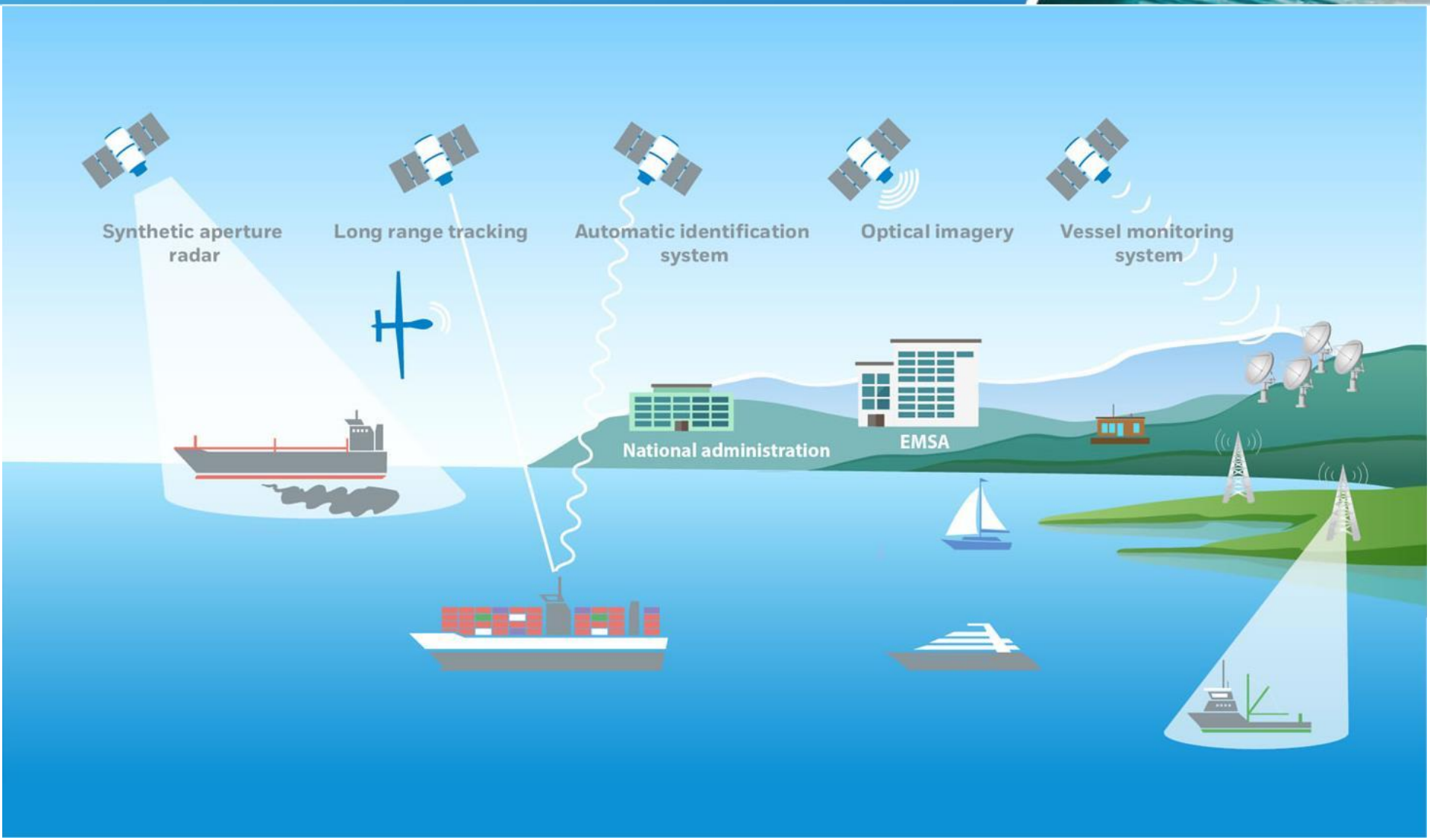
4 MaKCs e-Learning Portal

5 Have you been pwned?

EMSA maritime integrated ecosystem/1

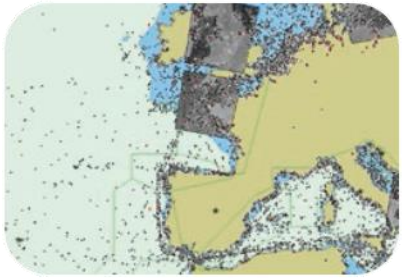


EMSA maritime integrated ecosystem/2



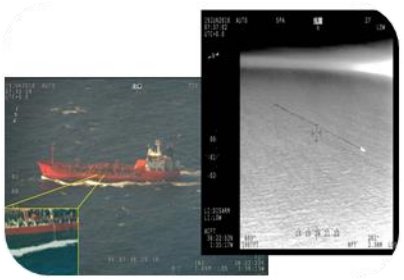
EMSA maritime integrated ecosystem/3

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

EMSA Layered IT security/1

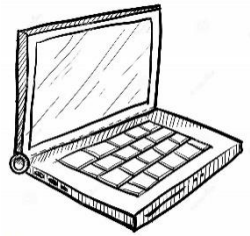
A layered Security approach

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

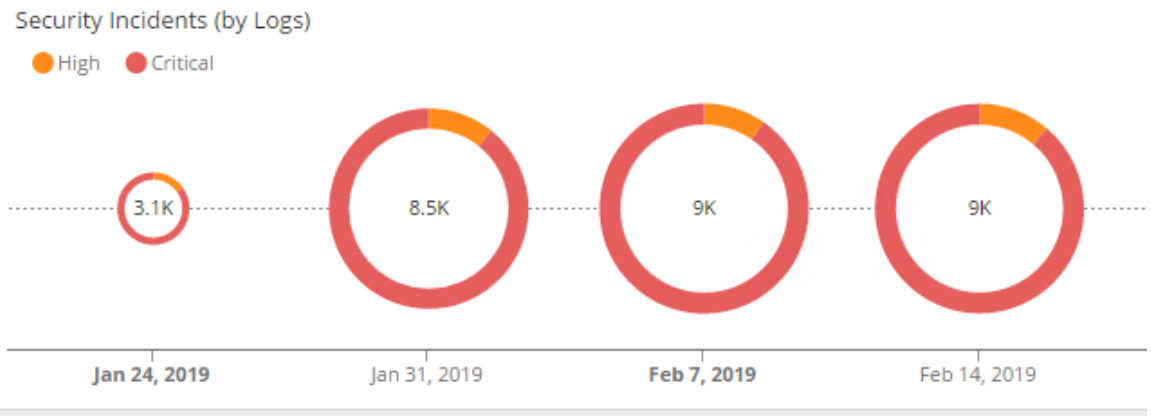
Security processes:

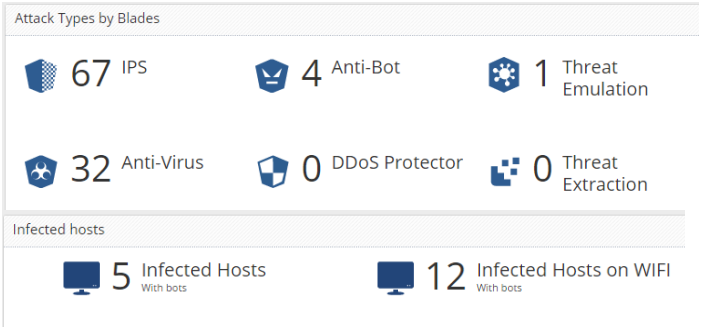
- ✓ Security Information and Event Management (Splunk) => CERT-EU
- ✓ Incident response support & forensics => CERT-EU
- ✓ Penetration testing => CERT-EU

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.





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.skybro...	Critical	IPS	148

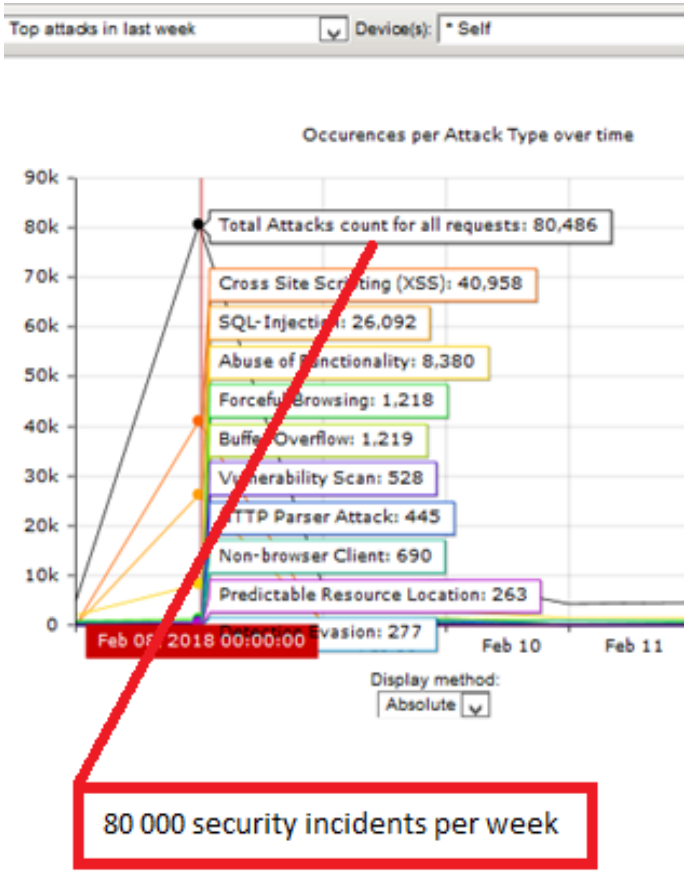
Top Destinations

Destination	Severity	Blade	Logs
EMSA_PI_91.231.2...	Critical	Multiple Blades	7.0K
no-mans-land.m2...	Critical	Firewall	89
EMSA_PI_91.231.2...	Critical	Multiple Blades	71
82.102.17.242	Critical	Firewall	44
EMSA_PI_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-2_PWGT1 ...	Critical	IPS	31
H_DMZ-1_QVLAN_...	Critical	IPS	29
EMSA_PI_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.



Top attacks:

#	Attack Type	Occurences
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

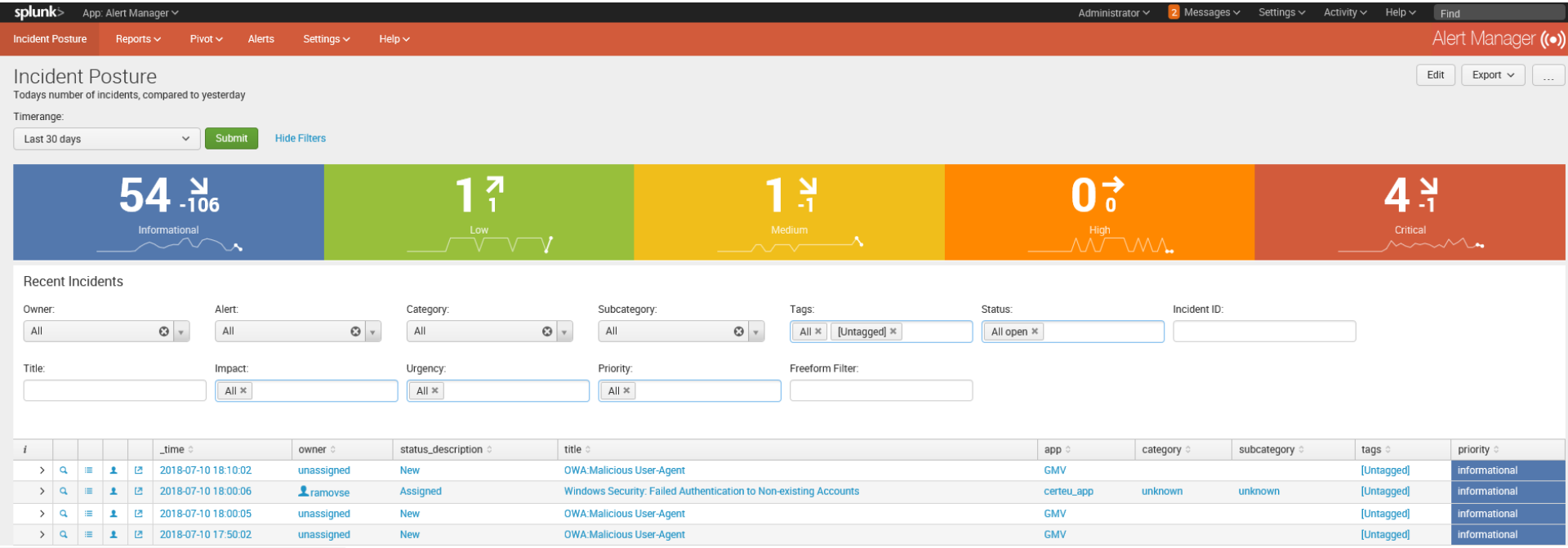
Top violations:

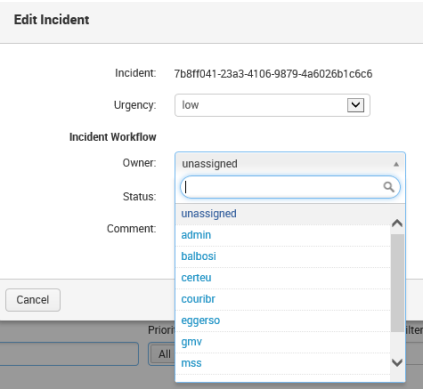
#	Violation	Occurences
1	Illegal meta character in URL	14179
2	Attack signature detected	9325
3	Illegal request length	8872
4	Illegal file type	8872
5	Illegal URL length	8750
6	Illegal meta character in parameter name	2210
7	HTTP protocol compliance failed	1701
8	Illegal query string length	1033

EMSA IT security measures/6

Security information and event management (SIEM)

EMSA adopted Splunk SIEM and built an integrated dashboard





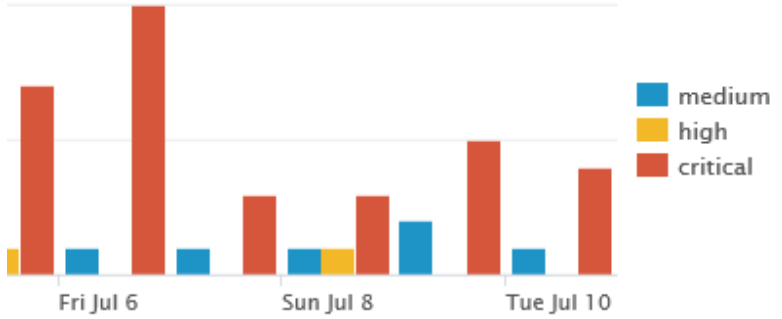


Table of Contents

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.

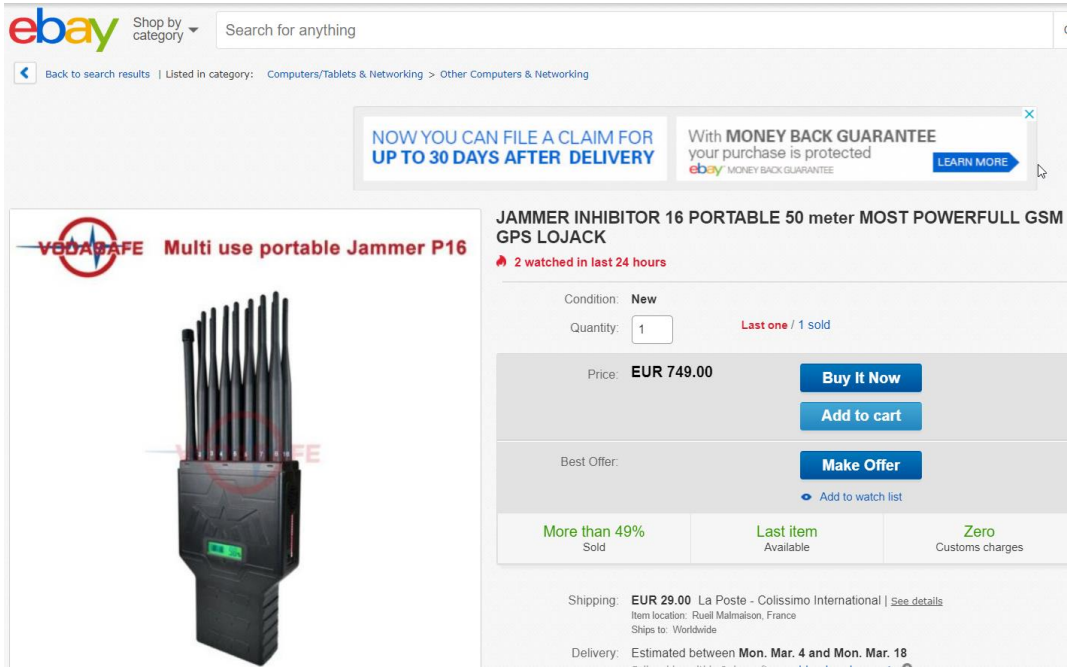
An **exploit** can be a piece of software or a sequence of commands that takes advantage of a software vulnerability to cause unintended behavior on computer software, hardware, or electronic devices.

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“.



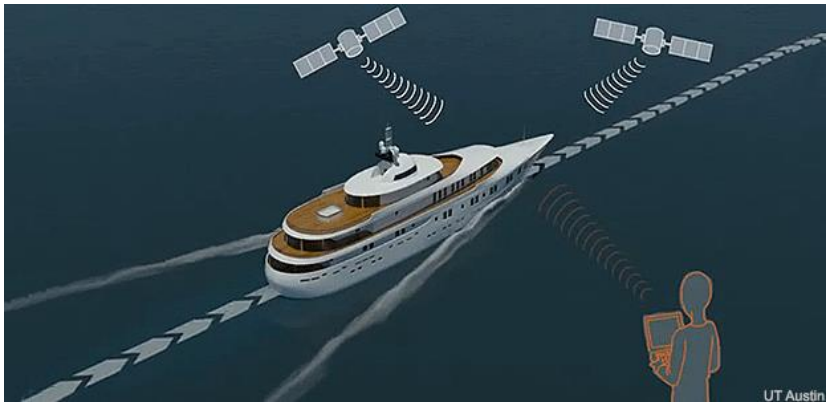
Terminology – SPOOFING

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).

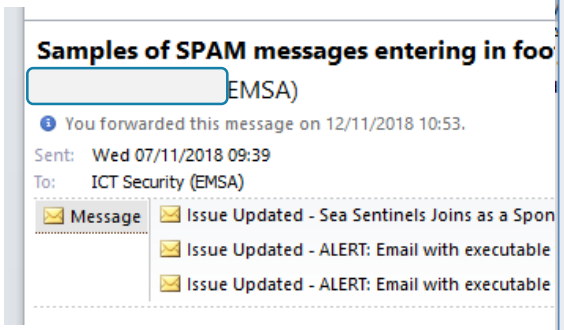
They take the form of SPAM mail, malicious Web sites, email messages **appearing to be from a legitimate source.**

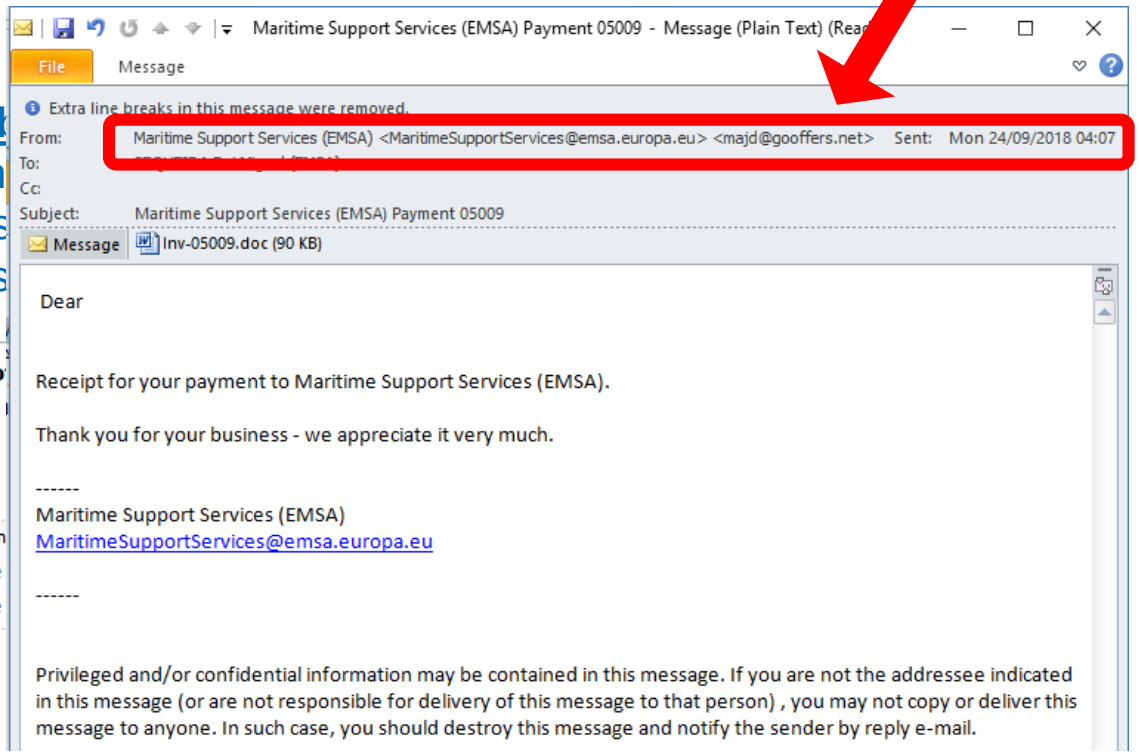
Spear phishing is a more sophisticated version of phishing in which the attack is **personalised to the specific victim**.

Spear Phishing email

With Spoofed sender

EMSA receives on a **daily b**
emails quite often imperson
service provides (workshops
operators, freight forwarders





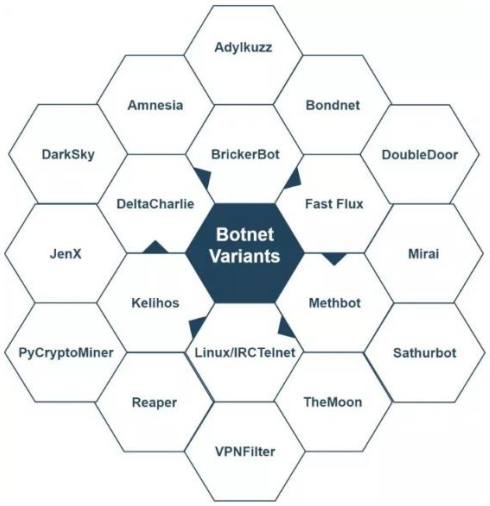
Terminology - Malware

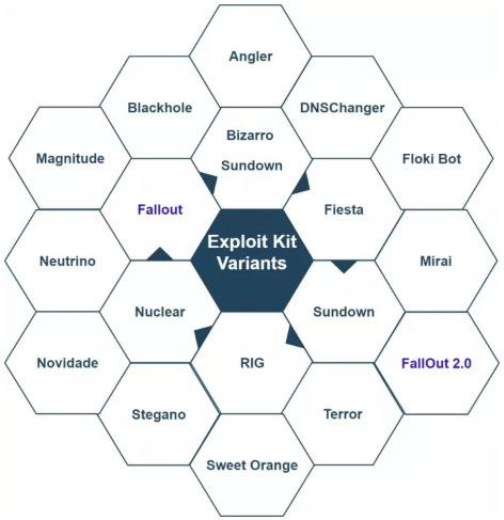
Malware is derived from the term '**Mal**icious Soft**ware**'.

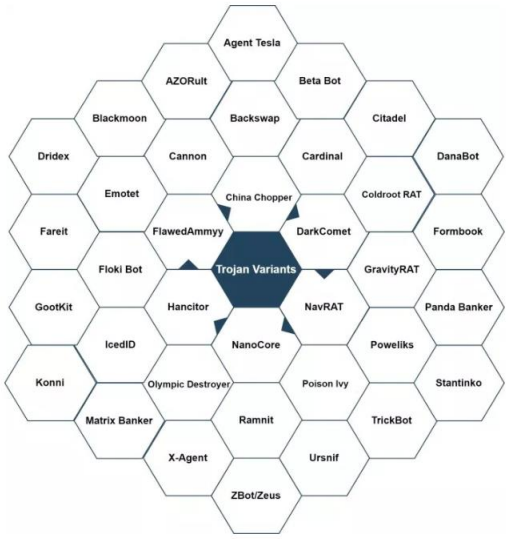
Any piece of software that performs undesirable operations such as Trojans, Viruses, Worms, and Spyware.

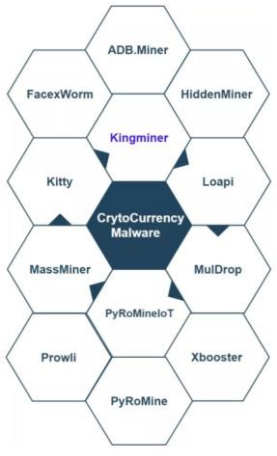
Malware families

Variants of malware families









Patch Management/1

computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

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	✓ Apply software patches as they become available ✓ 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 ✓ Identify and consider replacing any systems that cannot be updated

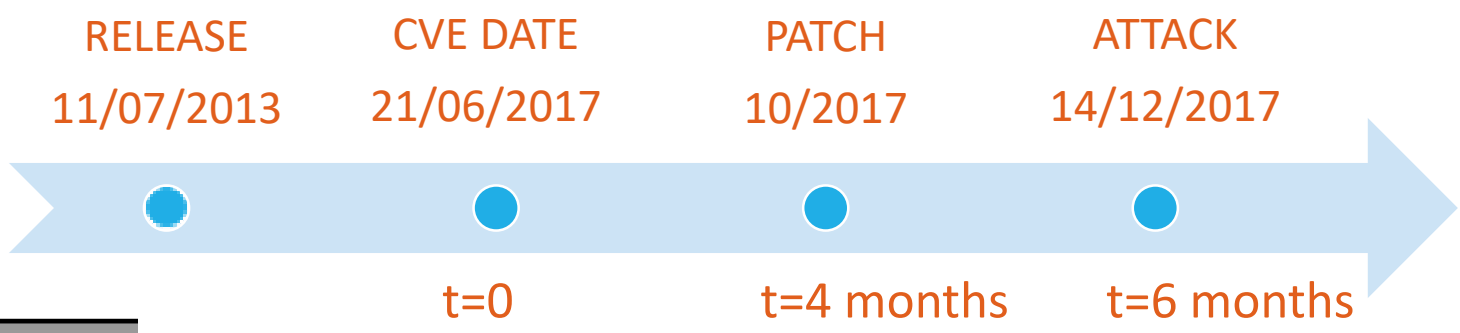
Software Patch

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

Patch Management/2

Vulnerability Lifecycle

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



CVE-ID
CVE-2017-10271

Common Vulnerabilities and Exposures (CVE) Published

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).

Patch Management/3 – Is patching enough?

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

Terminology - SUPPLY CHAIN ATTACK

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

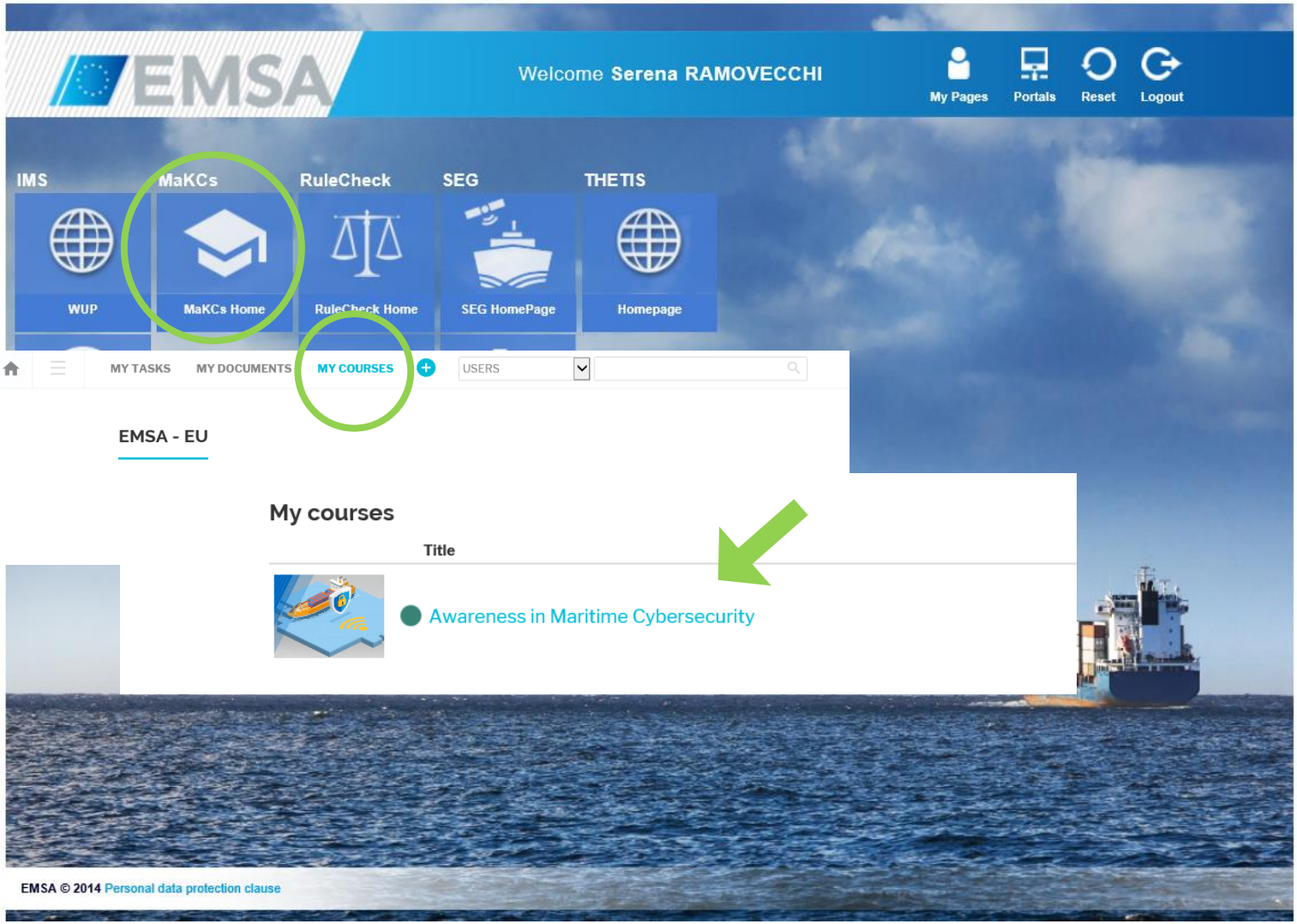
3 Cybersecurity Terminology

4 MaKCs e-Learning Portal

5 Have you been pwned?

MaKCs Learning Portal

https://portal.emsa.europa.eu



MaKCs Learning Portal
https://portal.emsa.europa.eu

Awareness in Maritime Cybersecurity

Info | Details

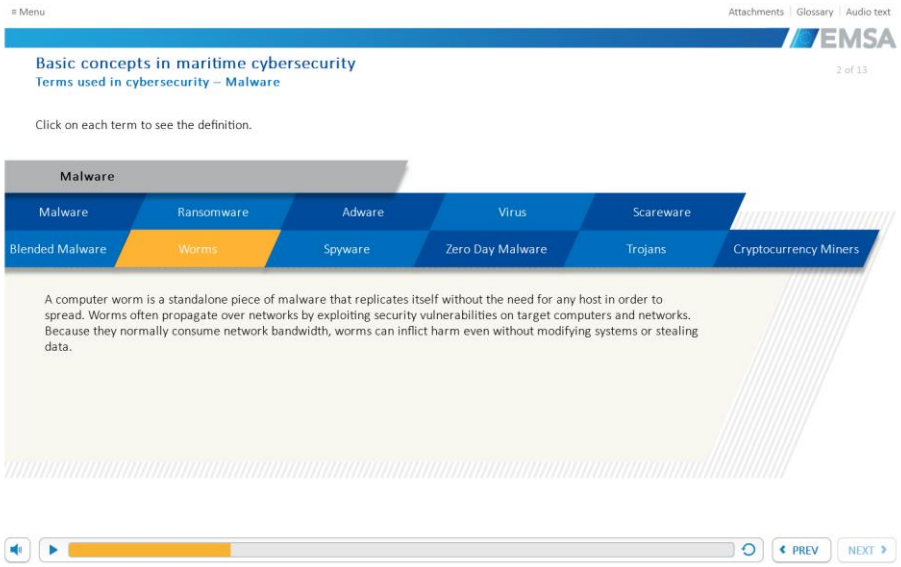
Description	This course has been designed to raise awareness in maritime cybersecurity. The course will be divided into six sections, covering from basic concepts in cybersecurity, to International and European legal aspects applying to the maritime world. Also, we will introduce the latest International 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

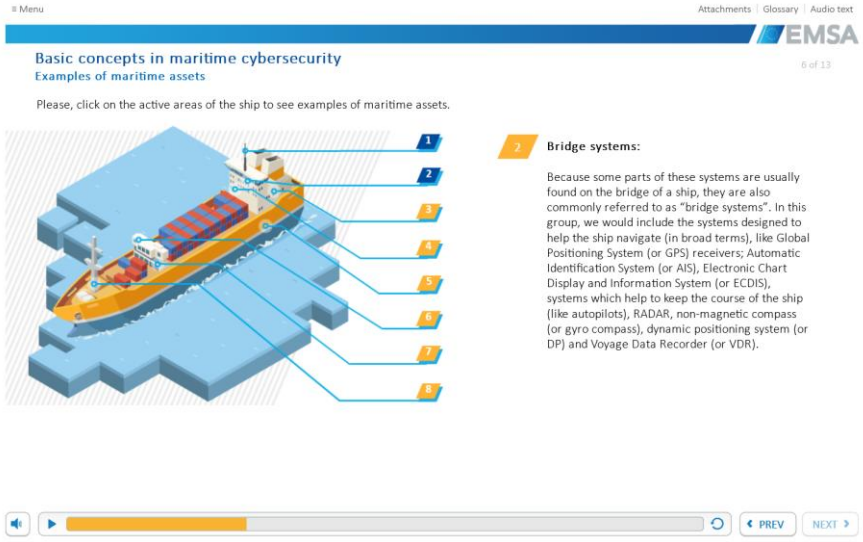
Learning Materials

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





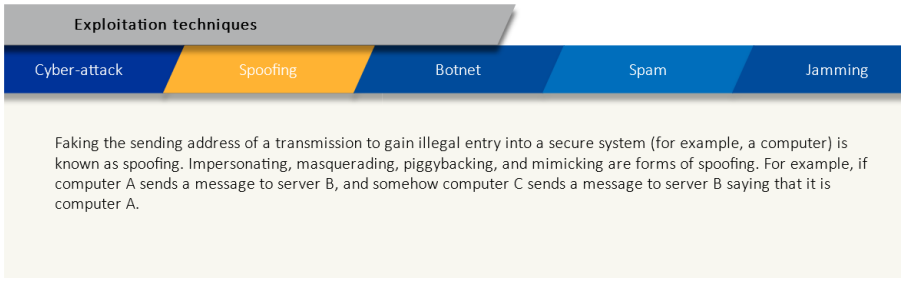


Table of Contents

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?

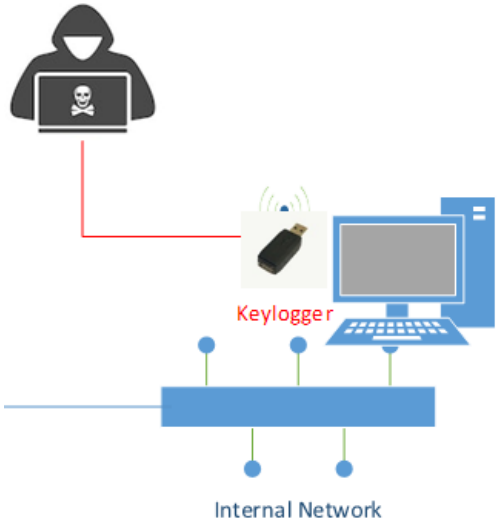
Password Vulnerabilities/1

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



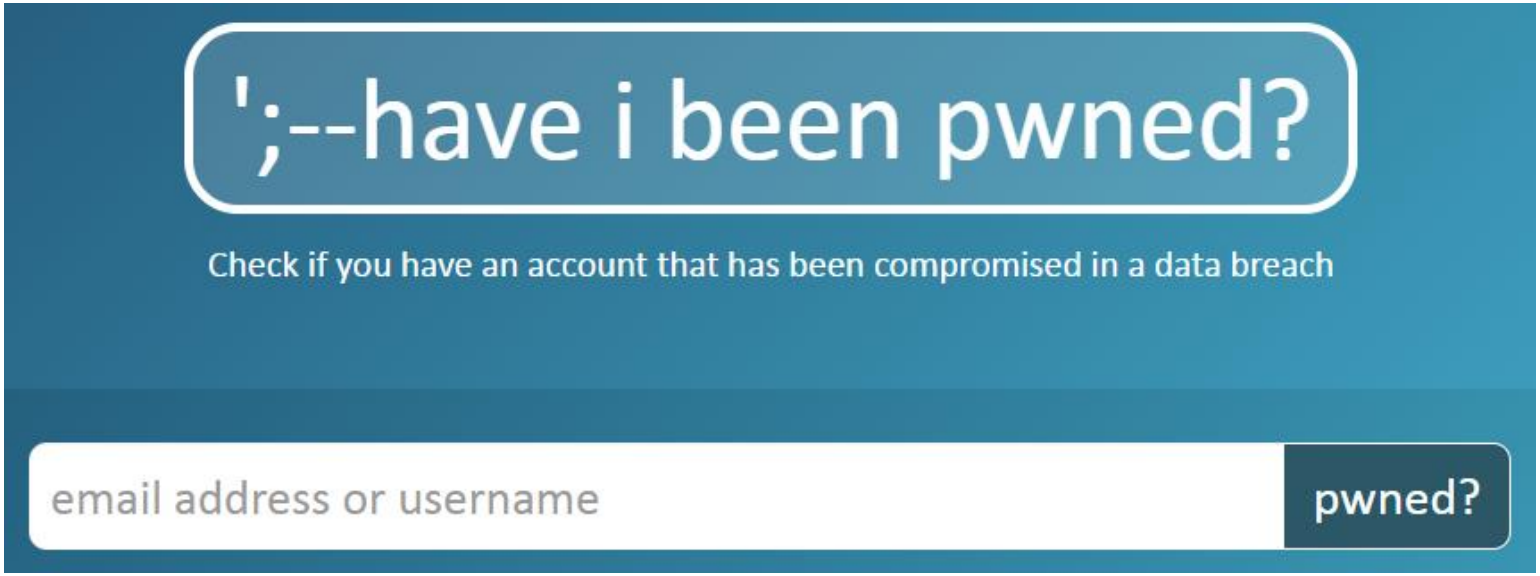
Dictionary attacks

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/



twitter.com/emsa_lisbon

facebook.com/emsa.lisbon

EMSA

European Maritime Safety Agency