# Cyber forensics case study

RUCD

20 October 2020

# Introduction

A critical cyber-incident has occurred at a *"Global Agency for Ship Tracking"* (GAST) affiliate agency. As a result, the agency suffers important reputation damage. Moreover, important clients are negotiating large penalties or are considering moving to other providers of the same or a similar service as the one that is being offered by GAST.

In chapter  you will find a brief description of the Agency, so you can better understand the wider context of the investigation.

In chapter  the design of the IT architecture of the agency is described. First an inventory of information assets is compiled, and specific threats against these assets that need to be addressed by the agency are identified. An appropriate network architecture is then introduced that should - in combination with the necessary internal processes and controls - protect the different types of information in an adequate ways and address the identified threats.

Nevertheless, an incident did occur. You are a member of a "security as a service" provider that provides a "Computer Emergency Response Team" (CERT) capacity for the Internet facing services (DMZ) and the administrative network (AdminLAN) of the agency. In chapter  the information that is at this time available about the incident is presented and your mission is defined.

# The GAST agency and its affiliates

On board a ship the watch-standing officer uses an *"Electronic Chart Display and Information System"* (ECDIS), which is a type of *"Geographic Information System"* (GIS) that is used for nautical navigation and that complies with the regulations of the *"International Maritime Organization"* (IMO) and therefore is a legally valid alternative to paper nautical charts.

Alongside its on-board radar and depth sounder, a ship's ECDIS relies on information from the *"Automatic Identification System"* (AIS) for providing situation awareness to the officer(s) on the bridge. The AIS system on-board a ship consists of a standardized VHF transceiver combined with a positioning system such as a GPS receiver, as well as other electronic navigation sensors.

Nowadays satellites equipped with AIS receivers are typically used for monitoring maritime traffic at a global scale. ORBCOMM is for instance operating a global satellite network that includes 18 AIS-enabled satellites. The AIS information is accessible to the general public through a number of free portals, like the one shown in figure 1.

AIS was originally developed for *"collision avoidance"* but since then a number of other applications are heavily relying on AIS as a source of information, such as fleet and cargo tracking, fishing fleet monitoring, search and rescue, accident

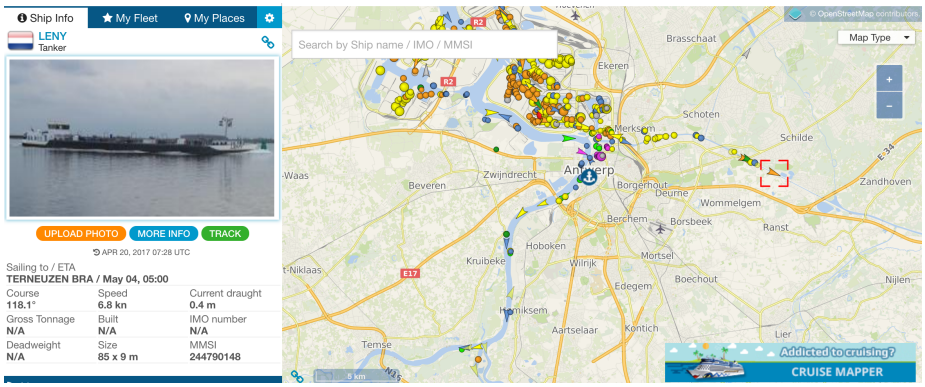


Figure 1: https://www.vesselfinder.com/

investigation, and underwater infrastructure protection. For that reason AIS is nowadays considered to be a *"critical infrastructure"*.

A number of high profile incidents in the recent past have shown that critical infrastructure is an increasingly popular target for cyber-attacks. A number of security researchers[1] have furthermore pointed out some security issues with the current AIS protocols and implementations, as is illustrated in figure 2.


Figure 2: AIS position spoofing

For the purpose of this exercise we will consider that GAST works togheter with multiple affiliates to distribute the administrative and application design

[1]Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. "A security evaluation of AIS automated identification system." In Proceedings of the 30th annual computer security applications conference, pp. 436-445. ACM, 2014.

work. The affiliate that is of imporance for this scenario works closely with GAST in the preparation, design and documentation of new projects. The affiliate is responsible for the project documentation and research for possible new applications that can be used in the GAST infrastructure.

# The IT environment

## Introduction

When the GAST agency was created, a thorough risk assessment was performed. The assets to protect and the specific threats to be mitigated are described in section .

A network architecture was designed from scratch that includes the necessary controls to address the risks that were found. Compliance with the appropriate policies and regulations has been assured and procedural controls have been developed and implemented to tie it all together. The GAST agency has established guidelines for each of its affiliates in regards to risk management and security. Because the large number of affiliates it is often difficult to impose and regulate that each different agency keeps up to standard and design their network in the most secure way possible. A brief overview of the architecture of the concerned affiliate is given in section .

## Data and threats

For the purpose of the risk analysis, two levels of confidentiality were distinguished:

- *"UNCLASS":* no special protection of the confidentiality is required
- *"RESTRICTED":* information that is to a certain extent sensitive and should not be freely accessible to the outside world
- *"CONFIDENTIAL":* information that is vital for the agency and must be protected following the pre-established guidelines and policies

Three levels of integrity were distinguished:

- *"NO_INTEGRITY":* there is no specific concern about the integrity of this information
- *"LOW_INTEGRITY":* this information is used for business purposes and therefore the integrity should be preserved
- *"HIGH_INTEGRITY":* it is essential for business operations that the integrity of this information is preserved

The following main categories of data were considered:

- *"AIS data":* the data that is obtained from the satellites and is to be processed and published to the end-users of the data. It is UNCLASS but HIGH_INTEGRITY because of its use for collision avoidance, search and rescue, accident investigation, etc.
- *"AIS processing software":* the software that is used for processing the AIS data. It is UNCLASS but HIGH_INTEGRITY since the integrity of the processed AIS data relies on the integrity of the software.
- *"administrative information":* the information that is used by for instance the HR and finance departments for administrative purposes. It ranges from unmanaged content in the team working areas, over managed content in a corporate memory area, to published content in a public information area. The corporate information is assigned organizational (e.g. HR, Finance, ...) and subject labels. It is considered to be LOW_INTEGRITY and RESTRICTED when it has not been made publicly available.
- *"the Internet":* we have no control over the data that is received from or stored in the Internet, therefore we consider this information to be UNCLASS and NO_INTEGRITY.
- The "administrative information" can initially be created inside the organization, received from the outside through incoming mail or retrieved from the outside by an internal user using a browser. It is then further processed and stored inside the organization by the appropriate departments. Frequently information will also be sent to recipients outside the organization through email or published on the corporate website.

The security meta-policy of the GAST agency can therefore be written as follows:

1. The integrity of the produced, archived, and published AIS data must absolutely be guaranteed. This of the utmost importance to the agency.
2. The integrity and confidentiality of the administrative data must be adequately protected using state-of-the-art solutions.

## Network architecture

As a result of the risk assessment performed when the agency was created, and the continuous risk management performed in the context of the "Information Security Management System" (ISMS), the current network architecture contains a large number of security controls. In this case the incident didn't occur in the main GAST network, but in the network in an affiliate of the GAST agency that deals with administration and application design. Figure 3.

Because of the the smaller size and budget of the affiliate, their network architecture is less sophisticated than that of the GAST agency. It still follows the guidelines and policies established during their parternship with goal to secure and protect vital documents.

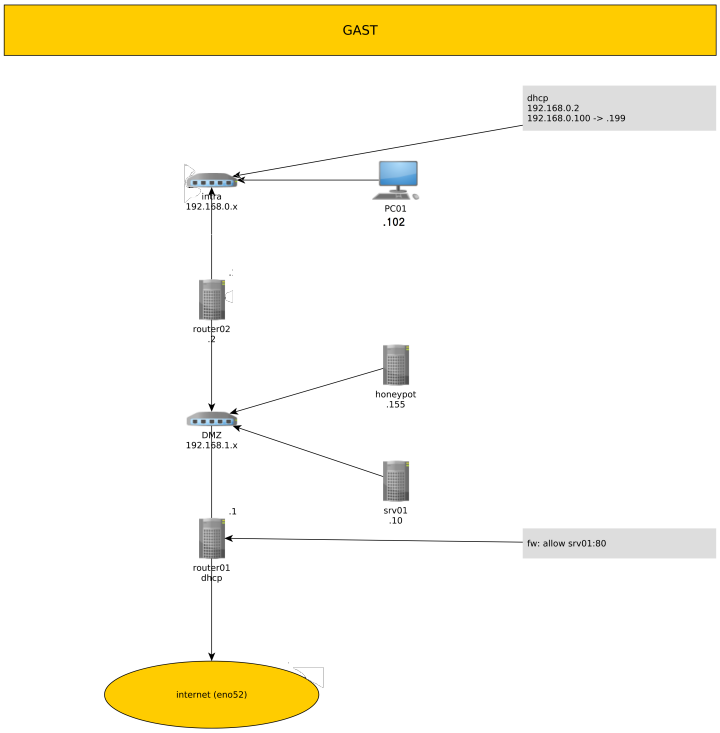


Figure 3: network architecture

Information received from the Internet is scanned for malicious content:

- incoming email messages enter through a mail server that is equipped with a commercial anti-virus software,
- web traffic is filtered through a web-proxy that is running an anti-malware solution.

There is furthermore a "Network Intrusion Detection System" (NIDS) and a "HoneyPot" (HP) deployed in the "DeMilitarized Zone" (DMZ).

# The requested digital forensic operation

## Introduction

Notwithstanding the importance given to security by the agency and its affiliates, a cyber-incident has occurred, and furthermore one with a major impact. This incident is currently under investigation.

A major part of the investigation consists of a forensic investigation of one of the Windows desktops in the administrative network. **It is your task to perform this investigation.**

You have received a *"Point of Contact"* (PoC) within the GAST agency's affiliate. You can ask him for additional information related to the host that you are examining.

## The incident

At time $t_i$ the affiliate of the GAST agency received an anonymous message from a hacker group demanding them ransom. The group let the affiliate know they had managed to obtain critical *"CONFIDENTIAL"* documents from the affiliate's network and wanted a certain amount payed by bitcoin in exchange for not releasing the documents. These documents are of cirtical importance to the currently running project inside the GAST agency and making them public will surely lead to major losses.

After an investigation of the logbooks in the network it seems that the intrusion may have occured through a Windows machine in the network. The person using the machine is charged with adminisatration work and application development. All documents and code are uploaded regularly to a central server, which serves as a repository for the affiliate agency. The connection to the server is done via SSH, using programs such as PuTTY and FileZilla.

The Windows machine that was considered dangerous was removed from the network and taken into custody. The harddisk and memory dump of the workstation were created and will be made available to you.

You can ask for additional information about this workstation by sending a request to your PoC, but take into account that it may take a while to get an answer. Furthermore, if you give a clear motivation based on forensic evidence you have already found, the agency will be more inclined to release the information you are requesting.

## Starting Point

The image of the workstation in question has been made available to you via a link to an online cloud. The technician involved in making the images had to use the cloud to upload the images because of the way the network of the affiliate was set up and the lack of possibility to connect USB devices to the machine in question. An overview of the produced hard disk image is available too. Figure 4.

Some extra information:

- The technician noted that the machine is a Windows 7 machine, configured to work in English with current European time.
- He didn't take pictures of the machine or any external devices.
- The technician arrived at the workstation at 13:50 pm
- The technician downloaded FTKImager from cloud.cylab.be and installed it at 13:58 pm
- FTKImager was ran at 14:00 pm
  - First he imaged the memory. Available at: (link)Nextcloud-Win7_memory_dump
  - Second he imaged the hard disk of the machine. Available at: (link)Nextcloud-Win7_Disk_Image
  - The Imaging process was concluded at 15:00 pm
- For any extra information contact your Point of Contact, questions should be thorough and well structured.

## Questions

The lead investigator wants you to answer the following questions:

1. give an executive summary of what happened based on your findings.
2. what is the exact time-line of the events that lead to the incident for as far as the Windows workstation is concerned ?
3. was workstation's user implicated in the incident, and if so:
   a. was he willfully committing sabotage,
   b. was he of good faith but negligent, or
   c. was he acting responsibly and could not have prevented the incident ?
4. what are the elements of evidence you have collected that support your answers to the previous questions?

```
Case Number: 01
Evidence Number: 02
Unique description: disk image windows 7
Examiner: ULB_student
Notes:

------------------------------------------------------------

Information for C:\dump\Image_Win_7:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 5,221
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 83,886,080
[Physical Drive Information]
 Drive Model: VBOX HARDDISK ATA Device
 Drive Serial Number: VBbd61b007-4c73ce08
 Drive Interface Type: IDE
 Removable drive: False
 Source data size: 40960 MB
 Sector count:    83886080
[Computed Hashes]
 MD5 checksum:    97f0c9d8036bb5ccd659806a65f3c2c4
 SHA1 checksum:   f1b74a8b83b44bf9ed4729912fd0dab61f0185f4

Image Information:
 Acquisition started:   Fri Mar 20 14:06:38 2020
 Acquisition finished:  Fri Mar 20 14:38:53 2020
 Segment list:
  C:\dump\Image_Win_7.E01
  C:\dump\Image_Win_7.E02
  C:\dump\Image_Win_7.E03
  C:\dump\Image_Win_7.E04
  C:\dump\Image_Win_7.E05
  C:\dump\Image_Win_7.E06
  C:\dump\Image_Win_7.E07
  C:\dump\Image_Win_7.E08
  C:\dump\Image_Win_7.E09
  C:\dump\Image_Win_7.E10
  C:\dump\Image_Win_7.E11
  C:\dump\Image_Win_7.E12
  C:\dump\Image_Win_7.E13
  C:\dump\Image_Win_7.E14
  C:\dump\Image_Win_7.E15

Image Verification Results:
 Verification started:  Fri Mar 20 14:38:53 2020
 Verification finished: Fri Mar 20 14:48:19 2020
 MD5 checksum:    97f0c9d8036bb5ccd659806a65f3c2c4 : verified
 SHA1 checksum:   f1b74a8b83b44bf9ed4729912fd0dab61f0185f4 : verified
```

Figure 4: Imaging overview

5. The report has to be submitted by **20th of DECEMBER, 12:00 am (midnight)**

**Write a clear investigation report, in which you answer the questions above.**

**Prepare an expert witness trial testimony. You will be given 15' and are allowed to use a pdf presentation.**