AMMITEC
Association of Maritime Managers in Information Technology & Communications

Promoting Seaworthy ICT

A cyber incident in Greek Shipping - The aftermath

Themistoklis Sardis, C.Eng., M.Sc., MBA
Head of IT, Costamare Shipping
President, AMMITEC

Who we are

•Established in 2003, AMMITEC is a non-profit organization of the Heads of ICT in the shipping sector and everybody else who is involved in maritime IT & communications.

•It aims to promote the diffusion and the most efficient usage of modern Technology and the relevant best practices in the global maritime sector and the empowerment of the ICT professionals.

•AMMITEC has more than 130 Full Members representing most major Greek shipping companies.

Cyber Incident – Round 1

• On October 30, 2021, customers of a leading shipping software vendor were attacked by the Polaris ransomware trojan.

• The malware spread through the vendor's OpenVPN based VPN with their customers. The VPN was used to support the customers directly. According to the vendor the infection started from an unspecified client and used the VPN to contaminate other clients.

• It affected Linux servers running a popular commercial DBMS.

• It stopped the DBMS daemons and encrypted the databases and user files.

Cyber Incident – Round 1

- It did not affect Windows servers and PCs, except mounted Windows filesystems.
- It did not affect any ships, as far as we know.
- Most companies returned to normal operation after restoring their backups.
- Some had corrupted backups or no backups at all.

Cyber Incident – Round 1

- The vendor contracted a major security company to do the forensics and to reversed engineer the malware to find out what it was doing.

- They held an open video conference to share their findings and issued a set of guidelines.

- The consensus at the time was that there was no data leakage.

- Everybody thought that was the end of it. But was it?

To persons responsible at XXXXXXXXXXXXXXXXXXXXXXXX,

we have secured exclusive access to backup of your Oracle database dated Sep. 2nd 2021 with size 2.1 GB (bzip compressed). To best of our knowledge database in question is used by XXXXXXXXX applications.

To claim database belonging to your company we request payment 0.5 Bitcoin (BTC).
Upon receipt of payment all copies of data will be permanently destroyed and are
guaranteed not to surface again.

Your payment address is:XXXXXXXXXXXXXXXXX

Offer is valid until October 7th 17:00 EEST.

Unclaimed databases will be offered on auction within shipping industry starting from October 10th 2022. Databases unclaimed on first auction will be
sold off to any party starting from November 7th 2022.

This message is signed with attached key (SHA1SUM):
11ecb97567edea4accc37784fe685a5c7750591e akron@serverghosts.org.public

Any further communication will be signed with same key.

Cyber Incident – Round 2

• On September 15, 2022, IT staff of the affected companies received an e-mail from a Protonmail e-mail address asking for 0.5 BTC as ransom in order not to sell or publish the content of their databases.

• The e-mail was signed by “Akron for ServerGhosts”.

• Samples of data were provided as proof together with lists of passwords.

• The author went on to attack the vendor with derogatory comments on their product quality and their security measures.

Remediation (Legal Requirements)

The company's DPO (Internal or Outsourced) should do the following:

- assess the likely risk to individuals as a result of a breach.

- inform affected individuals about a breach when their rights and freedoms are at high risk.

- notify the supervisory authority within 72 hours of becoming aware of it, even if we do not have all the details yet.

(Best practices summary according to independent bodies such as ICO UK)

Remediation (Legal Requirements)

• know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

• document all breaches, even if they don’t all need to be reported.

• report the incident to Hellenic Police Cyber Crime Unit and any other competent authority according to the law.

(Best practices summary according to independent bodies such as ICO UK)

Remediation (IT Measures)

• Reset credentials, including passwords (especially for administrator and other system accounts), but verify that you are not locking yourself out of systems that are needed for recovery.

• Preserve any evidence, in coordination with competent authorities

• Investigating the attack: create a forensic image of affected systems (or a system snapshot), create a RAM dump of the affected systems, and preserve any NetFlow or other network traffic logs.

(According to Hellenic Police / Europol guidance)

Remediation (IT Measures)

- Safely wipe the infected devices and reinstall the OS.

- Before you restore from a backup, verify that it is free from any malware. You should only restore if you are very confident that the backup and the device you are connecting it to are clean.

- Connect devices to a clean network to download, install and update the OS and all other software.

(According to Hellenic Police / Europol guidance)

Remediation (IT Measures)

- Install, update, and run antivirus software.
- Reconnect to your network.
- Monitor network traffic and run antivirus scans to identify if any infection remains.
- Re-evaluate your security policies and implement changes.
- Turn to experts for professional advice on how to deal with this or similar situations.

(According to Hellenic Police / Europol guidance)

Remediation

Never negotiate with Hackers. If your data are no longer encrypted there is no urgency to start discussions with hacker. If they do have possession of your data, you cannot be assured they will not use them against you. Your objective is to mitigate the impact.

AMMITEC's role

AMMITEC continues to support and sponsor events and discussions that address cybersecurity threats and protection methods.

- The incident was reported by our members in our closed forum less than 24 hours later.
- We organized online meetings with our members to exchange information and ideas.
- We participated as observers in the vendor's online meeting.
- In December 2021 we issued a Cyber Security Special newsletter, with contributions from our members and sponsors.
- On September 23, 2022, we organized an online discussion for our members on phase two of the incident.

Thank you

For further information you can contact AMMITEC at info@ammitec.org
Visit our website https://www.ammitec.org