Hackers target organizations in the naval and maritime industries

Introduction

Companies and infrastructure in the naval industry are under attacks, in the recent years security experts observed a growing number of attacks carried out by different types of attackers, including cybercrime syndicates and nation-state actors.

On September 20, 2018 morning, the Port of Barcelona was hit by a cyber attack that forced the operators of the infrastructure to launch the procedure to respond to the emergency. A few days later, several computers at the Port of San Diego were infected with a ransomware, the incident impacted the processing park permits and record requests, along with other operations.

The incidents raised the discussion about the security of such kind of critical infrastructure, and demonstrated that ports and other infrastructure are too vulnerable to cyber attacks.

The increased usage of computer systems for navigation, container inspection, design and manufacturing of vessels is exposing the industry to cyber threats.

Design center, ships and safe navigation, satellite communication, tracking systems, marine radar systems and automatic identification systems are just a few examples of potential targets for attackers.

According to the experts, the rapid and increasing convergence of IT and OT systems along with the diffusion of connected devices is exposing naval industry to cyber threats.

Threat actors could launch cyber attacks with both cyber espionage and sabotage purposes, to mitigate threats it is necessary to adopt a new model of cyber security based on threat intelligence and information sharing on cyber threats.

The Maritime sector is particularly threatened by disruptions due to the role of technology in global trade.

Many cyber attacks have been carried out on commercial ships, in one such incident a commercial ship on contract to the US military was the victim of a cyber attack powered by suspected Chinese military hackers. In 2012, the China-linked hackers compromised “multiple systems” on a commercial ship on contract to Transcom.

Earlier this year, the China-linked APT group Leviathan. aka TEMP.Periscope, has increased the attacks on engineering and maritime entities over the past months.

Early November, Austal, a top Australia defence firm also working with the United States Navy has suffered a serious security breach.

Unfortunately, many cyber events in the maritime industry had remained undetected or businesses didn’t want to reveal them in public.

Another worrisome aspect is that many organizations in the maritime industry are not properly conducting regular security assessments on evaluating their vulnerability to a cyber attack.

Case Study – MartyMcFly Cyberespionage Campaign targets Italian Naval Industry

A few weeks ago, malware researchers at Yoroi security firm uncovered a targeted attack against one of the most important companies in the Italian Naval Industry leveraging MartyMcFly Malware.

The victim is one of the most important firms of the defensive military grade Naval ecosystem in Italy.

The investigation started after a well-crafted email was sent to a certain office at an unnamed naval companies. The message was asking for naval engine spare parts prices, it was quite clear, written in a perfect language and detailed spare parts matching the real engine parts. The analyzed email presented two attachments to the victim:

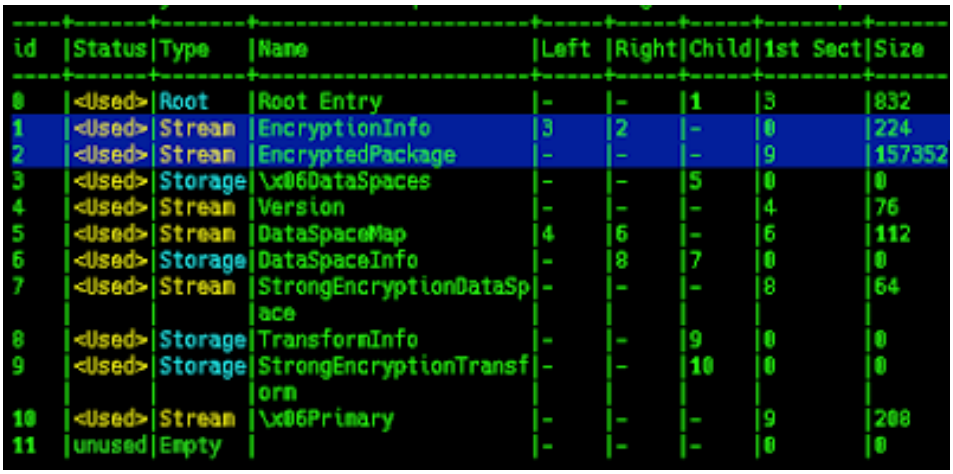
- A company profile, aiming to present the company who was asking for spare parts
- A Microsoft.XLSX where (apparently) the list of the needed spare parts was available

The attacker asked for a quotation of the entire spare part list that was reported in the attached spreadsheet. With this scheme, the attackers attempted to trick victims into opening Microsoft Excel file in attachment. Opening up the weaponized file it gets infected.

A deeper analysis of the weaponized file revealed it had an encrypted content available on OleObj.1 and OleObj.2. Both objects are real Encrypted Ole Objects where the Encrypted payload sits on “EncryptedPackage” section and information on how to decrypt it are available on “EncryptionInfo” xml descriptor. At the time of the analysis, the EncryptionInfo was holding the encryption algorithm and additional information regarding the payload, but no keys were provided.

The first challenge for the researchers was to discover how Microsoft Excel is able to decrypt such a content if no password is requested to the end user.

In another way, if the victim opens the document and he/she is not aware of “secret key” how can he/she get infected? Why the attacker used an encrypted payload if the victim cannot open it?



id	Status	Type	Name	Left	Right	Child	1st Sect	Size
0	<Used>	Root	Root Entry	-	-	1	3	832
1	<Used>	Stream	EncryptionInfo	3	2	-	0	224
2	<Used>	Stream	EncryptedPackage	-	-	-	9	157352
3	<Used>	Storage	\x06DataSpaces	-	-	5	0	0
4	<Used>	Stream	Version	-	-	-	4	76
5	<Used>	Stream	DataSpaceMap	4	6	-	6	112
6	<Used>	Storage	DataSpaceInfo	-	8	7	0	0
7	<Used>	Stream	StrongEncryptionDataSpace	-	-	-	8	64
8	<Used>	Storage	TransformInfo	-	-	9	0	0
9	<Used>	Storage	StrongEncryptionTransform	-	-	10	0	0
10	<Used>	Stream	\x06Primary	-	-	-	9	208
11	unused	Empty		-	-	-	0	0

Figure 1 - Stage1: Encrypted Content

Using an encrypted payload is quite a common way to evade Antivirus, since the encrypted payload changes depending on the used key. But what is the key?

Microsoft Excel implements a common way to open documents called “Read Only”. In “Read Only” mode the file can be opened even if encrypted. Microsoft excel asks the user a decryption key only if the user wants to save, to print or to modify the content. In that case, Microsoft programmers used a special and static key to decrypt the “Read Only” documents. The key has the value “VelvetSweatshop.”

The experts used the “key” to decrypt the content and they were able to extract more object wrapped in excel file, welcome to the stage 2.

The stage2 exposes a new object inclusion. (as shown in picture Stage2: OleOBJ inclusion). That object was crafted on 2018-10-09, but it was seen for the first time on 2018-10-12. At the time of the analysis, the extracted object is clear text and not encrypted content was find at all. The following image shows the extracted object from Stage2.

Figure 2 - Stage2: extracted Payload

The payload exploits the CVE-2017-11882 flaw by spawning the Equation Editor, dropping and executing an external PE file. We might define the Equation Editor dropping and executing as the Stage3.

The Stage 4 is represented by the GEqy87.exe executable, a common windows PE. It's placed inside an unconventional folder (js/jquery/file/…) into a compromised and thematic website. This placement usually has a double goal: (a) old school or un-configured IDS bypassing (b) hiding malicious software an into well-known and trusted folder structure in order to persist over website upgrades.

Stage4 malware is written in Borland Delphi 7. According to VirusTotal the software was "seen in the Wild" in 2010 but submitted only on 2018-10-12!

"This is pretty interesting, isn't it? Maybe hash collision over multiple years? Maybe a buggy variable on VirusTotal? Or maybe not, something more sophisticated and complex is happening out there." said Marco Ramilli, founder and CEO at Yoroi.

Figure 3 - Stage4: According to Virus Total

The analysis of the GEqy87 binary revealed that it was hiding an additional windows PE.

Stage5 deploys many evasion tricks
such as GetLastInputIn, SleepX, and GetLocalTime to trick debuggers and SandBoxes.

It makes an explicit date control check to 0x7E1 (2017). If the current date is less or equals to 0x7E1 it ends up by skipping the real behavior while if the current date is,

for example, 2018, it runs its behavior by calling “0xEAX” (typical control flow redirection on memory crafted).

The following evidence are very interesting:

- Assuming there were no hash collisions over years
- Assuming VirusTotal: “First Seen in The Wild” is right (and not bugged)

We might think that: “we are facing a new threat targeting (as today) Naval Industry planned in 2010 and run in 2018″.

The name MartyMcFly comes pretty naturally here since the “interesting date-back from Virus Total”. I am not confident about that date, but I can only assume VirusTotal is Right.

Technical details, including IoCs please are available here.

MartyMcFly is a broaden campaign

Security experts at Kaspersky Lab that analyzed the report published by Yoroi speculated the involvement of a cybercriminal group that is carrying out spear phishing attacks against various companies in several states, including Germany, Spain, Bulgaria, Kazakhstan, India, Romania, etc.

“We believe it is worth noting that well considered and carefully prepared phishing emails and remote administration tools can also be used by ‘advanced’ phishers. We believe that a cybercriminal group is behind this attack. The group conducts massive campaigns that involve sending phishing emails to various companies, some of which are critical infrastructure facilities. The objective of such groups is to steal financial data and money.” Reads the analysis published by Kaspersky.

“According to our data, the phishing documents mentioned in the Yoroi publication have been emailed, under different names, to companies located in many different countries, including Germany, Spain, Bulgaria, Kazakhstan, India, Romania, etc. The companies attacked work in a variety of areas, from supplying beans to providing consulting services.”

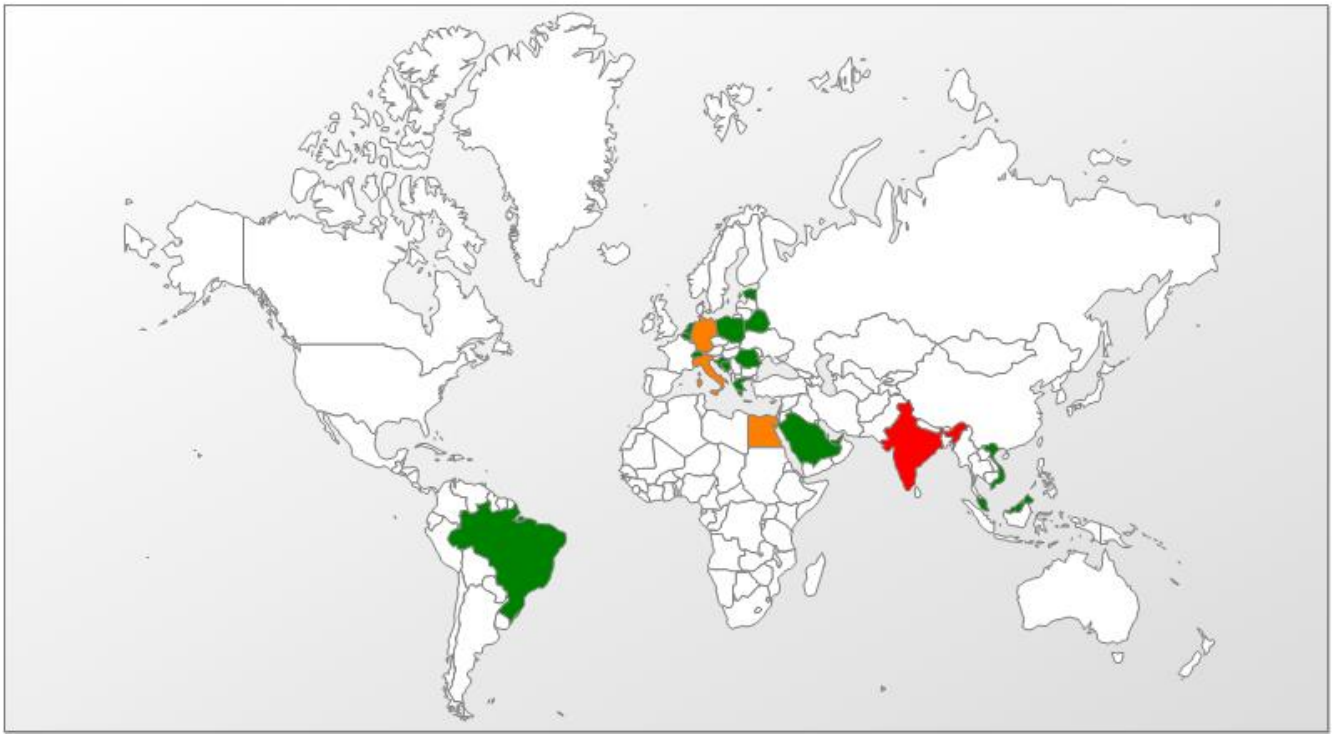


Figure 4 - MartyMcFly attacks

Researchers from Yoroi conducted further analysis on the campaign in a joint investigation with Fincantieri, one of the biggest player on Naval Industry across Europe. Fincantieri who was not involved in the previous 'MartyMcFly' attack identified and blocked additional threats targeting their wide infrastructure intercepted on during the week of 20th August 2018, about a couple of months before the 'MartyMcFly' campaign.

Yoroi Fincantieri team worked to find a link between the attacks targeting Italian Naval Industries and attempt to attribute them.

Fincantieri's security team shared with Yoroi a copy of a malicious email, carefully themed as the ones intercepted by the Yoroi's Cyber Security Defence Center between 9th and 15th October. At first look the message appears suspicious due to inconsistent sender's domain data inside the SMTP headers:

- From: alice.wu@anchors-chain.com
- Subject: Quotation on Marine Engine & TC Complete
- User-Agent: Horde Application Framework 5
- X-PPP-Vhost: jakconstruct.com

The evidence collected during the joint suggests some, still unspecified, threat actor is likely trying to establish a foothold at least into the Italian naval industry. At this time is not possible to confirm the two waves of attack have been planned and executed by the same threat actor behind the "MartyMcFly" campaign, many differences such as the distinct type of payload are relevant. However, at the same time, common elements impose to not discard the possibility of this relationship, for example, the following indicators are likely suggesting a correlations behind the campaigns:

- *personification of the service provider and satellite companies of the naval industry sector.*
- *usage of domain names carefully selected to appear similar to legit names of known companies.*
- *usage of professional sounding emails containing reference and documents carefully aligned with impersonification context.*
- *possible usage of "Microsoft Word 2013"*

Conclusions

The MartyMcFly is just the tip of the iceberg, hackers continue to target operators in the naval industry with the main intent of stealing industrial secrets. The level of sophistication of many attacks make it hard their detection, in some cases cyber espionage campaigns goes undetected for years.

A few days ago, Austal, a top Australia defence firm that works with the US Navy has suffered a serious security breach- Hackers accessed to personnel files and that it was the subject of an extortion attempt.

The only way to rapidly detect the campaigns carried out by threat actors is to share knowledge about their activities and adopt a multi-layered approach to defend organizations is this sector.

References

https://www.securityweek.com/troubled-waters-how-new-wave-cyber-attacks-targeting-maritime-trade

https://securityaffairs.co/wordpress/76623/cyber-crime/port-of-san-diego-attack.html

https://blog.yoroi.company/research/cyber-espionage-campaign-targeting-the-naval-industry-martymcfly/

https://ics-cert.kaspersky.com/news/2018/10/22/yoroi/

https://securityaffairs.co/wordpress/77600/data-breach/austal-security-breach.html

https://securityaffairs.co/wordpress/78000/malware/the-martymcfly-investigation-2.html

https://securityaffairs.co/wordpress/77195/malware/martymcfly-malware-cyber-espionage.html

https://securityaffairs.co/wordpress/76483/hacking/port-of-barcelona-hack.html

https://securityaffairs.co/wordpress/70355/cyber-crime/temp-periscope-espionage.html

https://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html

About the Author

Pierluigi Paganini is CTO at Cybaze Enterprise SpA

Pierluigi is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Professor and Director of the Master in Cyber Security at the Link Campus University. He is also a Security Evangelist, Security Analyst and Freelance Writer.
Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US.
Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines.