The European Union's efforts to tackle the phenomenon of ransomware attacks (Part II)

26/07/2022 DATA PROTECTION AND CYBERSECURITY, DIGITAL/TECH, PERSPECTIVES

Jacopo Piemonte

1. Introduction

As the transition to a digital society is accelerating in recent years, especially after the coronavirus outbreak, the expectations of the European Citizens for a safer digital environment are growing. There is then an urgent need to combat cybercrime. In a previous article published on Lexology on this topic we had started to discuss of the ransomware attacks. We had thus described the relevant phenomenon and we had pointed out the legislative and policy frameworks in place in the European Union for facing this issue. In this second contribution, reference will now be made (always in an EU perspective) to the main actors in charge of dealing with the ransomware attacks (**Chapter 2**); we will then look at the strengths and weaknesses of the current system of EU defence from this invasive form of cyber-criminality (**Chapter 3**); finally, we will try to make some recommendations for improving the security of the Citizens within the European Union in such area (**Chapter 4**).

2. The main actors on the EU scenario

As already highlighted in our previous contribution[2] the first step towards the creation and development of an EU cybersecurity ecosystem was the adoption of a cybersecurity strategy in 2013[3]. This strategy identified the achievement of cyber-resilience and the

[1] See *"The European Union's efforts to tackle the phenomenon of ransomware attacks (Part I)"*
[2] See *"The European Union's efforts to tackle the phenomenon of ransomware attacks (Part I)"*
[3] "*Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace*", dated 7 February 2013, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001.

development of industrial and technological resources for cybersecurity as its key objectives. As part of this strategy, the European Commission proposed the EU Network and Information Security directive 2016/1148 ("**NIS Directive**")[4].

We will now look at who are the main actors in charge of implementing the NIS Directive as well as the other initiatives advanced by the European Union to tackle the ransomware attacks.

2.1. The role of the Member States

In the first place, it shall be reminded that the NIS Directive has provided only that the EU countries shall put in place legal measures to boost the overall level of cybersecurity in Europe. This in essence with the intent of protecting the European critical infrastructure[5].

On the other hand, the NIS Directive has left basically to the free initiative of the Members States the regulation of aspects such as the sanctions to be imposed to the offenders in case of ransomware attacks. In addition, the NIS Directive did not impose on the EU Countries any obligation to share the information systematically with one another in case of "cross-border" ransomware attacks.

The above means that nowadays the single States of the European Union are the most important actors in the fight of the ransomware attacks. They indeed decide singularly on crucial aspects such as: *(i)* how the ransomware attacks shall be punished within their single jurisdiction; *(ii)* whether there must be any cooperation with the other Member States in case of ransomware attacks involving more countries.

2.2. The role of ENISA

It is then worthy to mention another important player which comes into consideration in the field of the cybersecurity in Europe, *i.e.* the European Union Agency for Cybersecurity ("**ENISA**"). ENISA contributes "*… to the EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow …*"[6].

ENISA was not entrusted with specific competences in the tackle of the ransomware "episodes" in the NIS Directive, but it is playing an important role *de facto* moving down the following directions:

- it has participated in the initiative "*No More Ransom*", which was the first public-private partnership of its kind created to help the victims of the ransomware. This initiative was launched in 2016 and was a public-private partnership between entities such as ENISA, Interpol and industry leaders. The project aims to:
  - "*... assist victims in the recovery of their encrypted files;*
  - *raise awareness of the ransomware threat in the public arena;*

[4] *"Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union",* available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[5] "*The NIS2 Directive: A high common level of cybersecurity in the EU*", dated 19 February 2021, available at https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)689333.

[6] Communication on the ENISA's website named "*EU cybersecurity certification framework*", available at https://www.enisa.europa.eu/topics/standards/certification. For reaching this objective, a summary of ENISA's strategy for the years 2016-2020 has been published. The following priorities were found: "*… anticipate and support Europe in facing emerging network and information security challenges … promote network and information security … support Europe in maintaining state of the art NIS capacities … foster the emerging European NIS community …*" (see ENISA's publication named "*ENISA Strategy 2016 - 2020*", available at https://www.enisa.europa.eu/publications/corporate/enisa-strategy).

- *provide direct links to the national police agencies of the EU Member States and beyond to encourage citizens to report the attacks ...*"[7].

- It publishes annually the report named "*ENISA Threat Landscape*". This publication provides an overview of threats, together with current and emerging trends. It is based on publicly available data which are based on the analysis of reports from security industry, networks of excellence, standardisation bodies and other independent institutes[8]. The "E*NISA Threat Landscape*" report focuses at length on the ransomware attacks contributing thus to raise the awareness on this phenomenon.

Finally, it must be stressed that on 23 June 2021 the European Commission laid out a vision to build a new Joint Cyber Unit[9]. The Joint Cyber Unit will be a new body (with its own resources and offices) intended to provide full support to ENISA in ensuring an EU coordinated response to large-scale cyber incidents and crises such as the ransomware attacks. This new initiative is an important step which will allow ENISA (together with the Joint Cyber Unit) to further achieve a higher common level of cybersecurity within the European Union[10].

2.3. The role of the Council

Finally, it is worth to be mentioned also the role played by the Council in tackling the cyber-crimes (and thus the ransomware attacks).

In this regard, in our previous contribution on this topic[11] we had reminded that the EU tried to reinforce its global response to the cyber-attacks (including ransomware) by establishing a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the so called "**Cyber Diplomacy Toolbox**")[12]. This framework basically allows the EU and its Member States (by way of an "initiative" to be taken by the Council) to use all necessary measures "*... to prevent, discourage, deter and respond to malicious cyber activities* [and thus also to the ransomware attacks] *targeting the integrity and security of the EU and its member states ...*". In particular, the Cyber Diplomacy Toolbox gives the possibility to the Council to impose "*... sanctions on persons or entities that are responsible for cyber-attacks or attempted cyber-attacks, who provide financial, technical or material support for such attacks or who are involved in other ways ...*"[13].

It is noticeable that, based on the Cyber Diplomacy Toolbox, the Council has been able to impose restrictive measures

[7] Communication on the ENISA's website named "*#Nomoreransome*", available at https://www.enisa.europa.eu/topics/cybersecurity-education/nomoreransom/nomoreransom.
[8] See ENISA's website where it is possible to download the ENISA Threat Landscape Reports, available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.
[9] European Commission's press release, dated 23 June 2021, named "*EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents*", available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088.
[10] ENISA's press release, dated 23 June 2021, named "*EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit*", available at https://www.enisa.europa.eu/news/enisa-news/eu-boost-against-cyberattacks-eu-agency-for-cybersecurity-welcomes-proposal-for-the-joint-cyber-unit.
[11] See *"The European Union's efforts to tackle the phenomenon of ransomware attacks (Part I)"*
[12] "*Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*", dated 7 June 2017, available at https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.
[13]See https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

against certain individuals and entities responsible for or involved in the ransomware-attacks publicly known as "*WannaCry*" and "*Operation Cloud Hoppe*"[14]. The sanctions imposed to the entities involved included severe measures such as the travel ban and the assets freeze.

Of course, it must not be forgotten that it is not particularly simple for the Council to take collective actions (such as the ones indicated above) based on the Cyber Diplomacy Toolbox. And indeed, the European Union's decision-making process to be activated in these cases is the same one to be applied for the foreign policy matters, requiring thus the unanimous decision of all EU governments. This is certainly a very high threshold not easy to be reached[15]. It follows that it is rather complicated for the Council to issue sanctions based on the Cyber Diplomacy Toolbox.

3. What are the strengths and weaknesses of the European framework?

Being understood all the above, we will now try to summarize the main strengths and weaknesses of the European Union framework put in place for fighting the phenomenon discussed.

3.1. The strengths

In the first place, it must be noted that the implementation of the NIS Directive and of the Cyber Diplomacy Toolbox has been very important at least in raising awareness in the European States regarding the cyber-criminal activities such as the ransomware attacks.

The NIS Directive has indeed given an incentive to the Member States to increase their cybersecurity capabilities for protecting themselves from these forms of criminality.

The Cyber Diplomacy Toolbox has, in turn, granted the possibility to sanction directly certain entities and individuals which have committed, *inter alia*, ransomware crimes.

3.2. The weaknesses

On the other hand, both the legal frameworks mentioned above have their downsides.

The NIS Directive resulted in fragmentation at different levels across the internal market (given that for example such directive did not provide for a system of harmonized sanctions to be applied in the European Countries). In addition, the ENISA has not been given enough powers to help the EU Member States to tackle issues such as the ransomware attacks.

Further, the Cyber Diplomacy Toolbox requires a too burdensome process for dealing with the cyber-crimes. Indeed, as we have seen above, the Council can focus just on the "major events" and, in any case, the unanimity of the EU Countries is required to take actions against offenders committing for example ransomware attacks.

3.3. Conclusions: possible improvements to be suggested?

As it may be appreciated the phenomenon of the ransomware attacks is quite a complicated one. In the EU the battle is "open" and efforts are indeed spent by the different stakeholders involved to combat this issue effectively.

On the other hand, there is certainly room for improvement.

Based on the above findings (and on what has been discussed in the other article published on Lexology

[14] Press release, dated 30 July 2020, named "*EU imposes the first ever sanctions against cyber-attacks*", available at https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.
[15] Ivan, Paul (2019) "*Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox*", 18 March 2019, available at http://aei.pitt.edu/97071/1/pub_9081_responding_cyberattacks.pdf.

on this topic[16]), we will then try to suggest some recommendations aimed at tackling the ransomware phenomenon in a more efficient way within the European Union. In this regard it is noted the following:

- In the first place, it is necessary to renovate the legal normative framework applicable to all the Member States in the cybersecurity field. The proposals put forward by the Commission in 2020 for the revision of the NIS Directive certainly goes in the right direction[17]. Pushing towards the introduction of more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU (as indeed suggested in the proposed NIS2 Directive) would certainly be very helpful in tackling the ransomware phenomenon. This would indeed at least allow to prevent criminals from taking refuge in countries where the lack of legislation "could make their lives easy". On the other hand, in the near future it may be even worthy to start to consider elaborating a specific European directive (or even a regulation) limited only to the ransomware issue. This topic, as highlighted above, is absolutely one of the most critical and crucial nowadays. Hence a specific set of rules fixed at European level on this matter could be considered as very useful for an effective resolution of this issue in the EU.
- In the second place, hopefully it shall be boosted as soon as possible the involvement of ENISA in facing the cybersecurity incidents and more in particular the ransomware attacks. The introduction of the support of the Joint Cyber Unit to ENISA goes in the right direction. On the other hand, more powers shall be conferred to ENISA also in the effective support to the Member States in dealing with such events. For this purpose, it is reasonable to envisage and confirm the need of "*... a larger budget, more staff and a permanent mandate for ENISA, together with an enhanced role to provide, not only expert advice, but also to carry out operational and coordination tasks ...*"[18].
- Thirdly, the European Union shall take full cognizance that when a problem goes global, it requires global and coordinated responses. In this regard, the introduction of the Cyber Diplomatic Toolbox was certainly helpful (especially for targeting the most relevant cyber-attacks). On the other hand, the EU shall continue to cooperate also with international organizations or with the other States which are key in the cybersecurity "arena" (*e.g.,* United States and China) to set a global policy for fighting issues such as the ransomware attacks in the most efficient way as possible.

Finally, apart from the above actions and recommendations (which are indeed directed at bolstering the fight of the specific kind of cybercrime at subject matter) one final consideration is worthy to be made.

It shall indeed not to be forgotten that issues such as the ransomware attacks in many cases can be avoided at the very beginning

[16] See *"The European Union's efforts to tackle the phenomenon of ransomware attacks (Part I)"*
[17] European Parliament's document, dated November 2021, named "*The NIS2 Directive A high common level of cybersecurity in the EU*", available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.
[18] European Parliament's document, dated March 2019, named "*ENISA and new EU Cybersecurity Act*" available at https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/625160/EPRS_ATA(2019)625160_EN.pdf.

explaining to the “users” how to avoid them.

It is thus of the utmost importance that are continued to be promoted specific initiatives and “dialogues” with the EU Citizens regarding the common ransomware attack scenarios with the effect of “*… aiming to raise awareness and share good practices and practical recommendations …*”[19]. This with the final goal to eliminate the issue even before the crime is perpetrated counting on the fact that the EU Citizens (if properly “trained”) should be able not to fall into the traps posed on their way by the cybercriminals.

[19] Communication on the ENISA’s website named “#*Nomoreransome*”, available at https://www.enisa.europa.eu/topics/cybersecurity-education/nomoreransom/nomoreransom.

Jacopo Piemonte

ASSOCIATE

j.piemonte@dejalex.com

+39 02 72554.1

Via San Paolo 7
20121 - Milano

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com