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

21/07/2022 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 two different articles we will address, in particular, the surging phenomenon of the ransomware attacks and how this issue is being tackled within the European Union. In this contribution we will introduce the relevant phenomenon (**Chapter 2**). In addition, it will be assessed what are the legislative and policy frameworks in place in the European Union for facing this issue (**Chapter 3**).

2. The ransomware attacks

Ransomware can be described as a type of malware (like viruses, trojans, *etc.*) that "*… infect the computer systems of users and manipulates the infected system in a way, that the victim cannot (partially or fully) use it and the data stored on it. The victim usually shortly after receives a blackmail note by pop-up, pressing the victim to pay a ransom (hence the name) to regain full access to system and files …*"[1].

The criminality resorts to different types of tactics to achieve their finalities. Ransomware attacks have the primary goal of making monetary gains by way of unlawful means. Ransomware typically encrypts target files and displays notifications, requesting payment before the data can be unlocked. Ransomware demands are usually in the form of virtual currency, such as bitcoin. This because

[1] Definition of "ransomware" available at https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware.

these types of payments are difficult to be tracked[2].

Ransomware attacks have certainly a global impact.

A report issued on 2021 has revealed that "*… the frequency and the* complexity *of ransomware attacks increased (by more than 150% in 2020 …"* such that ransomware can now be defined as *"… one of the greatest threats that organizations face today regardless of the sector to which they belong …*"[3]*.*

The above findings speak volumes on how this issue is serious and of concern for all the world. Consequently, it does not come as a surprise that it has been clearly recognized nowadays that ransomware is "*… a prime item in agendas for meetings on strategy among global leaders …"*[4].

In the fight against ransomware, several challenges need to be addressed. One of the main issues results in the lack of coordination and collaboration between the agencies and the authorities all over the world. There is indeed a lack of legislation in many countries that clearly criminalises ransomware attacks[5].

This problem holds true also for the European Union given that: *(i)* it is made of different Member States which, in some cases, have different internal law frameworks when it comes to cybersecurity and modalities to tackle the ransomware "problem"; *(ii)* the issue must be addressed also with reference to the States which are external to the European Union (in which the ransomware phenomenon flourishes).

3. How the European Union is dealing with the issue

Considering all the above, in the following chapter we will look at how the European Union is trying to face the ransomware attacks.

3.1. The European Union legislative interventions

The first step towards the creation and development of an EU cybersecurity ecosystem was the adoption of a cybersecurity strategy in 2013[6]. This strategy identified the achievement of cyber-resilience and the 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**")[7].

In particular, the NIS Directive[8] sets out that the EU Member States must have certain national cybersecurity capabilities and that there shall be a cooperation in the exchange of information amongst the same EU countries. Moreover, according to the NIS Directive, the EU Member States shall promote a culture of security across sectors very relevant for the EU and which rely on ICTs such as *"… energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure …*"[9].

[2] "*Ransomware: Current Trend, Challenges, and Research Directions"* October 2017, Conference: World Congress on Engineering and Computer Science (WCECS 2017) At: San Francisco, USA, author Segun I. Popoola of the Manchester Metropolitan University.

[3] ENISA Threat Landscape 2021 available at https://www.enisa.europa.eu/publications/ransomware.

[4] ENISA Threat Landscape 2021 available at https://www.enisa.europa.eu/publications/ransomware.

[5] ENISA Threat Landscape 2020 available at https://www.enisa.europa.eu/publications/ransomware.

[6] "*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.

[7] *"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.

[8] The NIS Directive has been adopted in 2016. After its adoption each EU Member State has started to adopt national legislation for transposing such Directive. The national transposition by the EU Member States was concluded on 9 May 2018 (see https://www.enisa.europa.eu/topics/nis-directive).

[9] https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

It is interesting to note that the NIS Directive limited to provide for measures by way of which the EU States shall increase their attention when it comes to cyber-attacks. On the other hand, it did not envisage a common and specific framework (for example in terms of sanctions to be applied) for tackling cyber-crimes (such as the ransomware attacks).

That is probably why in June 2017, 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**")[10].

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 ...*" [11].

Finally, also in the attempt to reinforce the attack to the malicious cyber activities (such as the ransomware) a revised version of the NIS Directive (to be named "**NIS2 Directive**") has been proposed by the European Commission in 2020. In particular[12]:

- it has been suggested to push towards the introduction of more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.
- It has then been envisaged to establish a framework for better cooperation and information sharing between different authorities and Member States creating a European vulnerability database.

The proposed NIS2 Directive though is now still under discussion[13].

3.2. The European Union policy interventions

The European Union has then dealt with the issue of the ransomware attacks also pursuing specific policies of international cooperation on this topic.

In particular, the European Union has soon realized that this problem was global and that it was thus necessary to tackle it also involving the other stakeholders.

That is why the European Union signed for example a joint EU-U.S. statement for working together in the fight against ransomware "*… through law enforcement action, raising public awareness on how to protect networks as well as the risk of paying the criminals responsible, and to encourage those states that*

[10] "*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/.

[11]See https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

[12] 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.

[13] In particular, the Committee on Industry, Research and Energy (to which the file was assigned by the European Parliament) adopted on 28 October 2021 its report on the revised version of the NIS Directive. The inter-institutional negotiations are now ongoing (see https://www.europarl.europa.eu/thinktank/it/document/EPRS_BRI(2021)689333).

turn a blind eye to this crime to arrest and extradite or effectively prosecute criminals on their territory …"[14].

Moreover, the EU takes part on a regular basis in international summits (together with important partners such as U.S.A., India and Australia) where it is discussed how to counter this "plague" on a global scale[15].

4. Conclusions

As we have seen above, the current framework set by the European Union to tackle the ransomware attacks is rather complex and worthy to be carefully assessed.

In a subsequent article to be published soon on Lexology, reference will then be made to the main actors in charge of dealing with such phenomenon in Europe and to the strengths and weaknesses of the current EU system of defence against this invasive form of cyber-criminality.

[14] "*Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial Meeting*", dated 22 June 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/06/22/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/.

[15] https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/.

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