Alessandro Pigoni (972871)

The harder they fall: A multilevel analysis of the Kaseya supply chain ransomware attack

Abstract

The digitalized world represents a perfect case of modern Goliath. A deeply interconnected system that lays itself open to an ever-increasing number of vulnerabilities that can be exploited with criminal intents. Within the *mare magnum* of malicious software used in the cyber domain, the category of ransomware has gained a singular interest among cybercriminals. This contribution is going to give an account of the recent spike in ransomware attacks targeting supply chains by presenting a multilevel analysis of the Kaseya VSA attack which embodies the quintessence of the current cyber-threat landscape. Based on these findings, the research is going to formulate guidelines as regards strategic measures to be taken at the national level so as to ensure the preparedness of a countrywide system for similar forthcoming threats. With reference to the Italian case, this paper is going to address the establishment of the National Cybersecurity Agency to assess whether this could represent the first step towards the right direction of lowering the overall domestic vulnerability to supply-chain attacks.

1 Introduction: New trends in the cyber-threat landscape?

Humans have generated an ever-expanding interconnected cyber domain that defies national borders. Nonetheless, alongside the evolution of this modern Goliath, the number of digitalized David able to defy it grew simultaneously, with most of them being exploited with criminal intents. Within the broadening cosmos of malicious software adopted in the cyber domain, the category of ransomware has recently gained a peculiar interest among cybercriminals. The term *ransomware* is generally understood to mean an extortion software that encrypts files contained within a device or system until a ransom, from the victim, has been paid[1]. This type of malicious software has become the preferred tool in many cyberattacks targeting individuals, small businesses, large multinational corporations, and even the IT system of a whole Italian region as highlighted by the recent attack at the *Centro Elaborazione Dati (CED)* of Lazio. The rise in the observed number of ransomware attacks may be explained by several factors. Nonetheless, a fundamental catalyst for this increase is undoubtedly the COVID-19 global pandemic and the relative major shift towards smart-working, which led to higher online accesses. In fact, according to the annual report by Bitdefender *2020 Consumer Threat Landscape Report*, between 2019 and 2020 there has been a surge of 485% in the number of labelled ransomware attacks with almost two-thirds of them occurring within the first eight months of 2020,

[1] Kaspersky, (n.d). Ransomware – definition, prevention, and removal [online*]. Kaspersky*. Available at: https://www.kaspersky.com/resource-center/threats/ransomware [Accessed 11 August 2021].

during the pike of the pandemic[2]. As the number of vulnerable devices sharing confidential information within unsecured networks steadily grew, so did the opportunity cost for cybercriminals to infect these devices to obtain access to profitable sources of data[3]. The profitability of these attacks is positively related to its propagating effect, with more infections meaning more potential ransoms to be collected by the criminals. Not surprisingly, a recent tendency in the landscape of cyber-threats is the adoption of these tools within supply chain attacks to generate considerable capital and reputational losses on a global scale[4]. As a matter of fact, according to the annual report of the European Union Agency for Cybersecurity (ENISA), the complexity and impacts of these cyberattacks have experienced an upward trend since the beginning of 2020, parallel to the one observed for ransomware attacks[5]. Within the variety of reported incidents, a recent cyber-attack has brought to the forefront of academic debate the vulnerabilities and risks related to supply chains. The case study at the center of this report is the ransomware attack targeting the service provider Kaseya and the supply chain of its server administrator software Kaseya VSA. The choice of this particular case is associated with the intent of this research. The aim of this paper is to underline the mandatory strategic measures to be taken at the national level to ensure the preparedness of the Italian countrywide system in the face of similar forthcoming threats. So as to address this multifaceted subject, this paper is going to be structured as follows. The first section begins by providing a comprehensive overview of the cyber-attack: the actors involved, technical analysis of the cyber-kill chain, the strategic measures adopted in aftermath of the incident to limit its potentiality, and an investigation as regards the geopolitical concerns posed by similar attacks. A second section is going to propose some useful recommendations to develop a more advanced and comprehensive plan of action for handling similar cyber-threats and to investigate whether the Italian cyber-security strategy is up to date as regards the current threat landscape. For reasons of space, the extensive analysis and evaluation of the structure of the newly constituted Italian National Cybersecurity Agency (ACN) within the *Piano Nazionale di Ripresa e Resilienza* (PNRR) are not dealt within this paper. The last section restates that, notwithstanding some minor concerns, the creation of a unified institution concerning national cyber-security and responsible for ensuring the resiliency of the countrywide

[2] Bitdefender, (2020). *2020 Consumer Threat Landscape Report*. [online], p.3. Available at: https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf [Accessed 16 August 2021].

[3] Harrod, B., (2021). The Increasing Popularity of Ransomware Amongst Cybercriminals. [online] *Ivanti.com*. Available at: https://www.ivanti.com/blog/the-increasing-popularity-of-ransomware-amongst-cybercriminals [Accessed 16 August 2021].

[4] The term *supply chain* is generally understood to indicate the biomes of activities, individuals, know-how, and processes connecting the supplier of a service or a product to its customers. European Union Agency for Cybersecurity (ENISA), (2021). *ENISA Threat Landscape for Supply Chain Attack.* [online], p.6. DOI: 10.2824/168593 .

[5] *Ibidem* p.4.

system has the potential to increase its efficacy in countering the current and prospective threats within the cyber-domain.

2 The Kaseya Case

The next sections are going to provide an overview of the incident with a particular focus given on the actors involved, the cyber-kill chain, the incident response plan adopted, and the geopolitical importance of the attack.

2.1 Within the mind of a cyber-criminal organization: behavioral analysis of REvil

Kaseya is a service provider of IT management software and cloud servers[6]. In particular, Kaseya VSA (Virtual Server/System Administrator) is an all-in-one tool for Remote Monitoring and Management (RMM) that permits Managed System Providers (MSPs) to administer from remote its clients' IT systems[7]. On the 2nd of July 2021, Kaseya has notified its customers of the occurrence of a ransomware incident targeting its management software Kaseya VSA[8]. Two hours prior to Kaseya's notification, the ransomware-as-a-service (RaaS) group REvil reported on its Darknet 'Happy Blog' a ransom demand of 70 000 000$ in BTC in exchange for the release of a universal decryption tool to recover the encrypted data[9]. Firstly discovered by the Federal Bureau of Investigation in 2019, the syndicate REvil, also known with the aliases Sodin and Sodinkibi, rapidly developed to become a high-profile ransomware group targeting primarily service providers, with a yearly estimated income of $100 Million[10]. A key problem with much of the literature on cyber-criminal groups is the absence of a comprehensive analysis regarding the logic which motivate their actions. To shed a light on these hidden aspects of REvil, the seminal report provided by the intelligence agency AdvIntel applied the classic methodological approach of criminology to the behavioral analysis of the group[11]. According to the findings, the conduct of the syndicate tends to be triggered by two main factors: the media resonance of its actions and a general sense of impunity which nourishes a tendency to be overconfident in the definition of its targets[11]. With regards to the first factor, what needs to be highlighted is the fact that an organized criminal group such as REvil thrive with the fame obtained on virtual forums and through media resonance[11]. In fact, the news

[6] European Union Agency for Cybersecurity, (2021). *ENISA Threat Landscape for Supply Chain Attack.* [online], p.18. DOI: 10.2824/168593.
[7] Kaseya, (n.d). The world's #1 rmm solution. [online] *Kaseya.com.* Available at: https://www.kaseya.com/products/vsa/ [Accessed 30 July 2021].
[8] European Union Agency for Cybersecurity, (2021). *ENISA Threat Landscape for Supply Chain Attack.* [online], p.18. DOI: 10.2824/168593.
[9] Allen, J., (2021*).* Kaseya Ransomware Attack Explained: What You Need To Know. [online] *PurpleSec.us* Available at: https://purplesec.us/kaseya-ransomware-attack-explained/#Responded [Accessed 20 August 2021].
[10] Avertium, (2021). REvil Ransomware Overview [online] *Avertium.com* Available at: https://www.avertium.com/revil-ransomware-overview/ [Accessed 23 August 2021].
[11] AdvIntel Advance Intelligence, (2020). Inside REvil Extortionist "Machine": Predictive Insights. [online] *AdvIntel Advance Intelligence* Available at: https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights [Accessed 23 August 2021].

headlines made by the attacks to the meat-processing firm JBL occurring in June 2021 followed by Kaseya's case in early July gave the organization the possibility to obtain the necessary celebrity online to attract new members in its ranks[11]. Nonetheless, this key driver for cyber-criminal activity can be considered endogenic considering the significant psycho-societal impacts of cyber-attacks. On the other hand, a second factor influencing the group's tendency to target high-profile/high-reward organizations is related to the complexity of the process of cyber-attribution in the aftermath of an incident[12]. The term *cyber attribution* is generally understood to encompass the technical and legal frameworks adopted to recognize a specific organized group, or individual, as the perpetrator of a cyber-attack, and to detect possible overt or covert implications of State actors in its criminal businesses[13]. If on the technological side of attribution many intelligence agencies have developed a comprehensive understanding of REvil's preferred ways of conducting its attacks, major limitations remain regarding the process of legal attribution. As a matter of fact, many features of REvil tends to point out its possible affiliation with the Russian government. Besides the fact that Russian is the main language used on its online forums, the syndicate tends to avoid targeting companies that are based on Russian soil, or which gravitate within the sphere of influence of the Russian government[12]. Furthermore, another factor pointing towards this possibility is related to the Geneva meeting of June 2021 between US president Joe Biden and the Russian president Vladimir Putin. During the convention, the United States threatened a coordinated action from NATO at the expense of Russia in the event that cyber-groups unofficially related to its government continued to target Western companies[14]. Given this intimidation, it can be argued that REvil's server shutdown happening less than two weeks after the Kaseya incident might be related to the Russian strategy of international appeasement towards the US counterpart. Notwithstanding these conjectures, it is necessary to highlight the fact that, given the propensity of State-actors to avoid the formal acknowledgment of cyber-attacks orchestrated from its grounds, a general sense of impunity will continue to foster the agency of criminal groups such as REvil[13].

[12] AdvIntel Advance Intelligence, (2020). Inside REvil Extortionist "Machine": Predictive Insights. [online] *AdvIntel Advance Intelligence* Available at: https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights [Accessed 23 August 2021].

[13] Strippoli Lanternini, A., (2020). Il Processo di Attribution nel Cyberspace: Strumenti Tecnico-giuridici di Difesa dai Cyber Attacchi. [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/soluzioni-aziendali/il-processo-di-attribution-nel-cyberspace-strumenti-tecnico-giuridici-di-difesa-dai-cyber-attacchi/ [Accessed 24 August 2021].

[14] Lezzi, P., 2021. *REvil, ecco cosa può succedere dopo la "scomparsa" del gigante del ransomware - Cyber Security 360.* [online] Cyber Security 360. Available at: https://www.cybersecurity360.it/nuove-minacce/ransomware/revil-ecco-cosa-puo-succedere-dopo-la-scomparsa-del-gigante-del-ransomware/ [Accessed 24 August 2021].

2.2 Technical analysis of the attack

As mentioned in the previous section, REvil tends to prioritize high-risk/high-reward targets for reasons of popularity and for the general sense of impunity that permeates the cyber domain[15]. This technical portion of the study is going to be entirely focused on providing an overview of the cyber-kill chain which characterizes the ransomware attack to the Kaseya VSA supply chain. According to the analysis conducted by the DIVD (Dutch Institute for Vulnerability Disclosure), the criminals exploited many 0-day vulnerabilities within the company's IT system to infiltrate within its network of customers[16]. Specifically, the attack has been carried out in six phases, culminating with the encryption of the files contained in the local disks of end-users:

1. By Exploiting vulnerability CVE-2021-30116 (SLQ Injection), the group bypassed the authentication process on Kaseya VSA and obtained the highest privileges as a Managed Service Providers (MSP)[16].
2. Taking advantage of these privileges, REvil delivered to the MSP's list of customers the payload in the form of a file named *agent.crt*, disguised as the software update 'Kaseya VSA Agent Hot-fix'[16].
3. Once opened, *agent.crt* executed the following script from Windows PowerShell:
   cmd.exe /c ping 127.0.0.1 -n 1543 > nul & C:WindowsSystem32WindowsPowerShellv1.0powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:WindowsSystem32certutil.exe C:Windowscert.exe & echo %RANDOM% >> C:Windowscert.exe & C:Windowscert.exe -decode c:kworkingagent.crt c:kworkingagent.exe & del /q /f c:kworkingagent.crt C:Windowscert.exe & c:kworkingagent.exe[17]
4. The script reported above carried out these commands:
   a. With the string '127.0.0.1 -n 1543 > nul' REvil sets a timer of 1543 seconds for the execution of the script[17].
   b. The section 'C:WindowsSystem32WindowsPowerShellv1.0powershell.exe Set-MpPreference-DisableRealtimeMonitoring$true -DisableIntrusionPreventionSystem $true-DisableIOAVProtection$true-DisableScriptScanning$true

[15] AdvIntel Advance Intelligence, (2020). Inside REvil Extortionist "Machine": Predictive Insights. [online] *AdvIntel Advance Intelligence* Available at: https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights [Accessed 23 August 2021].
[16] Pelliccione, A., (2021). La minaccia ransomware sale di livello: il caso Kaseya, com'è successo e come difendersi [online] *Agenda Digitale*. Available at: https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-caso-kaseya-come-successo-e-come-difendersi/ [Accessed 18 August 2021].
[17] Lezzi, P., 2021. Attacco a Kaseya: il ruolo del supply chain risk e dei processi DevSecOps [online] *Cyber Security 360.* Available at: https://www.cybersecurity360.it/nuove-minacce/attacco-a-kaseya-il-ruolo-del-supply-chain-risk-e-dei-processi-devsecops/ [Accessed 18 August 2021].

EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend' disables the security perimeter and functionalities of Windows Defender[18].

c. The string 'copy /Y C:WindowsSystem32certutil.exe C:Windowscert.exe & echo' creates a copy of the Windows software *certutil.exe* used for decoding online contents[18].
d. With the command 'C:Windowscert.exe -decode c:kworkingagent.crt c:kworkingagent.exe', *certutil.exe* is used to decodify the payload contained in file *agent.crt*, then saved as *agent.exe* in the working directory[18].
e. The last section 'del /q /f c:kworkingagent.crt C:Windowscert.exe & c:kworkingagent.exe' eliminates both the file *agent.crt* and the *decipher* while initiating the final phases of the attack[18].

5. The agent *agent.exe* executes files 'msmpeng.exe' and 'mpsvc.dll' with the latter importing a dynamic-link library (DLL) and the former allow its opening[19].
6. Once the library is opened, the last phase of the attack consists in the execution of a network discovery to identify the hosts and the encryption of the files contained in the devices[19].

The results of this analysis have important implications for the understanding of supply-chain attacks. In fact, they implicate that ransomware attacks to supply-chains leverage on the complex relationship linking each ring of the chain to the other. In particular, the asymmetry of the relation of dependency established among a single supplier and many users turns out to be a critical factor in the intensification of the impact of cyber-attacks of this sort. Having presented the technical analysis of the cyberattack that targeted the supply chain of Kaseya VSA, this paper is going to provide a brief, yet comprehensive, examination of the countermeasures adopted.

2.3 Incident Response and Remediation

Kaseya, alongside the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI, developed a timely plan to address the cyber-attack[20]. In fact, on the day of the incident, the company proceeded by shutting down their server *Software-as-a-Service (SaaS)* while recommending to its clientele to arrest the Kaseya VSA servers on-premise to limit the potential

[18] Lezzi, P., 2021. Attacco a Kaseya: il ruolo del supply chain risk e dei processi DevSecOps [online] *Cyber Security 360.* Available at: https://www.cybersecurity360.it/nuove-minacce/attacco-a-kaseya-il-ruolo-del-supply-chain-risk-e-dei-processi-devsecops/ [Accessed 18 August 2021].

[19] Pelliccione, A., (2021). La minaccia ransomware sale di livello: il caso Kaseya, com'è successo e come difendersi [online] *Agenda Digitale*. Available at: https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-caso-kaseya-come-successo-e-come-difendersi/ [Accessed 18 August 2021].

[20] Us-cert.cisa.gov, (2021). Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers [online] *Us-cert.cisa.gov.* Available at: https://us-cert.cisa.gov/kaseya-ransomware-attack [Accessed 20 August 2021].

impacts of the incident[21]. This recommendation played a crucial role in lowering the number of vulnerable servers online. In fact, according to a study conducted by Carlo Cadet for the security rating company BitSight, the number of compromised instances abruptly decreased from 1,900 to less than 100 in the aftermath of Kaseya's notification[22]. Simultaneously, Kaseya performed an examination of the cyber-kill chain of the attack to devise and implement a Compromise Detection Tool. The software permits Kaseya's users to inspect its systems in autonomy in search of Indicators of Compromise of the ransomware attack on the VSA servers[23]. So far, this section has examined the effective measures taken to immediately counter the attack and initiate the recovery of the systems. These types of strategies are usually labelled with the expressions *Incident Response* and *Business Continuity* plans. On the other hand, with regards to the measures taken to actually restore the functionality of its servers, the agency performed more poorly. As a matter of fact, if the reconfiguration and restarting of its servers *Software-as-a-Service (SaaS)* were initially announced for the 5th of July, the recovery of the systems was delayed by seven additional days, this, in turns, boosted the already significant economic and reputational damages to Kaseya[21]. Notwithstanding the effective implementation of the Incident Response Plan, the cyber-attack generated a significant spillover effect on a global scale. Furthermore, in the case of software supply chains, such as Kaseya's VSA, tracing the vastity of its network of clients can be challenging. In fact, the fiduciary connection linking vendor-customers tends to limit the understanding of the end-user as regards its placement within a supply chain and the potential vulnerabilities related to this position. Unawareness plays a crucial role in causing an escalation in the impacts of such attacks. Specifically, in the aftermath of the incident, seventeen countries were impacted with a final cost of the cyber-attack yet to be fully estimated, making Kaseya's case one of the worst ransomware attacks targeting a supply chain in the history of cyber-security[24]. What is clear is that targeting 30 Kaseya's Managed Service Providers (MSPs), produced a cascading effect that even reached giants such as the Swedish superstore company COOP[24]. In fact, according to a representative of the chain, Sweden COOP's system shut down overnight with more than 800 stores forced to remain

[21] Molinari, G., (2021). La minaccia cyber alle supply chain: il caso Kaseya VSA. [online] *Analytica for intelligence and security studies*. Available at: https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/la-minaccia-cyber-alle-supply-chain-il-caso-kaseya-vsa/ [Accessed 19 August 2021].

[22] Cadet, C., 2021. The Kaseya Ransomware Attack - What You Need To Know About. [online] *BitSight.* Available at: https://www.bitsight.com/blog/kaseya-ransomware-attack [Accessed 20 August 2021].

[23] The expression Indicators of Compromise (IoCs) is generally understood to mean forensic data signaling a potential compromission of a system or network. In particular, Kaseya has released a list of IoCs concerning IP addresses connected to malicious online activity and specific signatures of compromised files exploited by the attackers. Dvir, S., (2021). REvil Ransomware Attack on Kaseya VSA: What You Need to Know. [online] *Inside Out Security*. Available at: https://www.varonis.com/blog/revil-msp-supply-chain-attack/ [Accessed 19 August 2021].

[24] Dickens, S., 2021. *Full Impact of REvil Ransomware Attack on Kaseya Becomes Apparent*. [online] Futurum Research. Available at: <https://futurumresearch.com/research-notes/full-impact-of-revil-ransomware-attack-on-kaseya-becomes-apparent/> [Accessed 25 August 2021].

closed until further notice[25]. In light of the intensity and the amplitude of the effects of an attack that shut-down an entire supply chain, can a ransomware be considered as potential weapon in conflicts motivated by geopolitical reasons?

2.4 Is geopolitical 'Ransomwar' a reality?

Through centuries of development, humanity has learned to thrive in this planet instead of merely surviving in it. Mankind has adapted to the surrounding natural ecosystem and even conceived a domain in which conducting digitalized parallel lives[26]. Likewise their organic counterparts, these personas are intrinsically made of preferences, hopes, and especially valuable information. As outlined in the introduction, the evolution of the domain was paralleled by the mastering of tools for exploiting its possibilities with criminal intents. The past decade has witnessed a renewed interest in academia regarding the spread of online criminal activities while the geopolitical concerns of cyber-attacks have not been dealt with in-depth. In the light of recent major ransomware attacks such as SolarWinds, Colonial Pipeline, and more recently to the supply chain of Kaseya VSA, there is now significant concerns regarding the use of this software as potential weapons in geopolitical conflicts[27]. In her analysis of game theory applied to ransomware incidents, Jun reaches the conclusion that these tools will soon become cost-effective means for international coercion[27]. Since data are quickly turning into an asset, encrypting or threatening to encrypt these commodities is likely to represent a potential threat to a country in the same manner as more traditional security concerns[27]. Having addressed this possibility, what needs to be highlighted is that so far, no major ransomware attack has been conducted for overt geopolitical reasons. Nonetheless, the analysis conducted so far on the incident at the center of this study is likely to point out that this concern may soon become a trend rather than a supposition. Therefore, nation-states must be prepared to face similar forthcoming threats in an attempt to ensure the resilience of their public and private sectors.

3 Best practices to protect against ransomware supply-chain attacks

All in all, this paper has depicted a glooming future for the cyber-domain. New threats are constantly emerging, impunity reigns in the aftermath of a cyber-attack, and geopolitical considerations may soon foster the rise and the agency of ever organized cyber-criminals such as REvil. Nevertheless, each new incident offers fundamental insights regarding the necessary

[25] Tidy, J., (2021). Swedish Coop supermarkets shut due to US ransomware cyber-attack. [online] *BBC News*. Available at: https://www.bbc.com/news/technology-57707530 [Accessed 24 August 2021].
[26] Chittaro, L., (2014). La vita parallela sul web. [online] *Il Sole 24 ORE*. Available at: https://st.ilsole24ore.com/art/tecnologie/2014-02-14/la-vita-parallela-web--153800.shtml?uuid=ABSsacw [Accessed 22 August 2021].
[27] Jun, J., (2021). Opinion | Could Ransomware Become a Geopolitical Weapon? Game Theory Says Yes.. [online] *Politico.com* Available at: https://www.politico.com/news/magazine/2021/07/08/ransomware-game-theory-geopolitics-cyber-attack-498625 [Accessed 22 August 2021].

measures to be taken to counter the forthcoming one. Applying this acquired intelligence, it is now possible to conceive a list of recommendations targeted for end-users, suppliers, and even practitioners of this field to ensure their cyber-awareness as regards to the best practice to be implemented against possible ransomware attacks targeting supply chains. According to a recent report published by the European Union Agency for Cybersecurity (ENISA), particular attention should be focused on vendors' side of supply chains, which currently represents the weakest one of the two[28]. As a matter of fact, immature suppliers impose a great burden of risks to their network of customers while raising the overall level of vulnerability of a supply chain. Hence, suppliers should adopt security practices so as to guarantee that their services and products are not going to pose additional risks to the users. These methodologies are commonly identified with the term DevSecOps. This acronym identifies the cyclical process of actions that accompanies the lifecycle of a software from its development to its application while ensuring constant vulnerability controls, up to date incident response plans, and rigorous patch management to contrast the insurgence of vulnerabilities[29]. A supplier should ensure to its customers the full compliance to the standards on information security contained within the framework ISO 27001 to certify the maturity of the company as regards data confidentiality, integrity, and availability[30]. Furthermore, in case the company collected personal data coming from the European Union, the supplier should also prove its compliance to the norms contained within the framework of the General Data Protection Regulation (GDPR) on the matter of privacy and data security. On the other hand, customers should carefully vet the suppliers according to their maturity as regards their level of cyber-awareness[28]. According to some research on this matter, particular attention should be paid to devise and implement a profiling methodology for its assets and liabilities to be aware of their specific risks, importance, and dependencies in light of participating in a particular supply chain[31]. Even though this method provides a comprehensive depiction of the overall risks for customers of a supply chain, undoubtedly it remains a cost-ineffective strategy that may overrun the IT sector of a company and prevent it from performing its daily duties[31]. Moreover, according to ENISA the relation of trust between supplier and customer should be reinforced by compelling the vendor to adhere to a list of

[28] European Union Agency for Cybersecurity, (2021). *ENISA Threat Landscape for Supply Chain Attack.* [online], p.27. DOI: 10.2824/168593.

[29] Lezzi, P., (2021). Attacco a Kaseya: il ruolo del supply chain risk e dei processi DevSecOps [online] *Cyber Security 360.* Available at: https://www.cybersecurity360.it/nuove-minacce/attacco-a-kaseya-il-ruolo-del-supply-chain-risk-e-dei-processi-devsecops/ [Accessed 18 August 2021].

[30] Petters, J., (2020). What is ISO 27001 Compliance? Essential Tips and Insights [online] I*nside Out Security*. Available at: https://www.varonis.com/blog/iso-27001-compliance/ [Accessed 25 August 2021].

[31] Pelliccione, A., (2021). La minaccia ransomware sale di livello: il caso Kaseya, com'è successo e come difendersi. [online] *Agenda Digitale*. Available at: https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-caso-kaseya-come-successo-e-come-difendersi/ [Accessed 18 August 2021].

"obligations of suppliers for the protection of the organization's assets, for the sharing of information, for audit rights, for business continuity, for personnel screening, and for the handling of incidents in terms responsibilities, notification obligations and procedures"[32]. Lastly, but not for importance, users should diligently perform updates for its software as soon as they are released by the supplier to ensure the natural functioning of the patching system[32]. Having made these points, what needs to be highlighted is the fact that no system is inviolable, and even the most diligent supply chain may still be exposed to the risk of a ransomware attack especially if performed for geopolitical reasons with the *nulla osta* of a foreign nation-state. Hence, the agency of supra-national institutions may still be necessary for different reasons. First of all, to prevent the escalation of state-endorsed cyber-attacks through diplomatic means[33]. Second of all, in order to develop a common comprehensive framework for the legal attribution of cyber incidents. Lastly, international fora of discussion would prove vital as of the promotion of a system for information sharing as regards threats, vulnerabilities, and response strategies[34]. An initial step towards these objectives has been made within the proposal to update the Directive 2016/1148 on the European Security of Network and Information Systems (NIS). The so-called NIS2 is meant to increase the EU cyber-resilience by reinforcing the implementation of a unified framework on cyber-security with a particular focus being paid on the rising threats posed by supply-chains and cyber-dependencies[35].

4 The National Cybersecurity Agency: overdue update to the Italian Cyber-strategy

With the *Centro Elaborazione Dati (CED)* of Lazio getting back on its feet after sustaining the recent ransomware attack, it is clear that the matter of cyber-security cannot be sidelined anymore within the political debate. According to an interview given by Nunzia Ciardi, director of the *Servizio Postale e delle Comunicazioni*, the revolutionary process brought by digitalization so far has not been paralleled by a coherent development in the Italian cyber-strategy[36]. This argument is further supported by Vittorio Colao, Minister for Technological Innovation and Digital Transition, who states that approximately 95% of the servers used by the Italian Public Administration (PA) cannot be considered as secured with regards to the current national and international cyber-threat

[32] European Union Agency for Cybersecurity, (2021). *ENISA Threat Landscape for Supply Chain Attack.* [online], p.27. DOI: 10.2824/168593.
[33] *Ibidem* p.28.
[34] Pelliccione, A., (2021). La minaccia ransomware sale di livello: il caso Kaseya, com'è successo e come difendersi | Agenda Digitale. [online] Agenda Digitale. Available at: https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-caso-kaseya-come-successo-e-come-difendersi/ [Accessed 18 August 2021].
[35] Nunziante, E., (2021). Proposta di Direttiva NIS 2: analisi delle nuove misure di cyber sicurezza europee [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/cybersecurity-nazionale/proposta-di-direttiva-nis-2-analisi-delle-nuove-misure-di-cyber-sicurezza-europee/ [Accessed 30 August 2021].
[36] Bechis, F., (2021). Non solo Pegasus. Così difendiamo l'Italia dai cyberattacchi. Parla Ciardi [online] *Formiche.net*. Available at: https://formiche.net/2021/07/pegasus-spyware-cyber-attacchi-nunzia-ciardi/ [Accessed 27 August 2021].

landscape[37]. The epochal effort needed to address these deficiencies is what brought to the forefront of national debate the necessity of updating the domestic approach to cyber-security. This renewed interest in the topic has recently been reflected in the promulgation on Gazzetta Ufficiale (GU) of Law No 109 which implements Decree-law No 82 and establishes the National Cybersecurity Agency (ACN) having legal personality under public law and regulatory, administrative, and budgetary autonomy in respect of its chart[38].

4.1 The Structure and Functions of the Agency

The creation of the ACN takes place within the wider project of digital transformation named *Piano Nazionale di Ripresa a Resilienza* (PNRR). One of the main scopes of the Agency is to accompany this digitalization process by re-designing the national architecture for cyber-security to ensure the resilience of the IT infrastructures towards possible cyber-attacks that have the potentiality of mining the national security[38]. The urgency of this effort is clearly stated by Art. 1 of the Decree-Law June 14th 2021, No 82:

> Considerato che le vulnerabilità delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche di soggetti pubblici e privati possono essere sfruttate al fine di provocare il malfunzionamento o l'interruzione, totali o parziali, di funzioni essenziali dello Stato e di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, nonché' di servizi di pubblica utilità, con potenziali gravi ripercussioni sui cittadini, sulle imprese e sulle pubbliche amministrazioni, sino a poter determinare un pregiudizio per la sicurezza nazionale[39].

Following similar institutions established in Germany (1991) and France (2009), the creation of the Agency responds to the necessity of limiting the dispersion of resources on this matter[38]. In fact, another intended purpose of the Agency is to foster the coordination and centralization of the expertise and capitals to create a major European pole of excellence for cyber-security and the study of cyber-domain. According to GU 82, Art. 7 §§ 3-4, the National Cybersecurity Agency is going to adopt a centralized structure by adopting the responsibilities of the Italian Computer Security

[37] Ansa, (2021). Colao, 95% server PA non sono in condizioni di sicurezza. [online] *Ansa.* Available at: https://www.ansa.it/bannernews/notizie/breaking_news_eco/2021/06/06/-colao-95-server-pa-non-sono-in-condizioni-di-sicurezza-_3ebc27ab-1966-4cb9-b3c2-fee4c170ad01.html [Accessed 31 August 2021].

[38] Longo, A. and Tarsitano, P., (2021). Ecco l'Agenzia per la cybersicurezza nazionale: come cambia la sicurezza cibernetica dell'Italia. [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-lagenzia-per-la-cybersicurezza-nazionale-come-cambia-la-sicurezza-cibernetica-dellitalia/ [Accessed 31 August 2021].

[39] Considering that the vulnerabilities of the networks, information systems, IT services and electronic communications of the public and private sectors can be exploited in order to cause the total or partial malfunction or interruption of essential functions of the State and essential services for the maintenance of civil, social or economic activities fundamental to the interests of the State, as well as public utility services, with potentially serious repercussions on citizens, businesses and public administrations, up to the point of causing prejudice to national security. D.L. 14 giugno 2021 n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, Art. 1.

Incident Response Team (CSIRT) and the *Centro Valutazione e Certificazione Nazionale* (CVCN)[40]. Among the many functions delegated to the National Cybersecurity Agency, this paper is going to focus on two responsibilities that may be considered as fundamental for countering the cyber-threats at the center of the study. The first one consists of being the single interlocutor for both the public and private sectors within the national cybersecurity perimeter as far as the security of IT infrastructures is concerned. The second one involves the promotion of strategic measures, adopted in coordination with the public sector, aiming at the achievement of autonomy as regards to software and IT processes of national importance[41]. As was mentioned in the section *Best practices to protect against ransomware supply-chain attacks,* the opportunity cost for malicious actors of targeting supply-chains is proportional to two factors: the lack of coordination among the nodes of the chain and the asymmetry of the relation established between supplier and customers. Hence, the establishment of a singular entity responsible for promoting the dialogue among public and private sectors as well as seeking to curtail the length of supply-chains of national importance, represents the first crucial steps in the direction of lowering the overall domestic vulnerability to supply-chain attacks. Notwithstanding the above-mentioned important features, the definition of the sphere of action of the National Cybersecurity Agency can be considered as a cause for concern. In fact, the ACN must find room for maneuver within existing institutions engaged in the cyber-domain without causing an overlap of responsibilities which would prove detrimental for the entire System Country. These limits are represented by the *Polizia Postale* in charge of investigation, *Sistema di Informazione per la Sicurezza della Repubblica* (SISR) which is endorsed with the responsibility of cyber-intelligence, and the army tasked with the cyber-defence of the country[41]. Once fully in motion, will the Agency be able to perform its duties without stepping on any toes in this crowded environment? Only time will tell. What is certain is that the creation of a unified pole in charge of ensuring the resiliency of the IT infrastructure has, in theory, the potential to cut through the red tape, traditional limit for the Italian agency within the cyber-domain.

Concluding remarks: high hopes for a more resilient domestic system

This paper has given an account of the recent spike in ransomware attacks targeting supply chains. As stated in *Introduction: New trends in the cyber-threat landscape?* the study was conducted to

[40] D.L. 14 giugno 2021 n.82*,* Art. 7 §§ 3-4.

[41] Longo, A. and Tarsitano, P., (2021). Ecco l'Agenzia per la cybersicurezza nazionale: come cambia la sicurezza cibernetica dell'Italia. [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-lagenzia-per-la-cybersicurezza-nazionale-come-cambia-la-sicurezza-cibernetica-dellitalia/ [Accessed 31 August 2021].

highlight the urgent strategic measures to be taken at the domestic and international level to ensure the preparedness of the Italian countrywide system in the face of similar forthcoming threats.
This study has been focused on presenting a multilevel analysis of the Kaseya VSA case which embodies the quintessence of the current cyber-threat landscape. A case of study which has been dissected in its main features. The analysis has initially investigated the principal actors involved in the cyber-attack. Through the adoption of a methodology characteristic of the behavioral sciences, this paper delved into the psychological and sociological factors having an influence on the behavior of the criminal group REvil. The results of this section point towards the idea that the media resonance gained by the cyber-attacks and the impunity which reigns within the cyber-domain represent key drivers for cyber-criminal organizations such as the one at the center of this research. If the first factor can be considered as endogenic given the extensive psycho-societal impacts of cyber-attacks, additional work needs to be directed towards the improvement of the legal attribution of cyber incidents in order to lower the opportunity cost of conducting similar attacks.
Turning now to the second section, this predominantly technical portion of the study has been entirely focused on providing a comprehensive overview of the cyber-kill chain of the cyber-attack. Thanks to the analysis conducted by the Dutch Institute for Vulnerability Disclosure (DIVD), it was possible to precisely point out each stage of the incident, from the exploitation of the zero-day vulnerabilities which initiated the attack up until the thereof notification. These findings might not be generalized to other cyber-attacks, however, they have important implications for our understanding of supply-chain attacks. As a matter of fact, they suggest that these types of incidents leverage on the complex relationship of trust linking each ring of the chain to the other. Specifically, it is the asymmetry of the relation established between a single supplier and many dependent customers which proves to be a critical factor bolstering the impact of such cyber-attacks of this sort. The disruptive potentiality of the incident was undoubtedly limited by the timely measures of incident response taken by the company which have been addressed in depth by the section *The Mitigation Plan*. Nonetheless, its impact remained considerable not only for the company as result of poorly designed business continuity plans but also on a global scale. In fact, the impact was particularly intense and widespread given the vast amount of Kaseya VSA end-users scattered on a global scale. The vastity of the chain effect is what led this paper to question whether similar incidents may pose geopolitical concerns. The results suggest that soon nation-state must be prepared to face this reality. Hence, this paper has proposed some measures that could be taken to enhance the resilience of domestic systems. Presenting the creation of the National Cybersecurity Agency, this paper investigated whether *in fieri* this could represent the first step towards the right direction of lowering the overall domestic vulnerability to supply-chain attacks. Taken together, the

findings suggest that, apart from minor concerns, the establishment of a unified pole of cyber-security responsible for ensuring the resiliency of the IT infrastructure has the potential to increase its efficacy in countering the current and prospective threats in the cyber domain. This research clearly presents some limitations. Nevertheless, the results may suggest several courses of action to enhance our understanding of supply-chain attacks so as to efficiently address this problem. Moreover, future studies on these topics are necessary to assess the direction taken by the Italian cyber-strategy as regards supply-chain attacks within the EU framework of the Security of Network and Information Systems (NIS) and the proposed NIS 2.

Reference

AdvIntel Advance Intelligence, (2020). Inside REvil Extortionist "Machine": Predictive Insights. [online] *AdvIntel Advance Intelligence* Available at: https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights [Accessed 23 August 2021].

Allen, J., (2021*).* Kaseya Ransomware Attack Explained: What You Need To Know. [online] *PurpleSec.us* Available at: https://purplesec.us/kaseya-ransomware-attack-explained/#Responded [Accessed 20 August 2021].

Ansa, (2021). Colao, 95% server PA non sono in condizioni di sicurezza. [online] *Ansa.* Available at: https://www.ansa.it/bannernews/notizie/breaking_news_eco/2021/06/06/-colao-95-server-pa-non-sono-in-condizioni-di-sicurezza-_3ebc27ab-1966-4cb9-b3c2-fee4c170ad01.html [Accessed 31 August 2021].

Avertium, (2021). REvil Ransomware Overview [online] *Avertium.com* Available at: https://www.avertium.com/revil-ransomware-overview/ [Accessed 23 August 2021].

Bechis, F., (2021). Non solo Pegasus. Così difendiamo l'Italia dai cyberattacchi. Parla Ciardi [online] *Formiche.net.* Available at: https://formiche.net/2021/07/pegasus-spyware-cyber-attacchi-nunzia-ciardi/ [Accessed 27 August 2021].

Bitdefender, (2020). *2020 Consumer Threat Landscape Report*. [online], p.3. Available at: https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf [Accessed 16 August 2021].

Cadet, C., 2021. The Kaseya Ransomware Attack - What You Need To Know About. [online] *BitSight.* Available at: https://www.bitsight.com/blog/kaseya-ransomware-attack [Accessed 20 August 2021].

Chittaro, L., (2014). La vita parallela sul web. [online] *Il Sole 24 ORE*. Available at: https://st.ilsole24ore.com/art/tecnologie/2014-02-14/la-vita-parallela-web--153800.shtml?uuid=ABSsacw [Accessed 22 August 2021].

Dickens, S., 2021. *Full Impact of REvil Ransomware Attack on Kaseya Becomes Apparent*. [online] Futurum Research. Available at: <https://futurumresearch.com/research-notes/full-impact-of-revil-ransomware-attack-on-kaseya-becomes-apparent/> [Accessed 25 August 2021].

Dvir, S., (2021). REvil Ransomware Attack on Kaseya VSA: What You Need to Know. [online] *Inside Out Security*. Available at: https://www.varonis.com/blog/revil-msp-supply-chain-attack/ [Accessed 19 August 2021].

European Union Agency for Cybersecurity (ENISA), (2021). *ENISA Threat Landscape for Supply Chain Attack.* [online], pp.6-18-27-28. DOI: 10.2824/168593.

Harrod, B., (2021). The Increasing Popularity of Ransomware Amongst Cybercriminals. [online] *Ivanti.com*. Available at: https://www.ivanti.com/blog/the-increasing-popularity-of-ransomware-amongst-cybercriminals [Accessed 16 August 2021].

Jun, J., (2021). Opinion | Could Ransomware Become a Geopolitical Weapon? Game Theory Says Yes.. [online] *Politico.com* Available at: https://www.politico.com/news/magazine/2021/07/08/ransomware-game-theory-geopolitics-cyber-attack-498625 [Accessed 22 August 2021].

Kaseya, (n.d). The world's #1 rmm solution. [online] *Kaseya.com.* Available at: https://www.kaseya.com/products/vsa/ [Accessed 30 July 2021].

Kaspersky, (n.d). Ransomware – definition, prevention, and removal [online*]. Kaspersky*. Available at: https://www.kaspersky.com/resource-center/threats/ransomware [Accessed 11 August 2021].

Lezzi, P., 2021. Attacco a Kaseya: il ruolo del supply chain risk e dei processi DevSecOps [online] *Cyber Security 360.* Available at: https://www.cybersecurity360.it/nuove-minacce/attacco-a-kaseya-il-ruolo-del-supply-chain-risk-e-dei-processi-devsecops/ [Accessed 18 August 2021].

Lezzi, P., 2021. *REvil, ecco cosa può succedere dopo la "scomparsa" del gigante del ransomware - Cyber Security 360*. [online] Cyber Security 360. Available at: https://www.cybersecurity360.it/nuove-minacce/ransomware/revil-ecco-cosa-puo-succedere-dopo-la-scomparsa-del-gigante-del-ransomware/ [Accessed 24 August 2021].

Longo, A. and Tarsitano, P., (2021). Ecco l'Agenzia per la cybersicurezza nazionale: come cambia la sicurezza cibernetica dell'Italia. [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-lagenzia-per-la-cybersicurezza-nazionale-come-cambia-la-sicurezza-cibernetica-dellitalia/ [Accessed 31 August 2021].

Molinari, G., (2021). La minaccia cyber alle supply chain: il caso Kaseya VSA. [online] *Analytica for intelligence and security studies*. Available at: https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/la-minaccia-cyber-alle-supply-chain-il-caso-kaseya-vsa/ [Accessed 19 August 2021].

Nunziante, E., (2021). Proposta di Direttiva NIS 2: analisi delle nuove misure di cyber sicurezza europee [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/cybersecurity-nazionale/proposta-di-direttiva-nis-2-analisi-delle-nuove-misure-di-cyber-sicurezza-europee/ [Accessed 30 August 2021].

Pelliccione, A., (2021). La minaccia ransomware sale di livello: il caso Kaseya, com'è successo e come

difendersi [online] *Agenda Digitale*. Available at: https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-caso-kaseya-come-successo-e-come-difendersi/ [Accessed 18 August 2021].

Petters, J., (2020). What is ISO 27001 Compliance? Essential Tips and Insights [online] I*nside Out Security*. Available at: https://www.varonis.com/blog/iso-27001-compliance/ [Accessed 25 August 2021].

Strippoli Lanternini, A., (2020). Il Processo di Attribution nel Cyberspace: Strumenti Tecnico-giuridici di Difesa dai Cyber Attacchi. [online] *Cyber Security 360*. Available at: https://www.cybersecurity360.it/soluzioni-aziendali/il-processo-di-attribution-nel-cyberspace-strumenti-tecnico-giuridici-di-difesa-dai-cyber-attacchi/ [Accessed 24 August 2021].

Tidy, J., (2021). Swedish Coop supermarkets shut due to US ransomware cyber-attack. [online] *BBC News*. Available at: https://www.bbc.com/news/technology-57707530 [Accessed 24 August 2021].

Us-cert.cisa.gov, (2021). Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers [online] *Us-cert.cisa.gov.* Available at: https://us-cert.cisa.gov/kaseya-ransomware-attack [Accessed 20 August 2021].