

# Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, and Future Directions

Simone Raponi<sup>1</sup>, Maurantonio Caprolu<sup>1</sup> and Roberto Di Pietro<sup>1</sup>

<sup>1</sup>*Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar*

## Abstract

The just concluded 16th edition of the World Economic Forum's Global Risks Report has ranked Cybersecurity failure as a significant global threat. This awakening is not surprising, maybe even late, as witnessed by the reliance of large part of critical sectors on the cyber infrastructure during the under-going pandemic, or like shown by the recent and devastating SolarWinds attacks, whose implications and aftermaths are still to be completely understood.

In this paper, we provide several contributions towards the provisioning of a comprehensive, robust, and reliable framework for the cybersecurity of critical infrastructures. In particular, we first revise the scope and definition of critical infrastructures. Later, we expand the introduced concept to capture the modern deployment and operations of critical infrastructures, highlighting their interconnectedness and dependency with the software supply chain. Then, we show how the SolarWinds attack has exploited the defined model to perform one of the most devastating black hat operations ever seen. Finally, we also show some research directions to secure the software supply chain, calling for an approach that necessarily requires the interplay of sound theory, viable solutions, and legislation interventions.

## Keywords

SolarWinds Attack, Critical Infrastructures Security, Supply Chain, Industrial Control Systems

## 1. Introduction

The technological revolution of the last decades has profoundly changed the architecture and functioning of Information and Communication Technology (ICT) systems that manage modern industrial plants. New technologies such as Internet of Things (IoT), cloud computing, and the edge/fog network paradigm have driven the evolution, still ongoing, of today's Industrial Control Systems (ICSs). Production processes have become more efficient, advanced, and reliable thanks to the automation and digital management of every aspect of the production chain. On the one hand, the cited innovations have considerably optimized industrial plants, improving their production capacity and reducing management and personnel costs. On the other hand, the automation of production processes has introduced an almost total dependence on technological equipment. Modern industrial plants are now subject to new vulnerabilities due to possible malfunctions, malicious or not, of the devices that make up their ICSs [1]. Although Critical Infrastructures (CIs) are somewhat more isolated from the outside world,

---


*ITASEC '21: Italian Conference on Cyber Security, April 07–09, 2021, Online*

✉ sraponi@hbku.edu.qa (S. Raponi); mcaprolu@hbku.edu.qa (M. Caprolu); rdipietro@hbku.edu.qa (R. Di Pietro)

🆔 0000-0002-1813-546X (S. Raponi); 0000-0001-8237-0539 (M. Caprolu); 0000-0003-1909-0336 (R. Di Pietro)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

their ICSs have also experienced the same evolution. Specifically, the network architecture has undergone several structural changes, significantly increasing the attack surface available to malicious actors. Unfortunately, security systems have not evolved as quickly, leaving ICSs without effective protection. In fact, the fast change in the ICS architecture was not followed by a subsequent adaptation of the defensive strategies, leading to critical security flaws.

Several recent attacks against CIs demonstrate the inefficiency of defensive measures in protecting such sensitive targets. Cyberattacks against the Ukrainian power grid in 2015 and 2016, for example, highlight the fragility of existing security systems and show the potentially disruptive consequences of similar events [2]. Likewise, the Wannacry ransomware campaign, that infected hundreds of thousands of systems in 2017 [3], showed how even malware designed to target generic systems could infect ICSs as well, causing extent damages in different CIs. Not to mention the recent SolarWinds attack, described in detail later on.

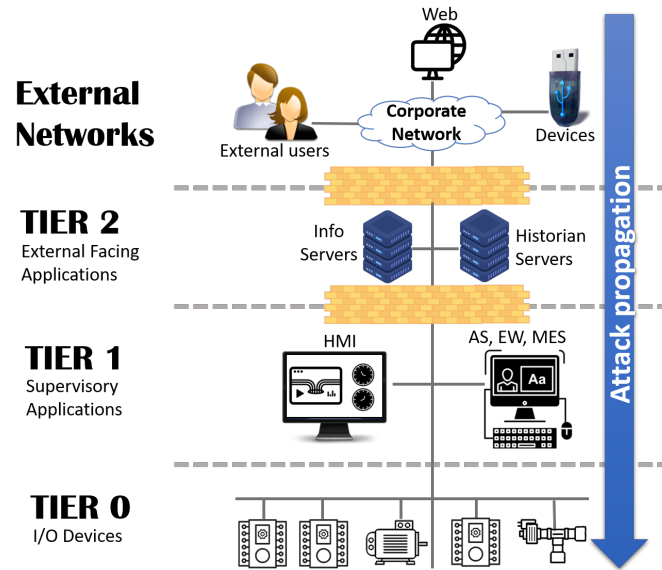
In this paper, we analyze the open security issues affecting CIs defensive strategies that may have significantly played a role in the success of recent attacks. The main objective is to better understand the systemic risks related to ICSs—focusing on the software supply chain—, identify how effective the current defense mechanisms are, and outline new directions for future development. To achieve this goal, we study the state-of-the-art of defense mechanisms currently used in CIs. Then, we discuss how CIs are identified and protected from a regulatory perspective by analyzing two significant directives that pave the way towards securing ICSs: the United States Presidential Directive 21 on ICSs Security, and the recent Decree [4] issued by the Italian government on the identification of a cybersecurity perimeter around CIs.

This analysis confirms a weakness in the current management of modern CIs security strategy: the software supply chain. Although considered a critical component of CI management, software installation and maintenance rarely receive the deserved attention. In fact, the different nodes of the supply chain, being not part of the ICS infrastructure, are not protected by the security systems of the CI. The software is generally checked before crossing the CI borders, but it may have already been compromised before. The vulnerability introduced by this problem was exploited by one of the most dreadful attacks of the last decade: SolarWinds. This attack, whose reach and consequences are still being evaluated, demonstrates the severity of this problem and the urgency to include the entire software supply chain within the virtual perimeter of the CIs.

**Roadmap.** The rest of the paper is organized as follows. In Section 2, we introduce the definition of CI, we discuss ICSs and their common architecture, and we analyze existing defense strategies usually applied to protect modern CI. We revise the scope of CI in Section 3, investigating the interconnection between ICS and the software supply chain, and also highlighting some research directions. Then, we discuss the SolarWinds attack from the software supply chain point of view in Section 4, while some final remarks in Section 5.

## 2. Background

Development, safety, and quality of life in industrialized countries strictly depend on the continuous and coordinated functioning of particular facilities, called CI. Such infrastructures deal with the production, distribution, and storing of assets crucial for the population’s well-being, national security, and economic growth.



**Figure 1:** ICS common multi-tier architecture.

Usually, each nation independently identifies the infrastructures within its national borders that must be considered critical. For example, the Presidential Policy Directive 21 (PPD-21) [5], issued by the President of the United States in 2013, identifies 16 critical sectors whose infrastructures must be maintained secure, functioning, and resilient. Simultaneously, the directive 2008/114 [6] of the European Program for Critical Infrastructure Protection (EPCIP) establishes methods and procedures for identifying and designating European Critical Infrastructures (ECIs) in the transport and energy sectors. Several facilities can be universally considered critical infrastructure. Among them, we can cite the power grid, communication networks, the nationwide networks and infrastructures for transporting people and goods, and the health system.

The Geneva Convention prohibits the attack, whether aimed at the total or partial destruction, of any object essential for the civilian population's survival, regardless of the reasons. Despite the cited legal framework, the risk of attacks on critical infrastructure, whether by criminal organizations (think of ransomware), or foreign governments (cyberwarfare as a political means), with its direct consequences to the safety of people and the possible damages to the national interests, is real—as shown by past attacks aiming directly at CIs.

## 2.1. Industrial Control Systems

In order to understand the cyber threats that can affect critical infrastructures, it is necessary to know the architecture, functionality, and deployment of the ICT systems typically used in the cited facilities. Usually, production activities of any kind are supported by ICS, integrated and interconnected hardware and software resources capable of managing and automating every production process phase. The typical architecture of an ICS infrastructure, shown in Figure 1, is made up of different levels.

The External Networks level is not considered part of the ICS infrastructure. However, systems operating at this stage are used to interact with it. For this reason, the devices used at this level should be protected with the same degree of security as the more internal levels. Tier 2 is the most external layer, directly connected with the outside world. All applications that need to interface with external systems are executed on special servers at this level. Examples include general-purpose web servers, information servers, and operational historian software, just to name a few. Tier 1 is the middle layer, also called the supervisory level. This layer includes every system used to supervise the underlying equipment while feeding data to the upper layers. This category includes Supervisory Control and Data Acquisition (SCADA) systems, software toolkits used to configure, monitor, and control cyber-physical systems, such as valves and switches. Tier 0 is the lowest level of the ICS architecture and, as such, the one closest to the physical world. Also called the “production network layer”, this level contains all the end-devices capable of controlling physical equipment, collecting data, and exchanging information with the levels above.

Figure 1, in addition to describing the various levels of the ICS architecture, also shows that the propagation of any cyber-attacks can only happen from top to bottom, i.e., from external systems to TIER 0. In fact, in the classic design, each device belonging to the ICS architecture can only be reached from the highest hierarchical level. As a result, devices operating in TIER 2 are the only ones that can be accessed directly from the outside. For this reason, the virtual perimeter of the CI with classic architecture includes only devices belonging to layer 2. However, with the adoption of modern network paradigms, such as IoT and edge/fog computing, the attack surface has grown dramatically in ICS architecture. In fact, new technologies have allowed the implementation of countless novel use cases, effectively making production processes smart and introducing significant benefits. However, some new scenarios require the devices operating at TIER 1 and TIER 0 also be directly reachable from the outside, introducing significant security problems.

## **2.2. Critical Infrastructure Protection**

Nowadays, any infrastructure devoted to producing, storing, or distributing resources is managed through ICT systems. On the one hand, the increasingly sophisticated technology has advanced production processes, improved quality, and decreased overall costs. On the other hand, however, it has induced new and unexpected vulnerabilities.

Any weakness in the ICS architecture of a CI assumes a much greater criticality than in private companies. Such infrastructures are targeted by multiple malicious actors, such as disgruntled employees, foreign governments, terrorist groups, and possibly others. Furthermore, in the event of crisis at state level, CIs are considered among the first targets of any hostile actions, both physical and digital [7]. As a result, these infrastructures are usually very well protected from intrusions, usually aimed at interfering with production processes and stealing confidential data. Before the advent of the internet, the architectures of the first ICSs were often disconnected from the outside world. Data exchange was only necessary to other CIs, using dedicated communication lines [8]. In such infrastructures, the defenses focus more on the physical perimeter since the chances of experiencing cyber attacks are extremely low. With the advent of new technologies, such as cloud computing, IoT, and edge/fog computing, production

processes have become entirely digitized. Furthermore, the network architectures of ICS systems have changed accordingly to support numerous interconnected devices. This evolution has led to a significant expansion of the digital perimeter of CIs, with the different ICS levels strongly connected to each other and often accessible directly from the Internet. The defense of the physical perimeter is a well-known and extensively studied area, given that the need for its protection arose at the same time as the CIs. On the contrary, virtual perimeter defense is a relatively new need, recently amplified by the increase in ICS connectivity, as discussed above. The CI virtual perimeter's defense is considerably complicated by the lack of standardization of ICS, which considerably increases the cost of research, design, and implementation of cybersecurity solutions and techniques tailored for these systems. In fact, ICSs are usually made up of many heterogeneous devices from multiple vendors, equipped with proprietary software, and with the need to be updated frequently. Besides, the production chain of these devices, both hardware and software, is beyond the control of the entity that manages the CI. These problems further complicate the protection of ICSs, leaving several possibilities for attackers.

Another relevant factor in the management of CI security is the availability of resources to devote to IT security. In current business models, companies tend to allocate almost all of their budgets to improving production processes, outsourcing other aspects to third-party firms. All these aspects contribute to creating disparities between the security of CIs managed by public or private companies, large or medium-sized.

Although the protection of CIs is a research area that has already been largely explored, its state-of-the-art is in continuous advancement. Among the most promising solutions, the so-called cyber deception is recently receiving particular attention. This technique aims to waste time for the attacker who manages to overcome the front lines of defense by illegally entering the digital perimeter. By deploying traps or decoys that mimic virtual assets' behavior, the defender deflects the attacker's attention from real targets, gains time, and increases the chances that the intruder is discovered [9]. A practical example of this technology aims to confuse the opponent from the early stages of the attack, responding with fake data to malicious requests such as network scans [10].

Another promising cyber attack management methodology, the Cyber Threat Information (CTI) sharing, is recently gaining large support among cybersecurity professionals. However, the liability of sharing data between the different operators that manage CIs, both public and private, greatly limits the diffusion of this technology [11].

### **3. Evolution of Critical Infrastructures**

According to the US Cybersecurity & Infrastructure Security Agency (CISA), there are 16 critical infrastructure sectors whose resources, including systems, networks, and generic assets, are considered vital to the United States. Those sectors are considered critical since their destruction (or even their incapacitation) would have a debilitating effect on national public health (or safety) and the security of national economy. According to CISA, the sectors to consider as critical are the chemical sector, the commercial facilities sector, the communications sector, the critical manufacturing sector, the dams sector, the defense industrial base sectors, the emergency services sector, the energy sector, the financial services sector, the food and agriculture sector, the

government facilities sector, the healthcare and public health sector, the information technology sector, the nuclear reactors, materials, and waste sector, the transportation systems sector, and the water and wastewater systems sector [12].

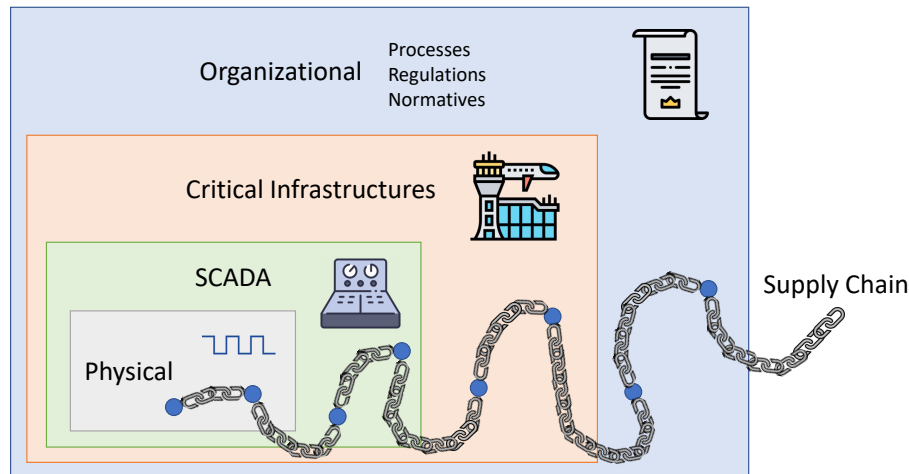
The pressing need to protect critical infrastructure led to the drafting of the Presidential Policy Directive 21 (PPD-21), on February 13th, 2013. This PPD, entitled “Critical Infrastructure Security and Resilience” claims that “the Federal government has a responsibility to strengthen its critical infrastructure’s security and resilience against both physical and cyber threats”. After the release of the PPD-21 and the Executive Order 13636 (“Improving Critical Infrastructure Cybersecurity”), a working committee has been established by the Interagency Security Committee, with the aim of reviewing “the risk management process for federal facilities” and assess its efficacy to improve the security and resilience of federal critical infrastructures [5]. Leveraging the experience matured in the US, and inspired by the discussion at the EU level, the Italian Government has issued a more comprehensive Decree, that tackles some of the limitations in the current definitions and provides directions for securing the logistic/National Cybersecurity Perimeter [4]. Indeed, such a decree defines the methods for identifying the subjects, being them public or private, included in the National Cybersecurity Perimeter. A cybersecurity perimeter is defined as the set of systems, technologies, and security policies that provides levels of protection on a conceptual borderline against remote malicious activities [13]. This decree represents a crucial step in constructing the national state perimeters and towards “securing” the ICT infrastructures, and is among the first to start including the supply chain as a fundamental component to meticulously safeguard. Given the high-level directions of the cited decree, it lacked some concrete definitions that could have helped in addressing the subsequent implementation plans. In the following, we provide a viable definition of supply chain, as well as discuss some examples of possible attacks it could be subject to.

A supply chain is the network of all the individuals, resources, organizations, and activities involved in the creation and distribution of specific products to the final buyer. A supply chain attack, also known as third-party attack or value-chain attack, refers to a type of cyber attack that exploits third-party vendors, such as software providers (considered the less-secure gateways of the chain), to target larger organizations. Threat actors exploit the relationship of trust between the organization and the third-party suppliers, as well as the established machine-to-machine communication channels (e.g., software updates) to lay the foundations for attacks, which turn out to be extremely challenging to identify.

Figure 2 shows an excerpt of the complexity of the software supply chain. A software, produced by a small/medium-sized company based in a specific country, with its own regulations and normative, may potentially be adopted from companies, corporations, and government agencies all over the world, across different business, organizational, and technical domains. To make an example, the SolarWinds monitoring and management platform, called Orion, has been adopted by more than 33,000 customers, including American companies such as Nvidia, Cisco, Intel, and FireEye, government agencies, including the US Department of the Treasury, the US Department of Homeland Security, and the US Department of Defense, and dozens of other technology and telecommunication organizations across Europe, Asia, and the Middle East. We provide details about the SolarWinds supply chain attack in Section 4.

The complexity of the supply chain, exemplified in the above paragraph calls for a solution that, on the one hand, should be manageable while, on the other hand, should provide strong





**Figure 2:** Excerpt of the complexity of the software supply chain: highlight of the Cross-domain, Cross-organizational, and Inter-dependency of the different components

security guarantees. One way to achieve this objective is to resort to cybersecurity certifications, such as the ISO/IEC 27001—an international standard that contains the requirements for setting up and managing an Information Security Management System (ISMS).

On June 27h, 2020, the European Cybersecurity Act entered into force, providing a permanent mandate for the European Network and Information Systems Agency (ENISA) with the establishment of a EU-wide cybersecurity certification framework for digital processes, services, and products. The mission of ENISA in the area of the EU cybersecurity framework is outlined as follows: “To pro-actively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, and additional services and tasks” [14]. The cybersecurity certification framework introduced by the Cybersecurity Act provides three levels of reliability and will be voluntary except for ICT processes, products, and services operating in critical areas (e.g., critical infrastructures and personal data management), for which the obligation may be requested.

Cybersecurity certifications for products and processes can be issued either by trusted third parties, such as private companies, or government agencies. However, it is worth noticing that the composition of products and processes individually certified does not necessarily lead to a certified final product or process. Furthermore, we cannot exclude malicious collusion by entities considered trusted with threat actors, perhaps due to conflicts of interest.

The above limitations could be tackled via solutions that automatically verify the integrability of individually certified solutions for cybersecurity purposes. A viable solution would involve

the definition (or exposure) of the software components' interfaces that identify, in a verifiable way, the functionalities provided, as in a black-box approach.

The cited black box approach would simplify software certification methodologies, but must still rely on the cybersecurity technologies' support to analyze the "content of the box". Indeed, even if the functionalities provided by the interface are verified and certified, the software may still have a silent backdoor within it, which may be activated only when specific objectives are reached (or after a specific period of time, as happened in the famous SolarWinds Supply Chain attack, discussed in detail in the next section). For the cited reason, the certification of the software interface functionalities should be supported by security tools that allow static and dynamic analysis of the software, as well as Intrusion Detection and Prevention Systems based on Artificial Intelligence [15, 16, 17]. While the above solution would thwart the attacker's objectives, it should be noted that advanced malware has the ability to realize whether it is running in a controlled environment [18]. This latter feature would be exploited by the malware to (temporarily) not activating the attack, thus avoiding detection. There is, therefore, a urgent need to find suitable ways to analyze malicious software without triggering its defenses [19].

Since the above technology countermeasures could impact on the safety and security of pieces of software that are at the heart of critical infrastructures, and hence of relevant national interest—or impact even on classified systems—, there should be a level of assurance that prevents from possible legal actions in the aftermath of incidents. As such, the legislator, or its regulatory bodies, should issue processes to be adhered by in order to prove that the highlighted countermeasures do satisfy minimal standard requirements. The cited standard should be at least at national level, even if a pan-EU regulation on the certification for cybersecurity elements would be ideal—some steps in this directions have been already taken [14].

In the next section, we will show how the violation of the above exposed principles have led to one of the most dreadful cyberattacks of the last decade: SolarWinds.

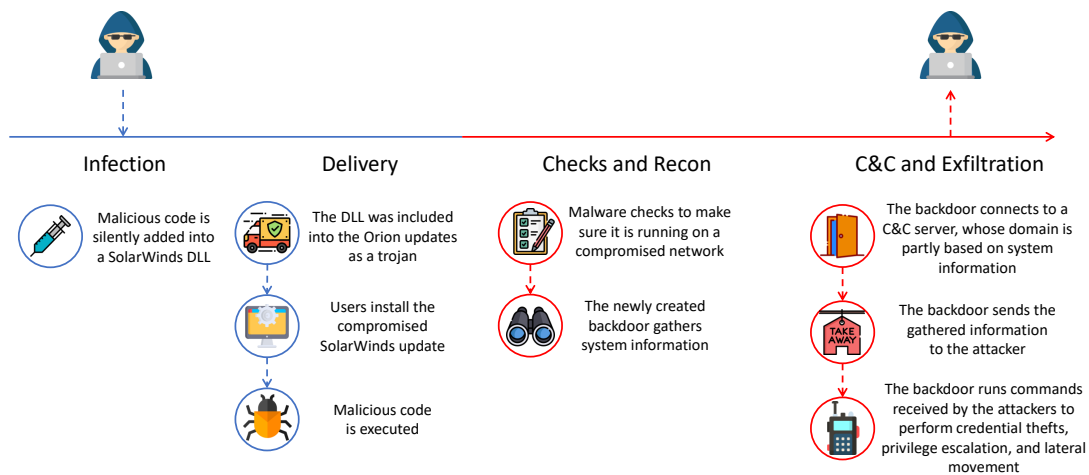
## **4. SolarWinds Supply Chain Attack**

On December 8th, 2020, FireEye's announcement about a breach carried out by a (possibly state-sponsored) sophisticated group of threat actors shook the world.

What surprised most was the attack's target, FireEye, one of the world's top cybersecurity firms that offers its clients (major governments and enterprises) top-notch incident response capabilities and high-profile breach investigation services, as well as the methodology of the attack. On December 13th, 2020, the Washington Post published an article reporting that FireEye was only one of the dozen victims of the breach. According to the article, the breach is part of a broad espionage campaign by Russian state-actors known by the nicknames APT29 or Cozy Bear. Such threat actors were able to virtually break into multiple government agencies, including the US Treasury Department, the US Department of Commerce's National Telecommunications and Information Administration, and the US Department of Homeland Security, after compromising the SolarWinds's Orion Software [20].

Such a breach has been called the SolarWinds Supply Chain Attack (also known as Solarigate, Sunburst, and UNC2452) after SolarWinds, a renowned American company that provides IT management software to help businesses manage their networks, systems, and IT infrastructures.





**Figure 3:** The SolarWinds Supply Chain Attack

With more than 33,000 customers, the SolarWinds Orion Platform is one of the most famous SolarWinds products, consisting of a scalable infrastructure monitoring and management platform thought to simplify the IT administration for hybrid, on-premises, and Software-as-a-Service (SaaS) environments.

The infamous attack started with a threat actor inserting malicious code into a specific portion of the SolarWinds' Dynamic Link Library (DLL), named *SolarWinds.Orion.Core.BusinessLayer.dll*. The threat actors chose to put the code within a method, called *RefreshInternal*, that gets invoked periodically, thus ensuring both its execution and persistence on the system [21]. Such malicious code is lightweight, does not interfere with the DLL's normal operations, and has been developed in such a way as to remain dormant for a random amount of time (around two weeks). According to a Microsoft 365 Defender Research Team analysis, the malicious code within the DLL called a backdoor composed of at least 4,000 lines of code, that allowed the threat actor to operate in the compromised networks without any restriction [21]. Indeed, the method inserted within the DLL file is part of a class, named *OrionImprovementBusinessLayer*, containing all the backdoor capabilities in 13 subclasses and 16 methods, whose strings have been compressed and encoded in Base64 to conceal the malicious code further. This backdoor allows threat actors to perform a wide range of actions, including reconnaissance on the network, lateral movements, privilege escalation, credential theft, and information exfiltration, to name a few.

To make the attack even more difficult to identify, the threat actor digitally signed the compromised DLL, evidence that made Microsoft's researchers think that the attacker was able to access either the company's software development or distribution pipeline. The digital signature allowed the malicious DLL to perform privileged actions while keeping a low profile.

In March 2020, such malicious DLL was included in the Orion updates, thereby *trojaning* them (i.e., making them unwittingly carry malicious code) and infecting multiple government agencies, including the US Department of the Treasury, the US Department of Homeland Security, the US Department of State, the US Department of Defense, and the US Department of Commerce, big tech companies, including Nvidia, Intel, Cisco, Belkin, and VMware, and government agencies networks.

As soon as the compromised DLL reaches a potential victim's machine, it performs several checks to assess the new environment. To make an example, it relies on multiple obfuscated blocklists to check whether processes identified as security-related software are running, such as Windbg, Wireshark, and Autoruns, and whether drivers from security-related software are loaded [21]. The malicious code's goal is to understand whether it is running on an enterprise network or an analyst's machine. Failure of any of these checks would lead to the sudden interruption of the attack, making the threat extremely challenging to detect. Conversely, if all checks are successful, the malicious DLL contacts a remote Command and Control (C&C) server [22]. The C&C domain is composed of four parts, three parts coming from strings that have been hardcoded within the backdoor, while the fourth one is generated dynamically according to some unique information extracted from the victim's device, including the network interface's physical address and the device's domain name. This allows the threat actor to boast a unique subdomain for each of the affected domain [21].

This incident, portrayed in Figure 3, highlighted the severe impact software supply chain attacks can have and showed how most organizations are acutely unprepared to identify and prevent such threats. Supply chain attacks prove to be one of the most difficult threats to prevent since they exploit the long-lasting relationships of trust between customers and suppliers, as well as established machine-to-machine communication channels, such as software updates that the customers inherently trust.

## 5. Conclusion

In this paper, we have discussed the criticalities involved in the current implementation of the supply chain for CIs. In particular, we have moved from the standard definition and scope of CIs, and extended the concept to capture some features of current CIs, as well highlighting the current vulnerabilities they are subject to, with specific reference to the software supply chain. What is more, we have shown that the SolarWinds attack has actually leveraged the current pitfall in the deployed software supply chain, demonstrating that securing it is of paramount importance for the security of the IT infrastructure at a global scale. To achieve this latter objective, we have discussed possible research directions as well as further steps to be undertaken—comprising technology and legislation. The objective of securing the supply chain is both a strategic and a difficult one, requiring the cooperation of different actors, standardization, and adherence to common best practices, to cite a few critical yet not exhaustive action points. It is relieving to note that advanced economies have started taking some steps in the right direction and, as discussed in this paper, Italy can sport probably the best reference framework to start tackling the challenge.

## 6. Acknowledgments

This publication was partially supported by the award NPRP 11S-0109-180242 from the Qatar National Research Fund (QNRF), a member of The Qatar Foundation, and by the Thematic Research Grant Program VPR-TG01-009, funded by Hamad Bin Khalifa University. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF or HBKU.

## References

- [1] J. M. Yusta, G. J. Correa, R. Lacal-Arántegui, Methodologies and applications for critical infrastructure protection: State-of-the-art, *Energy Policy* 39 (2011) 6100–6119. URL: <https://www.sciencedirect.com/science/article/pii/S0301421511005337>. doi:<https://doi.org/10.1016/j.enpol.2011.07.010>, sustainability of biofuels.
- [2] J. E. Sullivan, D. Kamensky, How cyber-attacks in ukraine show the vulnerability of the u.s. power grid, *The Electricity Journal* 30 (2017) 30–35. URL: <https://www.sciencedirect.com/science/article/pii/S1040619017300507>. doi:<https://doi.org/10.1016/j.tej.2017.02.006>.
- [3] S. Algarni, Cybersecurity attacks: Analysis of “wannacry” attack and proposing methods for reducing or preventing such attacks in future, in: M. Tuba, S. Akashe, A. Joshi (Eds.), *ICT Systems and Sustainability*, Springer Singapore, Singapore, 2021, pp. 763–770.
- [4] Gazzetta Ufficiale della Repubblica Italiana, Decreto del Presidente del Consiglio dei Ministri 30 Luglio 2020, n.131, <https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg>, 2020. (Last accessed: May 2021).
- [5] The White House: Office of the Press Secretary, Presidential Policy Directive – Critical Infrastructure Security and Resilience, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>, 2013. (Last accessed: May 2021).
- [6] Council of the European Union, Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, <https://eur-lex.europa.eu/eli/dir/2008/114/oj>, 2008. (Last accessed: May 2021).
- [7] J. A. Phillips, F. Petit, Measuring Critical Infrastructure Risk, Protection, and Resilience in an All-Hazards Environment, John Wiley & Sons, Ltd, 2021, pp. 325–356. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119287490.ch13>. doi:<https://doi.org/10.1002/9781119287490.ch13>.
- [8] B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, *International Journal of Critical Infrastructure Protection* 10 (2015) 3–17. URL: <https://www.sciencedirect.com/science/article/pii/S1874548215000244>. doi:<https://doi.org/10.1016/j.ijcip.2015.04.001>.
- [9] S. Jajodia, V. Subrahmanian, V. Swarup, C. Wang, *Cyber deception*, volume 6, Springer, 2016.
- [10] S. Jajodia, N. Park, F. Pierazzi, A. Pugliese, E. Serra, G. I. Simari, V. S. Subrahmanian, A

probabilistic logic of cyber deception, *IEEE Transactions on Information Forensics and Security* 12 (2017) 2532–2544.

- [11] L. O. Nweke, S. Wolthusen, Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection, in: 2020 12th International Conference on Cyber Conflict (CyCon), volume 1300, 2020, pp. 63–78. doi:10.23919/CyCon49761.2020.9131721.
- [12] Cybersecurity & Infrastructure Security Agency, Critical Infrastructure Sectors, <https://www.cisa.gov/critical-infrastructure-sectors>, 2020. (Last accessed: May 2021).
- [13] R. Di Pietro, S. Raponi, M. Caprolu, S. Cresci, *New Dimensions of Information Warfare*, volume 84, Springer International Publishing, 2021. doi:10.1007/978-3-030-60618-3, part of the *Advances in Information Security* book series.
- [14] European Union Agency for Cybersecurity, EU Cybersecurity Certification Framework, <https://www.enisa.europa.eu/topics/standards/certification>, 2020. (Last accessed: May 2021).
- [15] S. Raponi, M. Caprolu, R. Di Pietro, Intrusion detection at the network edge: Solutions, limitations, and future directions, in: T. Zhang, J. Wei, L.-J. Zhang (Eds.), *Edge Computing – EDGE 2019*, Springer International Publishing, Cham, 2019, pp. 59–75.
- [16] R. Di Pietro, L. V. Mancini, *Intrusion detection systems*, volume 38, Springer Science & Business Media, 2008.
- [17] A. Aldweesh, A. Derhab, A. Z. Emam, Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues, *Knowledge-Based Systems* 189 (2020) 105124.
- [18] A. Afianian, S. Niksefat, B. Sadeghiyan, D. Baptiste, Malware dynamic analysis evasion techniques: A survey, *ACM Computing Surveys (CSUR)* 52 (2019) 1–28.
- [19] M. Lindorfer, C. Kolbitsch, P. M. Comporetti, Detecting environment-sensitive malware, in: *International Workshop on Recent Advances in Intrusion Detection*, Springer, 2011, pp. 338–357.
- [20] E. Nakashima, C. Timberg, Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, [https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781\\_story.html](https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html), 2020. (Last accessed: May 2021).
- [21] Microsoft 365 Defender Research Team, Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers, <https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/>, 2020. (Last accessed: May 2021).
- [22] D. Dittrich, S. Dietrich, Command and control structures in malware, *Usenix magazine* 32 (2007).