# Securing the supply chain: How do we defend against cyber supply chain attacks?

Wolbers, Stephan

# Securing the supply chain

How do we defend against cyber supply chain attacks?

**Stephan Wolbers**

Student ID: s3890996
Supervisor: Dr Zeki Erkin (University of Delft)
Second reader: Dr Tommy van Steen (Leiden University)

January 2025

A thesis presented for the degree of
MSc Cyber Security

Universiteit
Leiden
The Netherlands

# Abstract

Modern society is increasingly reliant on interconnected IT systems, which serve as the backbone of economic and operational efficiency. However, as organizations embrace the digital transformation, they become more vulnerable to cyber supply chain (CSC) attacks. These attacks exploit trusted relationships between organizations and their vendors, impacting potentially thousands of targets through a single compromised supplier.

The rise of CSC attacks underscores their appeal to adversaries where they can attack multiple targets via a single exploit. Whether opportunistic actors seeking financial gain or state-sponsored advanced persistent threats (APTs) pursuing strategic objectives, the sophistication and impact of these attacks continue to challenge existing cybersecurity frameworks. As seen in incidents like SolarWinds, NotPetya, and Kaseya, adversaries leverage the interconnected nature of supply chains to severely damage their targets, either operationally, financially, or reputationally.

This thesis investigates the characteristics of CSC attacks and proposes a classification to distinguish between opportunistic and APT threats, enabling organizations to optimize their countermeasures. The findings highlight the importance of implementing controls proportionate to organizational risk profiles and encourages collaboration across supply chain stakeholders.

# Acknowledgements

I would like to express my sincere gratitude to everyone who has supported me throughout this research journey.

First, I want to thank the course lecturers for their dedication and willingness to share their expertise with us. Their knowledge and enthusiasm have been invaluable in shaping my understanding of the subject.

I am also grateful to my fellow students for their company and conversations, both in and outside the classroom. The discussions, shared experiences, and camaraderie made this journey all the more enjoyable and insightful.

A special thanks to my supervisors, Dr Zeki Erkin and Dr Tommy van Steen, for their guidance and insights. I am particularly grateful to Zeki for talking me through the thesis and assuring me I was on the right track. Their support and expertise have been instrumental in the completion of this work.

Finally, I want to thank my wife, my family, and my friends for their unwavering support throughout this journey. Their encouragement, patience, and belief in me have meant the world. I am truly blessed to be surrounded by so many supportive people.

## Table of Contents

# 1. Introduction

## 1.1 Growing dependence on the IT Supply Chain

The global economy has become increasingly dependent on information technology, which integrate a wide array of hardware, software, and services. In virtually every sector (e.g. manufacturing, finance, healthcare, telecommunications) businesses rely on the seamless functioning of these interconnected systems [1]. However, as organizations become more reliant on these systems, they often do not have the capacity to develop and maintain the assets themselves, which leads to organizations being increasingly dependent on outsourcing their software development [2] or even purchasing software as a service (SaaS) [3]. The dependence on outsourcing has grown alongside the digital transformation, with innovations such as cloud computing [4], [5], Internet of Things (IoT) devices [6], [7], and, more recently, artificial intelligence (AI) [8] becoming integral to operational efficiency and competitive advantage.

The trend toward outsourcing IT functions has also created new challenges in terms of control and risk management. Because the components of a supply chains are often procured from numerous vendors across the globe, organizations have less insight into the security measures applied by third parties [9]. Even open-source software can have vulnerabilities hiding in plain sight, either by mistakes happening during development [10] or by outside groups deliberately injecting malicious code [11]. The vulnerabilities in such scenarios create an inherent risk, as weaknesses or compromises in a single supplier can impact an entire supply chain [12].

As the reliance on IT suppliers grows, so too does the complexity of managing these supply chains [13]. Ensuring security across all suppliers becomes more difficult, especially given the diverse nature of the components and services that organizations use. Many businesses lack the necessary mechanisms to assess the security posture of every supplier in their ecosystem [14], and even fewer have the ability to continuously monitor these suppliers for emerging threats [15].

To combat these challenges governments and international institutions have recognized the need to ensure cybersecurity at every level of the supply chain. For example, in 2016 the European Union has issued a the NIS directive to address "measures for a high common level of security of Network and Information Systems across the Union" [16], with the NIS 2 update published in 2022 [17]. The United States issued an executive order with similar intensions "to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software" [18]. Both these initiatives acknowledge the risks and vulnerabilities of the growing dependency on cyber supply chains and emphasize the necessity of treating security as a core component of supply chain management, not just as an afterthought.

In summary, while the utilization of IT supply chains brings numerous benefits in terms of efficiency and innovation, it also significantly increases the attack surface for cyber criminals. The interconnectivity of modern technology means that vulnerabilities in even the smallest assets can have a significant impact throughout the entire chain, making cyber security a critical aspect of supply chain management. Optimizing cyber security against cyber supply chain (CSC) attacks requires proper understanding of the underlying mechanisms and tailored countermeasures to combat them.

## 1.2 Trend in Cyber Supply Chain Attacks

Over the past decade, cyber supply chain (CSC) attacks have steadily gained traction among adversaries, with their prevalence increasing significantly [12]. Since 2010, CSC attack types such as third-party applications, firmware, malicious attacker applications, and even Open-Source Software

(OSS) have risen sharply, reflecting a diverse array of tactics used to exploit vulnerabilities within supply chains as depicted in Figure 1 [19].

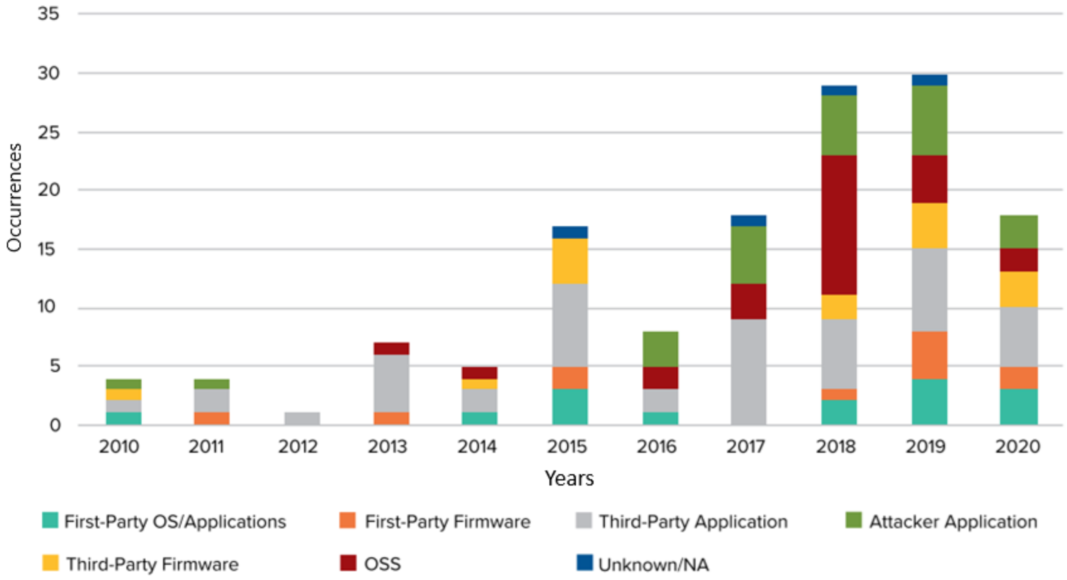

*Figure 1 - Increase in CSC attacks since 2010* [19]

The growing interest in CSC attacks can partly be attributed to their high potential return on investment (ROI): “One compromised organization can lead to hundreds or thousands of follow-on targets” [20]. Additionally, CSC attacks can serve as an entry point for “seeking to exploit a hardened end target” by first compromising less secure third-party entities [20]. This double advantage makes CSC attacks an increasingly attractive strategy for adversaries.

Despite changes in the focus of CSC attacks, the underlying techniques often exhibit continuity. Research indicates that behaviours observed in modern CSC attacks can sometimes be traced back 13 to 20 years, suggesting a persistence in the fundamental methods used by attackers [21]. This consistency offers companies opportunities to implement threat detection and prevention techniques as counter measures are less rapidly becoming obsolete.

## 1.3 Existing research

Due to this surge in CSC attacks several research and frameworks have been developed by governmental institutions, professional organizations, and academic scholars, to address the growing risks associated with them. For example, the U.S. Department of Defense (DoD) have compiled a catalogue of attack patterns and corresponding countermeasures to enhance awareness and guide mitigation strategies for CSC risks [22]. Similarly, the National Institute of Standards and Technology (NIST) has developed a comprehensive framework for Cyber Supply Chain Risk Management (C-SCRM), which provides a structured approach to identifying, assessing, and mitigating risks within supply chains [23]. Furthermore, in Europe the NIS2 Directive emphasizes updated cybersecurity obligations for essential and important entities, including requirements for supply chain security [24].

Professional organizations have also contributed significantly to addressing CSC threats. Microsoft, for example, has proposed strategies to secure software supply chains, emphasizing the importance of transparency and verification in the development and deployment of software [25], [26]. The MITRE Corporation has further contributed by documenting supply chain attack scenarios and proposing mitigations insights to improve supply chain cybersecurity practices [27].

Academically, significant research has focused on enhancing the understanding and management of CSC attacks. In accordance to the NIST framework mentioned earlier, a key element is emphasizing control over IT systems through C-SCRM, “combining elements of cybersecurity, supply chain management, and enterprise risk management […] to exert strategic control over the end-to- end processes” [28], [29]. Building on this framework, research was performed on improved methodology to accurately assess supply chain cyber risks [30]. Once risks could be assessment systematically improvements could be made on cyber threat predictive analytics, providing proactive insights to anticipate and mitigate potential threats [31].

However, most research and frameworks are treating CSC attacks as one type of attack vector when suggesting effective counter measures. One research proposed a classification of CSC attacks using three critical categories—counterfeit hardware and software, direct cyberattacks, and insider threats—that could accommodate in implementing countermeasures to enhance resilience [32]. Though this classification can definitely be useful in improving an organization’s cyber security, it provides only one perspective to distinguish between CSC attacks.

## 1.4 Research Questions

This thesis aims to investigate countermeasures against large-scale cyber supply chain (CSC) attacks and focuses on the following research question:

> *How can we optimize countermeasures for large-scale supply chains attacks within the NIST framework?*

To explore this, several sub-questions are examined. First, it is essential to identify the most impactful types of supply chain attacks:

> *What are the most impactful supply chain attacks?*

Second, we determine how these attacks can be categorized into distinct groups based on their characteristics:

> *How can we classify these attacks?*

Finally, we use this classification as the foundation for identifying targeted countermeasures and assigning priority based on experts’ opinions to determine the effectiveness of these countermeasures. This is assessed through interviews with cybersecurity experts, which helps identify which strategies are most effective for different types of attacks:

> *What priority should be given to countermeasures per classification type?*

## 1.5 Contribution to Controls Against Supply Chain Attacks

This thesis seeks to make a contribution to the development of more effective controls against cyber supply chain attacks. By analysing existing case studies, interviewing industry experts, and developing a classification system for CSC attacks, the research aims to propose optimized countermeasures that can be adapted to different elements of the supply chain. The research also provides insights into prioritizing these measures based on their effectiveness in mitigating specific types of attacks, thereby enhancing the resilience of organizations against CSC threats.

## 1.6 Outline

The thesis is structured to provide a thorough investigation of cyber supply chain attacks and propose solutions to optimize countermeasures.

It begins with an exploration of the background to the research question, detailing the increasing dependence on IT supply chains and the corresponding rise in cyber attacks that exploit vulnerabilities in these systems.

After documenting the chosen methodology, case study analysis and interviews with industry experts, the thesis analyses major cyber supply chain attacks, focusing on their impacts and underlying causes. From this analysis a classification system for CSC attacks is proposed, offering a structured way to categorize different types of threats based on their characteristics and methods.

The semi-structured interviews provide real-world insights into how organizations are responding to these threats, the effectiveness of current countermeasures, and the potential of using the proposed classification.

The discussion evaluates these findings, scrutinizing the proposed classification, reviewing the potential in using the classification, and contributing to any other insights in dealing with cyber supply chain attacks.

Finally, the thesis concludes with a summary of key findings and offers recommendations for future research and action in strengthening defences against CSC attacks.

# 2. Background

## 2.1. Definition of CSC attacks

To better understand the implications and possible countermeasures of Cyber Supply Chain (CSC) attacks we first need to establish a clear definition. A CSC attack is in its basis a cyber attack, which is defined by NIST as:

(1) *An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information* [33].

The second element of the attack concerns the supply chain, which refers to the ICT supply chain and is defined by NIST as:

(2) *The ICT supply chain infrastructure is the integrated set of components (hardware, software and processes) within the organizational boundary that composes the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned.* [23].

Combining both definitions gives you the definition for a CSC attack. Though the definition of the ICT supply chain mentions hardware, software, and processes, the scope of this thesis focuses on software only. Therefore, the final definition that is used for this thesis is:

(3) *A CSC attack is a cyber attack (1) originating outside the main target's organization but within the boundaries of the ICT supply chain infrastructure (2), with a focus on software.*

It is important to note that the definition for a CSC attack excludes a cyber attack on a non-ICT supply chain. For example, in 2012 and 2017 the Saudi-Arabian oil company Aramco was targeted by a malware attack, disrupting the operation [34]. Though it was clearly a cyber attack and Aramco is a crucial part in many supply chains, it is not considered a CSC attack as the attack was directed directly at Aramco and not on any of its ICT suppliers or vendors.

## 2.2. Short history and major incidents of CSC attacks

The rise of CSC attacks highlights the evolution of cyber threats exploiting vulnerabilities in interconnected systems and trusted relationships between organizations and their suppliers. The first incidents of CSC attacks occurred in the late 2000s, with a notable example being Operation Aurora. Major companies like Adobe, Google, and Juniper networks were targets of a phishing campaign where the visit to a malicious website in combination with a zero-day vulnerability in Internet Explorer allowed attackers to download encrypted malware on the victims' machines and to extract intellectual property and user credentials. The level of sophistication was unprecedented in the commercial sector and "it totally changed the threat model", according to McAfee expert Dmitri Alperovitch. Google has attributed the attack to hacking groups from China [35].

Focusing on the ICT supply chain, instead of going for the target directly, marked a new shift in attack strategy and CSC attacks would become more prevalent and more sophisticated in the next decade. The possible level of sophistication was demonstrated by the Stuxnet attack on Iranian uranium enrichment facilities in 2010 [36]. The Iranian nuclear program was considered highly classified and access to its facilities was limited and monitored, making a direct cyber attack quite difficult. To circumvent the security measures a worm was created, allegedly by the U.S.A. and Israel [37], that could autonomously spread through machines via local networks and hardware. As the Iranian nuclear facilities were air gapped as a safety precaution, the worm was targeted on external contractors working on the nuclear program. Their machines were first infected via the internet, after which the worm would be unknowingly brought into the facilities by the contractors on their machines. Once connected to the local network, the worm would spread to the centrifuges [38]. If the worm recognized the machine to be a centrifuge, the programmable logic controllers (PLC) in the centrifuges would be instructed to spin at a higher frequency without alerting engineers, eventually causing failures [36].

One of major advantages CSC attacks have over conventional cyber attacks is the potential to hit multiple targets with the same attack vector. Once you have access to the supplier you can attack all their clients within the same supply chain, though it depends on the internal cyber security of each client how much impact the attack will have. The Solar Winds attack illustrates the potential of supply chain attacks well. In 2020 security company FireEye noticed a breach in their systems and internal investigations showed it originated from SolarWinds' Orion platform. Orion is a platform used for remote monitoring and management of networks and as such requires access to its clients' environments. Further investigation revealed that the Russian hackers group APT-29 (also known as Cozy Bear) gained access to the build process of Orion and was able to inject malicious code in new updates of the software [39]. Through these updates the group was able to infiltrate multiple valuable targets, for example Microsoft, Department of Homeland Security, and the Pentagon [40] (see more in Section 4.5).

## 2.3. Existing research

As CSC attacks become more prevalent and sophisticated ample research has been conducted and many initiatives have been taken to combat them.

Already in 2014, the U.S. Department of Defense (DoD) created a catalogue in which each supply chain attack could be classified based on 12 attributes to correspond to one of 41 attack patterns. One major attribute is the attack type, which described four options of malicious insertion: hardware, software, firmware, and system information/data. Furthermore, they identified 20 different countermeasures which focuses on one of the four attack types and briefly describes what impact implementation would have [22].

In 2022, the European Union (EU) issued the NIS2 Directive as an update to the 2016 NIS1 Directive and in which supply chain security was explicitly mentioned [17]. NIS1 was issued to enhance cyber security for critical infrastructure and provide tools for member states and organizations to protect against cyber threats [16]. Though the directive required organizations to implement risk management that indirectly addressed third-party risks, it did not explicitly address supply chain attacks. After major incidents like SolarWinds [39], Kaseya [41] and NotPetya [42] the EU recognized the need for an update to deal with such incidents and provided specific assessments tools, reporting requirements, and stricter enforcement, specifically regarding CSC attacks.

The incidents concerning CSC attacks mentioned earlier and the attack on the Colonial pipeline [43] was also the trigger for the White House to issue Executive Order (EO) 14028 in 2021 [18], which has the same intention as NIS1 and NIS2 to explicitly provide regulation and guidelines to tackle CSC attacks. The EO has seven key components to achieve that goal:

1. *Removing Barriers to Threat Information Sharing* (section 2) – The federal government and private sector organizations need to enhance their collaboration and are both required to share information about threats and incidents.

2. *Modernizing Federal Government Cybersecurity* (section 3) – Federal agencies are to implement multi-factor authentication, encryption on data and communications, and zero-trust architecture. Furthermore, agencies must adopt modern and secure cloud services.
3. *Enhancing Software Supply Chain Security* (section 4) – Guidelines and standards are to be established by NIST to be used by IT organization in securing the IT supply chain. Furthermore, software suppliers need to provide a Software Bill of Materials (SBOM) to more easily identify components in their products.
4. *Establishing a Cyber Safety Review Board* (section 5) – Significant cyber incidents are to be reviewed by a special board, composed of governments and private sectors experts, and make recommendations for the industry to be used.
5. *Standardizing Federal Government Incident Response* (section 6) – Based on best practices from the industry regarding detection, response, and recovery from CSC attacks, a playbook is to be created to improve consistency and efficiency in cyber incidents response.
6. *Improving Detection of Cybersecurity Vulnerabilities and Incidents* (section 7) – In addition to section 6, the federal government needs to implement Endpoint Detection and Response (EDR) tools to identify and mitigate threats.
7. *Improving Investigative and Remediation Capabilities* – (section 8) – The federal government needs to improve logging of system activities to enable comprehensive investigations of incidents and retain those logs for extended periods.

Following executive order 14028 , section 4, the National Institute of Standards and Technology (NIST) developed a comprehensive framework for Cyber Supply Chain Risk Management (C-SCRM), which provides a structured approach to “identifying, assessing, and mitigating risks within supply chains” [23]. C-SCRM builds on the generic NIST Cyber Security Framework (CSF) and uses both its functions (i.e. Identify, Protect, Detect, Respond, Recover, and Govern) as well as its tiers to indicate maturity (i.e. 1. Partial, 2. Risk Informed, 3. Repeatable, 4. Adaptive) [44]. Based on the six CSF functions, the framework suggests eight key practices to properly manage supply chain risks:

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Know and Manage Critical Components and Suppliers
4. Understand the Organization’s Supply Chain
5. Closely Collaborate with Key Suppliers
6. Include Key Suppliers in Resilience and Improvement Activities
7. Assess and Monitor Throughout the Supplier Relationship
8. Plan for the Full Life Cycle

Simultaneously, professional organization also recognized the need to address the risk of CSC attack and started creating their own frameworks and initiatives. Microsoft already published a white paper in 2011 where it advocated that any supply chain security efforts must be risk-based, transparent, flexible, and reciprocal [25]. To assess any supply chains risks it uses one of two approaches: Standards Correlation and Business Process Modelling. Both have 6 phases of assessing risks: planning, discovery, assessment, development, validation, and implementation. The preferred approach is the Standard Correlations, where it uses mature standard and tends to be less resource intensive. If the standards are not available or not mature enough Microsoft uses the Business Process Model, where the supply chain process is properly detailed to help identify and process any risks and weaknesses in it [26].

In 2017 MITRE published their supply chain framework which focuses on four goals to defend against malicious parties [27]:

1. Reduce attacks
2. Diminish success of attacks
3. Gain and share information about attacks
4. Recover from attacks

To achieve these goals MITRE recognizes 5 possible phases. In the early phases (i.e. *Materiel Solutions Analysis* and *Technology Maturity & Risk Reduction*) the emphasis lies on techniques like privilege restriction, segmentation, non-persistence, and deception to reduce opportunities for adversary reconnaissance and limit initial footholds. During the following phases (i.e. *Engineering & Manufacturing Development* and *Production & Deployment*) controls are expanded to include substantiated integrity checks, analytic monitoring, and unpredictability. These techniques help detect adversarial presence, prevent the introduction of malicious components, and gather intelligence that can be used to further harden defences. Finally in the last phase (i.e. *Operations & Support Phase*), with the system fully operational, defenders have fewer opportunities to prevent attacks from occurring. Instead, they focus on adaptive response, coordinated defence, and analytic and monitoring techniques.

These frameworks are the subjects of the academic field as well. A survey on NIST's C-SCRM framework was conducted, outlining the research initiatives since its creation as well as a detailed analysis of the results of a four-year research project on CSCRM [28]. Moreover, in 2022 an exploratory survey was conducted to appraise the differences in perception between organization with the same supply chain [29]. It showed that the focus of implementation the framework should be organized over the entire supply chain, ideally with key players taking the initiative to orchestrate the C-SCRM process while simultaneously increase the amount of information shared throughout the supply chain.

One of the key elements in most framework is to accurately assess supply chain cyber risks. A new methodology, called MITIGATE, was proposed to analyse the risk level of the whole supply chain [30]. This methodology combines "publicly available information, well-defined mathematical approaches and best practices to automatically identify and assess vulnerabilities and potential threats of the involved cyber assets". It requires a complete list of assets within the entire supply chain, a list of all potential attack paths within the chain, an estimation of zero-day vulnerabilities, and an evaluation of vulnerabilities on an individual, cumulative, and propagated level, to finally create an optimal mitigation strategy.

To further automate the risk and threat analysis, efforts have been made to apply machine learning (ML) to the CSC attacks [31]. Using the Microsoft Malware Prediction dataset, it takes incidents reports and tactics, techniques, and procedures (TTP) as input to generate indicators of compromise (IoC) and vulnerabilities as output, trying out four different ML algorithms: Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT). It showed that Spyware and Ransomware, together with spear phishing are the most predictive threats in CSC.

The predictiveness of CSC attacks is further supported by an empirical study of the most prominent CSC attacks and their characteristics [21]. Based on the Atlantic Council's SSCA's (i.e. CSC attacks) dataset, 7 samples from over 100 attacks are selected, manually inspected and its behaviours characterized. Divided into three file classes, malware, benign, and Windows 10, binaries from a private industry partner's dataset are matched to the selected samples on behaviours and assigned a conditional probability. It showed that "the presence of an SSCA behaviour within a binary indicates malware with 86-100% probability". Furthermore, it showed that CSC attack behaviours have been available for 13-21 year prior to each attack, providing an opportunity for mitigation.

Finally, one research proposed their own classification of CSC attacks to assess the most effective countermeasures, based on three different categories [32]. It distinguishes between counterfeits (for both hardware and software), direct cyberattacks, and insider threats, which each have different issues. Counterfeiting involves to use of non-authentic or (in the case of an CSC attack) tampered components that jeopardize system performance and trustworthiness. Cyberattacks (e.g. malware, Distributed Denial of Service (DDoS) attacks, and data breaches) exploit system vulnerabilities, disrupting operations and causing significant damage. Meanwhile, insider threats come from individuals with authorized access who, intentionally or accidentally, reveal sensitive information or sabotage systems from within.

# 3. Methodology

## 3.1. Methodology overview

For this thesis the methodology begins with an analysis of several CSC attacks, selected by criteria outlined in Section 3.2. In this analysis for each attack we explain how the attack originated, what techniques were used, what level of complexity the attack had, and what the impact was on the target. Furthermore, the attacks are compared with each other using the MITRE ATT&CK framework [45] and highlighting the major differences by indicating what MITRE tactics and techniques were utilized. This analysis is used as a base for the proposed classification of CSC attacks to optimize counter measures.

Using the proposed classification interviews were conducted with cyber security experts in a semi-structured fashion and selected bases on the criteria outlined in Section 3.3. The interviews were used on one hand to cast a better light on the current situation in cyber space concerning CSC attacks, and on the other hand to assess the proposed classification, assign priorities to each category, and discuss effective counter measures for individual categories as well as CSC attacks as a whole.

The data gathered from the interviews are used to optimize counter measure against CSC attacks using the proposed classification, improve said classification with suggestions from the experts, and finally, make recommendations which can be used by the cyber security community.

## 3.2. Criteria for analysis

For the selection of incidents to be analysed in chapter 4 we exclude incidents caused by human errors from the scope. Though the recent incident with CrowdStrike software [46] demonstrated such errors can have major impacts in the IT supply chain, our aim is to optimize counter measures against purposeful attacks, not human error.

Developments are going fast in world of IT and organization need to keep up in order to defend themselves against cyber attacks. To make sure any recommendations based on the analysis attacks are not immediately outdated the attacks need to have happened in the last twelve years. This period also corresponds with the rise of CSC attacks, as mentioned in Section 1.2.

Modern cyber supply chains are often global in nature and to provide companies insights in protecting against CSC attacks the focus should be on the international domain or at least applicable around the world. Local attacks are specific to local contexts (e.g. laws, infrastructure), which are not applicable for global solutions.

Optimization of counter measures is only useful if the attacks are worth defending against. Selected attacks should have a high (potential) impact, which could be measured from an economical (i.e. at least 100.000 targeted users or $10.000.000 in damages), operational (i.e. significant disruption in critical or key sectors (e.g. energy, health, finance)), reputational (e.g. long lasting damage to the reputation, causing loss of customer trust, market share, or legal consequences) or compliance (i.e. compromise of sensitive, personal, or classified information) perspective.

As the attacks are also analysed from a technical perspective trustworthy sources are required. Even if the impact suits all other criteria, it could happen that an incident for example has been classified or too recent to be researched yet to find proper sources. We consider sources like peer-reviewed journals, official government reports, reports from respected cybersecurity firms (e.g., FireEye, CrowdStrike, Symantec), and articles from media outlets with respected investigative reporting on cybersecurity matters (e.g., The New York Times, The Guardian, The Washington Post).

Finally, we exclude CSC attacks focused on hardware components from the scope of this thesis. Though these types of attacks are worth further investigation, counter measures tend to be quite different from software focused attacks making the scope too large considering the timeframe of this research.

## 3.3. Criteria for interviewees and possible bias

As the scope of this thesis is not limited to any specific field, experts from all sectors were eligible to participate in the interviews. However, the experts were required to have several years of experience in the field of cyber security and hold (or have held) a leadership role within their organization. An effort was made to talk to experts from both (semi-)government institutions and business, as well as from the consultancy, vendor and consumer domain.

The first experts were selected based on the personal network of the author, who consequently recommended other experts in their respective networks. This could possible have led to experiences and perspectives with an emphasis on the Netherlands.

# 4. Analysis of notable CSC attacks

## 4.1. Target

The Target supply chain attack, revealed in late 2013, exploited vulnerabilities in a third-party vendor, Fazio Mechanical Services, to compromise Target’s network. Before the attack occurred, reconnaissance was done using open-source intelligence about suppliers [47]. Initial access was achieved when attackers deployed the Citadel Trojan via a phishing email to infiltrate Fazio's systems. Inside their systems, the attackers acquired Target-specific credentials and used them to upload a malicious executable to either Target's external billing system or business network [48]. Weak network segmentation within Target’s infrastructure facilitated lateral movement [49].

Once inside the Target systems, attackers deployed malware (BlackPOS/Kaptoxa) on Target’s Point of Sale (PoS) devices (e.g. card readers or terminals), enabling them to collect credit card numbers from transactions. Using the SMB (Server Message Block) protocol stolen data was transferred from PoS devices to be stored on internal FTP servers before final exfiltration [50].

Defence evasion techniques included string obfuscation, self-destructing code, data encryption, and limiting malware communication to business hours to blend in with normal activity. The customized malware also contained hardcoded IP addresses and credentials to evade detection [49].

Exfiltration of the stolen data was carried out using drop sites located in Miami and Brazil, ensuring a layered approach to avoid early detection [49], [51].

## 4.2. NotPetya

The NotPetya ransomware attack emerged in 2017 and targeted organizations globally, causing widespread disruption by encrypting entire systems. Though it masqueraded as traditional ransomware, it lacked a reliable mechanism to issue decryption keys, suggesting its primary goal appeared to be destruction rather than financial gain [52]. The attack was attributed to the Russian hackers group *Sandworm,* which operates under the Russian Main Intelligence Directorate (GRU) [53].

The initial injection of NotPetya occurred through the compromise of the Ukrainian MeDoc accounting software, a widely used platform for tax-related operations. Adversaries injected malicious code into MeDoc updates, which after installation downloaded a file named *perfc.dat* to the *C:\Windows* directory of the targeted systems [42]. After gaining a foothold, NotPetya escalated privileges using the Windows API to gain administration rights over the infected system. This allowed the ransomware to execute system-wide changes and propagate in an automated manner to remote machines within the same network, utilizing tools like PsExec and Windows Management Instrumentation (WMI) [42], [54].

NotPetya leveraged EternalBlue and EternalRomance, two exploits originally developed by the U.S. National Security Agency (NSA) and later leaked by the Shadow Brokers group [55]. These exploits allowed attackers to deploy the DoublePulsar malware on victim systems, which served as the C&C-centre for further malicious activities (Virsec, 2017).

Once deployed, NotPetya encrypted the entire system, including the Master File Table (MFT), rendering the operating system inaccessible. The ransomware used RSA encryption, making decryption theoretically only possible with the private key. However, due to a faulty implementation of the Salsa20 cipher, it allowed both Petya and NotPetya targeted systems to be decrypted and the data to be recovered (Eschweiler, 2017).

## 4.3. CCleaner

The CCleaner attack was a CSC attack targeting the widely used PC optimization tool, CCleaner, developed by Piriform (later acquired by Avast). It was discovered in September 2017 by Cisco Talos researchers using advanced exploit detection technologies. Adversaries infiltrated CCleaner's build process and injected malicious code into legitimate versions of the software distributed to major clients [56].

The attackers gained access to the software's build environment by exploiting vulnerabilities in its C++ runtime. Evidence of this infiltration includes a PDB (Program Database) file, an artifact of the compilation process, and the fact the malicious versions were signed using valid digital certificates issued to Piriform. Additionally, the IMAGE_DOS_HEADER in the malicious DLL was zeroed out to hinder reverse engineering [57].

The compromised CCleaner installer was distributed by legitimate servers and contained two malicious components:

1. A Position-Independent Code (PIC) Portable Executable (PE) loader used to load DLLs into memory for execution
2. A DLL file named CBkdr.dll, which contains the actual payload.

The DLL executed multiple tasks. First it checked user privileges and would only continue with administrator rights. It would then retrieve system information, encoding it in Base64 to be send to the C&C server. If any data would return from the C&C-server it would story it in memory and execute it. Finally, after the infection was completed, it would setup Return-Oriented Programming (ROP) to clean up memory associated with both the PE loader and the DLL and then exit the thread. The complete process can be summarized with the diagram from [57].

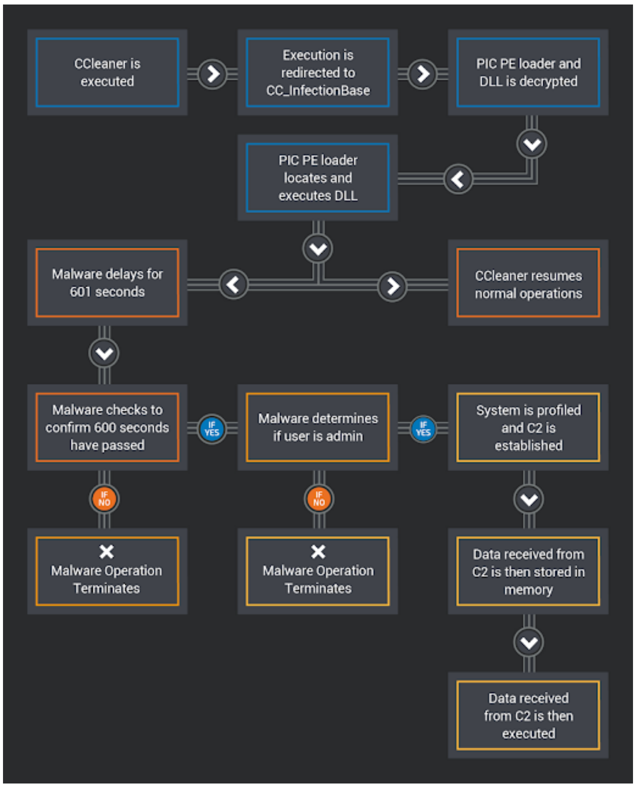
CCleaner is executed
Execution is redirected to CC_InfectionBase
PIC PE loader and DLL is decrypted
PIC PE loader locates and executes DLL
Malware delays for 601 seconds
CCleaner resumes normal operations
Malware checks to confirm 600 seconds have passed
IF YES
Malware determines if user is admin
IF YES
System is profiled and C2 is established
IF NO
IF NO
Malware Operation Terminates
Malware Operation Terminates
Data received from C2 is then stored in memory
Data received from C2 is then executed

*Figure 2 - CCleaner malware process flow* [57]

The malware connected to speccy[.]piriform[.]com, a legitimate Piriform platform. If no response was received, it used a Domain Generation Algorithm (DGA) to locate alternate C&C-servers. The C&C-server verified traffic was from an infected system and delivered the actual payload, which was Base64-decoded, decrypted, and executed in memory before being deallocated. The delivery code also contained a list of specific domains which identified high-value targets. A notable clue was the use of the PRC time zone, possibly suggesting Chinese involvement, although this may have been a deliberate decoy [57].

## 4.4. Shadowpad

The ShadowPad attack in 2017 involved a backdoor embedded within the legitimate code library *nssock2.dll* in software distributed by NetSarang, including tools like Xmanager, Xshell, Xftp, and Xlpd. Adversaries gained access to NetSarang's download servers, either compromising the build process or replacing legitimate installers with modified versions containing the backdoor. It was discovered after one of the customers noticed "a suspicious DNS request coming from an installed software package on their own network" [58].

To avoid detection, the malicious software was signed with a valid digital certificate, giving it the appearance of legitimacy. Once installed on a target system, the malware communicated with C&C-servers. Initially, it transmitted basic information such as the computer name, domain name, and usernames every eight hours. The backdoor remained dormant until it received a specific DNS TXT response from a designated C&C domain. These C&C domains were dynamically generated, changing based on the month and year. All data exchanged with the C&C server was encrypted using a proprietary algorithm and encoded into Latin characters to obfuscate its purpose [59], [60].

The malware included capabilities for lateral movement, allowing it to infect other hosts on the same network by exploiting existing vulnerabilities [58]. Once activated, the backdoor could download and execute arbitrary code from the C&C server or maintain a virtual file system (VFS) stored within the Windows Registry, enabling stealthy persistence on the compromised system [60].

## 4.5. SolarWinds

The SolarWinds Orion attack was a supply chain attack between 2019 and 2020, where the Russian APT29, also known as Cozy Bear, infiltrated SolarWinds' Orion platform and was able to inject malicious code into certificate signed updates [61]. The infiltration was first discovered by the security company FireEye [62]. It was attributed to the Russian hackers group *Cozy Bear,* which operates under the Russian Main Intelligence Directorate (GRU) [63].

Initial access was achieved after initial reconnaissance and eventually stealing authorized credentials from a third-party client that was using the platform [40]. Due to the nature of the platform abilities, where it has access and control over external networks to manage remotely, the attackers were able to gain access to major organization (e.g. Microsoft, Intel, Cisco) and government agencies (e.g. Infrastructure Security Agency, Department of Homeland Security, Department of the Treasury, Department of Justice, Pentagon) [40].

After gaining access to the platform the intruders managed to escalate their privilege by manipulating SAML tokens [64] and using those to extract legitimate credentials for lateral movement [39]. The main target was the build process where new updates of the platform were created and distributed to SolarWinds' clients. By using a temporary file replacement technique the infiltrates managed to inject code during the build process, but before the signing process which meant that new updates (with malicious code) would seem legitimate by clients [39]. After control of the building process a small code fragment was injected first to see if it could get published without detection [40].

Once the build process was infiltrated, the malware required a Command & Control (C&C) feature to continue communication after distribution to Orion's clients with the C&C server. A DomainName Generation Algorithm (DGA) was utilized to communicate using varying DNS requests, based on the subdomain *avsvmcloud[.]com* [39]. If compromised or deemed not worthwhile the malware could be deactivated using a kill switch, executed by the C&C server by sending an IP address from a hardcoded list [40]. In fact, the malware had multiple modes that could be switched between using DNS A records: passive, active, disabled. In active mode, communication would follow the HTTP protocol [65].

To prevent detection from Orion or their clients the malware leveraged multiple defence evasion techniques. The code starts using existing Dynamic Link Libraries (DLL) in the platform, in particular *SolarWinds.Orion.Core.BusinessLayer.dll*, to communicate similar to legitimate Orion activity [39]. One of the first thing the DLL checks is if any anti-virus or detection services are active by comparing running services with hard-coded blocklists. If services are found, the code will either try to disable it in Windows Registry or deactivate itself [39]. Furthermore, any messaging done by the malware is DEFLATE compressed and then XOR-ed to obfuscate the meaning. Finally, hostnames used by the malware mimic the victim's environment as close as possible, VPNs are utilized to use IP addresses from the victim's country, existing utilities and scheduled tasks are used to execute malicious actions, and any backdoors were removed once legitimate remote access was achieved [39]. After recovery of the code of the malware, no sign of human artifacts were found that could point to "anything that a human might have inadvertently left behind as a clue" [62].

## 4.6. Shadowhammer

The ShadowHammer attack was discovered in 2019 by Kaspersky using advanced supply-chain detection technologies. The CSC attack leveraged malicious updates to install a backdoor in targeted systems and was sophisticated in its execution and precision, targeting only devices with specific characteristics [66], [67]. The backdoor was an updated version of ShadowPad, a malware family previously identified in 2017 [67] (see also Section 4.4).

The attackers likely gained initial access through the compromised CCleaner platform (see also Section 4.3), as both attacks have many similarities and are likely executed by the same Chinese APT group BARIUM [68]. However, the injection for ShadowHammer was more sophisticated, targeting ASUS users through a malicious update tool called *setup.exe,* disguised as a legitimate executable [67]. This malicious file was based on an older version of ASUS's update utility from 2015, suggesting that attackers did not access the build server directly but worked with previously obtained software [66].

The adversaries employed different samples of Shadowhammer over the course of the attacks. Older samples replaced the WinMain function with a harmful version implemented in shellcode. The executable was copied into heap memory and executed using hard-coded offsets and sizes. New samples used a more advanced approach, involving a small patch to a C Runtime (CRT) function. This shellcode copied encrypted data into memory, where it was XOR-decrypted to avoid detection [67].

ShadowHammer setup communication with a C&C server at asushotfix[.]com. Once connected, the malware fetched a second-stage payload, which often included the PlugX backdoor [67]. However, the C&C-server was already shut down in November 2018, before the attack was publicly discovered [66].

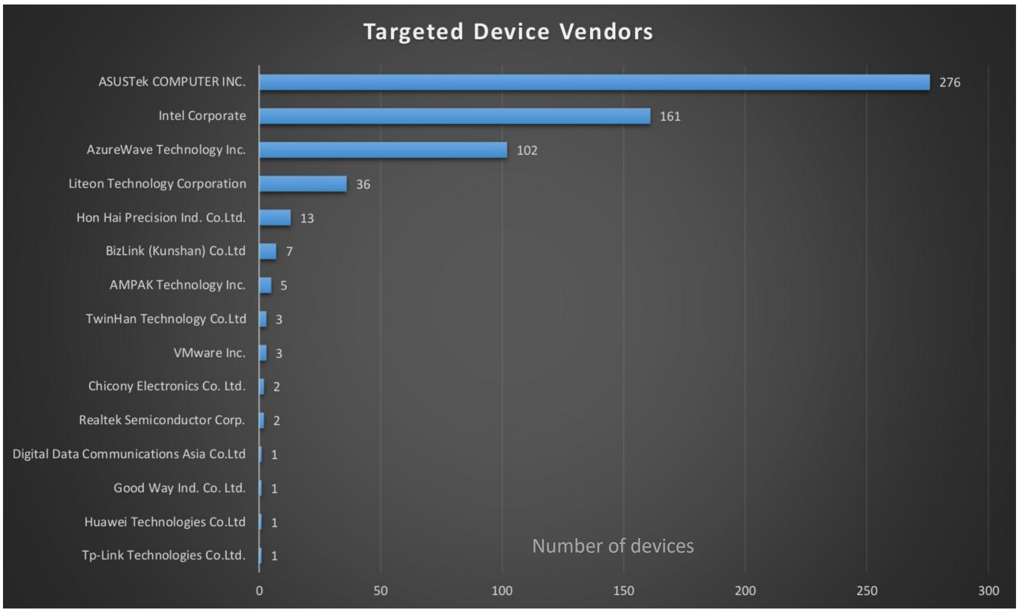

*Figure 3 - Target devices per vendor* [67]

The campaign’s execution was highly selective, targeting only 600 specific MAC addresses which were hardcoded stored in the malicious code (see Figure 3) [66], [67]. The attackers used compromised ASUS digital certificates issued by DigiCert SHA2 Assured ID Code Signing CA to authenticate the update files, providing an air of legitimacy. However, these certificates were also used to sign at least 3,000 legitimate ASUS files, delaying the invalidation of the certificates by ASUS [67].

## 4.7. Kaseya

The Kaseya ransomware attack in 2021 exploited vulnerabilities in Kaseya's Virtual System Administrator (VSA), a remote software management tool widely used by Managed Service Providers (MSPs) to manage customer systems, particularly for small organizations unable to do so themselves [41]. The vulnerability, identified as CVE-2021-30116, was discovered by the Dutch Institute for Vulnerability Disclosure (DIVD), which initiated a Coordinated Vulnerability Disclosure (CVD) process with Kaseya to develop a patch [41]. However, before the patch could be released, the Russian hacker group REvil exploited this vulnerability to gain unauthorized access to Kaseya VSA servers [69].

REvil claimed responsibility for the attack, which affected between 1,000 and 2,000 businesses. The group demanded a $70 million ransom from Kaseya in exchange for global decryption [70]. The ransomware was delivered through an automatic software update mechanism, inserting a malicious file named *agent.crt* into the Kaseya working directory as part of a hotfix update for Windows systems [71]. A synchronized PowerShell command was executed to load a malicious DLL into memory, encrypting data on the affected systems [72].

To evade detection, the attackers employed multiple defence evasion techniques, including disabling Windows Defender’s Real-Time Protection, masquerading the payload by appending random numbers to avoid hash-based detection, using Base64 encoding and decoding for malicious code snippets, removing the payload after execution, and signing the program with a valid certificate to appear legitimate [71].

## 4.8. 3CX

The 3CX attack in 2023 involved a double supply chain compromise, targeting the *3CX Desktop App*, a Voice over Internet Protocol (VoIP) application used for chat, video calls, and voice communications.

The initial compromise vector was the *X_Trader* software from Trading Technology, which was in turn used to deliver a malicious version of the 3CX Desktop App [73]. The X_Trader installer, downloaded from its legitimate website, was malicious but signed with a valid certificate. However, it remains unclear why the X_Trader software was present on 3CX machines [74].

The execution of the malicious X_Trader installer involved running a *setup.exe* file that contained two trojanized DLLs and a begin executable. The executable side-loaded the DLLs, which decrypted and loaded a modular backdoor named *VEILEDSIGNAL* into memory. *VEILEDSIGNAL* supported commands for sending implant data, executing shell code, and self-termination. Additionally, a process injection module targeted browser processes (e.g., Chrome, Firefox, Edge) to inject a communications module that send encrypted data to the C&C server using AES-256 GCM [73].

The attackers moved laterally within 3CX's environment using the Fast Reverse Proxy project [75] and by harvesting credentials, eventually compromising both Windows and macOS build environments [73]. This enabled them to deliver a trojanized version of the 3CX Desktop App. The malicious 3CX Desktop App used a downloader named *SUDDENICON*, which retrieved C&C server information from encrypted icon files hosted on GitHub. The C&C server subsequently delivered *ICONICSTEALER*, a data miner designed to steal browser information [73].

The attackers' infrastructure used the URL *www.tradingtechnologies[.]com/trading/order-management* to facilitate C&C communications [73]. Analysis of the attack pointed to North Korean involvement, specifically attributing the attack to the Lazarus Group (a.k.a. APT38) due to the use of similar malware, like *AppleJeus*, in cryptocurrency theft operations [73], [76].

## 4.9. XZ backdoor

The XZ backdoor attack was a CSC attack targeting the open-source XZ utils library, which was used in most Linux distributions. The backdoor was eventually discovered by Andres Freund, a Microsoft engineer, who identified performance anomalies in Debian systems linked to the SSH protocol [77].

The attack began with a social engineering campaign to gain developer access to the open-source project, starting in 2021. A user named JiaT75 (Jia Tan) created a GitHub account and authored multiple innocuous patches to establish themselves as a legitimate contributor [78]. In 2022, discussions initiated by users Jigar Kumar and Dennis Ens, who were not active in any other project discussions, pressured Lasse Collin, the original developer of the XZ project, to add Jia Tan as a developer [79]. By 2023, after gaining full trust, Tan merged their first commit, followed by changes to the testing infrastructure to obscure malicious content [80]. In March 2024, another account, Hans Jansen requested the inclusion of the compromised version in Debian. Its account was only one week old and didn't show any activity in other projects. Its pull request was supported by anonymous, recently created accounts, further advancing the infiltration (Kaspersky, 2024a).

The malicious version was executed by linking the XZ utilities library to the *sshd* process, a patched version of OpenSSH, leveraging *systemd* features (Kaspersky, 2024b). The malicious payload was distributed across two levels, a shell script and an object file, hidden within the build infrastructure and test data files (Kaspersky, 2024b). Once extracted, the malicious binary object hooked functions from the SSH library, enabling remote code execution (Leite & Belov, 2024).

To evade detection, the attackers incorporated an anti-replay mechanism to prevent capture or hijacking of the backdoor, used steganography to hide a public key, and suppressed logs of unauthorized SSH connections (Leite & Belov, 2024).

## 4.10. Comparison of attacks

To compare the complexity of the attacks in this Chapter, we use the MITRE ATT&CK framework to distinguish between the different tactics and techniques used [45]. The framework uses 14 different tactics (i.e. *Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact*) which can be further divided into numerous techniques. Not all tactics need to be used in an attack, just like not all techniques within a tactic are used. By characterizing the attack by their used MITRE ATT&CK techniques, we can more easily compare them and discuss the complexity. An overview of the comparison can be found in Table 1.

| Tactics | Subtech | *SolarWinds* | *NotPetya* | *Shadowhammer* | *CCleaner* | *Shadowpad* | *Target* | *XZ backdoor* | *Kaseya* | *3CX* |
|---|---|---|---|---|---|---|---|---|---|---|
| Collection | Data from Local System | v | | v | v | v | v | | v | v |
| Collection | Data from Network Shared Drive | v | | v | v | v | v | | v | v |
| Collection | Data Staged: Remote Data Staging | v | | | | | v | | | |
| Command and Control | Application Layer Protocol: Web Protocols | v | | v | v | v | v | v | | v |
| Command and Control | Application Layer Protocol: DNS | v | | v | | v | | | | |
| Command and Control | Ingress Tool Transfer | v | v | v | v | v | | | | |
| Command and Control | Data Encoding: Standard Encoding | v | | v | v | v | | v | v | |
| Command and Control | Dynamic Resolution: Domain Generation Algorithms | v | | | v | | | | | |
| Command and Control | Encrypted Channel: Symmetric Cryptography | | | v | v | v | v | v | v | v |
| Command and Control | Hide Infrastructure | v | | v | v | v | | v | v | |
| Credential Access | OS Credential Dumping: LSASS Memory | | v | | | | | | | |
| Credential Access | Unsecured Credentials | | | | | | | | | v |
| Credential Access | Credentials from Password Stores | v | | | | | v | | | |
| Credential Access | Steal or Forge Authentication Certificates | | | v | v | v | | | | |
| Defense Evasion | Obfuscated Files or Information | v | | v | v | v | v | v | v | v |
| Defense Evasion | Masquerading | v | v | v | v | v | | | v | |
| Defense Evasion | Indicator Removal: Clear Windows Event Logs | | v | | | | | | | |
| Defense Evasion | Indicator Removal: Clear Linux or Mac System Logs | | | | | | | v | | |
| Defense Evasion | Indicator Removal: File Deletion | v | | | v | | | v | v | |
| Defense Evasion | Indicator Removal | v | | | v | | | | | |
| Defense Evasion | Deobfuscate/Decode Files or Information | v | | v | v | v | v | v | v | v |
| Defense Evasion | System Binary Proxy Execution: Rundll32 | v | v | | | | | | | |
| Defense Evasion | Subvert Trust Controls: Code Signing | v | | | | | | | v | |
| Defense Evasion | Impair Defenses: Disable or Modify Tools | v | | | | | | | v | |
| Defense Evasion | Impair Defenses: Disable or Modify System Firewall | v | | | | | | | v | |
| Defense Evasion, Initial Acc | Valid Accounts: Local Accounts | v | v | v | v | | v | | | |
| Defense Evasion, Initial Acc | Valid Accounts: Cloud Accounts | v | | | | | v | | v | |
| Defense Evasion, Persistenc | Hijack Execution Flow: DLL Side-Loading | v | | | v | v | v | v | v | v |
| Discovery | Remote System Discovery | v | | v | v | v | v | | | v |
| Discovery | Process Discovery | v | | | | | v | | | v |
| Discovery | System Information Discovery | v | | v | v | v | v | v | v | v |
| Discovery | File and Directory Discovery | v | v | v | v | v | v | v | v | v |
| Discovery | Network Share Discovery | | | v | v | v | v | | | v |
| Discovery | Software Discovery: Security Software Discovery | v | v | | | | | | | |
| Execution | Windows Management Instrumentation | v | v | | | | | | | |
| Execution | Command and Scripting Interpreter: PowerShell | v | | v | v | v | | | v | v |
| Execution | Command and Scripting Interpreter: Unix Shell | | | | | | | v | | |
| Execution | System Services: Service Execution | v | v | | | | | | | |
| Execution, Persistence, Priv | Scheduled Task/Job: Scheduled Task | v | v | | | | | | | |
| Exfiltration | Exfiltration Over C2 Channel | v | | v | v | v | v | | | v |
| Exfiltration | Exfiltration Over Alternative Protocol | v | | | | | v | | | |
| Impact | Data Encrypted for Impact | | v | | | | | | v | |
| Impact | System Shutdown/Reboot | | v | | | | | | | |
| Impact | Loss of Productivity and Revenue | | v | | | | | | | |
| Impact | Financial Theft | | | | | | v | | | v |
| Initial Access | Exploit Public-Facing Application | v | | v | | | | | v | v |
| Initial Access | Supply Chain Compromise: Compromise Software Supply Chain | v | v | v | v | v | v | v | v | v |
| Initial Access | Trusted Relationship | v | v | v | v | v | v | v | v | v |
| Initial Access, Persistence | External Remote Services | v | | | | | v | v | | |
| Initial Access | Phishing: Spearphishing Link | | | | | | v | | | |
| Lateral Movement | Remote Services | | | | | | | | | v |
| Lateral Movement | Remote Services: SMB/Windows Admin Shares | v | v | | | | v | | | |
| Lateral Movement | Remote Services: Windows Remote Management | v | | | | | | | v | |
| Lateral Movement | Exploitation of Remote Services | | v | v | | | v | | | |
| Lateral Movement | Lateral Tool Transfer | | v | | | | | | | |
| Reconnaissance | Gather Victim Identity Information: Credentials | v | | | | | v | | | |
| Resource Development | Acquire Infrastructure: Domains | v | | v | v | v | v | | | |
| Resource Development | Develop Capabilities: Malware | v | v | v | v | v | v | v | v | |
| Resource Development | Obtain Capabilities: Digital Certificates | v | | v | v | v | | | v | v |
| Resource Development | Obtain Capabilities: Digital Certificates | v | | v | v | v | | | v | v |

*Table 1 - Analysis of MITRE ATT&CK techniques of the attacks*

# 5. Proposed classification

An Advanced Persistent Threat (APT) is a sophisticated, enduring cyberattack orchestrated by well-resourced and highly skilled adversaries, often nation-states or sponsored by them. It was first described in the following manner [81]:

- **Advanced** – "means the adversary can operate in the full spectrum of computer intrusion. They can use the most pedestrian publicly available exploit against a well-known vulnerability, or they can elevate their game to research new vulnerabilities and develop custom exploits, depending on the target's posture."
- **Persistent** – "means the adversary is formally tasked to accomplish a mission. They are not opportunistic intruders. Like an intelligence unit, they receive directives and work to satisfy their masters. Persistent does not necessarily mean they need to constantly execute malicious code on victim computers. Rather, they maintain the level of interaction needed to execute their objectives."
- **Threat** – "means the adversary is not a piece of mindless code. The opposition is a threat because it is organized and funded and motivated. Some people speak of multiple "groups" consisting of dedicated "crews" with various missions."

In 2011 NIST came with the following definition [82]:

> *"An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:*
>
> *(i) pursues its objectives repeatedly over an extended period of time;*
> *(ii) adapts to defenders' efforts to resist it; and*
> *(iii) is determined to maintain the level of interaction."*

Extending on the above definitions of APT we can describe two categories of CSC attacks, with a summary of the characteristics of both shown in Table 2.

## 5.1. APT attack

An **APT** CSC attack can be described by a focus on **long-term intelligence gathering**, targeting critical infrastructure or confidential intellectual property. The attacks are **elaborate and complex**, often using zero-day vulnerabilities to infiltrate and defence evasion techniques to remain undetected for extended periods. For CSC attacks they often **infiltrate the build process** of software or hardware, injecting malicious code during development to eventually gain access to the target's network. The victims are chosen with precision, often **targeting specific organizations or industries**, such as defence or government agencies. These attacks are typically carried out by **nation-states (or sponsored by them)**, seeking to gain strategic or political advantage through stealthy infiltration.

## 5.2. Opportunistic attack

An **opportunistic** CSC attack can be described by a focus on **blackmail or theft**, using ransomware to lock systems or steal data for financial gain. These attacks are **less concerned with stealth**, instead relying on **rapid deployment**, either by encryption of critical data and subsequent ransom demands, or the sale of data on the black market. The method of infiltration in CSC attacks often involves

**distributing a malicious copy of software** through phishing campaigns. The attack vector is more "shotgun" in nature, as attackers typically **target a wide range of organizations opportunistically**. These attacks are executed for profit and tend to have **less sophisticated tactics** compared to high-level attacks.

| Characteristic | APT attack | Opportunistic attack |
|---|---|---|
| **Goal** | Intelligence | Profit |
| **Execution** | Stealth and long-term | Visible and rapid |
| **Sophistication** | Complex | Simple |
| **Infiltration** | Build process | Malicious copy |
| **Target selection** | Focused | Opportunistic |
| **Attacker type** | State (-sponsored) | Criminal groups |

*Table 2 - Type of CSC attacks*

It is important to note that an attack does not have to meet all characteristics to be classified as one of the attacks, but rather what profile fits best.

# 6. Analysis of interviews

## 6.1. Considerations

This chapter analyses the data gathered from the semi-structured interview sessions held with experts to investigate the optimization of counter measures against CSC attacks.

Each interview consists of four parts. In the first part the expert introduces himself, details his experience in cyber security and describes known cases of CSC attacks and any trend they might observe. In this part the definition of a CSC attacks used for this thesis is also discussed. In the second part, the preferred controls against CSC attacks of the expert are being asked, as well as any challenges or concerns he sees for the future. In the third part, the focus shifts to the hypothesis of this thesis, i.e. the suggestion to distinguish between APT and opportunistic attacks regarding CSC attacks. The expert is asked to assess the different risk profiles and the potential differences in controls for both types. Finally, in the fourth and last part, the expert has the opportunity to share any final thoughts regarding CSC attacks and some practical matters are discussed as well. The full set of questions can be found in Appendix A.

Due to the nature of semi-structured interviews, it was not always possible to get complete answers to all questions. The experts interviewed volunteered to participate and took time out of their work schedule in support of this thesis, often with time limitations. The variety of backgrounds from the experts resulted in the interviews having different focuses and the interviewees were encouraged to follow their own line of thought whenever this was possible. This also meant that for each interview some areas were less explored than others.

Finally, as preparation the interviewees were only given the topic of the interview (i.e. cyber supply chain attacks) and how long the session would take (i.e. one hour). This was intentionally done to elicit spontaneous and unfiltered responses, which were used as a proxy for prioritization of controls against CSC attacks. Afterwards, the experts were given the opportunity to review their quotes used in this thesis and to decide how they would want to be referred to, regarding the level of anonymity.

## 6.2. Interviews

### Introduction

The background of the experts was, aside from cyber security, spread through multiple sectors (e.g. healthcare, construction, retail), represented both (semi-)government institutions and business, as well as the different domains in the supply chain: vendor, consumer, and consultancy. A full list of the interviewees can be found in Appendix B.

All experts were familiar with CSC attacks and could name notable cases (e.g. Solarwinds, Target, Kaseya), where some even had experienced the attacks in their line of work. Almost exclusively did they acknowledge that the number of CSC attacks have risen, where Expert 7 revealed that the publicly known attacks are just the tip of the iceberg:

> *"Attacks like XZ backdoor happen 10 times more often than you read in the newspaper."*

However, Expert 6 does see global events like the war in Ukraine temporarily lowers the frequency of CSC attacks on the Netherlands, which now only happen occasionally, for example when the Dutch government mentions the war. Furthermore, though Expert 5 does not deny the increased frequency, he is not as concerned as most others:

> *“I have the view that CSC attacks are somewhat hyped. It gets a lot of attention, but impact is minimal. In practice, it involves only a limited number of cases, which is why it doesn't hold a very prominent position in our risk model.”*

Each expert also provided their own definition of the attack (see Appendix C) which always shared the most important characteristics with the definition used in this thesis.

### Controls and challenges

The experts were then asked about their preferred controls against CSC attacks and though their answers are not necessarily exclusive due to the time limit, the spontaneous and unfiltered answers serve as a proxy to indicate prioritization. The controls are mapped against the controls mentioned in the NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations [23]. Table 3 shows the controls mentioned per expert and a full explanation of the controls can be found in Appendix D.

| Control | Exp1 | Exp2 | Exp3 | Exp4 | Exp5 | Exp6 | Exp7 | Exp8 | Exp9 |
|---|---|---|---|---|---|---|---|---|---|
| Access Control | v | v | v | v | v | v | v | v | v |
| Awareness and Training | | | v | | | | v | | |
| Audit and Accountability | v | v | v | v | v | v | v | v | v |
| Security Assessment and Authorization | v | v | v | v | v | v | v | v | v |
| Configuration Management | v | v | v | v | v | v | v | v | v |
| Contingency Planning | v | | | v | | | v | v | |
| Identification and Authentication | v | v | v | v | v | v | v | v | v |
| Incident Response | v | v | v | | v | v | v | v | v |
| Maintenance | v | v | v | | | v | v | | v |
| Media Protection | | | | | | | | | |
| Physical and Environmental Protection | | | v | | | v | v | | |
| Planning | | v | | | | | v | | |
| Program Management | | | | | | | v | | |
| Personnel Security | | | | | | | v | | |
| Provenance | v | v | | | | | v | | v |
| Risk Assessment | v | v | v | v | v | v | v | v | v |
| System and Services Acquisition | v | v | v | v | v | v | v | v | v |
| System and Communications Protection | | | | v | | v | v | | |
| System and Information Integrity | v | v | v | | | v | v | | V |

*Table 3 - Answers from experts mapped to NIST controls*

Most controls were mentioned (almost) uniformly and were considered by many as “basic hygiene”. Several experts, including Expert 9, argued however that this does not mean this is properly implemented in many organizations:

> *“Most organizations don’t have their basic hygiene measures in order, while they could prevent even semi-advanced CSC attacks.”*

Expert 7 adds to that:

> *“In most software organizations security is seen as a secondary requirement.”*

Expert 4 and 6 do see that new regulations, like the Baseline Informatiebeveiliging Overheid (BIO) [83] or NIS2 [17], have a positive impact on the implementation of basic cyber controls and raises the awareness for cyber security within organizations.

One control that was considered important but challenging by all experts was vendor assessment during acquisition and to trust them to adhere to the agreements made. According to Expert 2 a balance must be found:

> *"I believe that the measures [...] should be implemented as early as possible in the development process. When we bring something in-house [...], we start asking questions about the product and the supplier to determine whether, given its importance to our organization [...], the product's level of maturity in terms of information security and the supplier's maturity are proportionate. If these two are not aligned, you will need to take some additional measures [...] to ensure that the lack of maturity [...] does not become a risk to the rest of your organization. Because often, while the product may be lacking in terms of information security, it might still be a very good idea from a medical standpoint to bring it in-house."*

Expert 7 deems it even necessary to adjust the contract to be able to make a proper assessment:

> *"It is always very difficult to work with subcontractors [...] and we want to conduct an audit once every six months to check whether everything is still running as agreed. [...] But those people don't like it at all [...], so these days we include auditing in the contract."*

However, Expert 5 argues that even doing audits makes proper assessment difficult with the available tooling:

> *"A major concern is that we still don't have a standard to determine whether the tools you purchase are secure. It's all frameworks and auditing methods, but you can see that it's complicated. [...] I believe there is no independent assurance that truly assesses the effectiveness of the measures taken by the supplier."*

He adds that ultimately, you still need to assume that a supplier could be hacked, and your organization needs to prepare for that.

> *"The reliability of a partner plays a role [in acquisition], but you also see cases like SolarWinds and Microsoft, which are known as very reliable partners. To me, it's more about the conceptual idea: you're bringing in a tool that introduces additional vulnerabilities, regardless of the party. So, while the partner's reliability does matter, it plays a smaller role than you might initially think, because even the big players have proven capable of making mistakes."*

Another often mentioned counter measure regarding vendor assessment was the need to gain insight in the products and services they supply. This could range from proper documentation of the behaviour of the provided software for establishing a monitoring baseline to a list of used components within the software, often called a Software Bill of Materials (SBOM). Expert 1 sees this as the starting point of your cyber security:

> *"There is a difference between having insight and taking measures. [...] You can consciously choose to temporarily refrain from taking any measures, but you should perhaps choose to at least have that insight. [...] If you do eventually become the victim of a supply chain attack, you will already have the data. [...] Then you can at least respond*

> *more quickly and thus minimize the consequence or impact of that supply chain attack, which you accepted as a risk."*

Expert 3 observed that regarding IT supply chain people immediately think about IT, but that Operation Technology (OT) might be overlooked:

> *"Everyone's focus lays with IT, but OT might even be more complex. Though you implement roughly the same controls the priorities in OT are on safety (of people) and availability first. […] Better cyber security should therefore be demanded by the client, because if we are the only one to do it, we might lose our competitive edge."*

And although the IT supply chain has had a lot of advantages for organizations, expert 8 also argues that is has its downsides:

> *"The biggest concern I have [...] is the massive adoption of cloud technology, which has made the operational responsibility for cybersecurity extremely fragmented. It's often unclear to people: [...] where does my responsibility for cybersecurity actually end? [...] You often see very polished contracts that state they will respond within a certain number of hours, [...] but when **** hits the fan, you find out that things are actually not as well organized as they seemed."*

There are so many aspects in the IT supply chain to deal with that the call for cooperation is slowly becoming larger. Expert 2 sees this happening in the healthcare sector:

> *"I think that for a sector like healthcare, you really need to focus on forming partnerships. [...] We have the Z-Cert Foundation. They can organize things and are also working on issues like supplier management. This way, not every hospital will have to ask the same or slightly different questions to the supplier during contracting, but it can be handled collectively. I can easily imagine that you could do something similar for patching. [...] As an individual hospital, you're simply not big enough to have that conversation with your supplier on equal footing."*

Expert 4 says he would like to see something similar happen on the level of local government:

> *"You can imagine that there are many smaller municipalities with a part-time CISO who has to juggle a lot of responsibilities and has little time to stay fully up-to-date in the field. You need to support and assist them. It doesn't help to overwhelm them with messages like 'vulnerabilities have been found in this software' [...] without also explaining [...] how they could mitigate it."*

Furthermore, even in the commercial sector efforts have been taken between competitors within their supply chain to cooperate, according to Expert 8:

> *"I have seen a nice initiative within a sector where competitors created a circle of trust with each other to exchange valuable information to enhance their cyber security."*

Finally, most experts are not mentioning awareness training as a potential control and expert 1 even explicitly challenges it:

> *"[Awareness training], I'm not in favour of that. That's very similar to the phishing advice that we give as techies. Ultimately, it's very difficult to know what's real and what's not. [..] That's actually relying on a human chain that's not built for that. [...] I notice that I'm very allergic to that."*

### Classification

Most experts already distinguish CSC attacks based on the risk it would have for their organization, assessing the combination of likelihood and impact. Expert 9 looks at the techniques used, but also at the initial supplier targets:

> *"You could divide it into technical terms: software [...], hardware [...] and access [...]. You could also make a distinction between the type of [suppliers] involved: software that is widely used, [...] or parties that have a particular kind of access [to the main target]. You could draw [CSC attacks] along the technical categorization lines, but also along the type of organization that can serve as a springboard."*

When introduced to the proposed classification from Chapter 5, the experts agree that it would be a useful distinction as the risk profiles for both types are quite different. Expert 1 believes it can motivate companies in their implementation of the controls:

> *"That categorization is especially important to ensure companies not to throw in the towel. Because if you look at the number of measures that you can take [...] it quickly becomes a list of perhaps 20 or 30 measures. [...] Without such a categorization, you very quickly tend to take the measures that make the most sense based on gut feeling. But then it could very well be that you implement a measure that is super useful against an APT attack, but you may have two other measures that cover the foundation that you don't have in order at all."*

Several experts claim that every organization needs to defend against opportunistic attacks and that it differs per organization what additional risks you might have. Expert 3 needs to account for the risk of other nations trying to steal the intelligence embedded in their tender bids. Expert 4 remarks that within local government the responsibility for certain critical assets could invite APT attacks:

> *"I even see that within the sector, where for example the municipality of Haarlemmermeer with a Schiphol [...] is a more interesting attack vector for those state-sponsored APTs than for example the municipality of Dijk & Waard. Or the municipality of Katwijk where the transatlantic cable reaches land: that is also a different risk profile."*

The profiles of your clients could introduce additional risks as well, argues Expert 6. For his own organization this is limited to possibly some NGO’s that could potentially be under scrutiny from certain regimes where they operate, but he has seen a substantial impact at another software company:

> *"In theory, a state actor could always come and do something to us, but what would be their motive? […] Look at what happened to Visma in Finland, who at one point [facilitated] the procurement process and financial reporting of the Ministry of Defence. And then Visma was suddenly hacked, allegedly by a Russian or Chinese APT".*

However, when it comes to implementing controls against APT attack, many experts claim that the main difference is the maturity in which the same controls are implemented. Expert 5 describes it as follows:

> *"The measures are essentially the same as far as I’m concerned […]. Where you might say for an opportunistic [attack] that you accept a certain risk, I believe that for APT you implement the same measures but much more strictly. […] The more critical the situation*

> *becomes, the more strictly you apply those measures. […] If it can cause significant damage, then you also need to allocate more budget to implement measures."*

Expert 8 highlights the same point by explaining how he would implement controls if he needs to defend against APT attacks:

> *"Then you're talking more about redundancy. […] If you must defend against an APT, you probably want two different vendors for the firewalls. […] If they have a zero day for vendor A, they can't immediately exploit that to get in, because they also must go through vendor B."*

However, there are some controls that would only be used when defending against APT attacks. Expert 6 would wipe mobile device from directors before any business travels, while expert 9 names air-gapping the network containing crucial assets:

> *"For [opportunistic attacks], [an air-gapped network] is far too heavy, too costly, and too impractical a measure. But if you are talking about ASML's crown jewels […] then I would consider using an air-gapped network. Significant costs are involved, but it may be worth it given the risks they face."*

Ideally, to guard against APT attacks one should develop code themselves as much as possible. But if you need to acquire external software, do not use open-source solutions, warns Expert 7:

> *"It really makes a huge difference whether you use open source […] or whether you purchase something that you have custom-made, by a supplier with whom you have agreements and with whom you can also agree on the development process. […] Those are two completely different worlds."*

The experts also suggested some improvements to the characteristics in which both types of attacks are described. Several pointed out that opportunistic attacks are not limited to groups but could also be carried out by individuals. Furthermore, expert 3 named disruption as a potential goal for APT's, while expert 4 was missing disinformation (especially during elections) for opportunistic attacks. Expert 8 even argued that with the rise of *info stealers* intelligence has become a goal of opportunistic attacks as well.

Several experts felt that insider threats at suppliers should be considered a separate category as it fits in both an opportunistic and an APT attack but requires different type of controls. Expert 7 explains how as a supplier their organization deals with insider threats by implementing a *secure development process*:

> *"You are very welcome to apply here, but you will notice that we have all kinds of procedures that prevent you from doing something on your own that would not be noticed by your colleague. Not that we use four eyes principle everywhere, but you cannot get away with making a change in a repository without someone else seeing or reviewing it."*

### Conclusion

All experts agreed they could use the classification between opportunistic and APT to optimize controls against CSC attacks. However, many argued that the difference is not always black and white. Expert 2 described the types more "as two ends of a spectrum", rather than two distinct categories. Expert 7 remarks that recent development adds to this:

> *"These days you see bigger clubs that behave APT-like, […] that build entire frameworks of modular ransomware, where you can just place an order. […] Ransomware for hire is made by clubs that almost have APT potential in terms of capacity, money, time, resources. So the line is getting blurrier."*

Expert 9 comes with an additional insight regarding attacks conducted by state actors:

> *“We don’t know much about state actors conducting these types of attacks [...], but what can serve as an indication is that the Dutch Intelligence and Security Services Act explicitly allows our intelligence and security agencies to gain access to actual targets “via automated systems of a third party”. [...] So, if this is permitted even for our Dutch agencies, which I believe must adhere to stricter requirements than those in China and Russia, you can assume that this is a widely recognized and employed tactic.”*

# 7. Discussion

## 7.1. Summary of the research

### Summary

This research asked the question how to optimize counter measures against cyber supply chain attacks within the NIST framework. To answer this, data has been gathered by doing an analysis of notable CSC attacks and compare the characteristics of each attack using the MITRE ATT&CK framework. The analysis is then compared against an established distinction of APT and opportunistic attacks, which could be applied to CSC attacks as well. To confirm both hypotheses semi-structured interviews have been conducted with experts from the field of cyber security.

### Discussion structure

This chapter starts with an interpretation of the findings produced by the analysis and the interviews. It then continues with highlighting the limitations of the research, either by the scope of the research, the biases in the methodology, or the constraints of reality. Following the limitations, the research question and its sub-questions are answered, after which recommendations are made for future research regarding counter measures for CSC attacks.

## 7.2. Interpretation of findings

### Analysis of CSC attacks

We found nine attacks that we could analyse and fitted the criteria for the analysis as described in Section 3.2:

- The incidents were caused by malicious intent, not a human error.
- The incidents happened in the last twelve years to keep any recommendations relevant for today.
- The incidents were global in nature or could at least be happening anywhere in the world.
- The incidents had a high impact, either economically, operationally, reputationally or regarding compliance.
- The incidents have been researched by trustworthy sources.
- The incidents did not include hardware tempering.

The attacks were mapped on MITRE ATT&CK framework to indicate which techniques and tactics were used [45]. An overview of the comparison can be found in Section 4.10, Table 1. There are many similarities between the different attacks, which suggest that there are some basic techniques used in most CSC attacks. Obviously, *Supply Chain Compromise* is ticked, just like *Trusted Relationship,* as that is the scope of this research. For other techniques that most attacks share, a case can be made that these would be used in about any cyber attack, not just CSC attacks, e.g. *Data collection from local/network* system, *Obfuscated Files or Information*, *File and Directory Discovery, Develop Capabilities: Malware,* and *Command and Scripting Interpreter: PowerShell/UnixShell*. Some differences between the analysed attacks are more subtly: in several access is acquired by stealing credentials of legitimate users (e.g. *Unsecured Credentials* or *Credentials from Password Stores*) while for other attacks certificates are leveraged (e.g. *Steal or Forge Authentication Certificates*). Zooming in to the attacks *NotPetya, Target, and 3CX,* there are some noticeable differences compared to the other attacks. Firstly, less techniques are involved in the *Command & Control* tactic which could indicate that the attackers require less continuous communication with their malicious deployed code or are in general not concerned with keeping communication with their malware. A similar pattern is shown for the *Defense evasion* tactic which suggests that stealth was less required or at least not worth the extra effort. Finally, the same three attacks and *Kaseya* are the only attacks which have a clear *Impact* technique marked. Most likely, the other attacks had intelligence gathering as goal which is not a technique in the MITRE ATT&CK framework as this goal is hard to assess in retrospect. In summary, the differences between the attacks mentioned are indicating a difference in *stealth, sophistication* and *goal*, which aligns with a classification of CSC attacks based on Advanced Persistent Threats [81].

## Proposed classification

Advanced Persistent Threats (APTs) are a special type of cyber threat that, as the name suggests, is more sophisticated and often reflects a long-term strategy on the attacker's part. Traditionally, this label was used for direct threats or cyber attacks, as the concept of a CSC attack was still a novel concept when the term gained traction. However, as the MITRE ATT&CK mapping already indicated, it seems suitable for CSC attacks as well.

In addition to the original characteristics of APTs, i.e. *advanced, persistent*, and a *threat*, the analysis of Chapter 4 leaves room to add a few extra characteristics that could make the term more concrete and applicable for CSC attacks. Firstly, the *intent* or *goal* of the hackers could be an attribute as they seem to differ per attack. For example, *SolarWinds, Shadowhammer*, and *Shadowpad* were most likely executed for intelligence gathering, as it was suspected that the malware was present well before the discovery but didn't have any other impact. However, the attacks that were lacking *stealth* and *sophistication* in the MITRE ATT&CK mapping (*Target*, *NotPetya*, and *3CX)* also had a different goal, i.e. financial gain, either through ransomware or theft. Furthermore, *NotPetya, Target*, and *Kaseya* are also one of the few attacks where the hackers did not infiltrate the build process or leveraged a legitimate certificate to sign the malicious package. Additionally, *Target*, *NotPetya, Kaseya,* and *3CX*, are attacks where the adversaries did not seem to focus on a predefined target but rather try to target any victim that was vulnerable. Finally, *Target* and *Kaseya,* are the only attacks that have not been attributed to a state-sponsored group, aside from the *XZ backdoor* incident which has not been attributed to any group yet.

| Incident | Goal | Execution | Sophistication | Infiltration | Target selection | Attacker type |
|---|---|---|---|---|---|---|
| *Target* | Profit | Visible | Simple | Credentials | Opportunistic | Criminal group |
| *NotPetya* | Profit | Visible | Simple | Malicious copy | Opportunistic | State-sponsored |
| *CCleaner* | Intelligence | Stealth | Complex | Build | Focused | State-sponsored |
| *ShadowPad* | Intelligence | Stealth | Complex | Signed | Focused | State-sponsored |
| *SolarWinds* | Intelligence | Stealth | Complex | Build | Focused | State-sponsored |
| *Shadowhammer* | Intelligence | Stealth | Complex | Signed | Focused | State-sponsored |
| *Kaseya* | Profit | Visible | Complex | Malicious copy | Opportunistic | Criminal group |
| *3CX* | Profit | Visible | Complex | Build | Opportunistic | State-sponsored |
| *XZ backdoor* | Unknown | Stealth | Complex | Build | Unknown | Unknown |

*Table 4 - Analysed attacks mapped on proposed classification*

In summary, the added characteristics, *goal*, *infiltration*, *target selection*, and *attacker type* have considerable overlap with the classical definition of APTs when mapped on the analysed attacks and are useful in make the APT category more distinct. A complete overview of the mapping of the analysed attacks to the proposed classification can be found in Table 4. Based on this table there are four attacks that can clearly be categorized as an APT attack: *CCleaner, ShadowPad, SolarWinds,* and *Shadowhammer.* For the opportunistic attacks there are three clear nominees: *Target, NotPetya,* and *Kaseya*. *3CX* is an interesting case as it has characteristics that could fit both attacks. On one hand it is described as a *complex*, *state-sponsored* attack where they managed to infiltrate the *build* process, on the other hand it was also a highly *visible*, *profitable* attack where any organization with the vulnerability was targeted. The fact that this has been a recent attack (2023) might be an indication that the distinction between both attacks could become blurrier in the future. Finally, there is the *XZ backdoor* attack which has obvious signs that it can be considered an APT attack, especially considering the fact the hacking was done in plain sight targeting an open-source library. However, there are still many unknows, mainly because the exploit was discovered before it was distributed properly.

### Interviews

For this research nine experts in the cyber security field were interviewed in a semi-structured fashion, where they answered questions about their experiences with CSC attacks and shared their insights concerning optimizing controls against CSC attacks.

Almost all experts agreed with the trend described in Section 1.2 and saw the number of CSC attacks increase over the last years, with some mentioning the publicly known attacks are only “the tip of the iceberg”. However, some remarks were made that CSC attacks are getting hyped in comparison to regular cyber attacks, which is felt to still be the bigger threat at the moment, and that the focus of the attacks are dependent on the current geopolitical landscape (for example, the war in Ukraine).

When asked about the implementation of controls against CSC attacks there was quite an agreement on which controls to use (see Table 3). Often the first control mentioned was the assessment of the suppliers and what techniques or frameworks could be used to achieve this. However, many experts acknowledged that suppliers being compromised cannot always be prevented and that organization itself should also take internal measures to tackle CSC threats. These controls should be implemented regardless of the attack vector (via supply chain or directly) and are regarded as “basic hygiene”, the minimum an organization should do.

Comparing the controls mentioned by the experts to those listed in the NIST framework, there was a focus on the more technical controls, leaving a clear gap in what can be described as “soft” controls, i.e. with a focus on people and processes. *Program Management* and *Planning* was hardly mentioned, same as *Awareness training* which in one case was even discouraged. Most experts did not explicitly mention *Personnel security*, either in the form of background checks or hiring requirements, though insider threats was mentioned as a major concern. Interestingly, even though the focus was on technology, one of the more technical controls, *Media protection* (a.k.a. encryption at rest) was never mentioned at all.

Major concerns were mostly focused on the assessment of the suppliers, both during acquisition and collaboration. The experts suggested several ways to tackle this, e.g. requiring a list of components used in the acquired software (i.e. SBOM), proper documentation about the network behaviour of the software to establish a baseline for monitoring, using contracts and audits to formalize agreements in the way of working. However, all these measures require the cooperation, honesty and transparency of the supplier which is not always within the control of the organization.

Furthermore, with the increased sophistication of CSC attacks and the concept of Ransomware as a Service (RaaS), it becomes more difficult to defend against the whole spectrum of threats. Cooperation between organization could save time and resources, especially for smaller organization with a part-time CISO, but though some initiatives have already been taken there is still much to gain in this area.

The proposed classification, as described in Chapter 5, resonated with all experts and supports the risk management approach most experts use themselves. Organizations should implement the earlier mentioned “basic hygiene” measures to at least defend against opportunistic attacks and implement further controls depending on the risks the organization faces, either due to the assets controlled or the clients in their portfolio. Key in making this decision is a cost-benefit analysis to determine whether controls are proportional to the risks faced. Several experts admitted they regard APT attacks as an accepted risks and argued that implementing extra controls would not help if a state actor was targeting them. Only a few organizations need to account for such attacks, and they either have high valuable assets or intelligence (e.g. ASML) or work for organizations that demand security against them (e.g. Ministry of Defence).

However, the characteristics used for the classification could use some improvements. Firstly, the classification failed to mention individuals as a potential attacker. Secondly, the goal of an attack is not as black and white as is suggested in the description. Disruption and disinformation are for example not mentioned (though disruption might be a more suitable goal for the *NotPetya* attack) and intelligence in the form of data can be the goal of an attack as well. However, in opportunistic attacks intelligence is often sold for money, making profit the end goal after all, while for APT attacks the intelligence is used for long-term strategy. The description of the goal should take these nuances in account or, if this complicates the application of the classification too much, the characteristic should not be used. Finally, insider threats are not considered in this classification, even though this type of attack requires different counter measures than the attacks analysed in this research.

Instead of using opportunistic and APT attacks as two distinct categories, they should be used as two ends of the same spectrum as the main difference in controls is the maturity in which they are implemented. This approach helps in assessing cases like the earlier mentioned *3CX* case and allows for easier adjustments in assessing characteristics like *sophistication*, which evolves over time as the quality of both malware and controls improve.

### Limitations

For the scope of this research criteria were set to only allow for attacks that could benefit the research question. One of the criteria was the necessity of attacks happening on the global scene so the lessons learned can be applied to organization around the world. However, due to this scoping there is a slight bias towards APT attacks as they tend to have a further reach than opportunistic attacks. It would be interesting to research any local attacks as well and challenge the assumption they are not applicable for other regions.

In the analysis of the selected CSC attacks a comparison was made based on the MITRE ATT&CK framework, which has the advantage of having an extensive catalogue of techniques to select from and deduce the tactics used. However, there are multiple limitations with the framework, particularly for this research. First, there is no mention of intent or motivation and goals like intelligence cannot be mapped. Second, there is no option to attribute attacks to known groups, which is useful in the proposed classification. Third, the downside of using a fixed catalogue is any new techniques might be missed, especially in a rapid evolving field like CSC attacks. Fourth, the level of sophistication (e.g. use of zero-days) is difficult to assess, which is one of the classical characteristics of an APT attack.

Furthermore, the research relies on semi-structured interviews with experts in the cyber security field and in the interviews, experts were asked about their experiences with CSC attacks, in particular APT. Several experts admitted they had little to no firsthand experiences and relied on notable cases, while the ones who hinted they had could not always be as open as the author would like. Efforts were made to interview experts from the intelligence services and military, but these were not successful due to the limitations of the author's network and the discretion involved in those fields.

Finally, the interviews were conducted with time limitations as the experts took time from their work to contribute to this research. Ideally, a prioritization of all possible NIST controls would be asked for both opportunistic and APT attacks, but instead the experts' own suggestions against CSC attacks in general were used as a proxy for prioritization.

## 7.3. Answering the research question

To answer the research question, the sub questions should be answered first.

*What are the most impactful supply chain attacks?*

The following attacks were found, matching the criteria proposed in Section 3.2:

- *Target* (2013)
- *NotPetya* (2017)
- *CCleaner* (2017)
- *Shadowpad* (2017)
- *SolarWinds* (2019)
- *Shadowhammer* (2019)
- *Kaseya* (2021)
- *3CX* (2023)
- *XZ backdoor* (2024)

*How can we classify these attacks?*

A distinction between opportunistic and APT attacks is a useful classification. Classically, APT attacks are described as more *advanced* and *persistent*. Based on the analysis in Chapter 4 additional characteristics could improve the classification, describing a CSC attack using six attributes: *goal*, *execution*, *sophistication*, *infiltration*, *target selection*, and *attacker type*. Opportunistic and APT attacks are two ends of the same spectrum and the more attributes an attack shares with one, the more it can be classified as such. This allows to adjust for any new developments in the field as well.

*What priority should be given to countermeasures per classification type?*

Many controls used against opportunistic attacks are also implemented for APT attacks, the main difference is the maturity of the implementation, which depends on the risk faced by an organization regarding APT attacks and is influenced by the assets controlled or the clients in their portfolio. Any resources spend on implementing should be in proportion to the risks. In addition to these measures, there are some controls that would only be considered against APT attacks, e.g. air-gapped networks.

With the sub questions answered, the main research questions can be answered as well:

*How can we optimize countermeasures for large-scale supply chains attacks within the NIST framework?*

Based on notable CSC attacks it is useful to classify attacks and plot them on a spectrum, with opportunistic and APT attacks on both ends. The distinction between those two categories can be described using six characteristics: *goal*, *execution*, *sophistication*, *infiltration*, *target selection*, and *attacker type*. The controls implemented against both categories are in principle the same but differ in maturity. Each organization should assess the risk of being attacked by an APT attack and spend the number of resources proportionate to the risks faced.

## 7.4. Recommendations for future research

This thesis has identified several opportunities for future research regarding CSC attacks.

First, it would be interesting to investigate hardware CSC attacks as this has been out of scope for this research but pose a risk for many organizations. The same case can be made for insider threats as both categories differ significantly from software CSC attacks, regarding processes, controls, and potential targets.

The analysis of the selected CSC attacks was based on the MITRE ATT&CK framework which has some limitations (see also Section 7.2). The same analysis could be done but then applied to the Unified Kill

Chain, which uses phases similar to the tactics of MITRE but adds *Objectives* as an attack phase which can be used to assess the goal [84]. Additionally, the National Vulnerability Database (NVD) from NIST could be used to assess the severity of the attacks [85].

As mentioned in Section 7.2 due to time limitations the expert's own suggestions was used as a proxy for prioritizing controls against CSC attacks. A full assessment of the NIST controls applied to organizations with both a low and high risk for APT attacks could give additional insights in the implementation of the controls.

Finally, the attacks analysed in this research are focusing on IT, but it would be interesting to see the likelihood and impact of CSC attacks on Operation Technology (OT). On one hand OT networks tend to be more decentralized disconnected from the Internet, on the other hand are the assets in the network considered high-value targets.

# 8. Conclusion

The recent rise of cyber supply chain (CSC) attacks highlights the vulnerabilities inherent in today's interconnected IT ecosystems. This thesis explored the question of optimizing countermeasures for large-scale CSC attacks within the NIST framework, proposing a classification to distinguish attacks as either opportunistic or advanced persistent threats (APTs). Through analysis of notable CSC attacks and insights gathered from cybersecurity experts, this research provides contributions and suggestions to the field of supply chain cybersecurity.

Opportunistic attacks can often be mitigated through robust "basic hygiene" measures. In contrast, defending against APT attacks requires heightened control maturity and resource investment, particularly for organizations managing high-value assets or clients. The classification proposed in this thesis, detailing six distinct characteristics (*goal, execution, sophistication, infiltration, target selection,* and *attacker type*), serves as a practical framework for organizations to assess risk and allocate resources effectively. As the line between opportunistic and APT attacks continues to blur, the framework outlined here offers cybersecurity practitioners a flexible tool to adapt to an increasingly complex threat environment.

## 9. References

[1] E.-I. Apăvăloaie, “The Impact of the Internet on the Business Environment,” *Procedia Econ. Financ.*, vol. 15, no. 14, pp. 951–958, 2014, doi: 10.1016/s2212-5671(14)00654-6.

[2] N. V. Oza, T. Hall, A. Rainer, and S. Grey, “Trust in software outsourcing relationships: An empirical investigation of Indian software companies,” *Inf. Softw. Technol.*, vol. 48, no. 5, pp. 345–354, 2006, doi: 10.1016/j.infsof.2005.09.011.

[3] P. Buxmann, S. Lehmann, and T. Hess, “Software as a service,” *Wirtschaftsinformatik*, vol. 50, no. 6, pp. 500–503, 2008, doi: 10.1007/s11576-008-0095-0.

[4] B. Gammelgaard and K. Nowicka, “Next generation supply chain management: the impact of cloud computing,” *J. Enterp. Inf. Manag.*, vol. 37, no. 4, pp. 1140–1160, 2024, doi: 10.1108/JEIM-09-2022-0317.

[5] Z. R. Alashhab, M. Anbar, M. M. Singh, Y. B. Leau, Z. A. Al-Sai, and S. A. Alhayja’a, “Impact of Coronavirus Pandemic Crisis on Technologies and Cloud Computing Applications,” *J. Electron. Sci. Technol.*, vol. 19, no. 1, pp. 25–40, 2021, doi: 10.1016/j.jnlest.2020.100059.

[6] T. Kalsoom *et al.*, “Impact of IoT on manufacturing industry 4.0: A new triangular systematic review,” *Sustain.*, vol. 13, no. 22, pp. 1–22, 2021, doi: 10.3390/su132212506.

[7] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scuffham, “The Internet of Things: Impact and Implications for Health Care Delivery,” *J. Med. Internet Res.*, vol. 22, no. 11, 2020, doi: 10.2196/20135.

[8] Y. Lu, G. M. Phillips, and J. Yang, “The Impact of Cloud Computing and Ai on Industry Dynamics and Concentration,” *SSRN Electron. J.*, no. January, 2024, doi: 10.2139/ssrn.4922841.

[9] Accenture, “2021 Cyber Threat Intelligence Report,” 2021. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-172/accenture-2021-cyber-threat-intelligence-report.pdf#zoom=40

[10] J. Walden, “The Impact of a Major Security Event on an Open Source Project: The Case of OpenSSL,” *Proc. - 2020 IEEE/ACM 17th Int. Conf. Min. Softw. Repos. MSR 2020*, pp. 409–419, 2020, doi: 10.1145/3379597.3387465.

[11] Kaspersky, “XZ backdoor story – Initial analysis,” Secure List. Accessed: Nov. 08, 2024. [Online]. Available: https://securelist.com/xz-backdoor-story-part-1/112354/

[12] Symantec, “Internet Security Threat Report Volume 24, 2019,” 2019. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947

[13] C. Colicchia, A. Creazza, and D. A. Menachof, “Managing cyber and information risks in supply chains: insights from an exploratory analysis,” *Supply Chain Manag.*, vol. 24, no. 2, pp. 215–240, 2019, doi: 10.1108/SCM-09-2017-0289.

[14] T. Remencius, A. Sillitti, and G. Succi, “Assessment of software developed by a third-party: A case study and comparison,” *Inf. Sci. (Ny).*, vol. 328, pp. 237–249, 2016, doi: 10.1016/j.ins.2015.08.028.

[15] A. Ahmed and A. Abdullah, “Enhancing Software Supply Chain Resilience: Strategy for Mitigating Software Supply Chain Security Risks and Ensuring Security Continuity in Development Lifecycle,” *Int. J. Soft Comput.*, vol. 15, no. 1/2, pp. 01–18, 2024, doi: 10.5121/ijsc.2024.15201.

[16] European Parliament and the Council of the European Union, “NIS 1 Directive,” *Off. J. Eur. Union*, 2016, [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[17] The European Parliament and the Council of the European Union, “NIS2,” Official Journal of the European Union. [Online]. Available: https://www.nis-2-directive.com/NIS_2_Directive_Articles.html

[18] The White House, “Executive Order 14028 - On Improving the Nation’s Cybersecurity,” 2021, *The White House, Washington, D.C.* [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[19] T. Herr, J. Lee, W. Loomis, and S. Scott, “Breaking trust: Shades of crisis across an insecure software supply chain,” 2020. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

[20] CrowdStrike, “CrowdStrike 2024 Global Threat Report,” 2024. [Online]. Available: https://www.crowdstrike.com/global-threat-report/

[21] A. Andreoli, A. Lounis, M. Debbabi, and A. Hanna, “On the prevalence of software supply chain attacks: Empirical study and investigative framework,” *Forensic Sci. Int. Digit. Investig.*, vol. 44, p. 301508, 2023, doi: 10.1016/j.fsidi.2023.301508.

[22] M. Reed, J. F. Miller, and P. Popick, “Supply chain attack patterns: Framework and Catalog,” *Off. Deputy Assist. Secr. Def. Syst. Eng.*, p. 88, 2014.

[23] NIST, “NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” 2022.

[24] ENISA, “European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyberse- curity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repe,” 2022. Accessed: Oct. 21, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/eng

[25] S. Charney, E. T. Werner, and T. Computing, “Cyber supply chain risk management: Toward a global vision of transparency and trust,” *Microsoft Corp.*, pp. 6–8, 2011.

[26] T. Storch, “Toward a trusted supply chain: A risk based approach to managing software integrity,” *Microsoft Corp.*, pp. 1–25, 2014.

[27] W. J. Heinbockel, E. R. Laderman, and G. J. Serrao, “Supply Chain Attacks and Resiliency Mitigations,” 2017.

[28] S. Boyson, “Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems,” *Technovation*, vol. 34, no. 7, pp. 342–353, 2014, doi: 10.1016/j.technovation.2014.02.001.

[29] A. Creazza, C. Colicchia, S. Spiezia, and F. Dallari, “Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era,” *Supply Chain Manag.*, vol. 27, no. 1, pp. 30–53, 2022, doi: 10.1108/SCM-02-2020-0073.

[30] S. Schauer, N. Polemi, and H. Mouratidis, “MITIGATE: a dynamic supply chain cyber risk assessment methodology,” *J. Transp. Secur.*, vol. 12, no. 1–2, pp. 37–37, 2019, doi: 10.1007/s12198-018-0197-x.

[31] A. Yeboah-Ofori *et al.*, “Cyber Threat Predictive Analytics for Improving Cyber Supply Chain

Security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[32] B. Hammi, S. Zeadally, and J. Nebhen, "Security Threats, Countermeasures, and Challenges of Digital Supply Chains," *ACM Comput. Surv.*, vol. 55, no. 14 S, 2023, doi: 10.1145/3588999.

[33] NIST, "NIST Special Publication 800-30 (Revision 1) - Guide for Conducting Risk Assessments," 2012.

[34] S. Alelyani and H. Kumar, "Overview of Cyberattack on Saudi Organizations," *J. Inf. Secur. Cybercrimes Res.*, vol. 1, no. 1, pp. 32–39, 2018, doi: 10.26735/16587790.2018.004.

[35] K. Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired. Accessed: Dec. 11, 2024. [Online]. Available: https://www.wired.com/2010/01/operation-aurora/

[36] N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet Dossier, Symantec Security Response, Version 1.4, February 2011," *Symantec Secur. Response*, vol. 4, no. February, pp. 1–69, 2011.

[37] E. Nakashima and J. Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, Jun. 02, 2012. [Online]. Available: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

[38] H. Modderkolk and K. Zetter, "Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran," *Yahoo!News*, Sep. 02, 2019. [Online]. Available: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html?

[39] FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," Google Cloud. Accessed: Jul. 16, 2024. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[40] L. Sterle and S. Bhunia, "On SolarWinds Orion Platform Security Breach," *Proc. - 2021 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Internet People, Smart City Innov. SmartWorld/ScalCom/UIC/ATC/IoP/SCI 2021*, pp. 636–641, 2021, doi: 10.1109/SWC50871.2021.00094.

[41] G. Janssen, "Report DIVD-2021-00002 - KASEYA VSA," 2021. [Online]. Available: https://vintage.divd.nl/reports/2021-00002 - Kaseya VSA/

[42] Virsec, "Virsec Hack Analysis Lab: Deep Dive into NotPetya," Virsec. Accessed: Jul. 26, 2024. [Online]. Available: https://www.virsec.com/resources/blog/deep-dive-into-notpetya

[43] C. Bing and S. Kelly, "Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed," *Reuters*, New York, May 08, 2021. [Online]. Available: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

[44] NIST, "NIST Cyber Security Framework," 2024.

[45] MITRE, "MITRE ATT&CK Framework," 2018. Accessed: Sep. 01, 2024. [Online]. Available: https://attack.mitre.org/

[46] Iqra Naseer, "The crowdstrike incident: Analysis and unveiling the intricacies of modern cybersecurity breaches," *World J. Adv. Eng. Technol. Sci.*, vol. 13, no. 1, pp. 728–733, Oct. 2024, doi: 10.30574/wjaets.2024.13.1.0473.

[47] B. Krebs, "Email Attack on Vendor Set Up Breach at Target." Accessed: Aug. 19, 2024.

[Online]. Available: https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[48] F. Pigni, M. Bartosiak, G. Piccoli, and B. Ives, “Targeting Target with a 100 million dollar data breach,” *J. Inf. Technol. Teach. Cases*, vol. 8, no. 1, pp. 9–23, 2018, doi: 10.1057/s41266-017-0028-0.

[49] X. Shu, K. Tian, A. Ciambrone, and D. Yao, “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned,” pp. 1–10, 2017, [Online]. Available: http://arxiv.org/abs/1701.04940

[50] M. Yason, “Target Data Breach: Understand and Detect Kaptoxa POS Malware,” Security Intelligence. Accessed: Aug. 19, 2024. [Online]. Available: https://securityintelligence.com/target-data-breach-kaptoxa-pos-malware/

[51] B. Krebs, “Target Hackers Broke in Via HVAC Company.” Accessed: Jul. 12, 2024. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[52] A. Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” Wired. Accessed: Dec. 20, 2024. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[53] US Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” *Office of Public Affairs*, Oct. 19, 2020. [Online]. Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[54] S. Y. A. Fayi, “What Petya/NotPetya Ransomware Is and What Its Remidiations Are,” *Adv. Intell. Syst. Comput.*, vol. 738, no. January 2018, pp. 93–100, 2018, doi: 10.1007/978-3-319-77028-4_15.

[55] L. J. Trautman and P. Ormerod, “Wannacry, Ransomware, and the Emerging Threat to Corporations,” *SSRN Electron. J.*, no. January 2018, 2018, doi: 10.2139/ssrn.3238293.

[56] O. Vlček, “CCleaner APT Attack: A Technical Look Inside,” RSA Conference. [Online]. Available: https://www.rsaconference.com/library/presentation/ccleaner-apt-attack-a-technical-look-inside

[57] C. Brumaghin, E., Mercer, Williams, “CCleanup: A Vast Number of Machines at Risk,” Talos Intelligence. [Online]. Available: https://blog.talosintelligence.com/avast-distributes-malware/

[58] M. Beltov, “NetSarang Apps Riddled with ShadowPad Backdoor,” Sensors Tech Forum. Accessed: Jul. 19, 2024. [Online]. Available: https://sensorstechforum.com/netsarang-apps-shadowpad-backdoor/

[59] WeiRanLab, “Xshell Backdoor Analysis,” Huawei Security Center. Accessed: Jul. 19, 2024. [Online]. Available: https://isecurity.huawei.com/sec/web/viewBlog.do?id=1895

[60] Kaspersky, “ShadowPad in corporate networks,” Secure List. Accessed: Jul. 19, 2024. [Online]. Available: https://securelist.com/shadowpad-in-corporate-networks/81432/

[61] CISA, “Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations,” 2021, *CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

[62] D. Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack,” NPR. Accessed: Jul. 25, 2024. [Online]. Available:

https://www.npr.org/2021/04/16/985439655/ a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack. of the solarwinds hack

[63] S. Oladimeji and S. M. Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget. Accessed: Jul. 16, 2024. [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[64] L. Wang and C. A. Alexander, "Navigating the SolarWinds Supply Chain Attack," *AIMS Electron. Electr. Eng.*, vol. 5, no. 2, pp. 146–157, 2021.

[65] S. Eckels, J. Smith, and W. Ballenthin, "SUNBURST Additional Technical Details," Google Cloud. Accessed: Jul. 16, 2024. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/sunburst-additional-technical-details/

[66] K. Zetter, "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers," Vice. Accessed: Jul. 19, 2024. [Online]. Available: https://www.vice.com/en/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

[67] Kaspersky, "Operation ShadowHammer: a high-profile supply chain attack," Secure List. Accessed: Jul. 30, 2024. [Online]. Available: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

[68] Kaspersky, "Operation ShadowHammer," Secure List. Accessed: Jul. 19, 2024. [Online]. Available: https://securelist.com/operation-shadowhammer/89992/

[69] O. Krehel, "The 2021 Kaseya Attack Highlighted The Seven Deadly Sins Of Future Ransomware Attacks," *Forbes*, Jan. 25, 2022. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks/

[70] K. Paul, "Who's behind the Kaseya ransomware attack – and why is it so dangerous?," *The Guardian*, San Fransico, Jul. 07, 2021. [Online]. Available: https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers

[71] J. Gager, "Ransomware Education: Availability, Accessibility, and Ease of Use," 2021.

[72] J. Hammond, "Rapid Response: Mass MSP Ransomware Incident," Huntress. Accessed: Dec. 30, 2024. [Online]. Available: https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware-incident

[73] Mandiant, "3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible," Google Cloud. Accessed: Dec. 31, 2024. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise

[74] A. Greenberg, "The Huge 3CX Breach Was Actually 2 Linked Supply Chain Attacks," Wired. Accessed: Dec. 31, 2024. [Online]. Available: https://www.wired.com/story/3cx-supply-chain-attack-times-two/

[75] Fatedier, "Fast Reverse Proxy project," 2024, *GitHub*. [Online]. Available: https://github.com/fatedier/frp

[76] G. Kucherin, V. Berdnikov, and V. Kamalov, "Not just an infostealer: Gopuram backdoor

deployed through 3CX supply chain attack," Secure List. Accessed: Dec. 31, 2024. [Online]. Available: https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344/

[77] D. Goodin, "The XZ Backdoor: Everything You Need to Know," Wired. Accessed: Dec. 27, 2024. [Online]. Available: https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/

[78] R. Cox, "Timeline of the xz open source attack." Accessed: Dec. 27, 2024. [Online]. Available: https://research.swtch.com/xz-timeline

[79] Kaspersky, "Assessing the Y, and How, of the XZ Utils incident," Secure List. Accessed: Dec. 27, 2024. [Online]. Available: https://securelist.com/xz-backdoor-story-part-2-social-engineering/112476/

[80] E. Boehs, "Everything I know about the XZ backdoor," boehs.org. Accessed: Dec. 27, 2024. [Online]. Available: https://boehs.org/node/everything-i-know-about-the-xz-backdoor

[81] R. Bejtlich, "What APT Is," *Inf. Secur.*, 2010, [Online]. Available: http://www.academia.edu/6842130/What_APT_Is

[82] NIST, "NIST Special Publication 800-39 - Managing Information Security Risk," 2011.

[83] Rijksoverheid, *Baseline Informatiebeveiliging Overheid*. 2018. [Online]. Available: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/

[84] P. Pols, "The Unified Kill Chain," *Cyber Secur. Acad.*, p. 104, 2017, [Online]. Available: https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf?fbclid=IwAR3vEqqVMlVNwMY6mJ9ddDFsQXe7Jx2VP6JhTptwa9-kkKhq0FSJtQU6zhQ

[85] NIST, "Vulnerability Metrics," National Vulnerability Database. Accessed: Jan. 17, 2024. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss

# 10. Appendices

## A. Interview questions

### Introduction (5-10 min)

- Do you mind if I record the interview?
- What is your role within your company?
- Are you familiar with the concept of cyber supply chain attacks?
    - *Provide own definition of CSC attacks, to be used in the rest of the interview.*
- If so, what are your experiences with CSC attacks?
- If so, how prevalent are CSC attacks in your sector?

### Controls (15-20 min)

- What counter control do you (or would you) implement against CSC attacks?
- Do you have any concerns regarding these counter measures? If so, elaborate please.

### Classification (15-20 min)

- Do you use any categorization for type of CSC attacks within your company?
    - *Introduction of proposed classification (provide example scenarios)*
- Do you see a difference in risk between these types of classifications, regarding your company?
- Would you implement different or similar counter measures for both types?
- Would you make changes to the classification proposed?

### Conclusion (5-10 min)

- Is there anything else you would like to add about cyber supply chain attacks or effective countermeasures?
- Who else do you think I should talk to?
- How do you want to be referred to in the paper?
- Do you want a copy of the thesis once it is completed?

## B. List of interviews

| ID | Date | Title | Sector |
|---|---|---|---|
| Exp1 | 24-09-2024 | Research & Innovation Lead | Cyber consultancy |
| Exp2 | 03-10-2024 | CISO | Healthcare |
| Exp3 | 04-10-2024 | CISO | Construction |
| Exp4 | 11-10-2024 | CISO | Local government |
| Exp5 | 18-10-2024 | CISO | Retail |
| Exp6 | 18-10-2024 | CISO | Software development |
| Exp7 | 18-10-2024 | Principal Architect | Government and military |
| Exp8 | 28-10-2024 | Cyber security consultant | Cyber consultancy |
| Exp9 | 01-11-2024 | CTO | Cyber consultancy |

## C. List of definitions for CSC attacks

| ID | Definition |
|---|---|
| Exp1 | The piggybacking on or modification of legitimate software, ultimately performing actions that were not originally part of the legitimate software. |
| Exp2 | A cyber attack that is not directly targeted at the ultimate victim but instead infiltrates through a supplier of the victim, eventually causing damage to the victim. |

| | |
|---|---|
| Exp3 | Attacks that do not originate from us but occur within our IT chain, where the attacker exploits our trusted relationship with our partners. |
| Exp4 | A supply chain attack is a cyber attack in which something happens within our supply chain that reflects on us, causing us to experience issues, for example availability issues. |
| Exp5 | A cyber attack in which your organization experiences impact or damage as a result of an attack on one of the parties in your supply chain. |
| Exp6 | Hackers trying to breach suppliers in order to gain access to the networks of the target companies and causing (financial) damage |
| Exp7 | Cyber attack on a supplier in the supply chain of the actual target |
| Exp8 | Malicious actions happening in the cyber space supply chain of the intended target company |
| Exp9 | Attacks in which access, software, or hardware from another organization is used as a springboard to gain access to the actual targets. |

## D. List of NIST security controls

| **Security controls** |
|---|
| Access Control<br>• Ensures that access to systems, data, and services is limited to authorized personnel only.<br>• Includes controlling access to supplier systems and managing identity and credentials for both internal and external entities. |
| Awareness and Training<br>• Focuses on ensuring that personnel are properly trained to recognize and manage supply chain risks.<br>• Training employees and contractors to identify and mitigate risks related to third-party products, services, and software. |
| Audit and Accountability<br>• Involves tracking and auditing supply chain-related activities.<br>• Provides mechanisms for reviewing and auditing supplier activities, software updates, and hardware deliveries. |
| Security Assessment and Authorization<br>• Focuses on assessing and authorizing systems and suppliers to operate within certain security parameters.<br>• Continuous monitoring and reviewing of supplier contracts, products, and services to ensure they meet organizational standards. |
| Configuration Management<br>• Involves maintaining configurations for systems and software within the supply chain.<br>• Ensures that the products or services supplied adhere to secure configuration baselines. |
| Contingency Planning<br>• Plans and prepares for the possibility of a supply chain failure or compromise.<br>• Includes backup plans, business continuity strategies, and alternative suppliers or services. |
| Identification and Authentication<br>• Ensures that suppliers and supply chain partners are authenticated and that proper identity management practices are in place.<br>• Requires multi-factor authentication for access to critical systems that could affect the supply chain. |
| Incident Response<br>• Establishes protocols for managing supply chain-related incidents, including communication, containment, and recovery strategies.<br>• Requires coordination with external suppliers and service providers to address incidents. |

| |
|---|
| Maintenance<br>• Governs the maintenance of systems and services obtained from third parties.<br>• Ensures proper updates and patching processes are followed in the supply chain to reduce vulnerabilities. |
| Media Protection<br>• Controls the protection of data storage media, especially in relation to supply chain processes such as hardware handling.<br>• Focuses on the secure transportation and storage of media and the destruction of sensitive data when no longer needed. |
| Physical and Environmental Protection<br>• Ensures that physical security controls are in place at supplier locations, especially for critical hardware or software components.<br>• Includes facility access control and environmental protections for critical supply chain assets. |
| Planning<br>• Involves planning for supply chain security in all stages of the product lifecycle.<br>• Requires documentation and proactive strategies for managing supply chain risks over time. |
| Program Management<br>• Relates to the overarching management of supply chain security programs within the organization.<br>• Emphasizes leadership involvement and strategic coordination across various departments to address supply chain risks. |
| Personnel Security<br>• Focuses on ensuring the security and trustworthiness of personnel involved in supply chain activities.<br>• Includes background checks for personnel who have access to sensitive supply chain systems and information. |
| Provenance<br>• Tracks origin, history, and integrity of hardware and software components throughout the supply chain.<br>• Ensures transparency and traceability through chain of custody and authentication of providers to prevent tampering or counterfeit components. |
| Risk Assessment<br>• Involves the identification, assessment, and prioritization of risks associated with the supply chain.<br>• Provides mechanisms for evaluating the security practices of suppliers and third-party vendors. |
| System and Services Acquisition<br>• Controls the processes for acquiring and managing third-party systems and services.<br>• Ensures that security requirements are included in contracts with suppliers and that secure development practices are followed. |
| System and Communications Protection<br>• Focuses on protecting the data shared between organizations and their suppliers.<br>• Ensures that secure communication channels are used and that sensitive data is encrypted during transmission and storage. |
| System and Information Integrity<br>• Ensures the integrity of information and systems provided by or dependent on the supply chain.<br>• Includes vulnerability management and patching processes for third-party software and hardware. |