EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

JULY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use etl@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – European Union Agency for Cybersecurity
Sebastian Garcia, Veronica Valeros – Czech Technical University in Prague

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of ENISA ad hoc Working Group on Cyber Threat Landscapes for their valuable feedback and comments in validating this report. We would like to also thank Volker Distelrath (Siemens) and Konstantinos Moulinos (ENISA) for their feedback.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-509-8 – DOI: 10.2824/168593

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Supply chain attacks have been a security concern for many years, but the community seems to have been facing a greater number of more organized attacks since early 2020. It may be that, due to the more robust security protection that organizations have put in place, attackers successfully shifted towards suppliers. They managed to have significant impacts in terms of the downtime of systems, monetary losses and reputational damages, to name but a few. The importance of supply chains is attributed to the fact that successful attacks may impact a large amount number of customers who make use of the affected supplier. Therefore, the cascading effects from a single attack may have a widely propagated impact.

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021. Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

This report presents the Agency's Threat Landscape concerning supply chain attacks, produced with the support of the Ad-Hoc Working Group on Cyber Threat Landscapes[1].

The main highlights of the report include the following:

- A **taxonomy** to classify supply chain attacks in order to better analyse them in a systematic manner and understand the way they manifest is described.
- **24 supply chain attacks** were reported from January 2020 to early July 2021, and have been studied in this report.
- Around **50% of the attacks were attributed to well-known APT groups** by the security community.
- Around **42% of the analysed attacks** have **not yet been attributed to a particular group**.
- Around **62% of the attacks on customers** took advantage of their **trust in their supplier**.
- In **62% of the cases**, **malware was the attack technique** employed.
- When considering targeted assets, in **66% of the incidents** attackers **focused on the suppliers' code** in order to further compromise targeted customers.
- Around **58% of the supply chain attacks aimed** at gaining access to **data** (predominantly customer data, including personal data and intellectual property) and around **16%** at gaining access to **people**.
- **Not all attacks should be denoted as supply chain attacks**, but due to their nature many of them are potential vectors for new supply chain attacks in the future.
- **Organizations need to update their cybersecurity methodology with supply chain attacks in mind** and to incorporate all their suppliers in their protection and security verification.

[1] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

1. INTRODUCTION

Supply chain attacks have been a security concern for many years, but the community seems to have been facing a increased number of more organized attacks since 2020. It may be that, due to the more robust security protection that organizations have put in place, attackers have shifted towards suppliers and managed to cause significant impact in terms of the downtime of systems, monetary losses and reputational damages, to name but a few. This report aims at mapping and studying the supply chain attacks that were discovered between January 2020 and early July 2021.

The devastating and ripple effect of supply chain attacks was seen in full force with the SolarWinds attack[2]. SolarWinds is considered one of the largest supply chain attacks of the last few years, particularly taking into account the affected entities that included governmental organizations and large corporations. It received great media attention and led to policy initiatives around the globe[3]. More recently, in July 2021 the Kaseya[4] attack manifested itself and raised the need for further and dedicated attention to supply chain attacks affecting managed service providers. Unfortunately, these two examples are not isolated cases and the number of supply chain attacks has been steadily increasing over the last year. This trend further stresses the need for policymakers and the security community to devise and introduce novel protective measures to address potential supply chain attacks in the future and to mitigate their impact.

Through a careful survey and analysis, this report maps supply chain attacks based on incidents identified from January 2020 to early July 2021. Each incident has been broken down into its key elements, such as the attack techniques and assets of both suppliers and customers alike that are affected by adversaries. The introduction of a taxonomy for supply chain attacks will facilitate their classification and may be the starting point for a more structured approach in analysing such attacks and coming up with dedicated security controls to mitigate them. The proposed taxonomy also helps to classify, compare and discuss these attacks using a common ground. The similarities between the proposed taxonomy and other well-known frameworks are discussed.

This report also analyses the similarities between the lifecycle of supply chain attacks and the more well-known attacks by Advanced Persistent Threats (APTs). A summary of the most prominent supply chain incidents since 2020 is included in the Annex, each of which has been decomposed in accordance with the aforementioned taxonomy.

The core of the report is an analysis of all the reported supply chain incidents to identify their key characteristics and techniques. The analysis answers the questions: what are the most common attack techniques being used in supply chain attacks, what are the main customer assets that attackers are after, and which is the relationship between attacks and assets targeted?

With the rise in attention being paid to supply chain attacks, many other related security incidents were also highlighted as being related to the supply chain, namely they were assumed to be supply chain attacks. We therefore discuss what constitutes a supply chain attack and why many attacks are not really supply chain attacks, showing some cases as examples. Understanding the threat landscape concerning supply chain attacks is important since misclassification of incidents may lead to erroneous trend analysis and conclusions.

The report also includes a set of recommendations aimed at policymakers and organizations, in particularly suppliers, the adoption of which may increase the overall security posture against supply chain attacks.

[2] Russian SolarWinds hackers launch email attack on government agencies, The Guardian. https://www.theguardian.com/technology/2021/may/28/russian-solarwinds-hackers-launch-assault-government-agencies. Accessed on 08/07/2021.
[3] See https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html
[4] Ransomware Attack Affecting Likely Thousands of Targets Drags On, WSJ, https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071. Accessed on 09/07/2021.

This report is structured as follows:

- **Chapter 1** provides a brief introduction to the topic of supply chain and the dedicated ENISA threat landscape.
- **Chapter 2** discusses what constitutes a supply chain attack and introduces a structured taxonomy to classify relevant incidents that also relates to well-established cyber threat intelligence frameworks.
- **Chapter 3** gives an overview of the lifecycle of a typical supply chain attack.
- **Chapter 4** details key supply chain attacks that occurred in late 2020 and early 2021.
- **Chapter 5** gives a timeline of relevant incidents and provides a thorough analysis of the incidents.
- **Chapter 6** addresses the issue of misclassifying incidents as supply chain attacks.
- **Chapter 7** introduces high-level as well as technical recommendations to improve the security of the supply chain and mitigate the impact of supply chain attacks.
- **Annex A** summarises 24 supply chain incidents identified and analysed in this report.

2. WHAT IS A SUPPLY CHAIN ATTACK?

Supply chain **refers to the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product**[5]. In cybersecurity, the supply chain involves a wide range of resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software.

There are four key elements in a supply chain:

- *Supplier*: is an entity that supplies a product or service to another entity.
- *Supplier Assets*: are valuable elements used by the supplier to produce the product or service.
- *Customer*: is the entity that consumes the product or service produced by the supplier.
- *Customer Assets*: are valuable elements owned by the target.

An entity can be individuals, groups of individuals, or organizations. Assets can be people, software, documents, finances, hardware, or others.

A supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targets.

2.1. TAXONOMY OF SUPPLY CHAIN ATTACKS

This report proposes a taxonomy to characterize supply chain attacks and structure their subsequent analysis. This taxonomy considers all four key elements of a supply chain, as well as the techniques used by attackers. The taxonomy may help organisations in understanding the various parts of a supply chain attack, comparing them with other similar cyber-attacks, and more importantly identifying the incidents as supply chain attacks.

The taxonomy should be used as a guiding template where, upon a new potential supply chain attack, the community may try to analyse it by identifying and mapping out each of the four distinct taxonomy elements. If no customer is attacked, or no supplier attacked, then it is probably not a supply chain attack[6].

The taxonomy, as presented in Table 1, has one section for the supplier and one section for the customer. For the supplier, the first part is called “Attack Technique Used to Compromise the Supply Chain” and it identifies **how** the supplier was attacked. The second part for the supplier is called “Supplier Assets Targeted by the Supply Chain Attack” and it identifies **what** was the target of the attack on the supplier.

For the customer, the first part is called “Attack Techniques Used to Compromise the Customer” and it identifies **how** the customer was attacked. The second part for the customer is called “Customer Assets Targeted by the Supply Chain Attack” and it identifies **what** was the target of the attack on the customer.

For each of these four distinguishing elements in the taxonomy, we have defined the elements that better characterise a supply chain attack. By selecting the corresponding elements, it is possible to have a better understanding of what is known or not known about an attack. The taxonomy is conceptually different from MITRE ATT&CK® knowledge base and it does not aim to replace the latter but rather complement it. Attack techniques defined in the proposed taxonomy and illustrated in Table 1 are in some cases related to relevant attack techniques as identified in the MITRE ATT&CK® framework, and are accordingly marked with the respective MITRE ATT&CK®

[5] Beamon, B. M. (1998). Supply chain design and analysis: Models and methods. International journal of production economics, 55(3), 281-294.
[6] See Section “Not Everything is a Supply Chain Attack” for more examples.

identifier in square brackets, for example [T1189]. The following subsections clarify each of the four parts of the taxonomy and how to identify its elements.

Table 1: Proposed taxonomy for supply chain attacks. It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) assets attacked in the customer.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software	Trusted Relationship [T1199]	Data
Social Engineering	Software Libraries	Drive-by Compromise [T1189]	Personal Data
Brute-Force Attack	Code	Phishing [T1566]	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
Exploiting Configuration Vulnerability	Data	Physical Attack or Modification	Processes
Open-Source Intelligence (OSINT)	Processes	Counterfeiting	Bandwidth
	Hardware		Financial
	People		People
	Supplier		

An EU cybersecurity incident taxonomy[7] is used for the purpose of incident response coordination activities and information sharing at Union level. Since the taxonomy is conceptually different and does not allow for detailed analysis of supply chain incidents, we recommend the complementary use of both taxonomies.

2.2. ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN

The attack techniques refer to “how” the attack took place, and not “what” was used to attack. For example, this category distinguishes whether the supplier was attacked with a password found online (OSINT) or whether the password was brute-forced (Brute-Force Attack). However, it is not relevant for the taxonomy whether the password found online was leaked, a default password or sold in a black market. The categories of Attack Techniques below cover the attack techniques most commonly used in the supply chain attacks analysed in this report. It is evident that more than one technique may have been used in any given attack and, in several cases, entities may not have the knowledge on how the attackers gained access to their infrastructure, or this information was not divulged or duly reported.

[7] Cybersecurity incident taxonomy, Publications of the NIS Cooperation Group, July 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. Accessed on 28/07/2021.

Table 2: Attack techniques used to compromise the supplier in the chain. Each technique identifies how the attack happened, and not what was attacked. Several techniques may be used in the same attack.

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

2.3. SUPPLIER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK

The supplier assets targeted by the attackers refers to “what” was the target of the attack on the supplier, which allowed further attacks to be subsequently mounted. The targeted asset(s) usually has a direct relationship with the final target and it is usually possible to understand the final intentions of the attacker by analysing the list of affected assets. In some cases, because of a lack of information divulged or reported by the supplier, it is not possible to have information on the target assets. This might also be the case when suppliers do not have the knowledge or expertise to identify which assets were compromised by the attackers.

Table 3: Assets of the supplier targeted by attackers. Each element identifies what was attacked in the supplier. Several techniques that could affect several assets may be used in the same attack.

SUPPLIER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Pre-existing Software	e.g. software used by the supplier, web servers, applications, databases, monitoring systems, cloud applications, firmware. It does not include software libraries.
Software Libraries	e.g. third party libraries, software packages installed from third parties such as npm, ruby, etc.
Code	e.g. source code or software produced by the supplier.

SUPPLIER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Configurations	e.g. passwords, API keys, firewall rules, URLs.
Data	e.g. information about the supplier, values from sensors, certificates, personal data of customers or suppliers themselves, personal data.
Processes	e.g. updates, backups or validation processes, signing certificates processes.
Hardware	e.g. hardware produced by the supplier, chips, valves, USBs.
People	e.g. targeted individuals with access to data, infrastructure, or to other people.

2.4. ATTACK TECHNIQUES USED TO COMPROMISE A CUSTOMER

This element of the taxonomy refers to the attack techniques used to compromise the customer through their supplier. Under this element of the taxonomy, we identify “how” the customer was attacked and not with “what”. It is a technique and not a specific type of attack. For example, if the customer updates its software from the supplier and receives a type of malware, the attack is both on a 'Trusted Relationship’ and a ‘Malware Infection’. It is evident that more than one technique may be applied in several cases. Customers may not always have knowledge of the technique used by attackers to gain access to their assets via their suppliers, but have the means to identify that the technique used was not within their perimeter.

Table 4: Attack techniques used to compromise the customer. Each technique identifies how the attack happened, and not what was attacked. Several techniques may be used in the same attack.

ATTACK TECHNIQUES USED TO COMPROMISE A CUSTOMER	
Trusted Relationship [T1199]	e.g. trust a certificate, trust an automatic update, trust an automatic backup.
Drive-by Compromise [T1189]	e.g. malicious scripts in a website to infect users with malware.
Phishing [T1566]	e.g. messages impersonating the supplier, fake update notifications.
Malware Infection	e.g. Remote Access Trojan (RAT), backdoor, ransomware.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Counterfeiting	e.g. create a fake USB, modify a motherboard, impersonation of supplier’s personnel.

2.5. CUSTOMER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK

Customer assets are the main and final target of the attackers and usually the *raison d'etre* for a supply chain attack. These assets may vary depending on the industry sector and the type of service offered. The particular element in the taxonomy is meant to facilitate understanding of the impact of the attack and also enable comparisons concerning the goals of the attackers. Certain assets might have been directly targeted by attackers, whereas others may have been inadvertently affected. More than one customer are usually affected by typical supply chain attacks. It is possible that the customer may not be aware of the adversary's target (e.g., the attack was either unsuccessful or quickly detected).

Table 5: Assets of the customer targeted by attackers. Each element identifies what was attacked in the customer. Several techniques may be used in the same attack. This is usually the final target of the attack.

CUSTOMER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Data	e.g. payment data, video feeds, documents, emails, flight plans, sales data and financial data, intellectual property.
Personal data	e.g. customer data, employee records, credentials.
Software	e.g. access to the customer product source code, modification of the software of the customer.
Processes	e.g. documentation of internal processes of operation and configurations, insertion of new malicious processes, documents of schematics.
Bandwidth	e.g. use the bandwidth for Distributed Denial of Service (DDoS), send SPAM or to infect others on a large scale.
Financial	e.g. steal cryptocurrency, hijack bank accounts, money transfers.
People	e.g. individuals targeted due their position or knowledge.

2.6. HOW TO MAKE USE OF THE TAXONOMY

The following is an example of how applying the taxonomy to a real case can help identify its particular features and facilitate an understanding of the characteristics of the attack.

Codecov is a company that provides software for code coverage and testing tools. The company supplies tools to other companies such as IBM and Hewlett Packard Enterprise. In April 2021, Codecov reported that attackers obtained some of their valid credentials from a Docker image[8] due to an error in how those Docker images were created. Once the attackers obtained these credentials, they used them to compromise an "upload bash script" that is used by Codecov customers[9]. Once the customers downloaded and executed this script, the attackers were able to exfiltrate data from Codecov's customers, including sensitive information that would allow the attackers to access the customer resources[10]. Multiple Codecov customers reported that the attackers were able to access their source code

[8] Codecov supply chain attack breakdown, GitGuardian, https://blog.gitguardian.com/codecov-supply-chain-breach/. Accessed on 27/06/2021.
[9] Bash Uploader Security Update, Codecov, https://about.codecov.io/security-update/. Accessed on 27/06/2021.
[10] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Accessed on 27/06/2021.

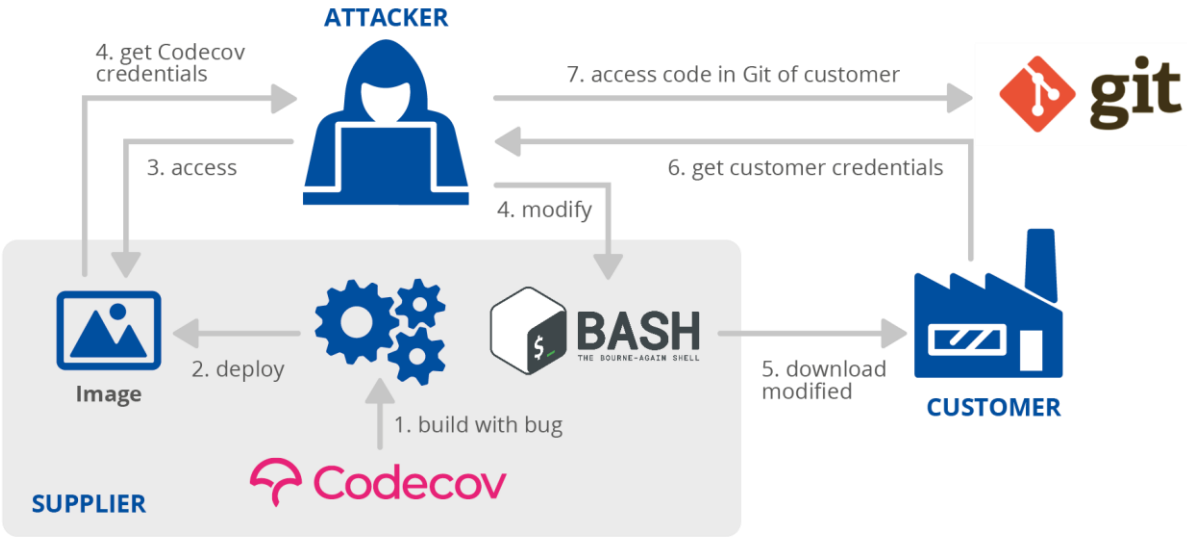
using stolen information from the Codecov breach[11]. The attack was not attributed to specific adversaries. Figure 1 (below) depicts the steps involved in this particular attack.

Using this information, we can identify the four elements in the proposed taxonomy. The attack on the supplier means how the attackers got access to the supplier, and in this case it was by "Exploiting a Configuration Vulnerability". Through this attack, the attackers target the asset of "code" in the supplier. After the elements for the supplier were identified in the taxonomy, we can move to how the customer was attacked. In the Codecov case is through a 'Trusted Relationship' with the supplier that was not secured and verified. The final asset targeted in the customer was reported to be source code, so 'Software'.

Table 6: Supply chain attack taxonomy applied to the attack involving the Codecov Company. The attackers exploited a configuration vulnerability in Codecov which was used to modify the supplier's code. The attackers abused the trusted relationship between Codecov and its customers to exfiltrate data necessary to access the customer's software source code.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Exploiting Configuration Vulnerability	Code	Trusted Relationship [T1199]	Software

Figure 1: Diagram of how the Codecov supply chain attack worked. The Codecov container creation process had a bug that was present in the online deployed containers (1). The attackers accessed the container and got Codecov's credentials (2). They then modified Codecov's bash script (3) that was updated in the customers (4). The malicious bash script exfiltrated the customer's credentials to the attacker (5), who used them to access the data of customers (6).



[11] Rapid7 Source Code Breached in Codecov Supply-Chain Attack, The Hacker News, https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html. Accessed on 27/06/2021.

2.7. SUPPLY CHAIN TAXONOMY AND OTHER FRAMEWORKS

2.7.1. MITRE ATT&CK® Knowledge Base

MITRE ATT&CK® is a curated knowledge base and model for cyber adversary behaviour. The taxonomy proposed in the report differs from MITRE ATT&CK®[12] because the purposes of both are very different. Therefore, it is not possible to use MITRE ATT&CK® in the supply chain taxonomy, since we opted for placing emphasis on the four aspects that typically characterise a supply chain attack and in particular the supplier-customer relationship. While MITRE ATT&CK® completely maps the options and steps in the lifecycle of all attacks, its coverage of the details of a supply chain are not yet that developed.

For example, in the MITRE ATT&CK® 'Initial Access' category, there is a technique called 'Supply Chain Compromise'[13]. This is very useful for companies to identify a supply chain as a risk, but too generic when focusing explicitly on the supply chain attacks themselves. The proposed taxonomy maps all the details of the supply chain attack itself, and therefore could potentially complement the MITRE ATT&CK® knowledge base.

2.7.2. Lockheed Martin Cyber Kill Chain® Framework

The proposed taxonomy also has a different purpose than the well-known Lockheed Martin Cyber Kill Chain® framework[14]. The cyber kill chain is a framework that was designed to identify the steps taken by attackers to achieve their goals. While these steps may be taken as part of a supply chain attack, they are too generic to classify, understand and compare supply chain attacks. The taxonomy presented here proposes a more detail analysis of these attacks and, more importantly, it helps map both attacks involved in a sole supply chain attack, one on the supplier and one on the customer.

[12] MITRE ATT&CK®, MITRE, https://attack.mitre.org/. Accessed on 08/07/2021.
[13] Supply Chain Compromise, Technique T1195 – Enterprise, MITRE ATT&CK®, https://attack.mitre.org/techniques/T1195/. Accessed on 08/07/2021.
[14] Cyber Kill Chain®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed on 08/07/2021.

3. THE LIFECYCLE OF A SUPPLY CHAIN ATTACK

It can be observed that a supply chain attack is usually composed of an attack on one or more suppliers and then a later attack on the final target, namely the customer. Each of these attacks may resemble very closely the lifecycle of APT attacks.

Although it is hard to agree on a unique definition of what an APT attack is, throughout this report it is considered that an APT attack is any attack that is targeted, obtains unauthorized access to an organization (usually code execution), is spread over a long period of time, and its final goal is in a specific relation to the target (as opposed to, for example, cryptomining). Of course, such a definition is not complete and many others may exist. However, a definition is important to understand that supply chain attacks are usually targeted, complex, costly and with attackers probably planning them for a long time. The mere fact that at least two types of successful attacks are involved in typical supply chain incidents, is an indicator of both the degree of sophistication of the adversaries, but also their persistence and intent to succeed.

It is worth noting that many APT attacks were considered not 'advanced' by the community in relation to the quality of their code, exploits and malware. However, it may be considered that the characterisation of being 'advanced' refers to the whole operation and not necessarily merely to the code. In the end, planning, staging, developing and executing two attacks in two organizations is a complex task.

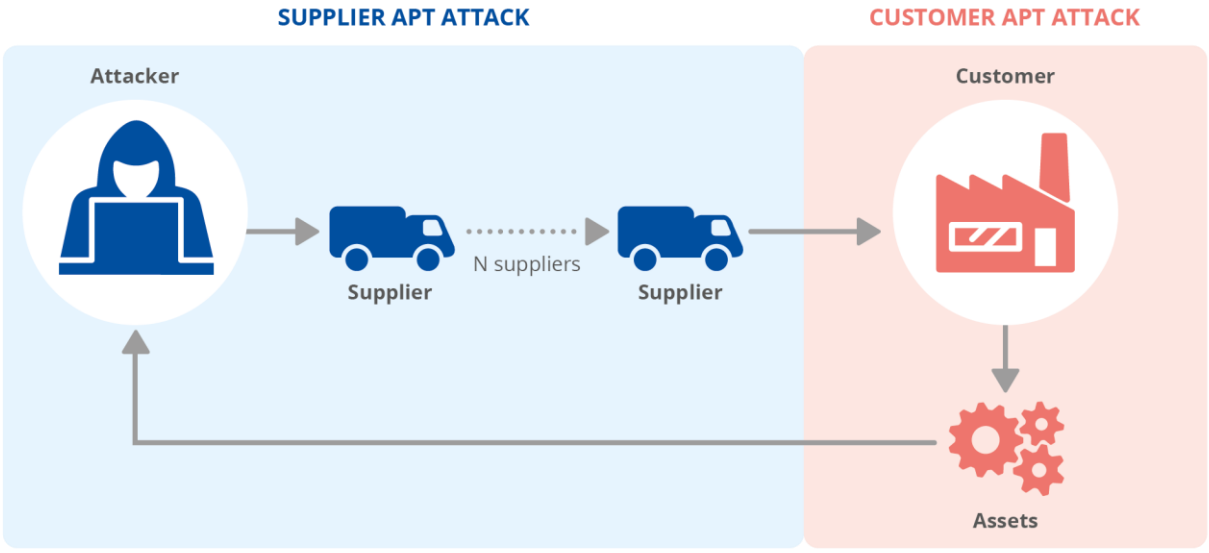
These distinctions are crucial to understand **that an organization could be vulnerable to a supply chain attack even when its own defences are quite good** and therefore the attackers are trying to explore new potential highways to infiltrate them by moving to their suppliers and making a target out of them. Moreover, the potential impact of supply chain attacks affecting numerous customers of the same supplier are probably immense. This is yet another reason why these types of attacks are becoming increasingly common as they provide adversaries with a means to potentially boost their reputations, as well as possibly make large financial gains.

An additional characteristic of supply chain attacks involves the complexity in handling them and the efforts required to mitigate and address such attacks. The mere fact that at least two organisational entities are affected and the use, most likely, of sophisticated attack vectors complicates the handling of an incident, forensics analysis and overall management of the incident. The fact that the supplier-consumer relationship is continuously evolving and both suppliers and customers are constantly updating their systems, introduces the need for continuous security of the supply chain and active risk assessment and management.

The lifecycle of a supply chain attack has two main parts, the attack on the supplier and the attack on the customer. Each of these attacks is usually complex, requiring one attack vector, one plan of action, and careful execution. These attacks may take months to be successful and, in many cases, may go undetected for a long time. The lifecycle of a supply chain attack can be seen in Figure 2.

The first attack in the lifecycle is called "Supplier APT Attack" and it focuses on compromising one or more suppliers. The second attack in the lifecycle is called "Customer APT Attack" and it focuses on the final target of the attack. These two parts are linked by the access to the supplier but otherwise may be quite different in techniques used, attack vectors exploited and time spent on the attack.

Figure 2: The lifecycle of supply chain attacks can be seen as two APT attacks intertwined. The first attack targets one or more suppliers, and the second attack targets the customers. These attacks require careful planning and execution.



In at least eleven attacks out of all the cases studied in this report, investigations confirmed that the supply chain attacks were conducted by known APT groups. These attributions were done by the security companies responsible for the reports referenced in Annex A. In the other thirteen cases the incidents were not fully investigated or attribution was not possible. Such attributions support the idea that both parts of the lifecycle of a supply chain attack can resemble the work of APT attacks. It is worth noting that attribution of attackers is very hard, prone to error, imprecise and politically challenging, but not impossible.

Since each part of the supply chain attack may be seen as an APT attack, its individual lifecycle would generally follow the same stages as other APT attacks. Such stages are detailed, for example, in the MITRE ATT&CK® Tactics for Enterprises[15].

[15] MITRE ATT&CK® Tactics - Enterprise Version 9, MITRE, https://attack.mitre.org/tactics/enterprise/. Accessed on 29/06/2021.

4. PROMINENT SUPPLY CHAIN ATTACKS

This section presents a summary of the most prominent supply chain attacks from January 2020 to early July 2021, along with a classification following the proposed taxonomy. These cases were selected because of the large impact produced in the community or because they highlight certain characteristics (as indicated in the elements of the taxonomy) that are important. The complete list and description of all supply chain attacks from January 2020 to early July 2021 is available in Annex A.

4.1. SOLARWINDS ORION: IT MANAGEMENT AND REMOTE MONITORING

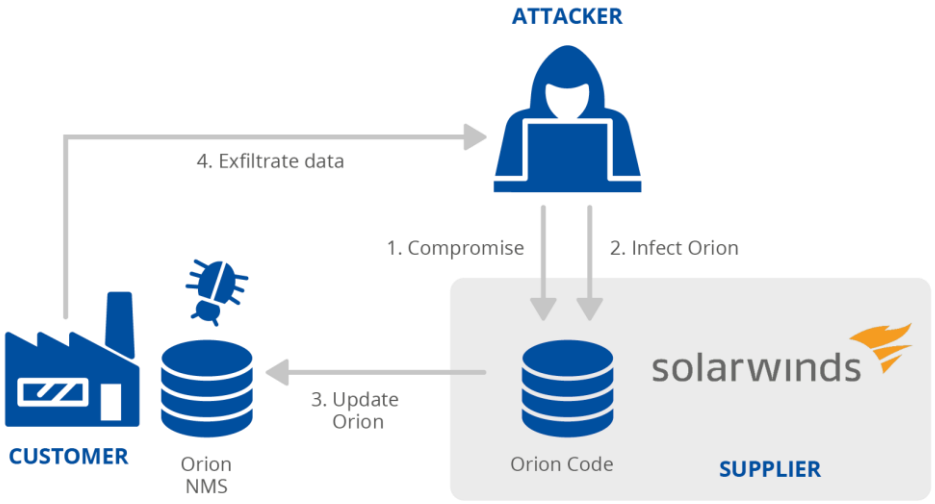
SolarWinds is a company that supplies management and monitoring software[16]. Orion is SolarWinds' network management system (NMS) product[17]. In December 2020 it was discovered that Orion had been compromised. An extensive investigation showed that attackers gained access to the SolarWinds network, possibly through exploiting a zero-day vulnerability in a third-party application or device, a brute-force attack or through social engineering. Once compromised, the attackers collected information for an extended period of time. The malicious software was injected into Orion during the build process[18,19]. The compromised software was then downloaded directly by the customers and was used to gather and steal information[20]. The attack was attributed to the APT29 group[21,22].

Table 7: Supply chain attack taxonomy applied to the attack involving SolarWinds. The attackers used multiple attack techniques to compromise SolarWinds Orion software. They modified code in the supplier and abused the trusted relationship of customers in SolarWinds to update the customers with malware. The attackers' final target was customers' data.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability, Brute-force attack, Social Engineering	Processes, Code	Trusted Relationship [T1199], Malware Infection	Data

[16] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Accessed on 08/07/2021.
[17] Orion Platform - Scalable IT Monitoring, SolarWinds, https://www.solarwinds.com/solutions/orion. Accessed on 08/07/2021.
[18] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Accessed on 08/07/2021.
[19] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Accessed on 08/07/2021.
[20] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Accessed on 08/07/2021.
[21] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Accessed on 08/07/2021.
[22] Russian hacker group 'Cozy Bear' behind Treasury and Commerce breaches, The Washington Post, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html. Accessed on 08/07/2021.

Figure 3: Diagram of SolarWinds supply chain attack. The attackers compromised SolarWinds and modified the code of ORION software. The ORION instances in the customers were updated with malware, which allowed the attackers to access the data of customers.



4.2. MIMECAST: CLOUD CYBERSECURITY SERVICES

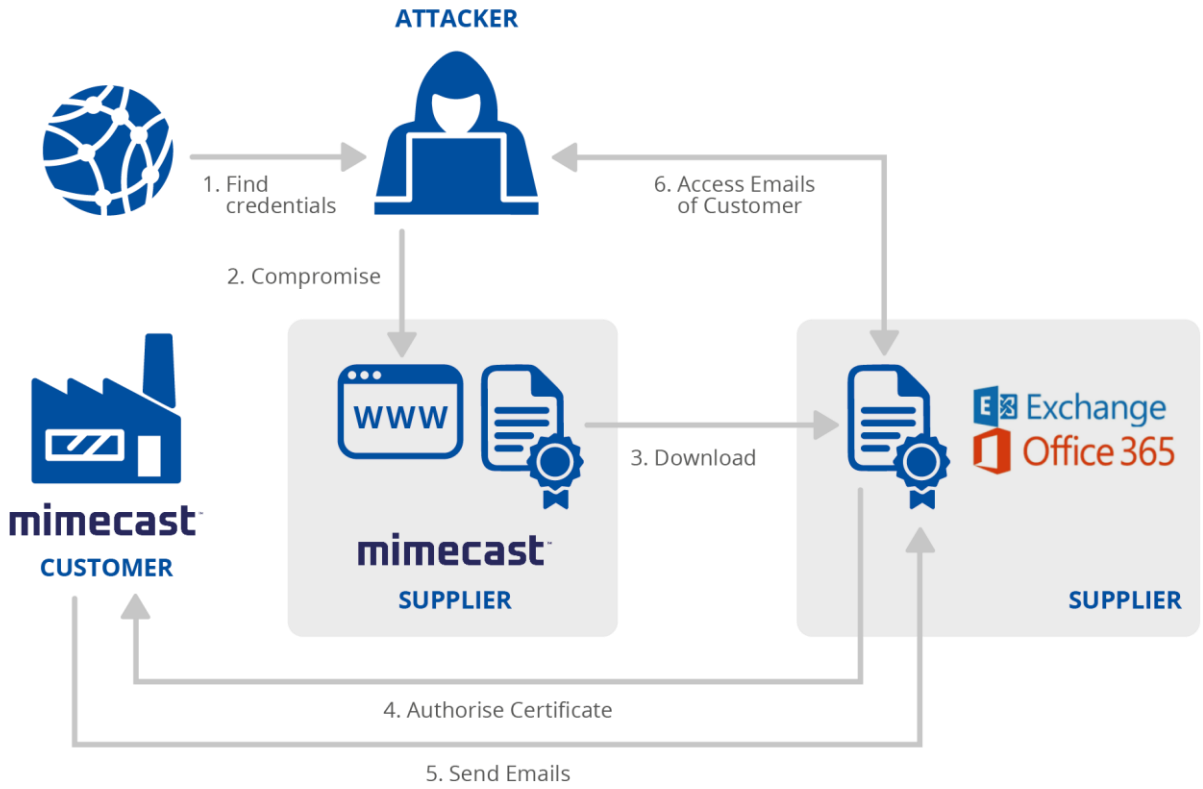
Mimecast is a supplier of cloud-based cybersecurity services. Among the services it provides, Mimecast offers email security services, which require customers to connect securely to Mimecast servers to use their Microsoft 365 accounts. In January 2021, it was discovered that attackers had compromised Mimecast (through the SolarWinds supplier). After the compromise, a Mimecast-issued certificate used by customers to access Microsoft 365 services was accessed by attackers, giving them the ability to intercept the network connections and to connect to the Microsoft 365 accounts to steal information[23,24]. The attack was attributed to the APT29 group[25]. The compromise of the supplier has been reportedly linked to SolarWinds, but there is no concrete information to validate this.

Table 8: Supply chain attack taxonomy applied to the attack involving Mimecast. It is unknown how attackers targeted the suppliers' data, specifically a Mimecast-issued certificate. The attackers abused the trusted relationship of customers uploading their data to Mimecast. The attackers accessed the data of customers in Mimecast.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Data	Trusted Relationship [T1199]	Data

[23] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. Accessed on 08/07/2021.
[24] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Accessed on 08/07/2021.
[25] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Accessed on 08/07/2021.

Figure 4: Diagram of Mimecast supply chain attack. The attackers found credentials that allow them to compromise the supplier and access their certificates. Then they use the certificates to access customer data after the customer validated and trusted the certificate.



4.3. LEDGER: HARDWARE WALLET

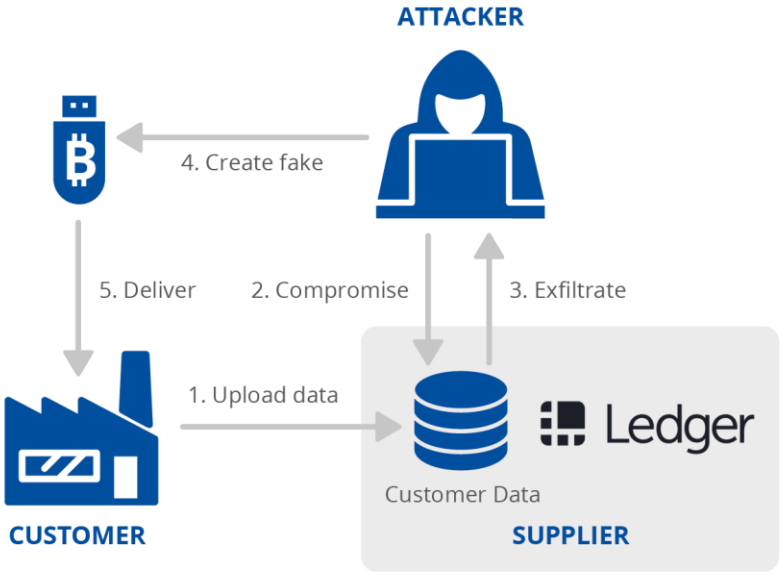
Ledger is a company that supplies hardware wallet technology for cryptocurrencies. In July 2020, attackers obtained valid credentials to access Ledger's e-commerce database[26]. The stolen data was released publicly in an online forum[27]. Attackers used the stolen data for online phishing and extortion of users[28,29], and for stealing users' money through a physical attack after supplying users with counterfeit Ledger wallets which, when connected to a computer that would ask users for their security keys, would infect the computer with malware and send the stolen information back to the attackers[30]. The attack was not attributed.

[26] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership, Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Accessed on 08/07/2021.
[27] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Accessed on 08/07/2021.
[28] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Accessed on 08/07/2021.
[29] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, Bitdefender HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html, Accessed on 08/07/2021.
[30] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Accessed on 08/07/2021.

Table 9: Supply chain attack taxonomy applied to the attack involving Ledger. The attackers used open-source intelligence techniques to find valid credentials to access Ledger records, and to steal customers' data. With that data the attackers abused the trust relationship of customers in Ledger by sending phishing emails and fake USB crypto wallet drives to steal cryptocurrency from the customers.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
OSINT	Data	Trusted Relationship [T1199], Phishing [T1566], Counterfeiting	Financial

Figure 5: Diagram of Ledger supply chain attack. The attackers found credentials of Ledger online, accessed their customers' database and used the information to attack the customers.



4.4. KASEYA: IT MANAGEMENT SERVICES COMPROMISED WITH RANSOMWARE

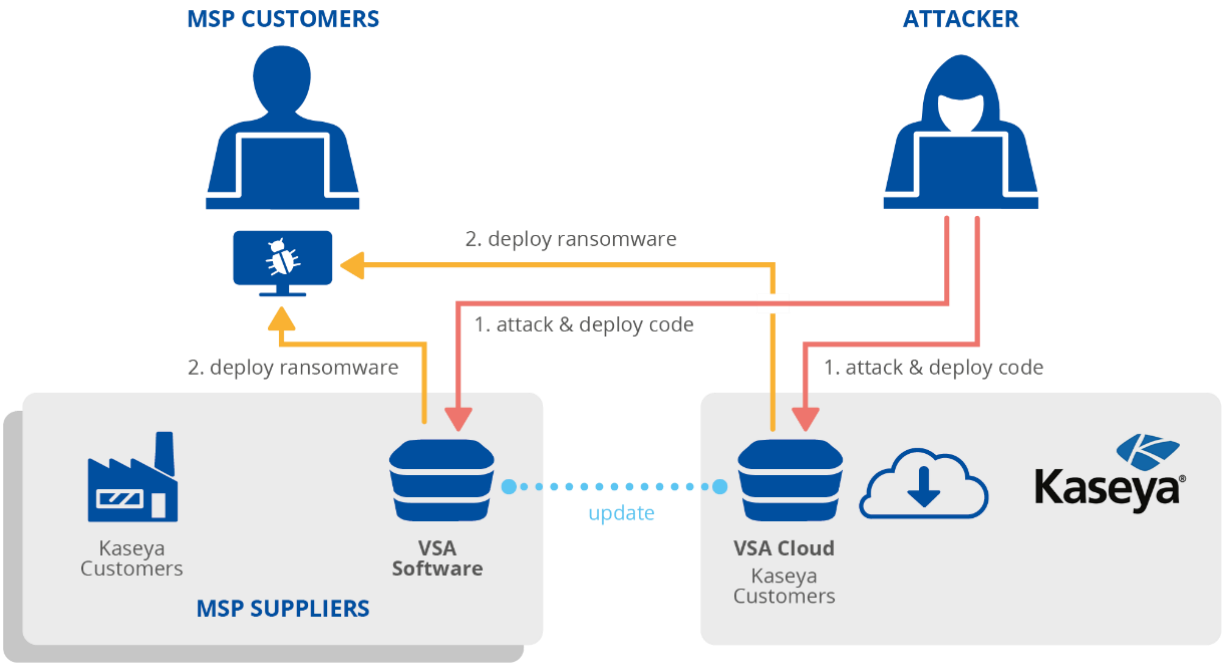
Kaseya is a software service provider specializing in remote monitoring and management tools. It offers VSA (Virtual System/Server Administrator) software for its clients to download, and also to work through its own cloud servers. MSPs (Managed Service Providers) can use the VSA software on premises or they can license the VSA cloud servers of Kaseya. MSPs in turn offer various IT services to other clients[31]. In July 2021, attackers exploited a zero-day vulnerability in Kaseya's own systems (CVE-2021-30116[32]) that enabled the attackers to remotely execute commands on the VSA appliances of Kaseya's customers. Kaseya can send out remote updates to all VSA servers and, on Friday July 2, 2021, an update was distributed to Kaseya clients' VSA that executed code from the attackers. This malicious code in turn deployed ransomware[33,34] to the customers being managed by that VSA.

[31] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Accessed on 08/07/2021.
[32] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116. Accessed on 08/07/2021.
[33] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/. Accessed on 08/07/2021.
[34] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Accessed on 08/07/2021.

Table 10: Supply chain attack taxonomy applied to the attack involving Kaseya. By exploiting a software vulnerability attackers gained access to Kaseya software. Attackers leveraged this access to install ransomware on customers' infrastructure. The attack targeted Kaseya's customers' data and financial resources through ransom demands.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability	Pre-existing Software	Trusted Relationship [T1199], Malware Infection	Data, Financial

Figure 6: Diagram of Kaseya supply chain attack. The attackers deployed code to VSA instances of MSP suppliers (whether in the cloud or on premises is still under investigation). Some MSPs, in turn, were exploited to deploy malware and ransomware to their clients.



4.5. AN EXAMPLE OF MANY UNKNOWNS: SITA PASSENGER SERVICE SYSTEM

The case of SITA is prominent due to the many components of supply chain attacks that remain **unknown** and the possible implications of their impact. It illustrates that there can be many circumstances where the details of the attacks are never published, due to technical impossibility or political and marketing decisions by the companies. There is a trade-off between a benefit for the community, which may improve its security by learning from the details of how others were compromised, and the benefits for the individual companies, e.g. financial, reputational and market[35].

SITA is a company that specializes in air information technology and transport information. SITA's passenger service system is used to provide airlines with passenger information at the time of boarding, including the risk passengers may pose to a country[36].

[35] Investors in SolarWinds sold millions in stock before Russia breach revealed, The Washington Post, https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/. Accessed on 09/07/2021.
[36] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Accessed on 08/07/2021.

In March 2021, it was disclosed that attackers had compromised SITA servers to gain access to passenger data from the customers of SITA. Some of SITA's customers also reported data breaches, such as Air India, Singapore Airlines and Malaysia Airlines[36].

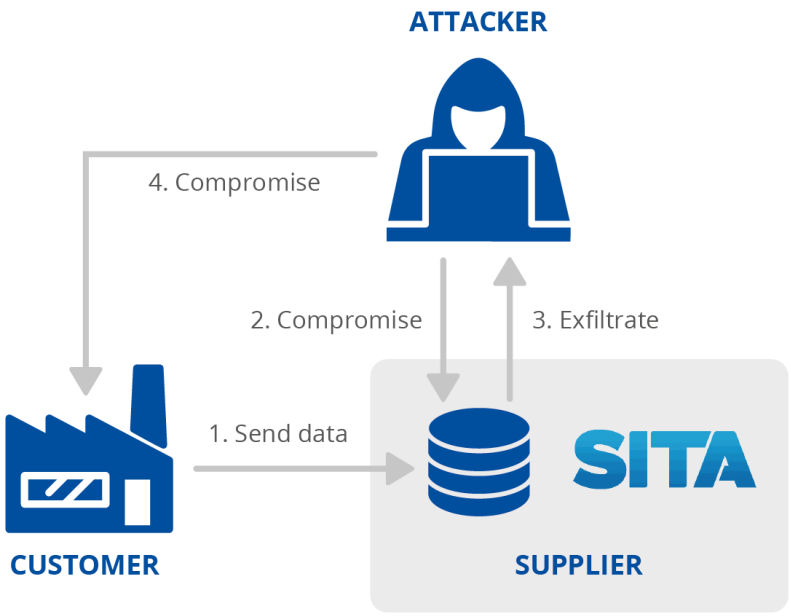
Following reports of leaked data on the Internet, Air India also reported that its networks were compromised and data was stolen.[37] The compromise of Air India internal networks was allegedly related to the SITA incident because a security company found that the name of one computer inside Air India was "SITASERVER4". To date, it remains unknown how the attackers gained access to the SITA servers and it is also not known how the attackers may have accessed Air India, or whether they actually did so. The internal attack to Air India's networks was attributed to the group APT41[37].

The number of unknown variables in this incident is an example of the threat landscape when it comes to supply chain attacks. The level of maturity concerning cyber investigations and preparedness of many organizations should also extend to their suppliers, due to their complex, intertwined relationships.

Table 11: Supply chain attack taxonomy applied to the attack involving SITA. It is not known how the attackers accessed the supplier. The attackers accessed data on the supplier about its customers. It is not known how the attackers managed to infiltrate Air India. The information available indicates that the attackers' main goal was customer data.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Data	Unknown	Personal data

Figure 7: Diagram of SITA supply chain attack. The attackers stole passenger data from the customer companies of SITA. To date, it remains unknown how the attackers gained access to the SITA servers and it is also not known how the attackers may have accessed Air India, or whether they actually did so.



[37] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Accessed on 08/07/2021.

5. ANALYSIS OF SUPPLY CHAIN INCIDENTS

In this section we present an analysis of supply chain attacks based on attacks reported from early 2020 up to early July 2021. The analysis focuses on publicly known supply chain attacks and a detailed overview may be found in Annex A. As discussed later, some attacks appeared to be supply chain attacks but were not and so were omitted from the analysis. A summary of all the incidents analysed in the report is shown in Table 12.

Table 12: Summary of the supply chain attacks identified, analysed and validated from January 2020 to early July 2021.

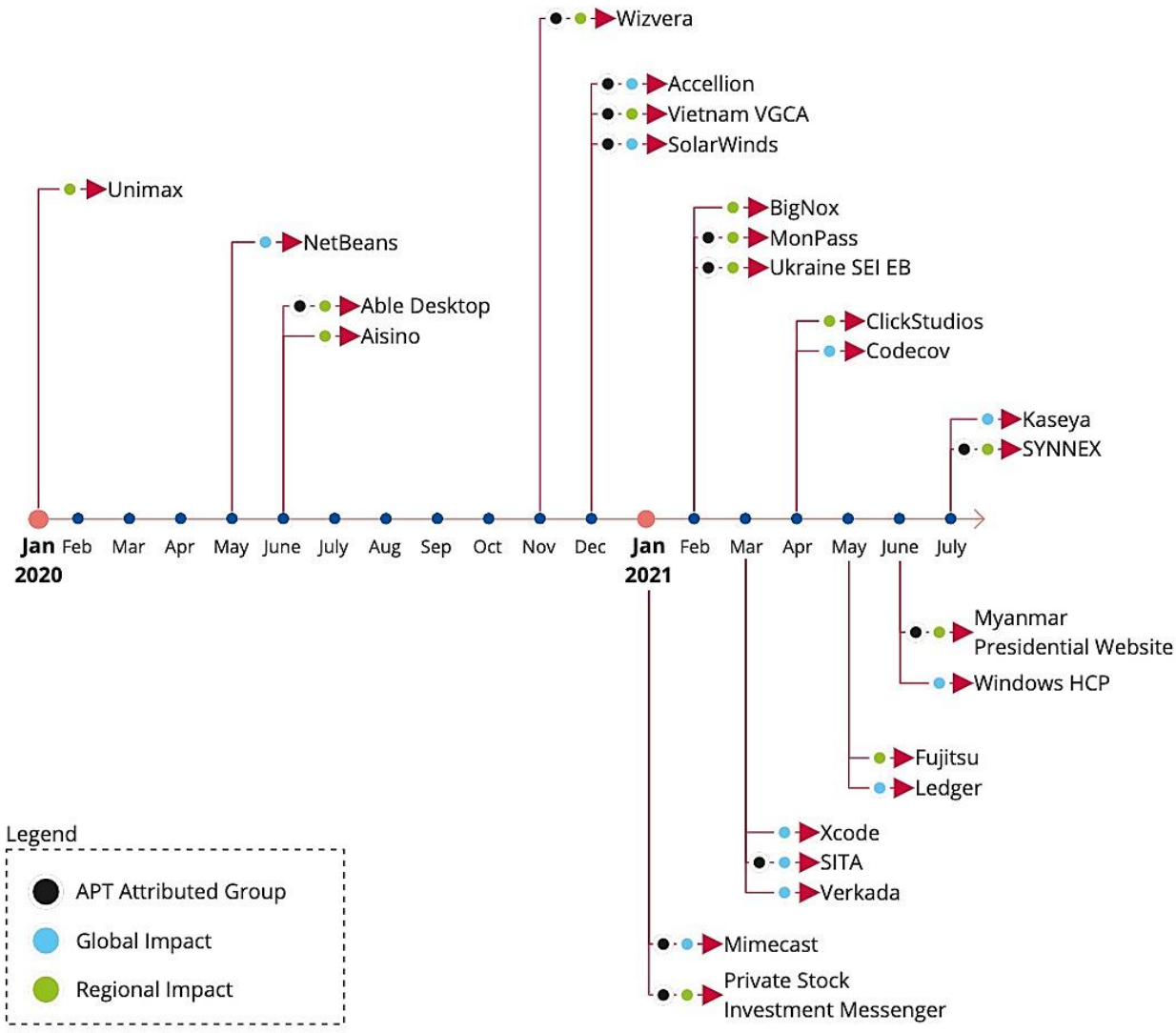
SUPPLIER	SUPPLIER CATEGORY	YEAR	IMPACT	ATTRIBUTED GROUPS
Mimecast	Security Software	2021	Global	APT29
SITA	Aviation	2021	Global	APT41
Ledger	Blockchain	2021	Global	-
Verkada	Physical security	2021	Global	Hacktivist Group
BigNox NoxPlayer	Software	2021	Regional	-
Stock Investment Messenger	Financial Software	2021	Regional	Thallium APT
ClickStudios	Security Software	2021	Regional	-
Apple Xcode	Development Software	2021	Global	-
Myanmar Presidential Website	Public Administration	2021	Regional	Mustang Panda APT
Ukraine SEI EB	Public Administration	2021	Regional	-
Codecov	Enterprise Software	2021	Global	-
Fujitsu ProjectWEB	Cloud Collaboration	2021	Regional	-
Kaseya	IT management	2021	Global	REvil Group
MonPass	Certificate Authority	2021	Regional	Winnti APT Group
SYNNEX	Technology Distributor	2021	Regional	APT 29
Microsoft Windows HCP	Software	2021	Global	-
SolarWinds	Cloud Management	2020	Global	APT29
Accellion	Security Software	2020	Global	UNC2546
Wizvera VeraPort	Identity Management	2020	Regional	Lazarus APT
Able Desktop	Enterprise Software	2020	Regional	TA428
Aisino	Financial Software	2020	Regional	-
Vietnam VGCA	Certificate Authority	2020	Regional	TA413, TA428
NetBeans	Development Software	2020	Global	-
Unimax	Telecommunication	2020	Regional	-

5.1. TIMELINE OF SUPPLY CHAIN ATTACKS

The analysis shows that out of 24 confirmed supply chain attacks, 8 (33%) were reported in 2020 and 16 (66%) from January 2021 to early July 2021. **Based on this data, the trend forecasts that 2021 may have 4 times more supply chain attacks than 2020.**

Figure 8 shows a timeline of the attacks analysed in this report, highlighting those incidents that were attributed to APT groups, and whether they had a global or regional impact. The impact is categorised in each attack as global or regional. The attacks are considered to have a global impact if their customer base is global or if the number of end-users possibly affected are in the millions. Alternatively, attacks that impact users in a specific region or country, or that affect only a handful of users are considered to have a regional impact.

Figure 8: Timeline of supply chain attacks reported from January 2020 to early July 2021. The month indicated in the Figure refers to the month the incident was reported and not when the attack happened. Incidents attributed to APT groups are marked with black dots, incidents with global impact are marked with violet dots, and incidents with regional impact are marked with green dots. A detailed summary of each incident is available in Annex A.



5.2. UNDERSTANDING THE FLOW OF ATTACKS

Each of the incidents shown in Figure 7 was analysed, summarized, and classified according to the proposed taxonomy. The taxonomy supports and facilitates the study of supply chain attacks as a whole in a structured manner.

Figure 8 is a Sankey diagram[38], which illustrates the flow of the most common attack techniques and assets observed in the supply chain attacks that were studied in this report. **Attack techniques [ST] are used against supplier assets [SA], which are used in attack techniques [CT] to compromise customers' assets [CA].**

From Figure 8, it is clear that most attack techniques used to compromise the supplier (first column [ST]) are:

- **Unknown (66%)**, followed by
- **Exploiting software vulnerabilities (16%)**.

In terms of suppliers' assets targeted (second column [SA]), most attacks aimed to compromise:

- **Code (66%)**,
- **Data (20%)**
- **Processes (12%)**.

The compromised suppliers' assets are used as an attack vector to compromise the customers. Those attacks are mostly done (third column [CT]):

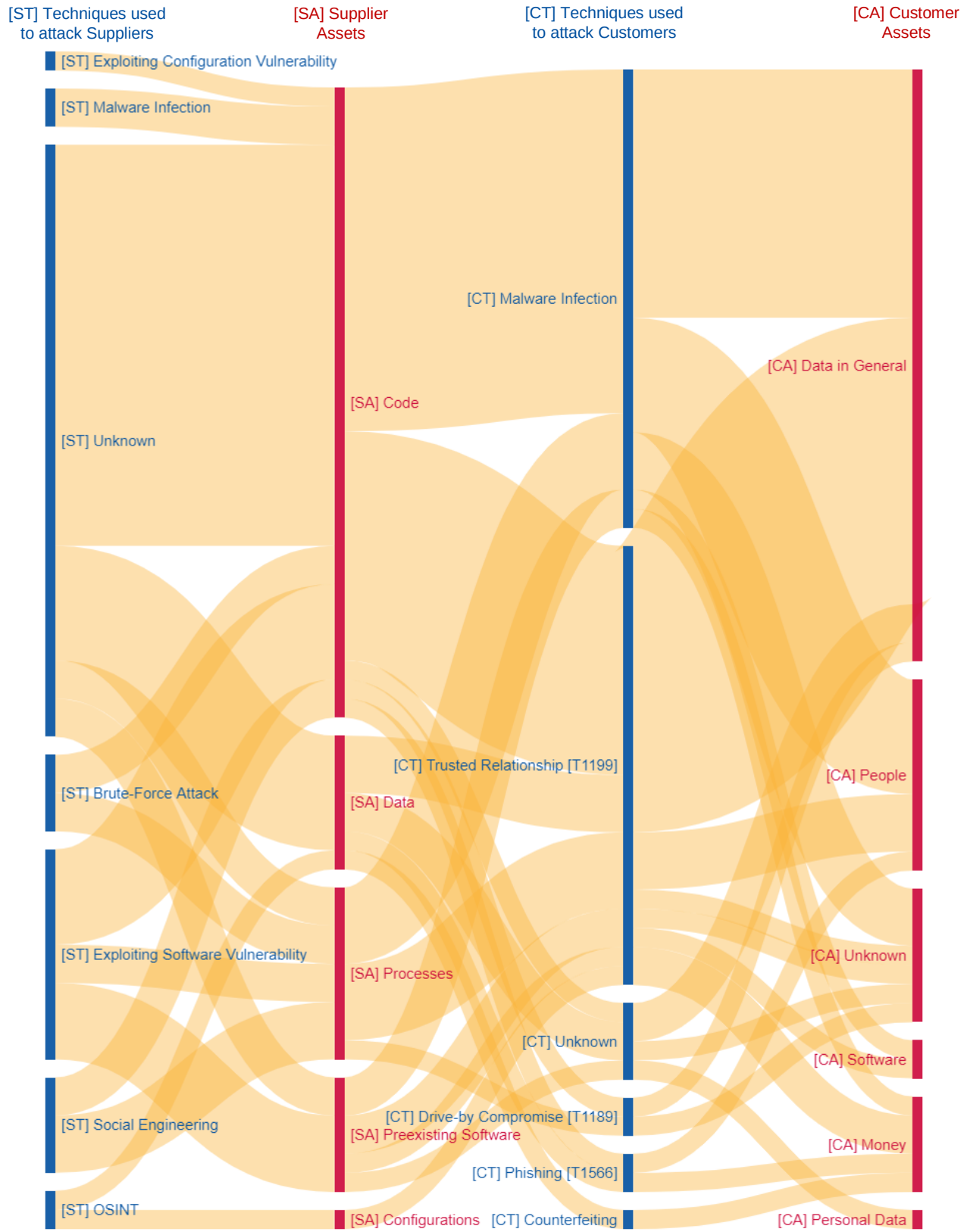
- by **Abusing the trust of the customer (62%)** in the supplier, or
- by using **Malware (62%)**.

Independently of the technique used, most supply chain attacks aim at gaining access to (fourth column [CA]):

- customer **Data (58%)**,
- key **People (16%)** and
- **Financial resources (8%)**.

[38] Sankey diagrams are a specific type of flow diagram, in which the width of the arrows is shown proportionally to the flow quantity.

Figure 9: Analysis of Supply Chain Incidents based on the proposed taxonomy. The Sankey diagram depicts the flow of attack techniques [ST] against supplier assets [SA], which are then used in attack techniques [CT] to compromise customers' assets [CA]. The width of the connections between the various elements increases when the relation has been observed in a larger number of supply chain attacks.



5.3. GOAL ORIENTED ATTACKERS

When considering targeted assets, in **66%** of the incidents attackers focused on the suppliers' **code** in order to further compromise the targeted customers. In **20%** of the analysed incidents attackers' targeted **data**, and in **12%** the targets of the attack on the supplier were **internal processes**. This is key to understanding where to focus efforts in terms of cybersecurity protection. Organizations should focus their efforts on validating third-party code and software to ensure it has not been tampered with or manipulated.

The final customer assets targeted on these supply chain attacks seem to be predominantly customer data, including personal data and intellectual property. This was the case in 58% of the supply chain incidents analysed. Attackers also targeted to a lesser degree other assets including people, software, and financial resources.

5.4. MOST ATTACK VECTORS TO COMPROMISE SUPPLIERS REMAIN UNKNOWN

Our findings show that in **66%** of the supply chain attacks analysed, **suppliers did not know**, or were not transparent, about how they were compromised. In contrast, less than **9%** of the customers compromised through supply chain attacks did not know how the attacks happened. **This highlights the gap in terms of maturity in cybersecurity incident reporting between suppliers and end-user facing companies.**

Considering that **83%** of the suppliers are in the **technology** sector, the lack of knowledge on how attacks happened could either indicate a **poor level of maturity** when it comes to cyber defence in suppliers' infrastructure or unwillingness to share the relevant information. There are other factors that may contribute to a lack of understanding of how suppliers are compromised, including the complexity and sophistication of the attacks and slowness in discovering the attacks which in turn may hinder investigation.

5.5. SOPHISTICATED ATTACKS ATTRIBUTED TO APT GROUPS

More than **50% of the supply chain attacks were attributed to** well-known cybercrime groups, including APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 and TA428. The analysis shows that APT groups seem to have a slight preference for targets with regional impact, and that a significant number of these attacks aimed to gain access to customer data.

Out of the 24 incidents analysed, 10 were not attributed to a particular group. The main reason for the lack of attribution may be that 7 of these attacks happened in the last 7 months. Incidents of this kind may take a longer time to investigate, and even then, in certain cases, attribution is still not possible. However, given the sophistication of these attacks, suppliers should expect to be targeted by organized cybercrime groups and prepare accordingly.

6. NOT EVERYTHING IS A SUPPLY CHAIN ATTACK

From January 2020 to early July 2021, there were many incidents that initially **appeared** to be supply chain attacks or were considered part of a probable future supply chain attack. Many traditional software vulnerabilities that were found were reported as a 'risk' for future supply chain attacks. Some cases involved vulnerabilities that were thought to be intentionally placed in software or hardware but that were later found to be bugs or unintentional errors. Many of these cases were not supply chain attacks since they did not involve a supplier being compromised.

On at least three occasions attackers targeted software libraries or dependencies. In one of these cases, reported in December 2020, attackers uploaded malicious packages to RubyGems repository[39]. A very similar case was reported in March 2021, when a security researcher managed to upload malicious NPM packages using names known to be the names of components or infrastructure used by well-known companies[40]. A third case was reported in April 2021, when attackers uploaded a malicious NPM package trying to deliberately impersonate a well-known package in an attack dubbed brandjacking[41]. In all these cases, the attackers did not compromise existing packages nor the software repositories themselves thus, without a clear attack on supplier assets, we don't consider them as supply chain attacks.

In many cases, vulnerabilities in software were discovered but not used in attacks, or were discovered to be errors and not intentionally introduced. The first example of such a case was reported in February 2020, in which a security researcher disclosed a 0-day vulnerability in the firmware developed by the company Xiaongmai and used for DVRs, NVRs and IP cameras[42]. Other examples include the vulnerabilities reported in Visual Studio Code extensions in May 2021[43], and on Pling-based free and open-source software (FOSS) marketplaces in June 2021[44]. In all these cases, vulnerabilities were discovered though no active attacks using them had been reported at the time of writing this report. As mentioned in previous sections, a supply chain attack involves at least two attacks, namely on a supplier and on a customer. Without an attack on a customer or a supplier, the attack is not considered a supply chain attack.

Additionally, there were other cases of cybersecurity attacks and vulnerabilities that were not supply chain attacks. One such case was the attack on Centreon systems. Centreon is a company that supplies IT monitoring services and offers an open-source software IT monitoring tool. In January 2021, it was discovered that attackers had exploited outdated public facing instances of Centreon to compromise customers' infrastructure[45,46,47]. The attackers, attributed to be the Sandworm APT group, conducted their campaign for three years until they were discovered. The attack aimed to exfiltrate information from the affected customers. The attack was targeted at French IT providers. This is a case where a particular software vulnerability was exploited in a software installed by customers. However, the supplier itself was not compromised and the vulnerabilities were not intentional.

[39] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Accessed on 08/07/2021.
[40] Malicious NPM packages target Amazon, Slack with new dependency attacks, Bleeping Computer, https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/. Accessed on 08/07/2021.
[41] Damaging Linux \& Mac Malware Bundled within Browserify npm Brandjack Attempt, Sonatype, https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt. Accessed on 08/07/2021.
[42] Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras, Habr, https://habr.com/en/post/486856/. Accessed on 08/07/2021.
[43] Newly Discovered Bugs in VSCode Extensions Could Lead to Supply Chain Attacks, The Hacker News, https://thehackernews.com/2021/05/newly-discovered-bugs-in-vscode.html. Accessed on 08/07/2021.
[44] Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks, The Hacker News, https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html. Accessed on 08/07/2021.
[45] Sandworm Intrusion Set Campaign Targeting Centreon Systems, CERT-FR, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf. Accessed on 08/07/2021.
[46] France Reveals 3-Year Long Supply Chain Attack, Secure World Expo, https://www.secureworldexpo.com/industry-news/france-supply-chain-attack-centreon-software. Accessed on 08/07/2021.
[47] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Accessed on 08/07/2021.

7. RECOMMENDATIONS

Supply chain attacks **leverage the interconnectedness of the global markets**. When multiple customers rely on the same supplier, the consequences of a cyber-attack against this supplier are amplified, potentially resulting in a large-scale national or even cross-border impact. For some products, such as software and executable code, the existence of a supply chain is opaque or even completely hidden to the end user. End-user software depends, directly or indirectly, on software provided by the supplier. Such dependencies include packages, libraries, and modules — all of which are used pervasively to lower development costs and accelerate shipping times.

The better protected against cyber-attacks organizations become, the more the attention shifts to suppliers. The math is simple, suppliers are becoming the weakest link on the supply chain. At the same time, customers demand products that are more cybersecure but that remain at a low cost, two needs that it is not always possible to reconcile.

As we observed in numerous incidents of supply chain attacks, organizations are becoming increasingly aware of the need to **assess of the cybersecurity maturity of their suppliers** and the **level of exposure to the risk arising from this customer-supplier relationship**. Customers need to assess and take into account the overall quality of the products and cybersecurity practices of their suppliers, including whether they apply secure development procedures. Moreover, customers should exercise increased due diligence in selecting and vetting their suppliers, and in managing the risk that stems from these relationships.

To **manage supply chain cybersecurity risk**, customers should[48]:

- identify and document types of suppliers and service providers,
- define risk criteria for different types of suppliers and services (e.g. important supplier and customer dependencies, critical software dependencies, single points of failure),
- assess supply chain risks according to their own business continuity impact assessments and requirements,
- define measures for risk treatment based on good practices,
- monitor supply chain risks and threats, based on internal and external sources of information and on findings from suppliers' performance monitoring and reviews,
- make their personnel aware of the risk.

To **manage the relationship to suppliers**, customers should:

- manage suppliers over the whole lifecycle of a product or service, including procedures to handle end-of-life products or components,
- classify assets and information that are shared with or accessible to suppliers, and define relevant procedures for their access and handling,
- define obligations of suppliers for the protection of the organisation's assets, for the sharing of information, for audit rights, for business continuity, for personnel screening, and for the handling of incidents in terms responsibilities, notification obligations and procedures,
- define security requirements for the products and services acquired,
- include all these obligations and requirements in contracts; agree on rules for sub-contracting and potential cascading requirements,
- monitor service performance and perform routine security audits to verify adherence to cybersecurity requirements in agreements; this includes the handling of incidents, vulnerabilities, patches, security requirements, etc.,
- receive assurance of suppliers and service providers that no hidden features or backdoors are knowingly included,

[48] Derived by cybersecurity controls in standards ISO/IEC 27002, ISO 9001 and ISO 31000.

- ensure regulatory and legal requirements are considered,
- define processes to manage changes in supplier agreements, e.g. changes in tools, technologies, etc.

On the other hand, suppliers should ensure the **secure development of products and services** that is consistent with commonly accepted security practices[49]. Suppliers should:

- ensure that the infrastructure used to design, develop, manufacture, and deliver products, components and services follows cybersecurity practices,[50,51];
- implement a product development, maintenance and support process that is consistent with commonly accepted product development processes,
- implement a secure engineering process that is consistent with commonly accepted security practices[52, 53],
- consider applicability of technical requirements based on product category and risks[54],
- offering Conformance Statements to customers for known standards, i.e. ISO/IEC 27001, IEC 62443-4-1, IEC 62443-4-2 (or specific ones such as the CSA Cloud Controls Matrix (CCM) for cloud services), and ensuring and attesting to, to the extent possible, the integrity and origin of open source software used within any portion of a product,
- define quality objectives such as the number of defects or externally identified vulnerabilities or externally reported security issues, and use them as an instrument to improve overall quality,
- maintain accurate and up-to-date data on the origin of software code or components, and on controls applied to internal and third-party software components, tools, and services present in software development processes,
- perform regular audits to ensure that the above measures are met.

Moreover, as any product or service is built from or based on components and software that is subject to vulnerabilities suppliers **should implement good practices for vulnerability management**[55], such as:

- the monitoring of security vulnerabilities reported by internal and external sources that includes used third-party components,
- the risk analysis of vulnerabilities by using a vulnerability scoring system (e.g. CVSS[56]),
- maintenance policies for the treatment of identified vulnerabilities depending on the risk,
- processes to inform customers,
- patch verification and testing to ensure that operational, safety, legal, and cybersecurity requirements are met and that the patch is compatible with non-built-in third-party components,
- processes for secure patch delivery and documentation concerning patches to customers, or
- participating in a vulnerability disclosure program that includes a reporting and disclosure process.

Vulnerabilities should be managed by suppliers in the form of patches. Likewise, a customer should monitor the market for potential vulnerabilities or receive respective vulnerability notifications from his suppliers. Some **good practices for patch management** include[57]:

- maintaining an inventory of assets that includes patch-relevant information,

[49] e.g. IEC 62443-4-1.
[50] e.g. the ones in ISO/IEC 27001.
[51] These may include technical measures, such as (a) separation of environments; (b) auditing trust relationships; (c) establishing multi-factor, risk-based authentication and conditional access across the organisation; (d) minimizing dependencies on products that are part of the environments used to develop, build, and edit software; (e) encrypting data; f) monitoring operations and alerts and responding to attempted and actual cyber incidents.
[52] e.g. IEC 62443-2-4
[53] These may include the use of automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code; or the use of automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them.
[54] Standards like IEC 62443-4-2 provide a comprehensive set on security requirements which are categorized for requirements applicable for all products, applicable for software applications (SAR), applicable for embedded devices (EDR), applicable for host devices (HDR) and applicable for network devices (NDR).
[55] More guidance on vulnerability and patch management can be found in standards IEC 62443-4-1, IEC 62443-2-4 and IEC TR 62443-2-3.
[56] See https://www.first.org/cvss/specification-document ;.
[57] Derived by ISO/IEC 27002.

- using information resources to identify relevant technical vulnerabilities,
- evaluating the risks of identified vulnerabilities and having a documented and implemented maintenance policy available,
- receiving patches only from legitimate sources and testing them before they are installed,
- applying alternative measures should a patch not be available or applicable,
- applying rollback procedures and effective back-up & restore processes.

Beyond what customers and suppliers can do individually, there are initiatives that can take place at the industry level. Google introduced, in June 2021, an End-to-End Framework for ensuring the integrity of software artifacts throughout the software supply chain called SLSA (Supply chain Levels for Software Artifacts)[58]. The goal of SLSA is to improve the state of the industry, particularly open source, to defend against the most pressing threats to integrity. Even though SLSA focuses on software supply chain attacks and not all the other types, it is a good starting point that may benefit organizations.

A more general but extensive set of recommendations for defending against cybersecurity threats was launched in June 2021 by MITRE, known as the MITRE D3FEND project[59]. MITRE D3FEND is a framework or structured knowledge base that allows organizations to find specific mitigations to prevent specific attacks as shown in the MITRE ATT&CK® framework. The project is not specific to supply chain nor to APT attacks but the recommendations can be used to increase the basic level of security of organizations.

Still, not all supply chain risks can be mitigated by good practices implemented by customers, suppliers or organisations. In particular, hidden functions and undocumented access capabilities (backdoors) in hardware components cannot be exhaustively identified by the most common certifications or standard penetration tests. Additionally zero-day vulnerabilities, i.e. vulnerabilities known only to and used by a specific group, remain a challenge. Consequently, action may be needed at the national or even European level. National competent authorities could perform national security risk assessments for supply chain risks, which take into account known actors in order to derive measures on sourcing from suppliers at a national level. Moreover, supply chain attacks may be sponsored by state actors with advanced capabilities, and in this case the assistance of relevant authorities may be needed to mitigate the risks of state-sponsored attacks.

[58] Google Online Security Blog: Introducing SLSA, an End-to-End Framework for Supply Chain Integrity, Google, https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html. Accessed on 08/07/2021.
[59] MITRE D3FEND™, D3FEND Matrix, Version 0.9.2-BETA-3, https://d3fend.mitre.org/. Accessed on 29/06/2021.

8. CONCLUSIONS

As the cost of direct attacks against well-protected organizations increases, attackers prefer to attack their supply chain, which provides the additional motivation of a potentially large-scale and cross-border impact. This migration has resulted in a **larger-than-usual number of supply chain attack cases reported**, with a forecast **of four times more supply chain attacks in 2021 than in 2020**. The inherent global nature of current supply chains increases the potential impact of these attacks and broadens the attack surface for malicious actors. This report covers a number of known attacks but, in reality, there may be more supply chain attacks that go undetected, not investigated or attributed to other causes.

Particularly in software, supply chain attacks undermine trust in the software ecosystem. The incidents described highlight the potential for malicious actors to **compromise the software supply chain from its very early stages** (development phase). New approaches need to be developed to secure the supply chain by design. In this direction, new initiatives such as Google SLSA and MITRE D3FEND, appear to be quite promising.

The analysis in this report shows that there is still a large number of unknown factors in the incidents investigated. **66% of the attack vectors used on suppliers still remain unknown**. A lack of transparency or the ability to investigate poses a serious risk to the trust of the supply chain. Improving the process of transparency and accountability is the first step to improving the security of all elements in the supply chain and protecting final customers.

Supply chain attacks can be complex, require careful planning and often take months or years to execute. While **more than 50% of these attacks are attributed to APT groups or well-known attackers**, the effectiveness of supply chain attacks may make suppliers an interesting target for other, more generic, types of attackers in the future. It is therefore critical that organizations focus their security not only in their own organizations, but also on their suppliers. This is particularly the case for cloud service providers and managed service providers, where recent attacks highlight the increased need for cybersecurity controls in these sectors.

Due to increased interdependencies and complexities, the impact of attacks on suppliers may have **far reaching consequences**. This is not only due to the large number of affected parties but, especially in cases where classified information is exfiltrated, is a cause for concern for national security or for consequences of a geopolitical nature.

In this complex environment for supply chains, establishing **good practices at EU level and coordinated actions are both important** to support all Member States in developing similar capabilities – to reach a common level of security.

ANNEX A: SUMMARY OF SUPPLY CHAIN ATTACKS

This section presents a summary of the 24 supply chain incidents identified and analysed in this report. Each incident is identified by the supplier involved in the attack. The taxonomy proposed in this report is then applied to each case, and a diagram illustrating how the attack happened is included for clarity. The information included in the summaries refers to information available at the time of writing of this report.

LIST OF SUPPLY CHAIN INCIDENTS:

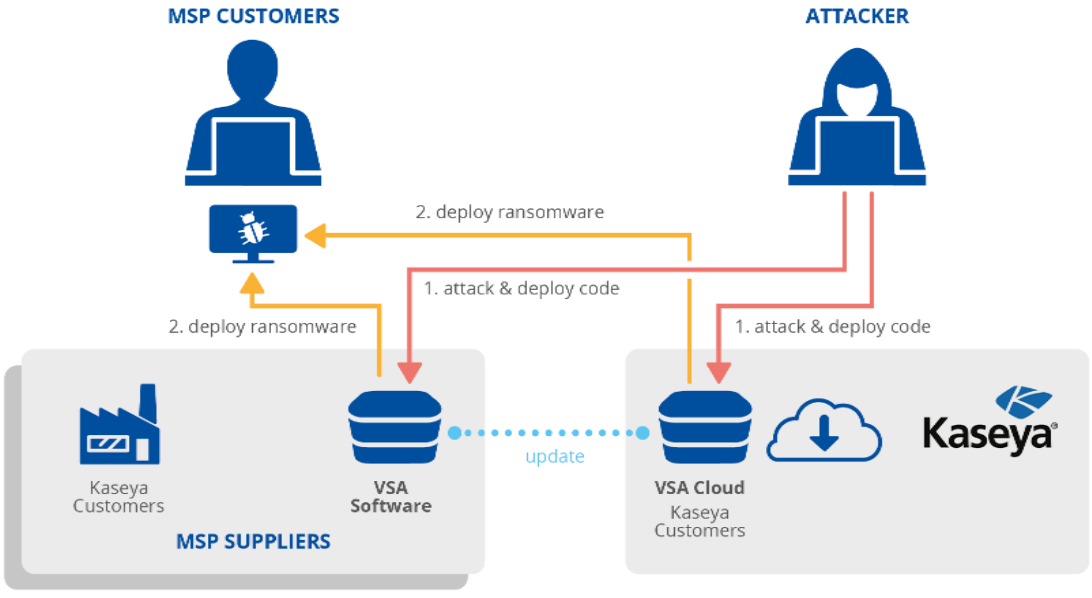
A.1 KASEYA: IT SOFTWARE MANAGEMENT

Kaseya[60] is a software service provider specializing in remote monitoring and management tools. It offers VSA (Virtual System/Server Administrator) software and provides its own cloud servers. MSPs (Managed Service Providers) can use the VSA software on premises or they can license the VSA cloud servers of Kaseya. MSPs in turn offer various IT services to other clients[61].

In July 2021, attackers exploited a zero-day vulnerability in Kaseya's own systems (CVE-2021-30116[62]). Attackers could remotely execute commands on the VSA appliances of Kaseya's customers. Kaseya can send out remote updates to all VSA servers and, on Friday July 2, 2021, an update was distributed to Kaseya clients' VSA that executed code from the attackers. This malicious code in turn deployed ransomware[63,64] to the customers being managed by that VSA.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability	Pre-existing Software

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Malware Infection	Data, Financial

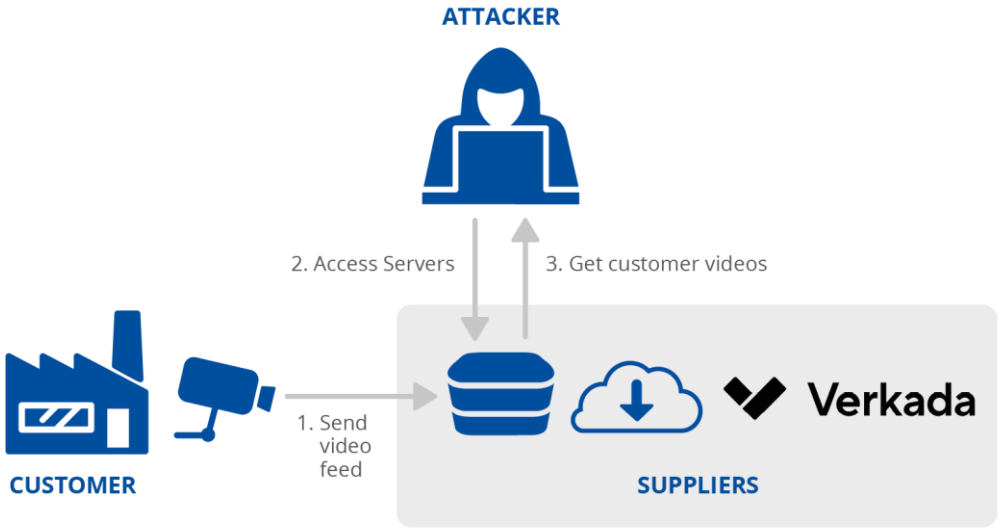


[60] IT Management Software - for MSPs and IT Teams, Kaseya, https://www.kaseya.com/. Accessed on 09/07/2021.
[61] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Accessed on 09/07/2021.
[62] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116, Accessed on 09/07/2021.
[63] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/, Accessed on 09/07/2021.
[64] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Accessed on 09/07/2021.

A.2 VERKADA: CLOUD-BASED SECURITY SURVEILLANCE SOLUTIONS

Verkada offers cloud-based security surveillance solutions to more than 5,000 customers[65]. In March 2021, a production server was compromised. This allowed the attackers that obtained the privileged credentials to access the security cameras deployed in customers' facilities[66]. The credentials were allegedly found 'on the Internet'[67]. The attackers gained access to customers' video and images from more than 150,000 cameras located at schools, jails, hospitals, police stations, and Tesla factories[68]. A hacktivist group claimed responsibility for the attack[69].

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
OSINT	Configurations, Data	Trusted Relationship [T1199]	Data



[65] The Future of Physical Security for the Enterprise: About Verkada, Verkada, https://www.verkada.com/about/. Accessed on 09/07/2021.
[66] Verkada Security Update, Verkada, https://www.verkada.com/security-update/. Accessed on 09/07/2021.
[67] Verkada Mass Hack, IPVM, https://ipvm.com/reports/verkada-hack. Accessed on 09/07/2021.
[68] A hacker who exposed Verkada's surveillance camera snafu has been raided, The Verge, https://www.theverge.com/2021/3/12/22328344/tillie-kottmann-hacker-raid-switzerland-verkada-cameras. Accessed on 09/07/2021.
[69] Tesla (TSLA), Cloudfare (NET) Breached in Verkada Security Camera Hack, Bloomberg, https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams. Accessed on 09/07/2021.

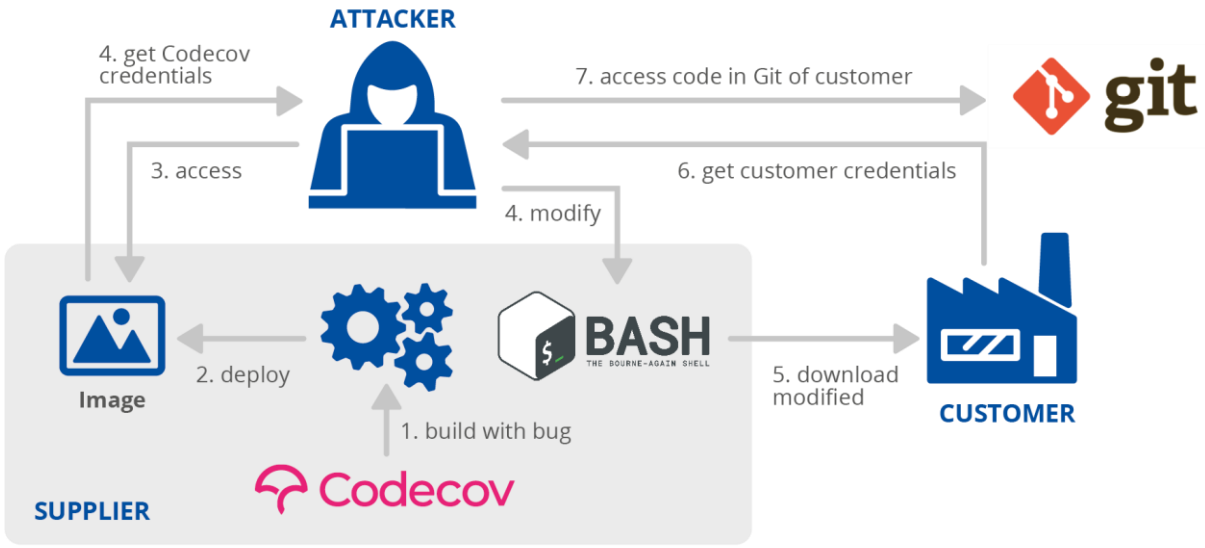
A.3 CODECOV: CODE MANAGEMENT AND AUDIT SOLUTIONS

Codecov is a company that provides software for code coverage and testing tools. The company supplies tools to other companies such as IBM and Hewlett Packard Enterprise. In April 2021, Codecov reported that attackers obtained some of their valid credentials from a Docker image due to an error in how those Docker images were created.

Once the attackers obtained these credentials, they used them to compromise an "upload bash script"[70] that is used by Codecov customers. Once the customers downloaded and executed this script, the attackers were able to exfiltrate data from Codecov's customers, including sensitive information that would allow the attackers to access the customers' resources[71]. Multiple Codecov customers reported that the attackers were able to access their source code using stolen information from the Codecov breach[71]. The attack was not attributed.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Configuration Vulnerability	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Software



[70] Codecov supply chain attack breakdown, https://blog.gitguardian.com/codecov-supply-chain-breach/. Accessed on 27/06/2021.

[71] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Accessed on 27/06/2021.

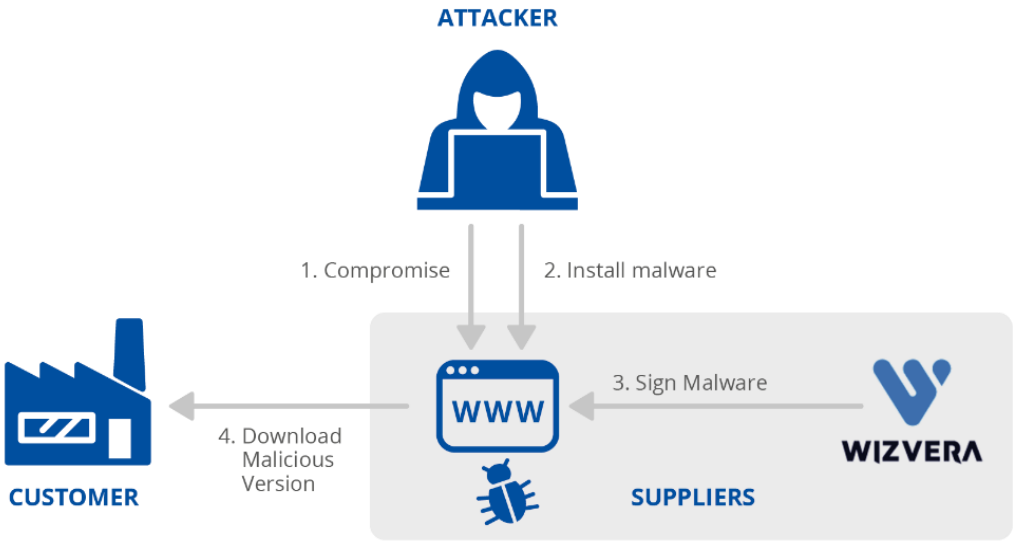
A.4 WIZVERA VERAPORT: INTEGRATION INSTALLATION PROGRAM

Wizvera is a company that provides solutions for identity verification, password management, and cloud certificates[72]. Wizvera has a product called VeraPort, an installation integration product that allows users to install security software required by their employers[73]. In November 2020, attackers compromised a legitimate website that had VeraPort support. They replaced the VeraPort configuration in the compromised website to deliver malware instead of the expected security software.

The configuration was digitally signed by Wizvera[73]. VeraPort checks whether the software being downloaded has a valid digital signature, however it does not check who issued the certificate. Through this mechanism, South Korea users that accessed the compromised website downloaded the malware. The attack was attributed to the Lazarus APT group[73].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Processes

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Drive-by Compromise [T1189], Malware Infection	Data



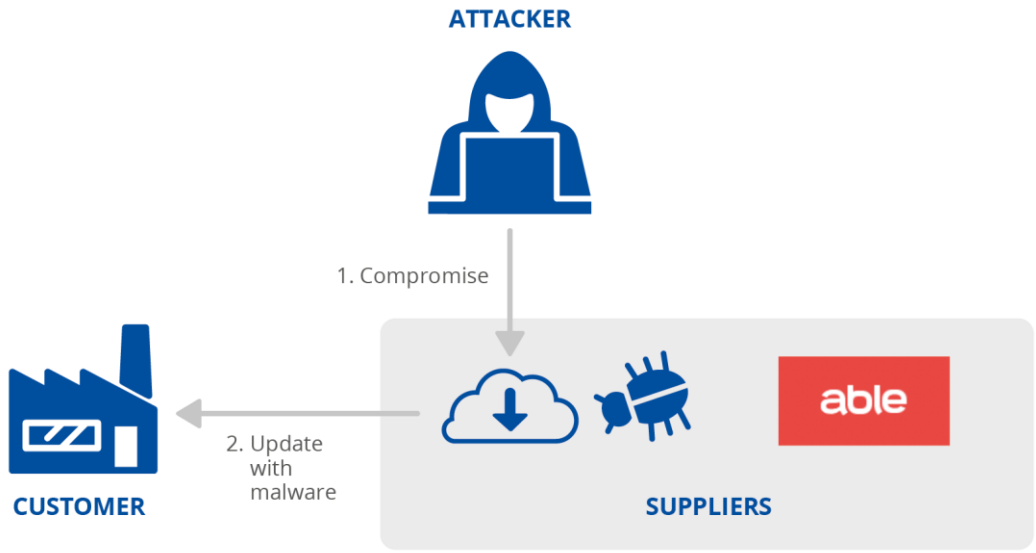
[72] Wizvera Company Profile & Funding, Crunchbase, https://www.crunchbase.com/organization/wizvera. Accessed on 09/07/2021.
[73] Lazarus supply-chain attack in South Korea, WeLiveSecurity, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/. Accessed on 09/07/2021.

A.5 ABLE DESKTOP: CHAT SOFTWARE

Able is a company based in Mongolia that supplies software solutions to government agencies and businesses in the region[74]. In June 2020, attackers appear to have accessed Able's backend and compromised the system that delivers software updates to all customers. Attackers added malware to the "Able Desktop" application (an add-on that provides instant messaging to Able's main product)[75]. While it is unknown how the supplier was compromised, attackers were able to force users to install malware[75]. The malware was then used to steal information from the customers infected devices[75]. The attack was attributed to APT TA428.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Malware Infection	Data



[74] Able - Working online, Able, https://web.able.mn/, Accessed on 09/07/2021.
[75] Operation StealthyTrident: corporate software under attack, WeLiveSecurity, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/. Accessed on 09/07/2021.

A.6 AISINO INTELLIGENT TAX SOFTWARE SUITE

Aisino Credit Information Company supplies tax payment software to international customers through its "Golden Tax" department, including the "Aisino Tax Software Suite". In June 2020, researchers disclosed that the "Aisino Tax Software Suite" was compromised to include malware[76]. It is not known how the software was compromised and what the goal of the attack was[76]. The attack was targeted at businesses in China as this software is part of a national program in that country[77]. The attack was not attributed.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Code	Trusted Relationship [T1199], Malware Infection	Unknown

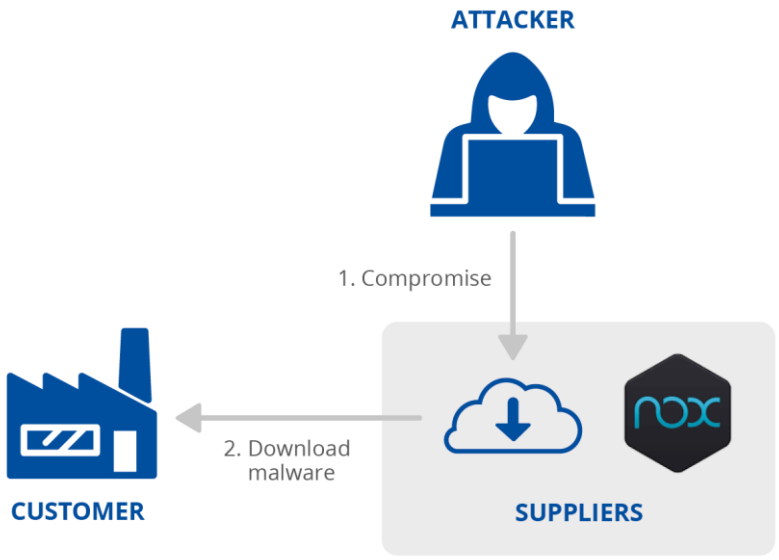
[76] The Golden Tax Department and Emergence of GoldenSpy Malware, Trustwave SpiderLabs, https://trustwave.azureedge.net/media/16929/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf. Accessed on 09/07/2021.
[77] GoldenSpy Chapter 4: GoldenHelper Malware Embedded in Official Golden Tax Software, Trustwave, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/. Accessed on 09/07/2021.

A.7 BIGNOX NOXPLAYER: ANDROID EMULATOR FOR PCS AND MACS

BigNox is a company that supplies emulation software. Their main product, NoxPlayer, is a very popular Android emulator for Windows and Macs[78]. In February 2021, researchers reported that the NoxPlayer infrastructure had been compromised. It could abuse the tool's update mechanism and, instead of updates, deliver malware[79].

Once the initial payload was delivered, attackers could gather information on their victims and deliver further malware to specific targets[79]. The goal of the attackers seems to be to have the ability to survey specific targets[79]. The attack was not attributed.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Code	Trusted Relationship [T1199], Malware Infection	People, Data



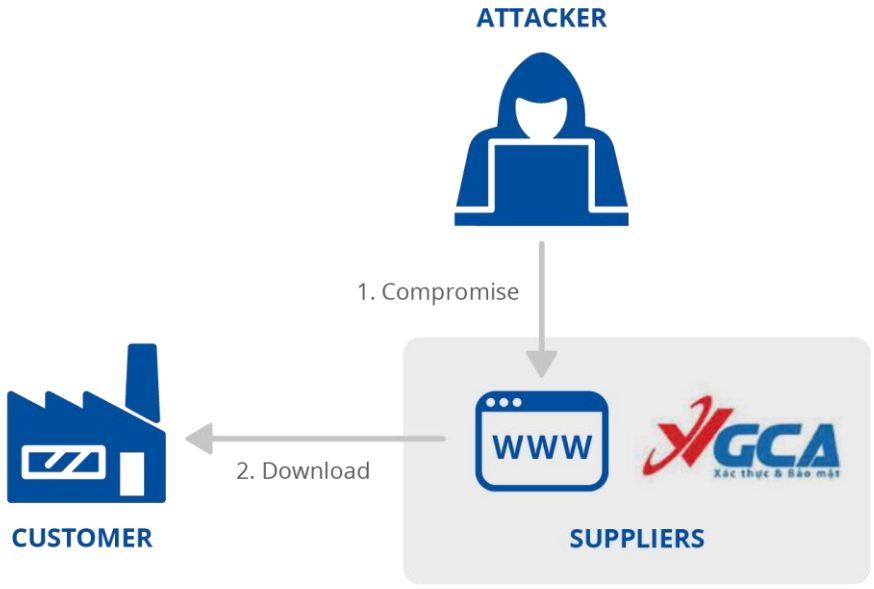
[78] NoxPlayer - Free Android Emulator on PC and Mac, BigNox, https://www.bignox.com/. Accessed on 09/07/2021.
[79] Operation NightScout: Supply-chain attack targets online gaming in Asia, WeLiveSecurity, https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/. Accessed on 09/07/2021.

A.8 VIETNAM GOVERNMENT CERTIFICATION AUTHORITY (VGCA)

The Vietnamese government certification authority (VGCA) provides digital certificates and a set of applications that help citizens and businesses digitally sign documents[80]. In December 2020, researchers reported that the VGCA infrastructure website was compromised to replace legitimate binaries with trojanized applications[81]. The goal of the attack is unclear, however researchers believe this could be part of a larger attack[81]. The tools used indicate that APT groups (TA413, TA428) may be behind the attack[82].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Malware Infection	People



[80] Vietnam targeted in complex supply chain attack, ZDNet, https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/. Accessed on 09/07/2021.
[81] Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia, WeLiveSecurity, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/. Accessed on 09/07/2021.
[82] Panda's New Arsenal: Part 3 Smanager, Hiroki Hada, https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager. Accessed on 09/07/2021.

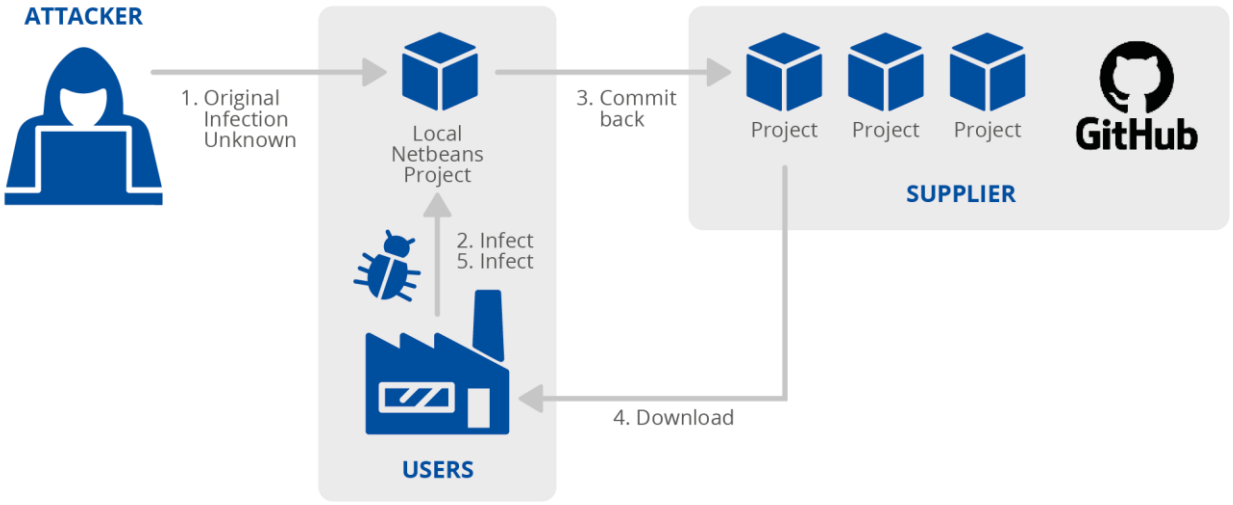
A.9 APACHE NETBEANS: DEVELOPMENT PLATFORM

NetBeans is an integrated Java development platform by Apache. In May 2020, researchers reported that some NetBeans projects on GitHub contained malware without the knowledge of the owners. Everyone downloading and using these projects would get infected, trojanising all their local NetBeans projects, and uploading them to GitHub.

Users were also infected with a RAT malware[83,84]. The attacker's goal seems to be the collection of proprietary information. This attack seems to be part of a larger supply chain attack. In this case the users are both the supplier and the victims. GitHub is the only sharing medium used. The attack was not attributed.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Malware Infection	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Software, Data



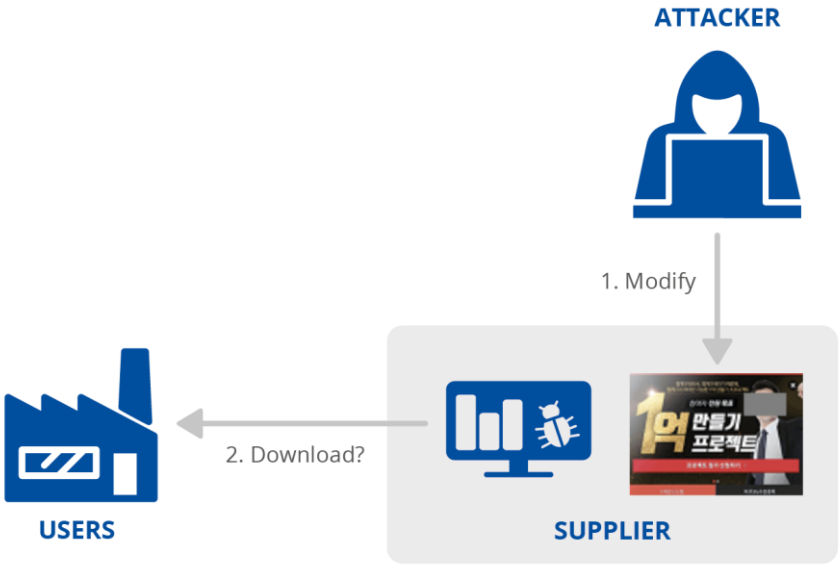
[83] The Octopus Scanner Malware: Attacking the open source supply chain, GitHub Security Lab, https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/. Accessed on 09/07/2021.
[84] Supply Chain Attack Event - Targeted Attacks on Java Projects in GitHub, NSFOCUS, https://nsfocusglobal.com/supply-chain-attack-event-targeted-attacks-on-java-projects-in-github/. Accessed on 09/07/2021.

A.10 PRIVATE STOCK INVESTMENT MESSENGER

In January 2021, researchers reported that stock investors were being targeted by the Thallium APT group which was compromising a widely used private stock investment messenger application[85]. The attackers trojanized the installers of the messaging application to include malware[86]. The malware was used to spy on the infected users[87]. There is no reliable information on the attack or methods used.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	People



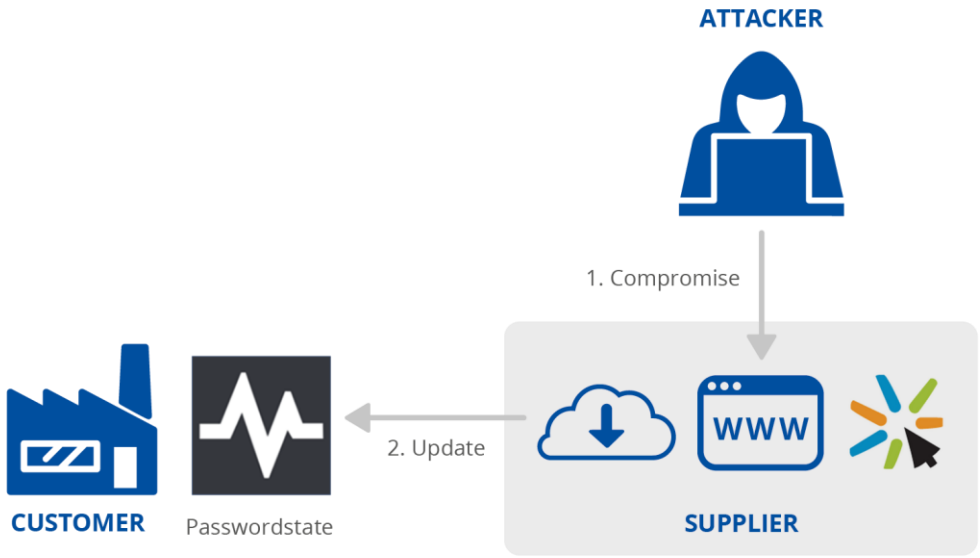
[85] Thallium Hacker Targeted Users of Private Stock Investment Messenger, Cyware Alerts - Hacker News, https://cyware.com/news/thallium-hacker-targeted-users-of-private-stock-investment-messenger-ac33d20d. Accessed on 09/07/2021.
[86] Thallium Altered the Installer of a Stock Investment App, E Hacking News, https://www.ehackingnews.com/2021/01/thallium-altered-installer-of-stock.html. Accessed on 09/07/2021.
[87] Thallium organization exploits private equity investment messenger to launch software supply chain attack, ESTsecurity, https://blog.alyac.co.kr/3489. Accessed on 09/07/2021.

A.11 CLICKSTUDIOS PASSWORDSTATE: PASSWORD MANAGER

ClickStudios is a company that supplies enterprise password management solutions[88]. Their main product is a tool called Passwordstate. In April 2021, the Passwordstate 'upgrade director' web mechanism used to update the tool was compromised[89], redirecting users to download malware instead of the expected updates. The malware installed was designed to steal information from the compromised systems[89, 90]. The attack was not attributed.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Malware Infection	Data



[88] Enterprise Password Management Software - Web based Server Password Manager, ClickStudios https://www.clickstudios.com.au/. Accessed on 09/07/2021.
[89] ClickStudios PASSWORDSTATE Incident Management Advisory #01, ClickStudios, https://www.clickstudios.com.au/advisories/Incident_Management_Advisory-01-20210424.pdf. Accessed on 09/07/2021.
[90] Moserpass supply chain, CSIS Security Group, https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/. Accessed on 09/07/2021.

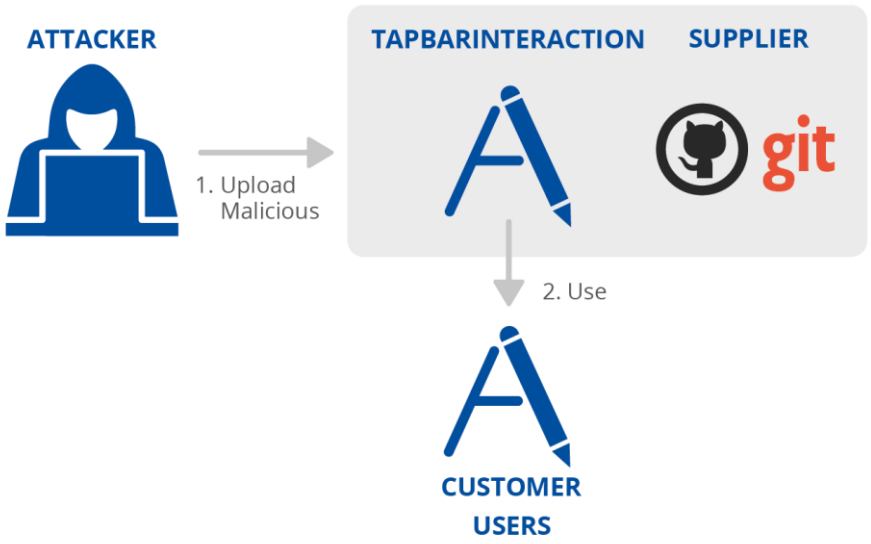
A.12 APPLE XCODE: INTEGRATED DEVELOPMENT ENVIRONMENT

Apple Xcode is a development environment used to develop OSX and iOS applications[91]. In March 2021, researchers reported that an individual malicious Xcode project was being used to infect Xcode developers with a backdoor[92]. The malicious Xcode project was a copy of a real one. The malicious Xcode project infected the user by exploiting a weakness in Xcode that allowed attackers to automatically run a script when the project build was launched[92].

There is no attribution to this attack and it is not clear whether customers where ever attacked[93]. It is also not clear how the trojanized Xcode project was delivered to the potential victims, or if it ever was.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Unknown



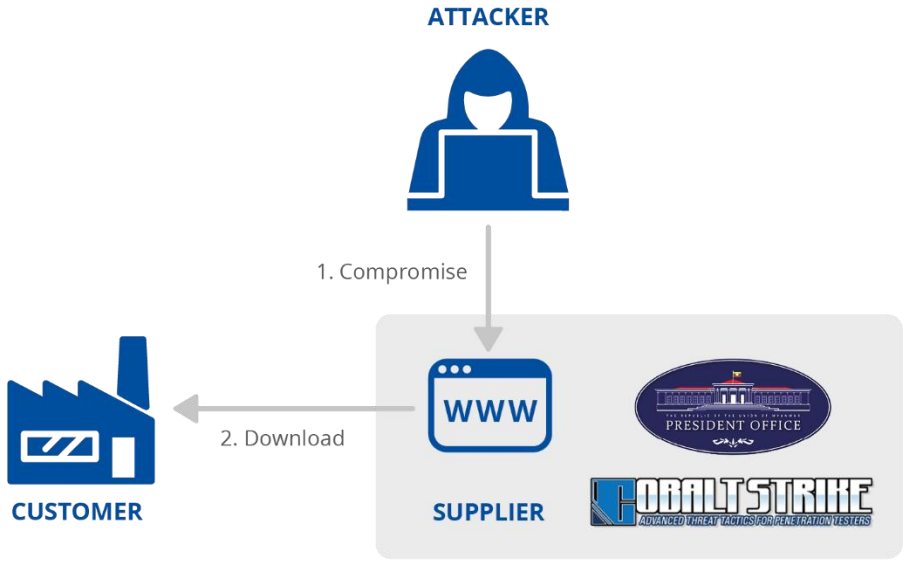
[91] Xcode 13 Overview, Apple Developer, https://developer.apple.com/xcode/. Accessed on 09/07/2021.
[92] New macOS Malware XcodeSpy Targets Xcode Developers with EggShell Backdoor, SentinelLabs, https://labs.sentinelone.com/new-macos-malware-xcodespy-targets-xcode-developers-with-eggshell-backdoor/, Accessed on 09/07/2021.
[93] XcodeSpy Mac Malware Targets Developers, SecureMac, https://www.securemac.com/news/xcodespy-mac-malware-targets-developers. Accessed on 09/07/2021.

A.13 MYANMAR PRESIDENTIAL WEBSITE

In June 2021, researchers reported that resources hosted in the Myanmar presidential website had been trojanized to deliver malware[94]. The attack was not officially attributed to a specific APT group[95], however, resemblances with the Mustang Panda APT group were highlighted[94,96].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Phishing [T1566], Malware Infection	People



[94] "ESETresearch uncovered a supply chain attack on the Myanmar president office website", Twitter, https://twitter.com/ESETresearch/status/1400165767488970764. Accessed on 09/07/2021.
[95] Backdoor malware found on the Myanmar president's website, again, The Record by Recorded Future, https://therecord.media/backdoor-malware-found-on-the-myanmar-presidents-website-again/. Accessed on 09/07/2021.
[96] Cobalt Strike Beacons Being Hosted on Myanmar President's Website, Binary Defense, https://www.binarydefense.com/threat_watch/cobalt-strike-beacons-being-hosted-on-myanmar-presidents-website/. Accessed on 09/07/2021.

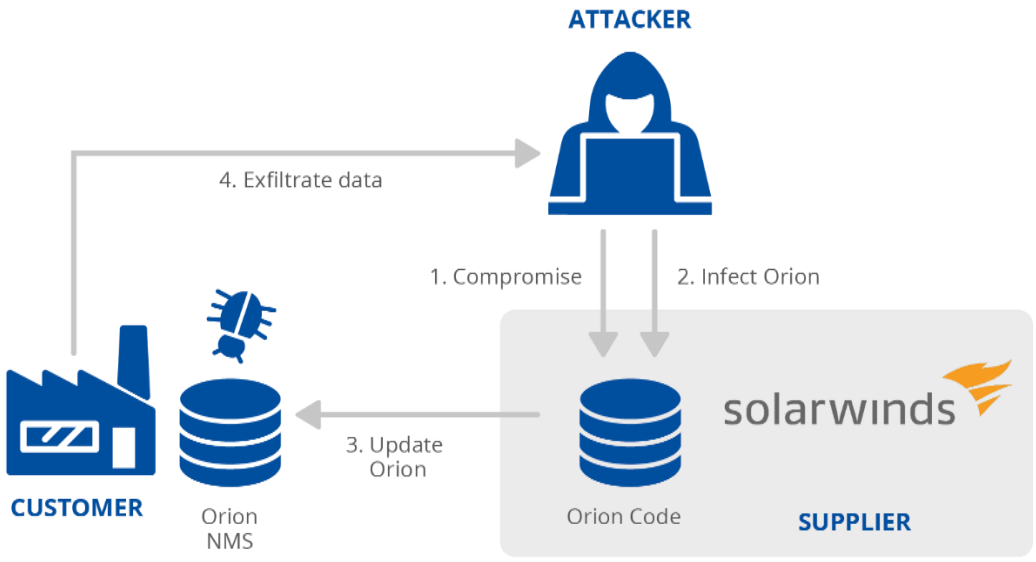
A.14 SOLARWINDS ORION: IT MANAGEMENT AND REMOTE MONITORING

SolarWinds is a company that supplies management and monitoring software[97]. Orion is SolarWinds' network management system (NMS) product[98]. In December 2020 it was discovered that Orion had been compromised. An extensive investigation showed that attackers gained access to SolarWinds' network, possibly by exploiting a zero-day vulnerability in a third-party application or device, a brute-force attack, or through social engineering[99]. Once compromised, the attackers collected information for an extended period of time.

After the compromise, a malicious software was injected in Orion's build process[99,100]. The compromised software was then directly downloaded and execute by customers and was used to gather and steal information[101,102]. The attack was attributed to the APT29[103] group.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability, Brute-force attack, Social Engineering	Processes, Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Malware Infection	Data



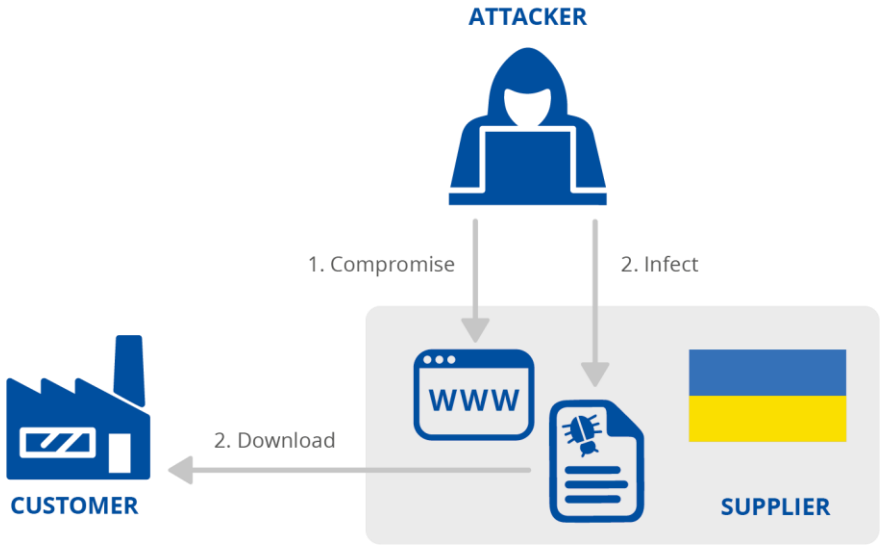
[97] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Accessed on 09/07/2021.
[98] Orion Platform, SolarWinds, https://www.solarwinds.com/solutions/orion. Accessed on 09/07/2021.
[99] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Accessed on 09/07/2021.
[100] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Accessed on 09/07/2021.
[101] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, ireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Accessed on 09/07/2021.
[102] SUNBURST Additional Technical Details, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html. Accessed on 09/07/2021.
[103] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Accessed on 09/07/2021.

A.15 UKRAINE SEI EB: SYSTEM OF ELECTRONIC INTERACTION OF EXECUTIVE BODIES

Ukraine government and public authorities use the System of Electronic Interaction of Executive Bodies (SEI EB), a web portal system designed to exchange documents[104]. In February 2021 it was reported that the system had been compromised by attackers who managed to upload malicious documents into the portal[105]. The malicious documents would later infect users with malware designed to gather and steal information. The attack was attributed to various APT groups, but not to any particular sole group[104].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	People, Data



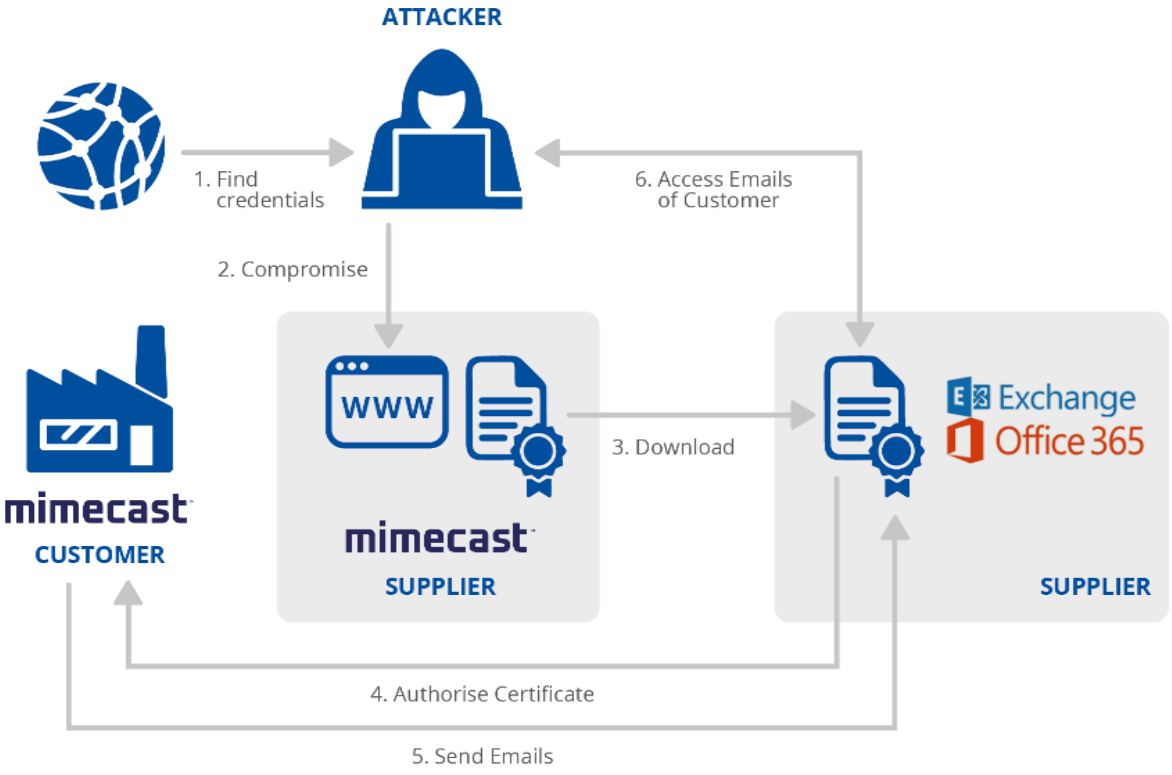
[104] Russian hackers aim cyber attack on Ukrainian government agencies, Teiss News, https://www.teiss.co.uk/russian-hackers-targeting-ukrainian-government-agencies/. Accessed on 09/07/2021.
[105] The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies, National Security and Defense Council of Ukraine, https://www.rnbo.gov.ua/en/Diialnist/4823.html. Accessed on 09/07/2021.

A.16 MIMECAST: CLOUD CYBERSECURITY SERVICES

Mimecast is a supplier of cloud-based cybersecurity services[106]. Among the services it provides, Mimecast offers email security services which require customers to connect securely to Mimecast servers to use their Microsoft 365 accounts. In January 2021, it was discovered that attackers had compromised Mimecast (through the SolarWinds supplier). After the compromise, a Mimecast-issued certificate used by customers to access Microsoft 365 services was accessed by attackers, giving them the ability to intercept the network connections and to connect to the Microsoft 365 accounts to steal information[107,108]. The attack was attributed to the APT29 group[109]. The compromise of the supplier has been linked to SolarWinds, however there is no reliable information on the details of how this occurred.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Data

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Data



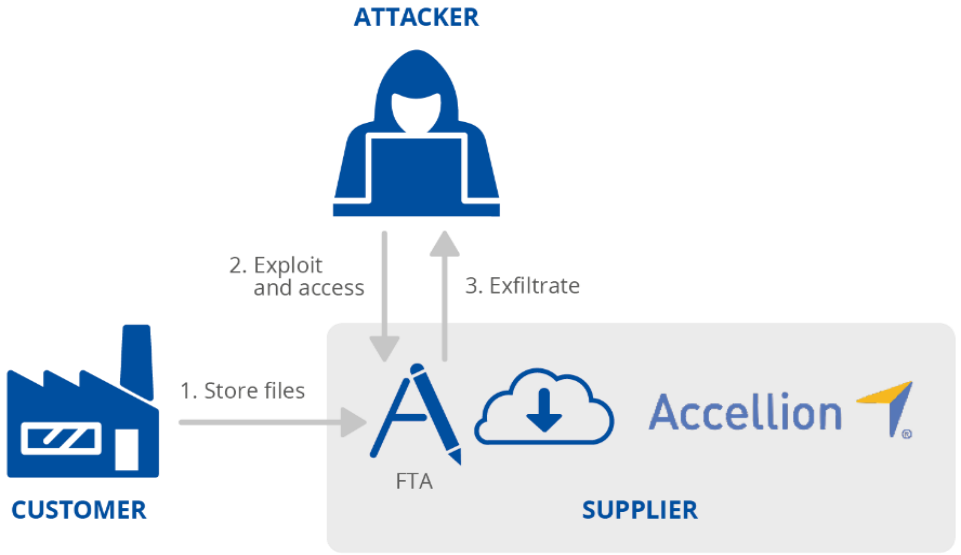
[106] Our Company, Mimecast, https://www.mimecast.com/company/. Accessed on 09/07/2021.
[107] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. Accessed on 09/07/2021.
[108] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Accessed on 09/07/2021.
[109] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Accessed on 09/07/2021.

A.17 ACCELLION: FILE TRANSFER APPLIANCE (FTA) SOFTWARE

Accellion is a company that supplies security software to enterprises, in particular applications for secure file sharing and collaboration[110]. In December 2020, Accellion reported that attackers were exploiting multiple zero-day vulnerabilities in their File Transfer Appliance (FTA) software to gain access to customers' records[111,112] and exfiltrate them using a Webshell. Many companies affected by these vulnerabilities were extorted after attackers threatened to publish their stolen files. The attack was attributed to a cybercrime group known as UNC2546[112].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Data



[110] About Accellion, Accellion, https://www.accellion.com/company/. Accessed on 09/07/2021.
[111] File Transfer Appliance (FTA) Security Assessment, Accellion, https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf. Accessed on 09/07/2021.
[112] Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, FireEye Inc, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html. Accessed on 09/07/2021.

A.18 SITA PASSENGER SERVICE SYSTEM

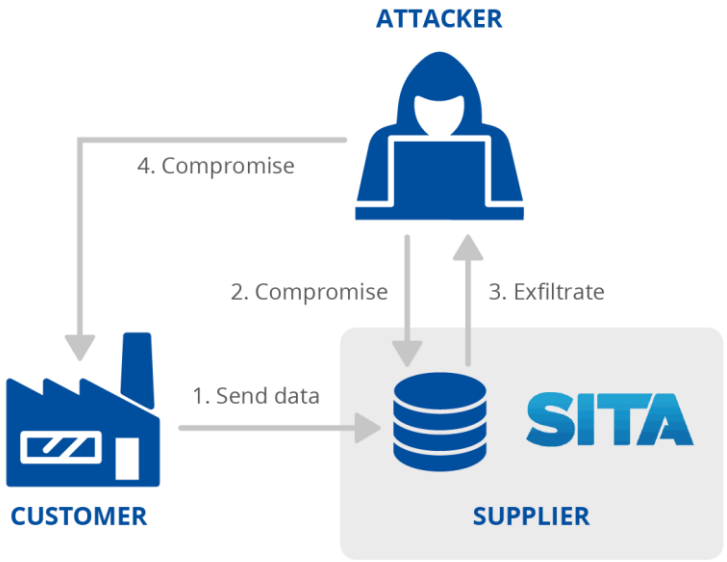
SITA is a company that specialises in air information technology and transport information[113]. SITA's passenger service system is used to provide airlines with passenger information at the time of boarding, including the risk passengers may pose to a country[114]. In March 2021, it was disclosed that attackers had compromised SITA servers to gain access to passenger data from the customers of SITA. Some of SITA's customers also reported data breaches, such as Air India, Singapore Airlines and Malaysia Airlines.

Following reports of leaked data on the Internet, Air India also reported that its networks were compromised and data was stolen. The compromise of Air India internal networks was allegedly related to the SITA incident because a security company found that the name of one computer inside Air India was "SITASERVER4".

To date, it remains unknown how the attackers gained access to the SITA servers and it is also not known how the attackers may have accessed Air India, or whether they actually did so. The internal attach to Air India's networks was attributed to the group APT41[115].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Data

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Personal data



[113] About us, SITA, https://www.sita.aero/about-us/. Accessed on 09/07/2021.
[114] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Accessed on 09/07/2021.
[115] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Accessed on 09/07/2021.

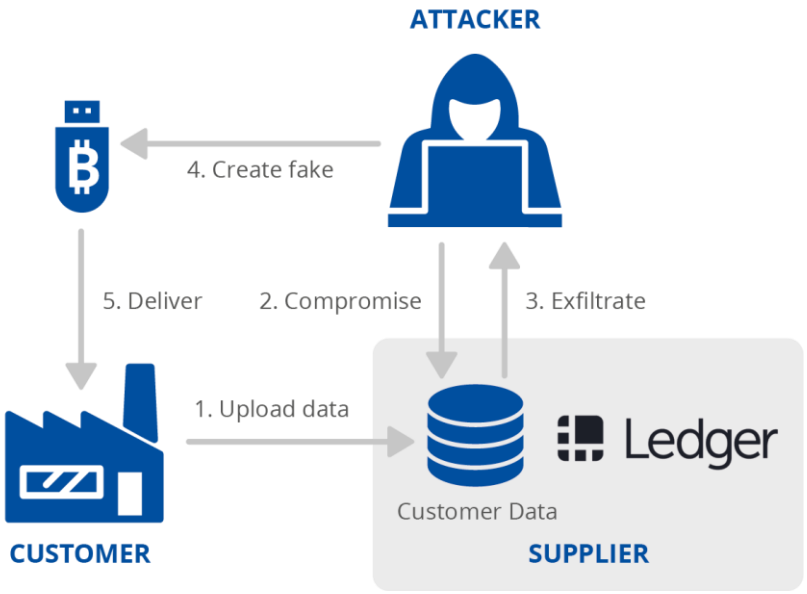
A.19 LEDGER: HARDWARE WALLET

Ledger is a company that supplies hardware wallet technology for cryptocurrency[116]. In July 2020, attackers obtained valid credentials to access the Ledger e-commerce database[117]. The way attackers accessed these credentials is unknown. The stolen data was released publicly in an online forum[118].

Attackers used the stolen data for online phishing and extortion of users[119,120], and for stealing users' money through a physical attack after supplying users with counterfeited Ledger wallets, which when connected to a computer will ask users for their security keys, infect the computer with malware, and send back the stolen information to the attackers[121]. The attack was not attributed.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Data

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Phishing [T1566], Counterfeiting	Financial



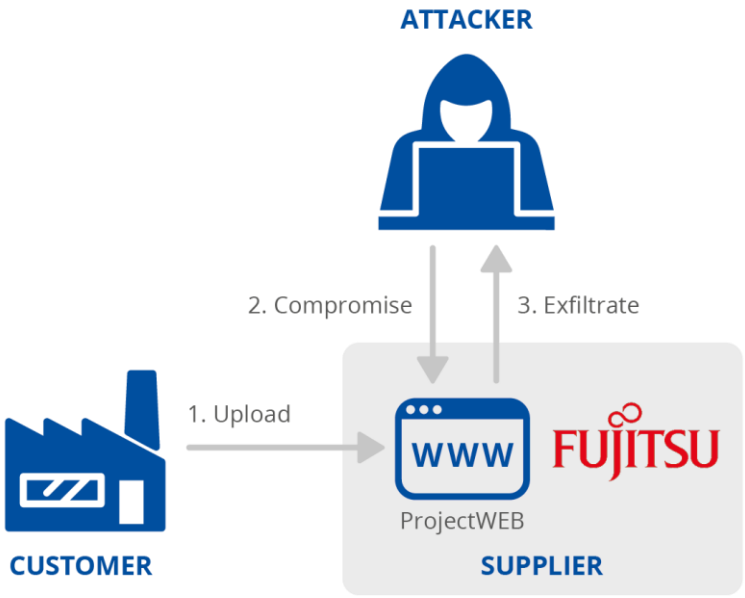
[116] Hardware Wallet, Ledger, https://www.ledger.com/. Accessed on 09/07/2021.
[117] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership | Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Accessed on 09/07/2021.
[118] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Accessed on 09/07/2021.
[119] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Accessed on 09/07/2021.
[120] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html. Accessed on 09/07/2021.
[121] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Accessed on 09/07/2021.

A.20 FUJITSU PROJECTWEB: COLLABORATION AND PROJECT MANAGEMENT SOFTWARE

Fujitsu ProjectWEB is a cloud-based software used by companies for online collaboration, software management, and file-sharing[122]. The tool is popular among Japan's government agencies. In May 2021, attackers gained access to Japanese government data[123] after exploiting weaknesses in ProjectWEB installations[122,124]. Due to the location of the compromised servers, Japanese Air Traffic Control data was also stolen in the attack[122,125]. The attack was not attributed.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code, Data

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Data



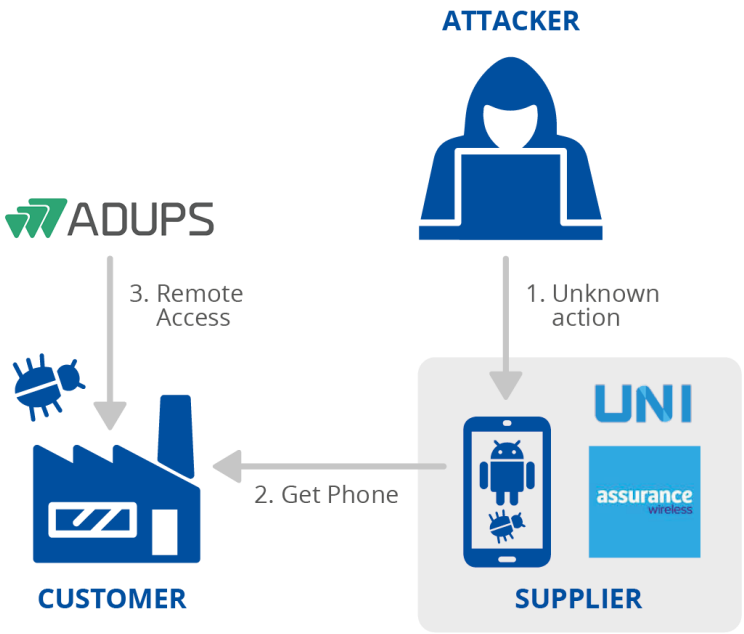
[122] Japanese government agencies suffered breaches after ProjectWEB hack, Teiss News, https://www.teiss.co.uk/japanese-government-agencies-suffered-breaches-following-fujitsus-projectweb-hack/. Accessed on 09/07/2021.
[123] Japanese government agencies suffer data breaches after Fujitsu hack, Bleeping Computer, https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/. Accessed on 09/07/2021.
[124] Data theft via Fujitsu ProjectWEB, INCIBE-CERT, https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/data-theft-fujitsu-projectweb. Accessed on 09/07/2021.
[125] Fujitsu pulls ProjectWEB tool offline after apparent supply chain attack sees Japanese infosec agency data stolen, The Register, https://www.theregister.com/2021/05/27/fujitsu_projectweb_supply_chain_attack/. Accessed on 09/07/2021.

A.21 UNIMAX COMMUNICATIONS MOBILE PHONES

Unimax, also known as UMX, supplies low-cost mobile devices. Customers for UMX phones included persons who receive their phones through the United States Government Lifeline Assistance Program[126]. In January 2020, researchers reported that the mobile devices came with unremovable pre-installed malware designed to spy on users[127,128]. It was not possible to remove the malware even with a hard-reset. Another mobile manufacturer which was discovered with the preloaded malware, Transsion, cast blame on an unidentified vendor along the supply chain[126]. The attack was not attributed[126].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199], Malware Infection	People



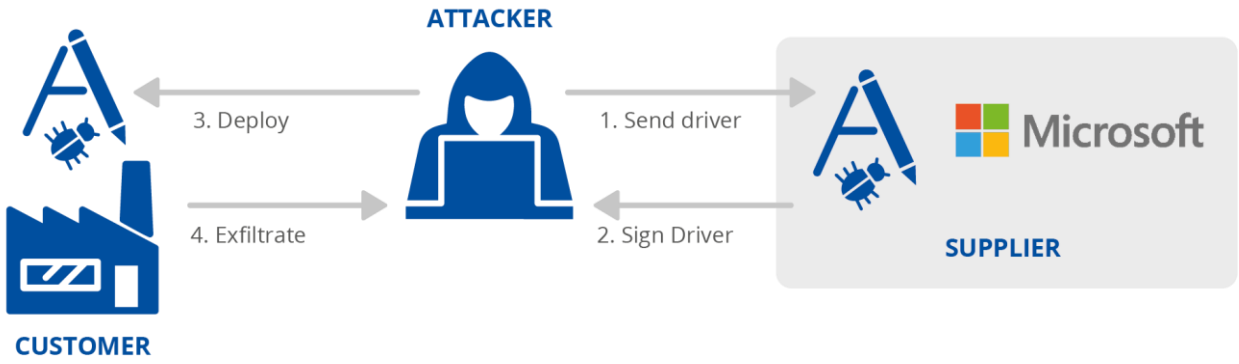
[126] Chinese Cell Phones Ship Preloaded with Malware, BlueVoyant, https://www.bluevoyant.com/blog/chinese-cell-phone-malware/. Accessed on 09/07/2021.
[127] UMX Phone: US-funded Gov Phones come pre-installed with malicious apps, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/. Accessed on 09/07/2021.
[128] We found yet another phone with pre-installed malware via the Lifeline Assistance program, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/07/we-found-yet-another-phone-with-pre-installed-malware-via-the-lifeline-assistance-program/. Accessed on 09/07/2021.

A.22 MICROSOFT WINDOWS HARDWARE COMPATIBILITY PROGRAM

In June 2021, it was disclosed that attackers abused the code signing processes Microsoft uses to validate third-party drivers to sneak and distribute a rootkit malware[129]. Through the valid signature, the malware could be installed in users' systems[130]. The attack appeared to be targeting the gaming sector in China[129]. The attack was not attributed.

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Social Engineering	Processes

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Data



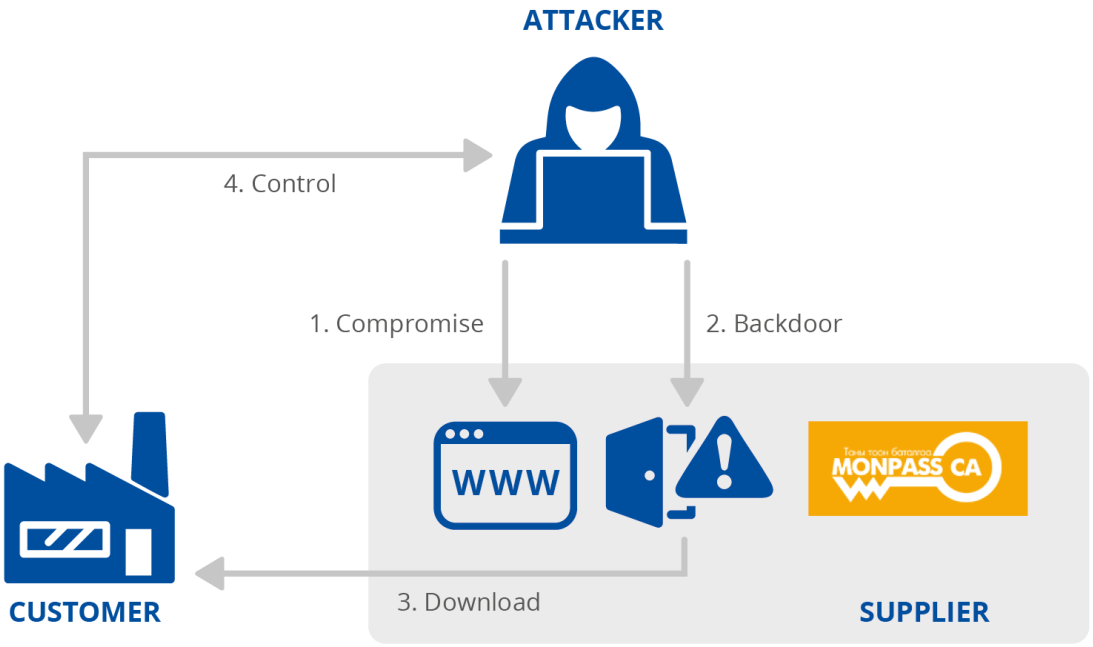
[129] Microsoft admits to signing rootkit malware in supply-chain fiasco, Bleeping Computer, https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/. Accessed on 09/07/2021.
[130] Microsoft signed a malicious Netfilter rootkit, G DATA, https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit. Accessed on 09/07/2021.

A.23 MONPASS CERTIFICATE AUTHORITY

MonPass is Mongolia's major certification authority. In February 2021, its website was compromised and at least one binary installer was backdoored with a Cobalt Strike binary[131]. The website was repeatedly compromised and several Webshells and backdoors were found[132]. The malicious code was downloaded by visitors to the MonPass website, which executed the malware upon download. At least one customer is known to have been infected and found by Avast Software[131].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Drive-by Compromise [T1189], Malware Infection	Unknown



[131] Backdoored Client from Mongolian CA MonPass, Avast Threat Labs, https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/. Accessed on 09/07/2021.

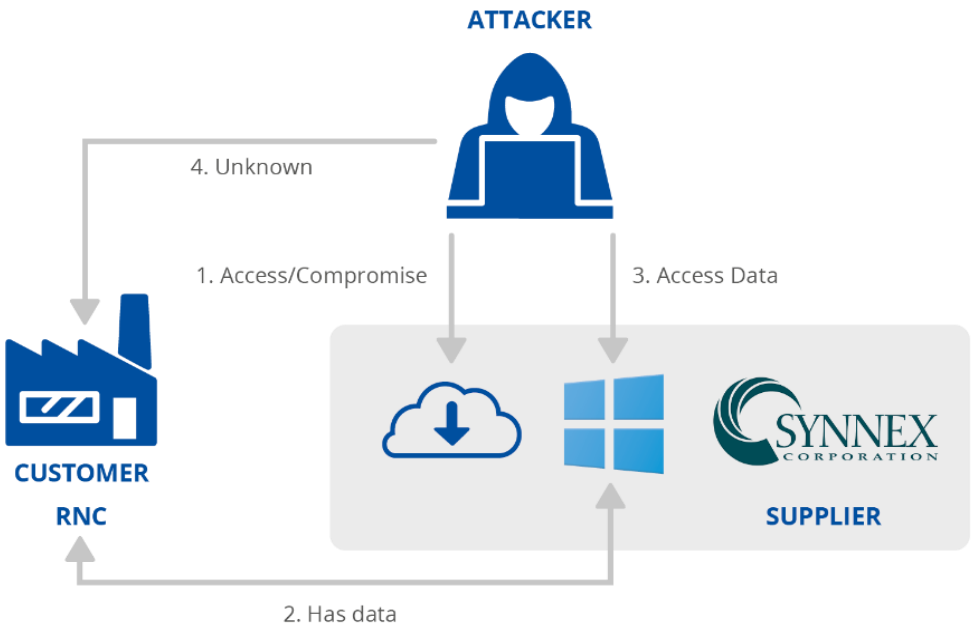
[132] Mongolian Certificate Authority Hacked to Distribute Backdoored CA Software, The Hacker News, https://thehackernews.com/2021/07/mongolian-certificate-authority-hacked.html. Accessed on 09/07/2021.

A.24 SYNNEX IT DESIGN-TO-DISTRIBUTION COMPANY

Synnex is a technology distributor and integrator. In July 2021 their systems were breached[133]. Synnex admitted that the attacks may have been in connection to the recent Kaseya MSP attacks[134]. The attackers used Synnex to access customer applications within the Microsoft cloud environment. These applications included the National Committee of the US Republican Party (RNC), which reported it had been breached through Synnex[135].

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability	Code

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Drive-by Compromise [T1189], Malware Infection	Unknown



[133] Mega-distie SYNNEX attacked and Microsoft cloud accounts it tends tampered, The Register, https://www.theregister.com/2021/07/07/synnex_rnc_microsoft_attack/. Accessed on 09/07/2021.

[134] SYNNEX Responds to Recent Cybersecurity Attacks and Media Mentions, SYNNEX Corporation, https://ir.synnex.com/news/press-release-details/2021/SYNNEX-Responds-to-Recent-Cybersecurity-Attacks-and-Media-Mentions/default.aspx. Accessed on 09/07/2021.

[135] Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit, The Washington Post, https://www.washingtonpost.com/business/on-small-business/russia-cozy-bear-breached-gop-as-ransomware-attack-hit/2021/07/06/3e9e200a-de9b-11eb-a27f-8b294930e95b_story.html. Accessed on 09/07/2021.

TP-05-21-171-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-509-8
DOI: 10.2824/168593