# Secure Software Engineering Assignment (SEZG566)

## *Threat Analysis -Supply Chain Attack*

MTech. Software Systems

WILP

BITS, Pilani

Submitted By:


| | |
|---|---|
| **SAQUIB** | 2021MT12266@wilp.bits-pilani.ac.in |

# INDEX

# Introduction

A supply chain (SC) is a collection of different organizations that align their business processes, goals, objectives, and some components of their systems to third party organizations, suppliers, consumers, and partners. When someone gains access to the system through an external partner or supplier with access to the systems and data, it is known as a supply chain attack, value-chain attack, or third-party attack. With more suppliers and service providers touching sensitive data than ever before, this has significantly altered the attack surface of the typical organization during the past few years.

As a weak link in the supply chain might provide hackers access to the bigger organization holding the desired data, the supply chain network is a common target for cybercrimes. Attacks on a supply chain reveal a problem with the supply network of a corporation and reveal that the cyber security measures of an organization are only as strong as the weakest link in the chain. Due to new attack methods, increasing public awareness of the risks, and increased regulatory monitoring, the risks connected with a supply chain attack are higher than they have ever been. A perfect storm is being created by the fact that attackers have access to more resources and equipment than ever before. Examples include the Saudi Aramco electric-grid cyber-attack in 2017, and the Ukraine power grid attack in 2015.These indicate that supply chain attacks are on the rise and require an attack model and threat analysis to gather threat intelligence.

# Software Supply Chain Problem

As outsourcing and expanded use of commercial off-the-shelf (COTS) and open-source software products increase and as end users exploit opportunities to reconfigure or make limited additions to deployed products and systems, supply chain security risk becomes a growing concern. Software is rarely defect-free, and many common defects2 can be readily exploited by unauthorized parties to alter the security properties and functionality of the software for malicious intent. Such defects can be accidentally or intentionally inserted into the software at any point in its development or use, and subsequent acquirers and users have limited ways of finding and correcting these defects to avoid exploitation. Participation in the software supply chain is global, and knowledge of who has touched each specific product or service may not be visible to others in the chain. Typically, an acquirer such as a ecommerce owner or Health care product supply organization will only know about the participants directly connected to it in the supply chain and will have little insight into its suppliers' suppliers, each of these indirect suppliers can insert defects for future exploitation.

Supply chain security risks must be addressed in every phase of the acquisition life cycle: initiation, development, configuration/deployment, operations/maintenance, and disposal. The view of the supply chain in applies primarily to the initiation and development phases of the acquisition life cycle. A somewhat different picture applies to the operations/maintenance phase, where software supply chain security risk occurs through the delivery of sustainment upgrades and configuration changes. In addition, coding and

design defects newly identified and reported as vulnerabilities may require patches and special security monitoring to prevent compromise, and these patches are delivered by various suppliers

# Assets of Supply Chain Attack

***The term "supply chain" describes the entire ecosystem of activities, individuals, groups, and distributors involved in developing and distributing a finished good or service. The supply chain for cybersecurity includes a variety of resources (hardware and software), storage (local or in the cloud), distribution channels (web apps, online shops), and management tools.***

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.

# Supply Chain Attack Surface

One of the recent research states that attacks on Windows systems typically exploited open ports, services running by default, and services running with system-level privileges dynamically generated web pages enabled accounts, including those in administrative groups enabled guest accounts, weak access controls

Concentrate on the features that were most likely to be exploited. These features compose the system's *attack surface*. A system with a greater number of exploitable features has a larger attack surface and is at greater risk of exploitation. Howard's initially intuitive description of an attack surface led to a more formal definition with the following dimensions.

- targets: data resources or processes desired by attackers (a target could be a web browser, web server, firewall, mail client, database server, etc.)
- enablers: processes and data resources used by attackers to reach a target (e.g., web services, a mail client, XML, JavaScript, or ActiveX10)
- channels and protocols (inputs and outputs): used by attackers to obtain control over targets
- access rights: constraints intended to limit the set of actions that can be taken with respect to data items or functionality

# Threat Analysis of Supply Chain Attack

Supply chain attacks work by delivering viruses or other malicious software via a supplier or vendor. For example, a keylogger placed on a USB drive can make its way into a large retail company, which then logs keystrokes to determine passwords to specific accounts. Cybercriminals can then gain access to sensitive company information, customer records, payment information etc.

**Supply chain attack from supplier perspective**:
*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*

**Supply chain attack from the customer perspective.**
*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.*

**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. |

**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. |

## ATTACK TECHNIQUES USED TO COMPROMISE A CUSTOMER

| | |
|---|---|
| **Trusted Relationship** | e.g. trust a certificate, trust an automatic update, trust an automatic backup. |
| **Drive-by Compromise** | e.g. malicious scripts in a website to infect users with malware. |
| **Phishing** | 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. |

## 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 |

Supply chain attacks come in many forms including People, software, hardware, and firmware attacks, some of them explained in detail.

**Software Supply Chain Attack**

A software supply chain attack only requires one compromised application or piece of software to deliver malware across the entire supply chain. Attacks will often target an application's source code, delivering malicious code into a trusted app or software system.
Attackers often target software or application updates as entry points. The problem with software supply chain attacks is that they're so difficult to trace, with cybercriminals often using stolen certificates to "sign" the code to make it look legitimate.'

**Firmware Supply Chain Attack**

Inserting malware into a computer's booting code is an attack that only takes a second to unfold. Once a computer boots up, the malware is executed, jeopardizing the entire system. Firmware attacks are quick, often undetectable if you're not looking for them and incredibly damaging.

**Hardware Supply Chain Attack**

Hardware attacks depend on physical devices, much like the USB keylogger we mentioned earlier. Attackers will target a device that makes its way through the entire supply chain to maximize its reach and damage.

# Supply Chain Attack and Framework consideration

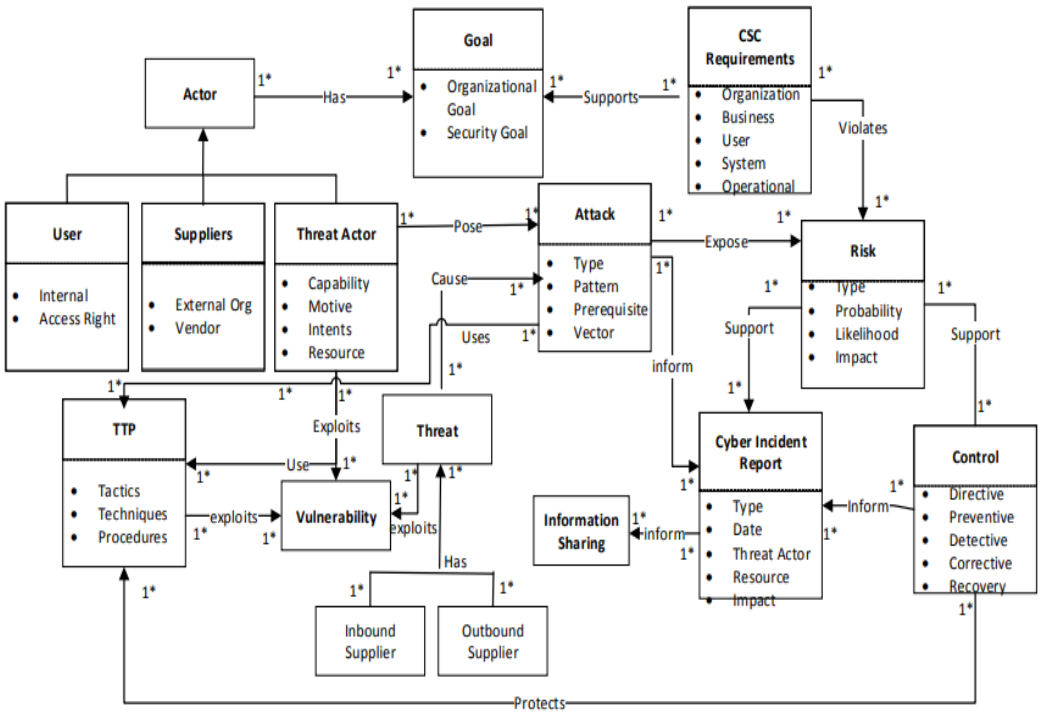
**MITRE ATT&CK**

MITRE ATT&CK 'Initial Access' category, there is a technique called 'Supply Chain Compromise'. 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

**Lockheed Martin Cyber Kill Chain® Framework**

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. We 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.

# Supply Chain Threat Model




**Threat Modelling for Supply Chain Process**

**Actor**: An actor describes an entity that has goals and intentions within the system or within the organizational setting. The actors are the employees, suppliers, and distributors, as well as those with the potential to cause a threat to the supply chain system (which could be different from the threat actor). Legitimate actors or system users are categorized as organization employees, or users with permission to access or use the supply chain system
Actors can be recognized either by their password, process, identity, or privileges. Suppliers are the various organizations on the supply chain system, including distributors, third party vendors, and suppliers

**Vulnerability**: vulnerabilities are flaws or weakness that can be exploited by a threat actor or a threat agent. In an SC system, a vulnerable can be identified from various sources, including the software, network, website, user, process, application, and configuration, or from a third-party vendor

**Attack**: An attack is any deliberate action or assault on the supply chain system with intent to compromise its processes, procedures, and delivery of electronic products, information flows, and services. A supply chain compromise attack is the manipulation of product delivery mechanisms prior to receipt by final consumer.

**Tactics, Techniques, and Procedures (TTP**) is a representation of the behaviour or modes of operations of the adversary or threat actor . TTP leverages specific adversary capabilities, behaviours, and exploits it can use on victims. TTP could be used to gather cyber threat information about the attack pattern, resources deployed, and exploits exhibited

• **Tactics** describe how threat actors operate during the various attack campaigns. This includes how the adversary carries out reconnaissance for initial intelligence gathering, how the information is gathered, and how the initial compromises were conducted. For instance, tactics may be to send a spear phishing email to a group on the supply chain.
• **Techniques** are the strategies used by the adversary to facilitate the initial compromises such as tools, skills, and capabilities deployed. This includes how the adversary establishes control, manoeuvres within the supply chain system infrastructures, and exfiltrates data, as well as how to obfuscate through the system. The adversary conceals the email contents in such a way that is not obvious to detect.
• **Procedures** are the set of tactics and techniques put together to perform an attack. Procedures may vary depending on the threat actor goal, purpose, and nature of the attack. A procedure includes carrying out reconnaissance on the victim's systems to identify vulnerable spots, gather information, access rights, and control mechanisms to determine what could be exploited.

**Inbound and outbound supply threats**: The inbound and outbound supply chains are the organizational systems that integrate with third party companies, suppliers, and distributors to achieve the organizational goal. The inbound suppliers include the external organization and third-party vendors who have remote access to the Supply chain system and who provide electric power transmissions.

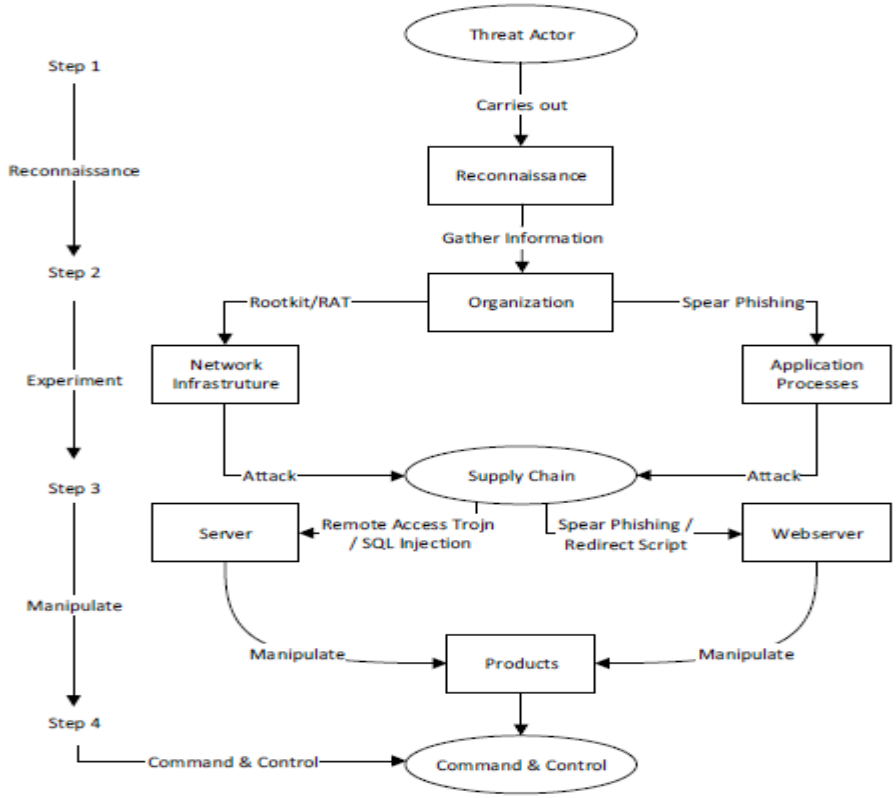
**Risks**: Risk is the potential negative impact from an attack. The probabilities of attacks being initiated from the vendor systems are high, as they represent a single point of failure. Supply chain risk is the potential for an adversary to sabotage the supply chain, maliciously introduce unwanted functions, or subvert the design, product, or integrity of the system.

**Controls** are security strategies and measures that are formulated and implemented to ensure that the organizational goal and objectives are achieved, and that risks are mitigated with minimal threat or no threat at all. CSC security controls are managerial, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the systems and their information

**Cyber incident reports**: Incident report systems provide CSC attack victims the platform to report attacks and threats that have occurred, including their impact and the degree of severity. The purpose is to gather and analyse threat information that can assist organizations and stakeholders to achieve their security goals

**Threat information sharing**: Cyber threat information sharing is a platform that provides the information necessary to assist an organization in identifying, assessing, monitoring, and responding to cyber threats.

# Kill Chain Supply Chain Attack




**Step 1. Reconnaissance:** The adversary carries out research online and uses other social engineering methods to gather information such as:
_ What infrastructure is the organization using: topology, IPs, software, or configurations.
_ Profile of the organization, business applications, third party vendors, and other organizations.
_ Is the supply chain a corporate and public network system (e.g., virtual private network VPN);
_ What type of attack can be initiated (e.g., malware, redirect script, injection, and phishing)? For instance, the adversary could use passive attack tools such as Nmap or Kali Linux.
**Step 2. Experiment:** The adversary uses various attack methods (TTP) and tools to penetrate and gain control of the victim's systems to try and explore vulnerable spots. For instance:
_ The adversary creates an executable malware remotely.
_ The adversary inserts a remote access Trojan (RAT), and the malware is installed and executed when a user downloads or opens it through a spear phishing email
**Step 3. Exploit:** At this stage, the threat actor gains control of the systems and determines the attack goal. The threat actor penetrates the workstations of the internal users, gains access into the system resources and the supply chain environment and manipulates the organization's products.
**Step 4. Command and control:** The adversary use remote access and Advance Persistent Threat (APT) techniques to establish control of the Supply chain system, at which point they can monitor business processes and activities, and to manipulate the system, exfiltrate information, and obfuscate.

**Mapping of Supply chain System with the threat modelling process**

| Concept | Properties | Description |
|---|---|---|
| **Goal** | Organization goal | Distribute the Order, goods to the customers<br>Provide partner remote access to the company portal.<br>Enable Payment Transactions<br>Receive Payments |
| | Security Goal | |
| **Actor** | User<br>Supplier | Employees internal, external<br>Supplier<br>Distributors |
| | Threat Actor | A person, user account, or processes that can be identified by the intent, motives, and capabilities of an attacker |
| **Requirements** | Organizational requirement, user categories, ID, stakeholders, description, acceptance criteria | Specify high level organizational environment overall and integrate with the security constraints to achieve the organizational goal |
| **Supply Chain Systems** | Inbound | Organizations Financial institutions Third party vendors Individual consumers Services providers |
| | Outbound | Organizations Stakeholders Manufacturers, Distributers Packaging and Shipping goods |
| **Vulnerabilities** | Router, firewall, wifi Remote services: remote login, remote command execution CSC Source and destination, Timestamp, Dynamic, host configuration protocol, (DHCP) server logs | Domain name, TCP/UDP port number, media, MAC address IP Address |
| **Attack** | Attack goal Compromise system of:<br>Attack pattern Malware, spyware, injection Attack prerequisites Information on vulnerabilities<br>Attack vectors | Compromise system of: Attack pattern Malware, spyware, injection Attack prerequisites Information on vulnerabilities Attack vectors |
| **Threats** | Indicators | Determines vulnerabilities, flaws, and loopholes that can be exploited by a threat actor Adversary behaviors Risky events State of an incident |

## Analysis of Supply Chain Control Parameters

| No | Control | Principle | Critical | Security Purpose | Implement | Activity |
|---|---|---|---|---|---|---|
| 1 | Inventory and Control of Hardware Assets | Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access. | Network, laptops, (BYOD) might be out of synch with security updates or might already be compromised. | Attackers can take advantage of hardware installed but not configured and patched with security updates until later. | Utilize active discovery tool to identify devices connected to network and update the hardware asset inventory. | Maintain up-to-date inventory of stored assets or process information and hardware, whether connected to network or not. |
| 2 | Inventory and Control of Software Assets | Manage CSC network so that only authorized software is installed. Unauthorized software is found and prevented from installation or execution. | Attackers scan targets sites with vulnerable software that can be remotely exploited and distribute hostile web pages or to third-party sites. | Managing and control of all software plays a critical role in planning, backup, incident response, and recovery. | Utilize inventory tools throughout to automate the documentation of all software on business systems. | Utilize application whitelisting technology on all assets to ensure that only authorized software executes. |
| 3 | Continuous Vulnerability Management | Continuously assess and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attacks. | Understanding and managing vulnerabilities must become a continuous activity, requiring significant time, attention, and resources. | Threat actors try to exploit vulnerabilities and attack victim's systems before the organization becomes aware. Due to lack of CSC risk assessment. | Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. | Utilize an up-to-date compliant vulnerability scanning tool to automatically scan all systems to identify potential vulnerabilities, Deploy automated security updates. |
| 4 | Controlled use of Admin Privileges | Not changing hard-coded password default. Impacts on the processes and tools used to track, control, and prevent the correct use, assignment, and configuration of administrative privileges. | Misuse of admin privileges is a primary method for attacks to spread inside a target system. | A privileged user can open a malicious email attachment or website hosting exploited browsers. Second guessing password for an administrative user. | Change default hard-coded password. Ensure all users with administrative account access use a dedicated or secondary account for elevated activities. | Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. |
| 5 | Secure Configuration for Hardware and Software on Mobile Device Laptop and Servers | Implement and manage (track, report, correct) security configuration of assets by using configuration management and change control process. | Developing configuration settings with good security properties is complex. It requires system analysis. | Implement regular security updates on configuration. Ensure vulnerabilities are reported and update to support new operational requirements. | Maintain documented, standard security configuration standards for all authorized operating systems and software. | Utilize Security Content Automation Protocol compliant configuration monitoring system. Verify security configuration. Catalog approved exceptions and alerts in the event of unauthorized changes |
| 6 | Maintenance, Monitoring, and Analysis of Audit Logs | Collect and analyze audit logs of events that could help detect, or recover from an attack. | Deficiencies in loggings and analysis allow attacker to hide location and activities. | Keep logging records for audit and compliance purposes. Attackers hide their trails nowadays. | Ensure that local logging has been enabled on all systems and networking devices. | Ensure that appropriate logs are being aggregated to a central log management system for analysis and review. |

# Analysis of Threat Modelling

Threat modeling and analysis looks at the various instances of how threat actors pursuing an intent and exploit it, such as an adversary's motives, opportunities, and the methods deployed by the threat actor. We analyzed the pattern of behaviors as observed through sets of incidents and the TTP used across the organization's supply chain with third parties. We characterized threat actor activities, including presumed intent and historically observed behavior, for the purpose of ascertaining the current threats that could be exploited. The intelligence gathered provides us with an understanding of the adversaries' capabilities, actions, and intents of the organizational supply chain domain. We asking the following questions as we look to investigate further attacks for our analyses and threat intelligence gatherings:

- What attacks have occurred before (malware, SQL injection, session hijacking, XSS)
- How did they occur (causes of action and intrusion sets)
- Who are the threat actors (internal and external staff, adversaries, and threat actors)
- What are the likely occurrences (risk assessments, indicators)
- How can they be detected (penetration tests, vulnerability assessments, threat modeling)
- How can they be mitigated (risk management, controls, policies, regular updates, insurance, and awareness)

# Software Supply Chain Security Risk

Major concern in today's highly interconnected software environment is the risk that an unauthorized party would change a product or system in ways that adversely affect its security properties.
These software security risks are introduced into the supply chain in several ways:

- poor security requirements that lead to ineffective security considerations in all acquisition steps.
- coding and design defects incorporated during development that allow the introduction of code by unauthorized parties when the product or system is fielded. In addition, there are those defects that compromise security directly by allowing unauthorized access and execution of protected functionality.
- improper control of access to a product or system when it is transferred between organizations (failures in logistics), allowing the introduction of code by unauthorized parties.
- insecure deployed configuration (e.g., a deployed configuration that uses default passwords).
- operational changes in the use of the fielded product or system that introduce security risks or configuration changes that allow security compromises (configuration control and patch management).
- mishandling of information during product or system disposal that compromises the security of current operations and future products or systems

Software supply chain security risk exists at any point where organizations have direct or indirect access to the final product or system through their contributions as a supplier. Suppliers include distributors, transporters, and storage facilities, as well as organizations directly responsible for creating, enhancing, or changing product or system content. Without mitigation, these risks are inherited from each layer in the supply chain, increasing the likelihood of a security compromise. Reduction of supply chain security risk requires paying attention to all of the following within the acquisition life cycle:

**acquirer capabilities:** policies and practices for defining the required security properties of a particular product or system (not addressed in this initial version)
**supplier capability:** ensuring that a supplier has good security development and management practices in place throughout the life cycle
**product security:** assessing a completed product's potential for security compromises and determining critical risk mitigation requirements
**product logistics:** the methods for delivering the product to its user and determining how these methods guard against the introduction of malware while in transit
**operational product control:** ensuring that configuration and monitoring controls remain active as the product and its use evolve over time
**disposal:** ensuring software data and modules are effectively purged from hardware, locations, libraries, etc. when removal is needed (not covered in this initial version)

Addressing these risks impacts each phase in the acquisition life cycle and becomes a shared responsibility of the program office, each supplier, and operations management. Both the security of the supply chain and the security of the resulting product or system need to be considered. For each acquisition life-cycle phase, Fig identifies key activities that are needed in order to focus

the proper attention on software supply chain security risk.

| Acquisition Phase | Key Activities for Managing Software Supply Chain Security Risks |
|---|---|
| Initiation | Perform an initial software supply chain security risk assessment and establish required security properties.<br>Include supply chain security risk management as part of the RFP.<br>Develop plans for monitoring suppliers.<br>Select suppliers that address supply chain security risk. |
| Development | Monitor practices for supply chain security risk management.<br>Maintain awareness of supplier's sub tier relationships. |
| Configuration/Deployment | Assess delivered products/systems.<br>Configure/integrate with consideration of supply chain security risks.<br>Develop user guidance to help mitigate supply chain security risk. |
| Operations/Maintenance | Manage security incidents.<br>Review operational readiness.<br>Monitor component/supplier. |
| Disposal | Mitigate risks of information disclosure during disposal. |

*Acquisition Life-Cycle Phases and Corresponding Supply Chain Security Risk Management Activities*

The threat should be access in the initial phases to reduces supply chain security risk in several ways:

- A system with more targets, more enablers, more channels, or more generous access rights provides more opportunities to the attacker. An acquisition process designed to mitigate supply chain security risks should include requirements for a reduced and documented attack surface.
- The use of product features influences the attack surface for that acquirer. The attack surface can define the opportunities for attacks when usage changes.
- Attack surface analysis helps to focus attention on the code that is of greatest concern for security risk. If the code is well- partitioned so that features are isolated, reducing the attack surface can also reduce the code that has to be evaluated for threats and vulnerabilities. For each element of a documented attack surface, known weaknesses and attack patterns can be used to mitigate the risks.
- The attack surface supports deployment, as it helps to identify the attack opportunities that could require additional mitigation beyond that provided by the product.

# *Recent Case Study related to Supply Chain Attack*

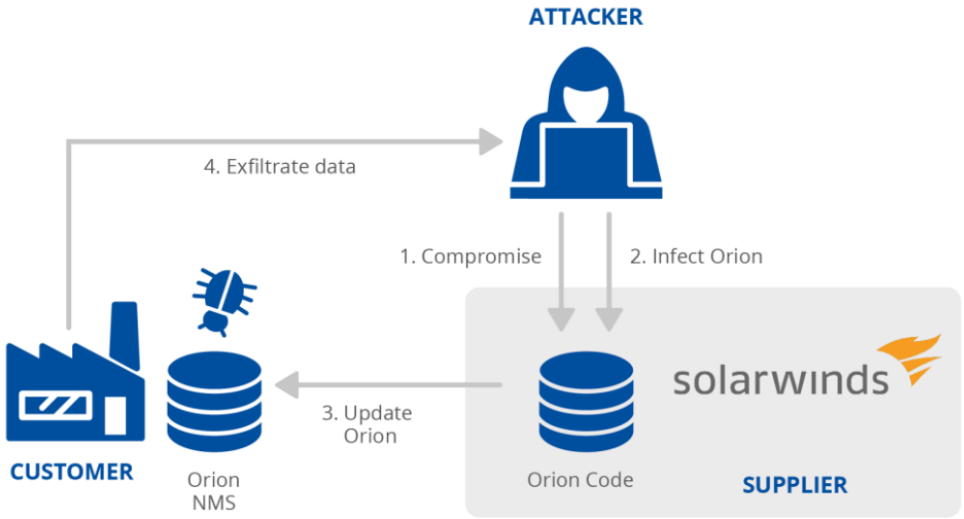
**SOLARWINDS ORION: IT MANAGEMENT AND REMOTE MONITORING**

SolarWinds is a company that supplies management and monitoring software16. Orion is SolarWinds' network management system (NMS) product17. 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 process18,19. The compromised software was then downloaded directly by the customers and was used to gather and steal information20. The attack was attributed to the APT29 group

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 Malware Infection | Data |

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



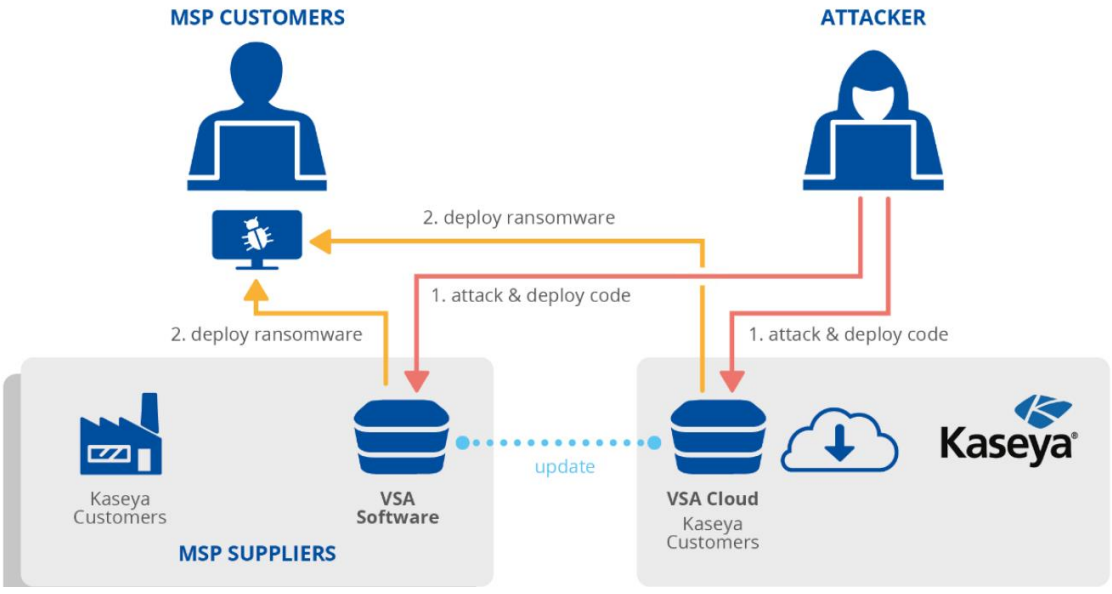
## KASEYA: IT MANAGEMENT SERVICES COMPROMISED WITH RANSOMWARE

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 clients31. In July 2021, attackers exploited a zero-day vulnerability in Kaseya's own systems (CVE-2021-3011632) 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 ransomware33,34 to the customers being managed by that VSA.

Supply chain attack taxonomy applied to the attack involving Kaseya. By exploiting 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<br>Malware Infection | Data, Financial |

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



# 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.

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 consider 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,
- 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. Suppliers should:

- ensure that the infrastructure used to design, develop, manufacture, and deliver products, components and services follows cybersecurity practices.
- 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.
- consider applicability of technical requirements based on product category and risks.
- 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**, 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. CVSS56),
- 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:

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

## Some recommended Prevention Steps:

Ask software supplier/vendor (or check the vendor's website) whether the supplier:

- Uses a software development lifecycle incorporating secure software development
- Looks for known weaknesses and development practices vulnerabilities in their source code and compiled code and demonstrates the degree of rigor they apply. This may include requiring a specified level of developer testing and evaluation (e.g., static code analysis, threat modelling and vulnerability analysis, third-party verification of processes, manual code review, penetration testing, 15 dynamic code analysis, etc.).
- Actively identifies and discloses vulnerabilities while maintaining a vulnerability response program
- Enables patch management capabilities
- Develops, maintains, and uses approved supplier lists for its products

Request a software component inventory with each contemplated software purchase Actively identifies and discloses vulnerabilities.

- If a vendor cannot provide a component inventory, consider using that as a differentiator when selecting among competing products
- Post-purchase, incorporate that in the software inventory
- Participates in Common Vulnerabilities and Exposures (CVE) generation, including whether the supplier participates as a CVE Numbering Authority (CNA).
- Develops, maintains, and uses approved supplier lists for its products and services.

## Some recommended Mitigation Steps:

1. Implement a documented vulnerability management program
    - Using instructions from the vendor, configure software to automatically check for and install patches
    - • Register software licenses with the vendor, including contact information, so that vulnerabilities and mitigation strategies can be communicated
    - Follow vendor instructions to harden software, operating systems, and firmware

2. If vendor specifies URLs or IP ranges and ports to and from which software should communicate, consider establishing firewall rules to ensure such communications do not occur outside of those parameters

3. Where feasible, apply basic network segmentation to isolate different parts of the enterprise (e.g., maintain a separate network for guest users, separate the networks used by different functional areas of the organization, etc.)

4. Monitor endpoints and/or servers for unexplained deviations from your software inventory; remove or isolate unauthorized software

5. Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification.