VERSA NETWORKS

WHITE PAPER

How Adopting A Zero Trust Architecture Can Help Protect Against Digital Supply Chain Management Attacks

Introduction

Supply Chain Attack is "A cyber-attack that seeks to damage an organization by targeting less secure elements in the supply chain."

Supply Chain attacks can occur across any industry vertical that relies on 3rd party products to manufacture the final product that is delivered to its end customers. However, with the increase in digitization and digital transformation, IT Software/Services are one of the most popular targets for attackers. This type of supply chain attacks is also referred to as Digital Supply chain attacks and this article will exclusively focus on Digital Supply Chain Attacks.

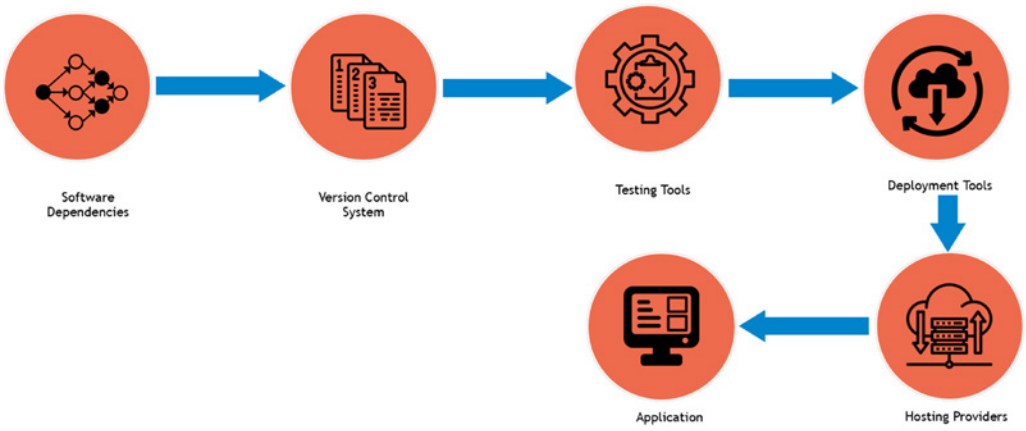
Digital Supply Chain Attacks – Deep Dive

A digital supply chain attack commonly referred to as a value-chain or a third-party attack, occurs when an attacker accesses an organization's network by infiltrating a supplier or business partner that has access to its data.

A Digital Supply Chain attack will typically target either the source code, update mechanisms, the CI/CD system, or the build process of the vendor's software with the eventual aim of gaining uninhibited access to the vendor's ecosystem. Below are various types of supply chain attacks:

- Compromised software building tools like Website Builder tools, 3rd party open-source libraries or software update infrastructure.
- Stolen code, stolen keys/certificates or signed malicious apps using the identity of the development company.
- Compromised code shipped in hardware or firmware components.
- Pre-installed malware on devices (cameras, USB, phones, etc.)

A typical digital supply chain is illustrated in the figure below:



A digital supply chain attack will broadly consist of the following steps:

a) Reconnaissance – This process will involve the attackers studying the code of the targeted vendor, the composition of the vendors' software, and the possible organizations that may be using the vendors' software in their ecosystem.

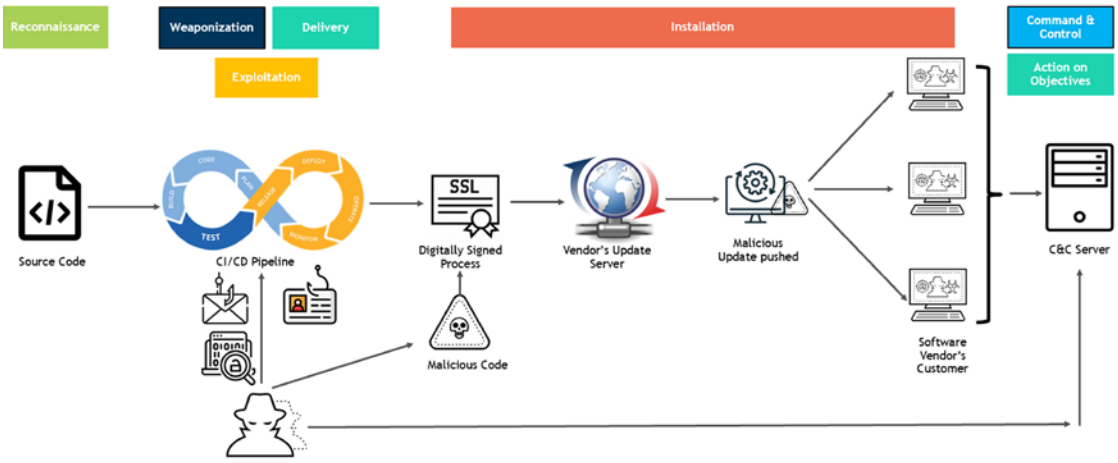
b) Initial Compromise (Infect the CI/CD Pipeline) – Most software vendors today will have a Continuous Integration/ Continuous Delivery (CI/CD) pipeline to build, test, and deploy the production releases of their software. The attackers through initial compromise will attempt to infect the CI/CD pipeline to insert the malicious code.

c) Insert the malicious code in a digitally signed process – Once the attacker has access to the CI/CD pipeline they will identify a digitally signed process in which they can insert the malicious code. Since the digitally signed process will be trusted by the software vendor and will be used to communicate with the existing installations of the software vendor's products, this will allow the malicious code to pass undetected into the victim's network.

d) Push the Malicious code through the Vendors Software update process – The malicious code will then typically be pushed to the vendors customers as a part of the regular software update by piggybacking on the digitally signed process.

e) Gain Initial Access to the Vendors Customer Network – Once the malicious code has been downloaded to the vendors software and installed in the customer's premises, the malicious code will execute to perform further actions including installing a backdoor and communicating with the Command and Control (C&C) server.

The below diagram illustrates the various steps in a digital supply chain management attack and the mapping of these steps to "The CyberKill Chain ".



A Brief Anatomy of the most famous Digital Supply Chain Attack in recent history

SolarWinds Attack – One of the most famous Digital Supply chain management attacks in the recent past was the SolarWinds attack. Here attackers were able to insert malicious code into an Orion Platform plugin called "SolarWinds.Orion.Core.BusinessLayer.dll" which was distributed to SolarWinds Customers as a part of the Orion platform updates. The attacker

chose the file since it was digitally signed, and the malicious code contained a backdoor that communicated with 3rd party servers controlled by the attackers. This component was nicknamed Sunburst.

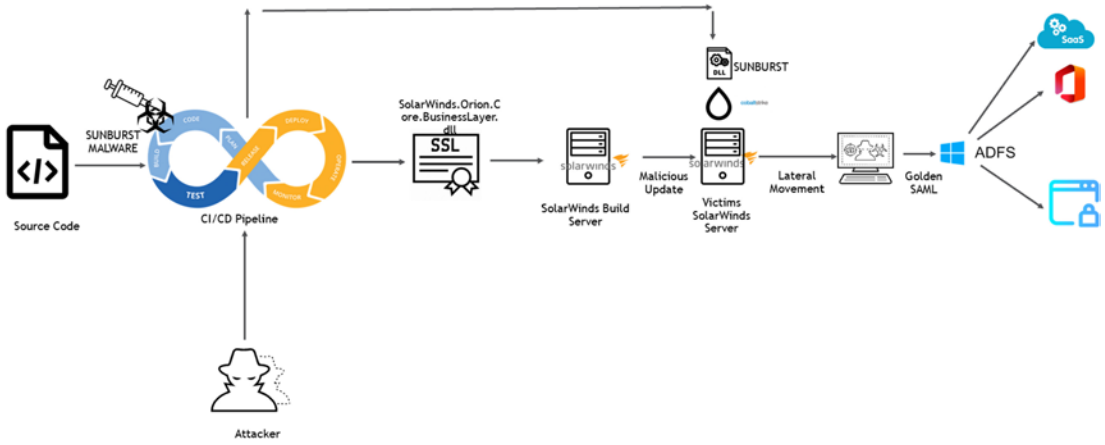
After an initial dormant period, which could last up to 2 weeks, the malware would start to retrieve and execute commands including the ability to transfer files, execute files, profile the system, and disable system services. The malicious code was also used to install a lightweight malware dropper which was referred to as Teardrop. The dropper would load directly in memory and would be used to deploy a customized version of Cobalt Strike Beacon which is a commercially off the shelf penetration testing tool.

Once the Cobalt Strike beacon package was installed on the compromised host, it allowed the attackers to move on the next stages of their attack including hands on keyboard access , spreading laterally from the compromised SolarWinds hosts to gain access to domain admin credentials to move to the ADFS server and steal the SAML signing certificate .

This allowed the attackers to execute the “Golden SAML attack” which enables attackers to forge SAML responses and bypass ADFS authentication to access federated services. This allowed them to gain access to any application using SAML authentication and more specifically o365 access to gain access to confidential data. The initial compromise was traced back to March 2020. Since the attack was discovered in December 2020, the malicious update had been pushed to literally thousands of SolarWinds customers including 9 US Federal agencies, and 100’s of private enterprises.

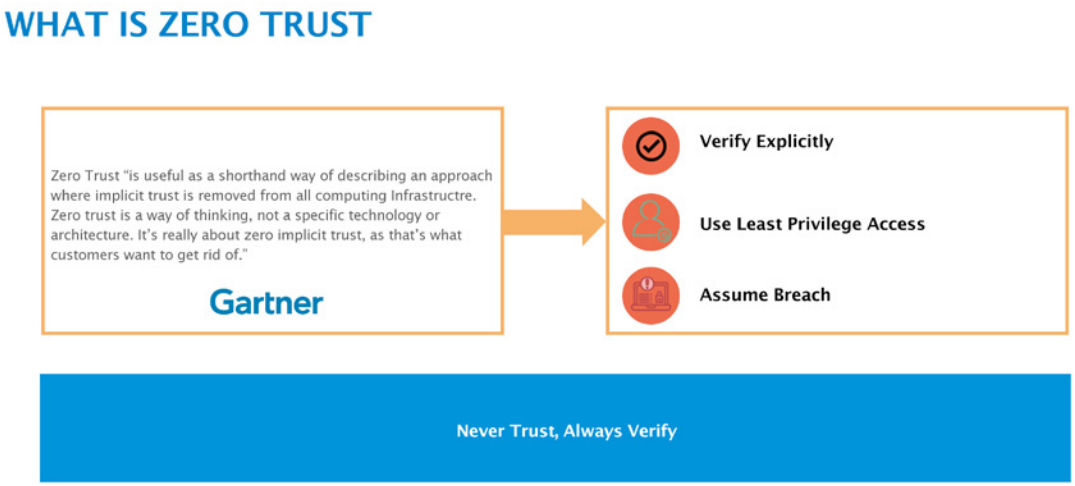
The below diagram illustrates the SolarWinds Supply Chain Attack.

SOLARWINDS SUPPLY CHAIN ATTACK



What is Zero Trust and How Migrating to a Zero Trust Architecture can help protect against Supply Chain Attacks?

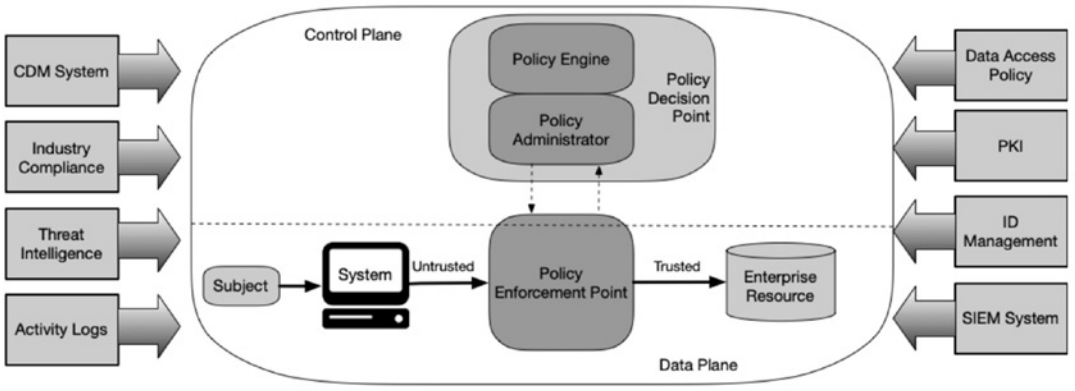
Zero trust systematically replaces implicit trust with calculated adaptive explicit trust based on identity and context. Zero trust is an idea that allows one to pragmatically approach security architecture without being related to a specific technology/vendor or architecture.



What is Zero Trust Architecture

Zero Trust architecture as defined by NIST SP 800-207 is an enterprise's cybersecurity plan that utilizes zero trust concepts as outlined in the previous section and encompasses component relationships, workflow planning, and access policies.

The Zero Trust architecture as per NIST SP 800-207 has been logically defined as per the diagram below:



Where in the core components to implement a Zero Trust Architecture are

a) Policy Engine – Responsible for making the final decision to grant access to a resource for a given subject.

b) Policy Administrator (PDP) – Responsible for establishing a communication path between a subject and a resource.

c) Policy Enforcement Point (PEP) – Responsible for enabling, monitoring, and terminating connections between a subject and an enterprise resource.

Zero Trust architecture (ZTA) utilizes PDP and PEP, for making policy decisions, and enforcing policy actions respectively, to provide contextual, risk-based and least privilege access to applications. It creates an identity- and context-based, logical access boundary around an application or set of applications. In ZTA, applications are hidden from discovery, and access is restricted to a collection of named entities only. This minimizes lateral movement elsewhere in the network. It adaptively offers the appropriate trust-based access using identity and other attributes such as time, geolocation, device posture, user confidence level, historical behavior patterns and threat intelligence. It results in a more resilient environment, with improved flexibility and better monitoring.

How can adopting a Zero Trust Architecture help protect against Digital Supply Chain Management attacks?

Any enterprise implementing /adopting a Zero Trust architecture will be able to protect against Digital Supply chain management attack in the following ways:

a) Continuous Verification – By continuously verifying the access for all resources, a Zero Trust Architecture ensures that no access is allowed based on implicit trust and the access to the resource can be revoked immediately if the associated risk level of the subject or the resource changes at any given point in time.

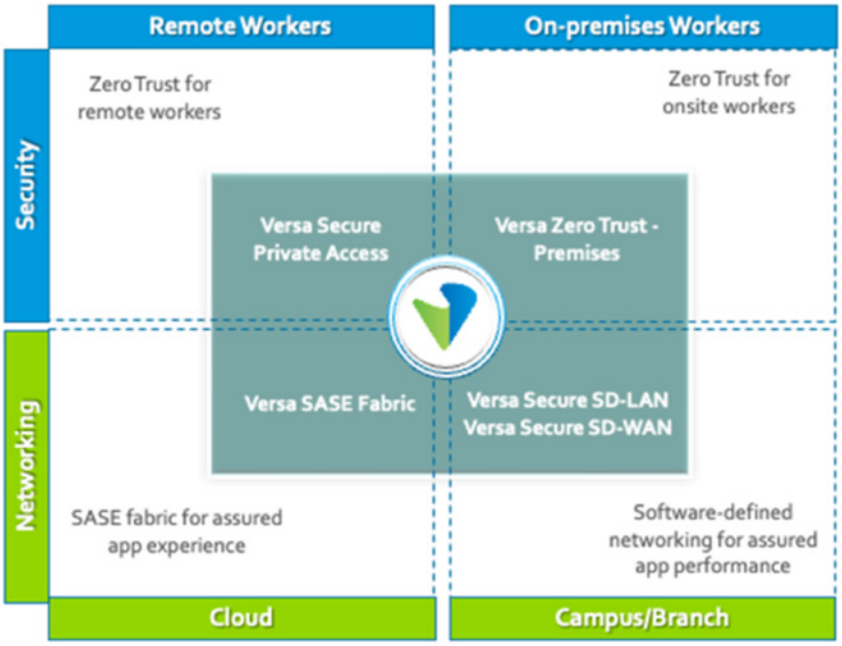
b) Limiting the Blast Radius/Preventing Lateral movement - A Zero Trust Architecture will ensure that in the event a vulnerability is exploited, the impact is localized to that specific resource only and doesn't propagate to the other parts of the system. By applying principles of Micro-Segmentation and Least Privilege, organizations can ensure that the impact of the breach is localized to the initial impacted resource/asset.

c) Continuous Monitoring and Automated Response – By continuously monitoring the access to enterprise resources and the users accessing these resources, a Zero Trust Architecture can identify any anomalous behavior pertaining to either the subject or the resource and take automated pre-defined steps to mitigate the same. This ensures that any change in behavior or the risk profile of either the subject or the resource can be identified and acted upon in real time.

Versa Zero Trust Everywhere

Versa Zero Trust Everywhere ™ is the industry's first solution delivering Zero Trust security for both remote and on-premises users, with optimized user-to-application performance. Versa Zero Trust Everywhere ™ compromises of the following components:

- Versa SASE Platform
  - Versa Secure Private Access
  - Versa Secure Internet Access
  - Versa Traffic Engineered Backbone.
- Versa Zero Trust – Premises (ZT-Prem)
- Versa Secure Software-Defined WAN (Secure SD-WAN)
- Versa Software-Defined LAN (SD-LAN)



Hit the Contact Us and drop us a line. We will get you in touch with a security expert to brief you how Versa Zero Trust Everywhere ™ can help you architect and implement Zero Trust Architecture for your enterprise and help your organization protect against "Digital Supply Chain Management Attacks."

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com