Third parties are scary

The trends in Cyber Supply chain attacks

16 November 2022

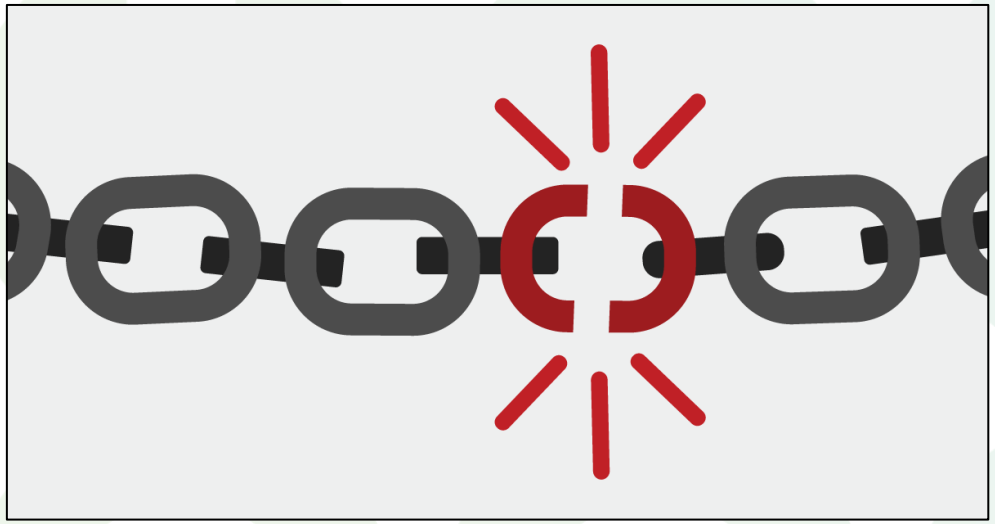
RISKEVENT'22

ISACA Netherlands Chapter

What are Supply Chain attacks?

Supply Chain Risk encompasses

- any type of risk related to
- working with suppliers, data processors or other external parties
- where dependencies or integrations with the own organisation exist



Security breaches at third parties can have a huge impact on your organisation

Supply Chain Attacks are the targeting of an organization's suppliers to gain unauthorized access to that organization's systems or data.

It is the compromise of one, to further compromise many.

What are the different sort of attacks?

There are multiple IT supply chains attacks the most common are:

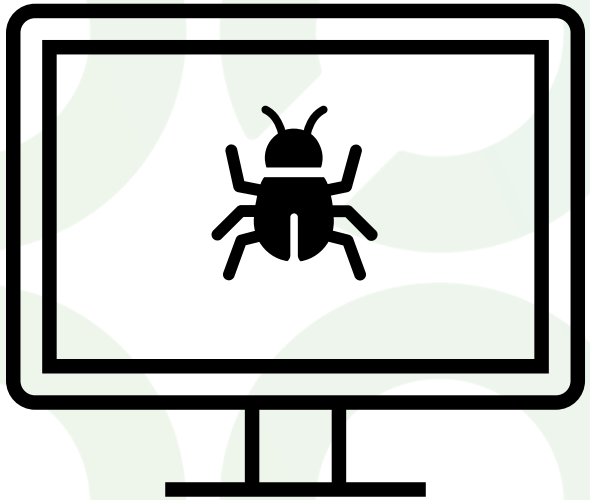
- Software supply chain attacks
- Services supply chain attacks
- Credential supply chain attacks

Software supply chain attacks have and additional component when the use of open-source software in supply chains is considered.

- Attacks on open-source repositories have increased **633%**.
- Java, JavaScript, Python and .NET will surpass **3 trillion** downloads soon.
    - This popularity brings risk.

Who is committing supply chain attacks?

- Many mediatized supply chain attacks are often attributed to nation state actors; however, these aren't the only actors looking to break the chain.
  - This attack type is being **increasingly utilized** by **criminal groups:**
    - Kaseya VSA targeted by REvil Ransomware,
    - Exploiting of Log4J vulnerability by Conti.



How to model supply chains attacks?

Using ENISA's taxonomy, Supply Chain Attacks can be separated based on **who** and **how** they are targeted.

- Supplier targeted attacks are furthered divided into:
  - Attack Techniques,
  - Targeted Assets.
- Customer targeted attacks can also be divided into:
  - Attack Techniques,
  - Targeted Assets.
- The value of this taxonomy is the emphasis on the multiple parts of the supply chain that can be targeted.
  - Which helps in the identification of incidents as Supply Chain Attacks.

Supplier Targeted Attacks

SUPPLIER	
Attack Techniques Used to Compromise the Supplier	Supplier Assets Targeted by the Supply Chain Attack
Malware infection	Pre-existing Software
Social Engineering	Software Libraries
Brute-Force Attack	Code
Exploiting Software Vulnerability	Configurations
Exploiting configuration Vulnerability	Data
Open source (OSINT)	Processes
	Hardware
	People
	Supplier

- In these attacks, the attack technique can vary or multiple methods can be utilized.
- When reported, the attack technique is not often disclosed as the supplier is not the final target.
- The supplier is suitable target due to the trusted relationship they have with their customers. This relationship has been abused in several past supply chain attacks.

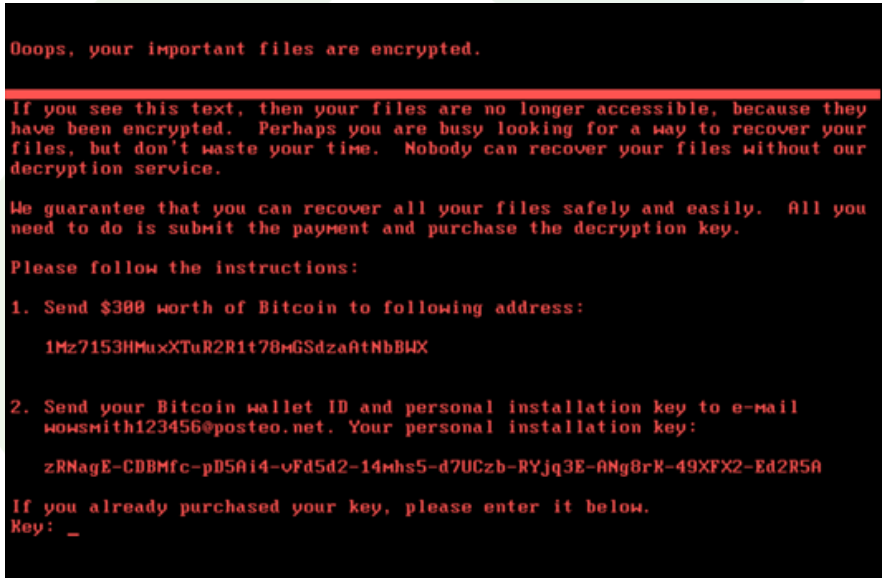
Customer Targeted Attacks

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationships	Data
Driven-by Compromise	Personal Data
Phishing	Intellectual Property
Malware Infection	Software
Physical Attack or Modification	Processes
Counterfeiting	Bandwidth
	Financial
	People

- The techniques deployed in such attacks (right column) can be multiple and are not always registered by customers through the legitimacy of the supplier they enter under.
- Ultimately, the customer's assets are the targets of such attacks. These can be targeted directly or inadvertently affected.

Prominent Supply Chain Attacks: NotPetya

- Ukrainian company Linkos was breached and NotPetya was installed on MEDoc's update server.
- Once MEDoc updated, the attackers had access to thousands of PCs and customers including FedEx TNT, Mondeles Food and Merck.
- During this timeframe, Maersk's Odessa office had purchased and installed MEDoc.
- This enabled NotPetya to effect Maersk globally and indirectly affect other companies resulting in the loss of billions.



SUPPLIER	
Attack Techniques Used to Compromise the Supplier	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
Trusted Relationship Malware Infection	Processes

Prominent Supply Chain Attacks: FishPig

- Reported on August 19th, FishPig, a maker of e-commerce software used by at least 200,000 websites was compromised enabling criminal actors to create backdoors to customer's systems.

- Once the actors entered FishPig's systems they injected malware into the platform's plug-in software, Magento, that installed the Rekoobe backdoor on online e-commerce stores using it.

SUPPLIER	
Attack Techniques Used to Compromise the Supplier	Supplier Assets Targeted by the Supply Chain Attack
Unknown	Code Processes
CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship Malware Infection	Software Processes

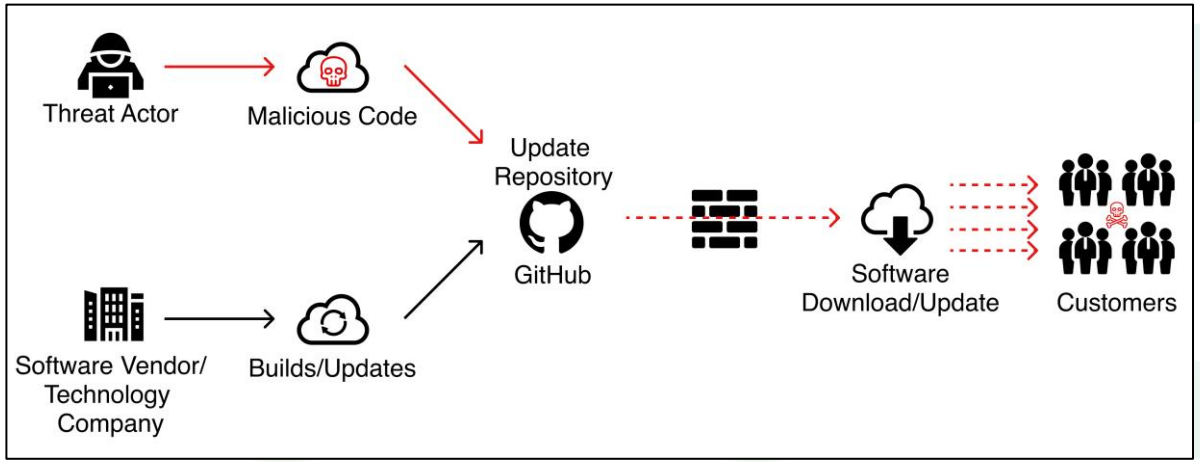
Prominent Supply Chain Attacks: Solar Winds

- SolarWinds, a supplier of management and monitoring software, had one of its network management systems, Orion, compromised by APT29.
- Access to Orion was possibly achieved by exploiting a zero-day vulnerability, social engineering or a brute-force attack.
- Once inside, the attackers injected malicious software directly into Orion during it's build process before it was later downloaded by customers.

SUPPLIER	
Attack Techniques Used to Compromise the Supplier	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 Malware infection	Data

Prominent Supply Chain Attacks: GitHub

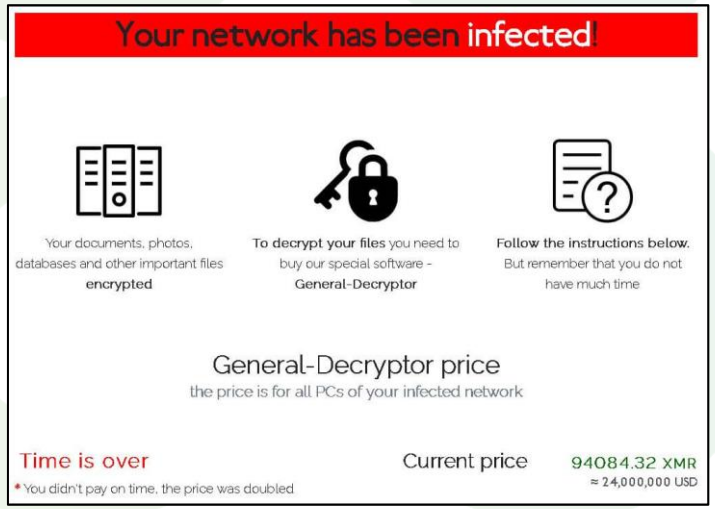
- A malicious threat actor cloned 35,000+ GitHub repositories, maintaining their identity to to the original source code with additional malicious code.
- If downloaded, this code could then fingerprint the environment it was executed in and retrieve additional malware from a third-party site.
- The implications would be catastrophic for any developer who mistakenly downloads the infected cloned code repository, uses it in their project and then unknowingly pushes the malware to the project users.



SUPPLIER	
Attack Techniques Used to Compromise the Supplier	Supplier Assets Targeted by the Supply Chain Attack
Exploiting Configuration Vulnerability Open-Source Intelligence	Software Libraries Code
CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Counterfeiting Malware Infection	Data Software

Prominent Supply Chain Attacks: Kaseya

- REvil compromised Kaseya VSA servers, using a zero-day vulnerability.
- Using this server, a malicious hotfix containing the ransomware payload, Sodinokibi was pushed, compromising and encrypting thousands of nodes at different clients.
- The attack exploited internet-facing VSA servers running upstream of many victims, making it difficult for victims to detect or prevent infection.



SUPPLIER	
Attack Techniques Used to Compromise the Supplier	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 Malware Infection	Data Financial

The supply chain attack surface is much larger than organizations realize.

And it is a case of when your supply chain becomes a target, not if…

Supply Chain Risk Mitigations

- Understand the risks
  - Know your attack surface and manage it!
  - Maintain updated inventories of your assets and suppliers,
  - Understand the security risk posed by your supply chain.
- Establish controls
  - Do the basics right (it is not easy)
  - Enable multifactor authentication where possible,
  - Segment networks to limit resources accessible to threat actors should they gain access.

Supply Chain Risk Mitigations

- Integrate security into your development cycle
  - Maintain overviews of code usage, vulnerability management, license management and secret management.
- Prepare an Incident Response Process
  - When your supply chain is compromised, have a response plan ready so you can:
    - Contain the attack,
    - Control the damage,
    - Protect your assets.

RISKEVENT'22

ISACA®
Netherlands Chapter

RISKEVENT'22

ISACA®
Netherlands Chapter