EUROPEAN UNION AGENCY
FOR CYBERSECURITY

UNDERSTANDING SUPPLY CHAIN ATTACKS

Ifigeneia Lella, ENISA,
Knowledge and Information Team

etl@enisa.europa.eu

05 | 11 | 2021

AGENDA

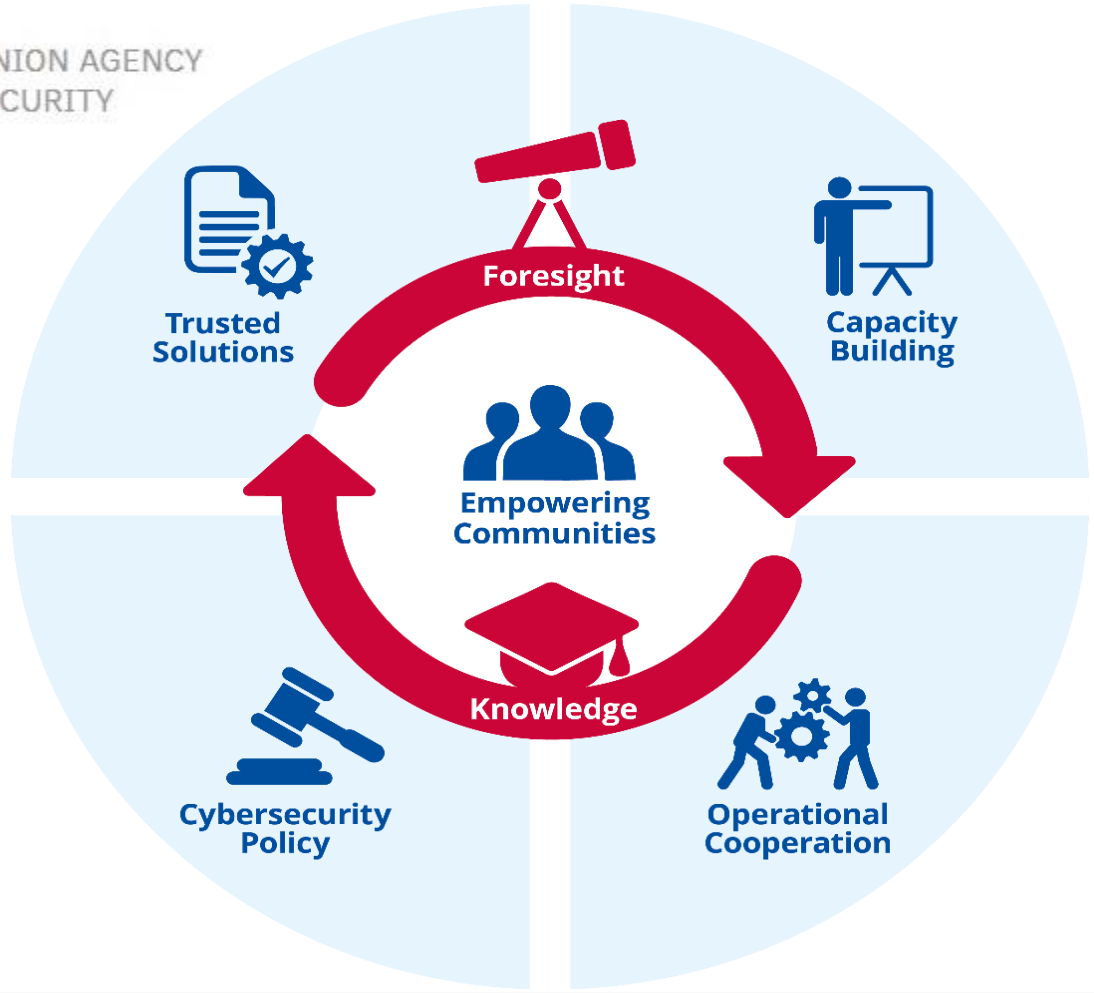
ROLE OF ENISA – WHO WE ARE

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

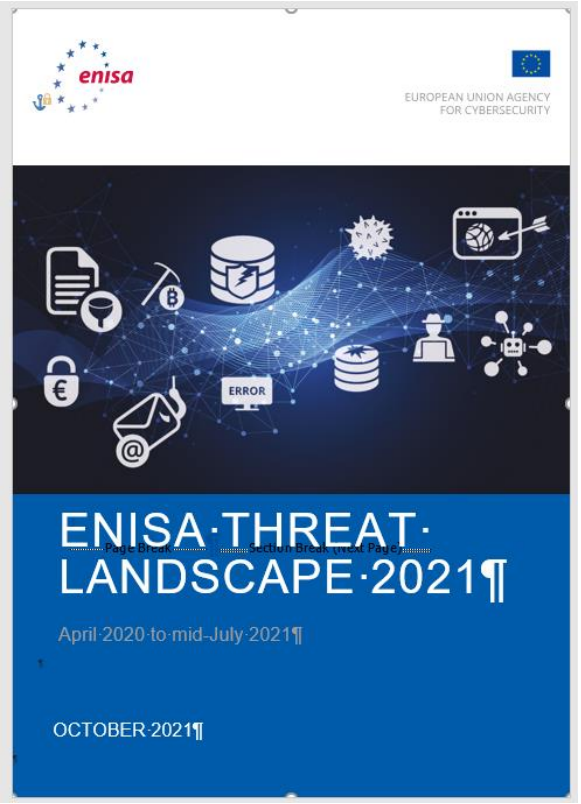
A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



ENISA THREAT LANDSCAPE SO FAR

- Publicly available data (mainly reports and some incidents)
- Observed threats, threat agents and threat trends
- Top threats prioritized according to the frequency of appearance and NOT according to the impact caused
- Appears on a yearly basis

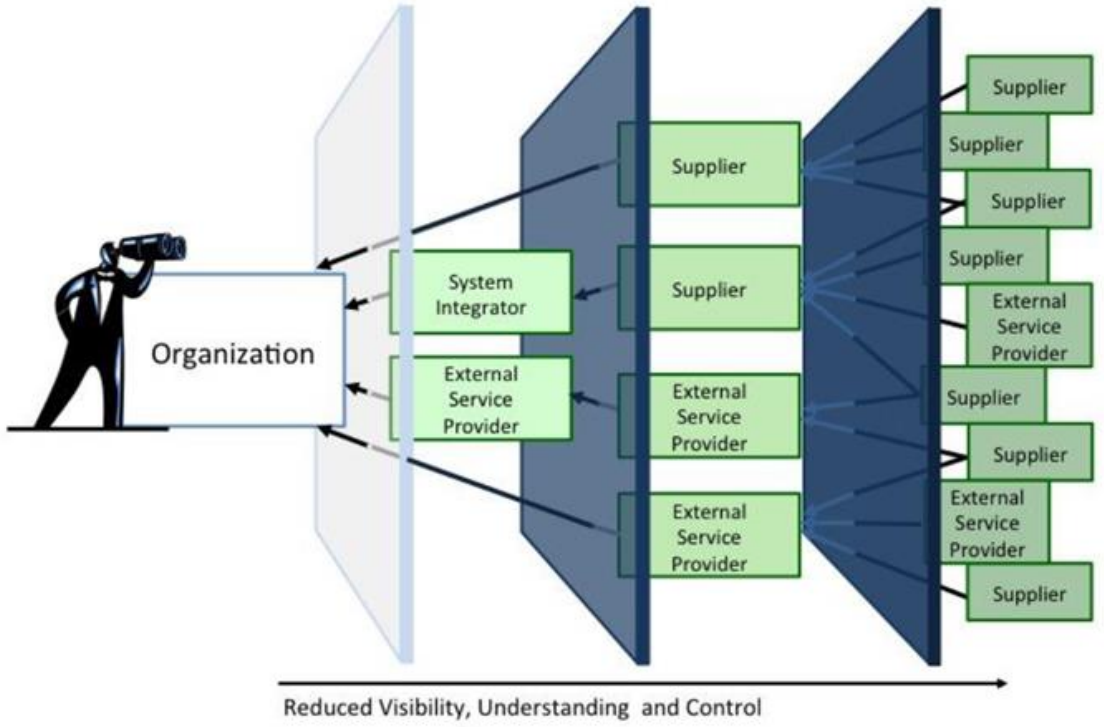


A collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends

SUPPLY CHAINS CHALLENGES

SUPPLY CHAIN CHALLENGES

- The supply chain can be highly **complex**, with **global distribution channels** and multiple, often **hidden to the end user**, **interconnections** and/or **interdependencies**.
- Such dependencies include packages, libraries, and modules—all of which are used pervasively to lower development costs and accelerate shipping times.



Visibility, Understanding and Control of an organisation along the supply chain (Source: NIST Special Publication 800-161)

SUPPLY CHAIN PROBLEM

- In the last two years, **24 supply chain attacks** were reported, including attacks with both global and regional impact.
- When multiple entities rely on the same supplier, the consequences of a cyber-attack against this supplier are amplified, **potentially resulting to a national-wide or even cross-border scale impact**.
- Objectives of supply chain attacks have been **financially** or **politically motivated e.g. espionage, ransom, destabilization of political systems.**
- Attacks are either **specific to one entity** or have a **wide range of target groups** in view.

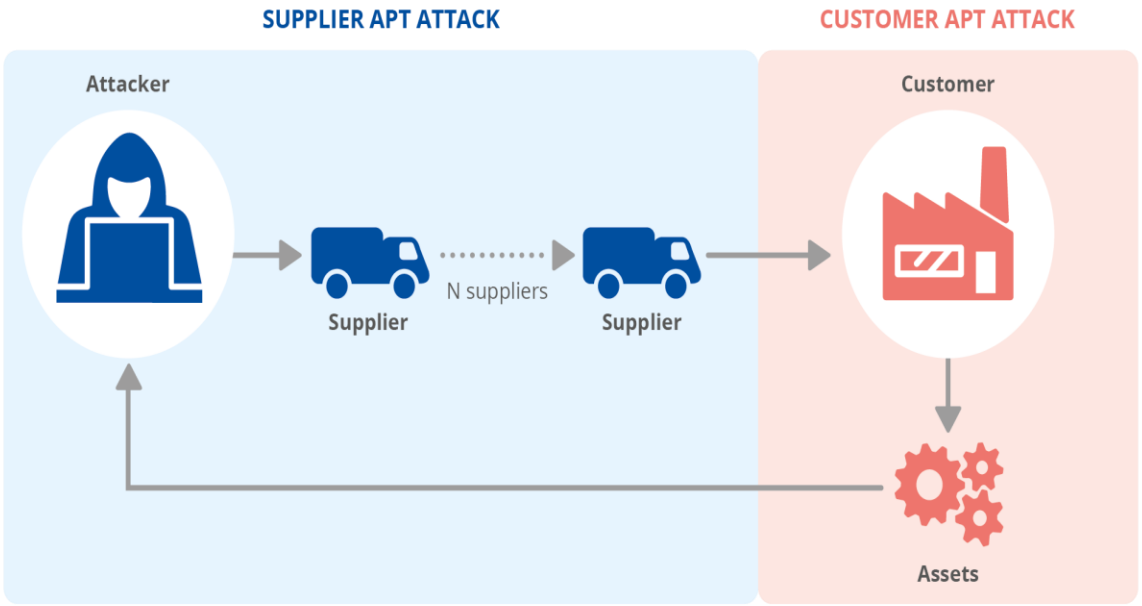
ENISA REPORT: “THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS”

- Published in July 2021
- Analysis of 24 supply chain attacks
- Based on publicly reported incidents
- Reporting period: Jan. 2020-July 2021
- Incidents with either regional or global impact
- Use of taxonomy allows for comparability in case of update
- Recommendations for suppliers and customers

https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

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.



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.**

PROPOSED TAXONOMY

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	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 Intelligence (OSINT)	Processes
	Hardware
	People
	Supplier

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Data
Drive-by Compromise [T1189]	Personal Data
Phishing [T1566]	Intellectual Property
Malware Infection	Software
Physical Attack or Modification	Processes
Counterfeiting	Bandwidth
	Financial
	People

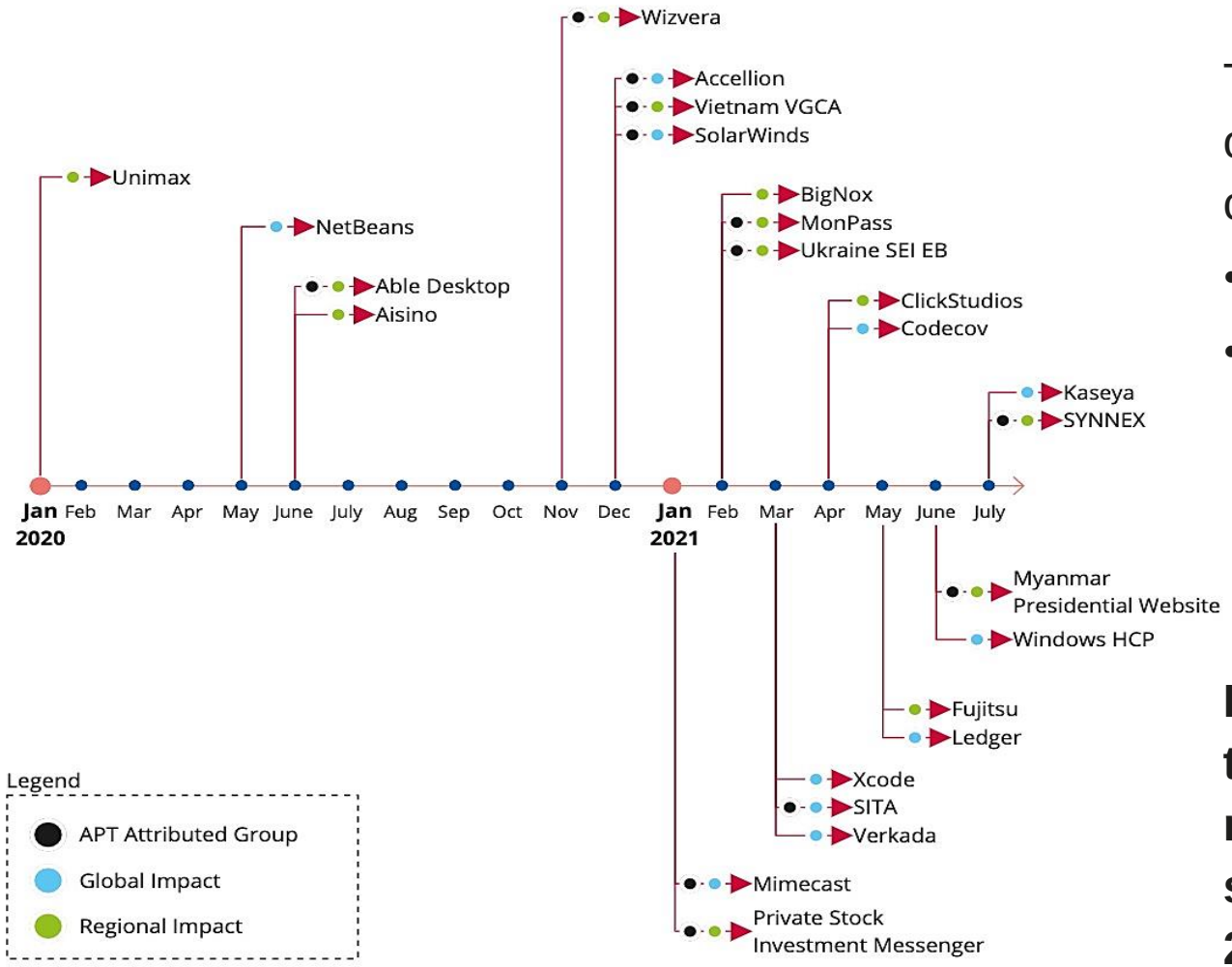
Supplier: an entity that supplies a product or service to another entity

Supplier Assets: valuable elements used by the supplier to produce the product or service

Customer: the entity that consumes the product or service produced by the supplier

Customer Assets: valuable elements owned by the target

TIMELINE OF SUPPLY CHAIN ATTACKS

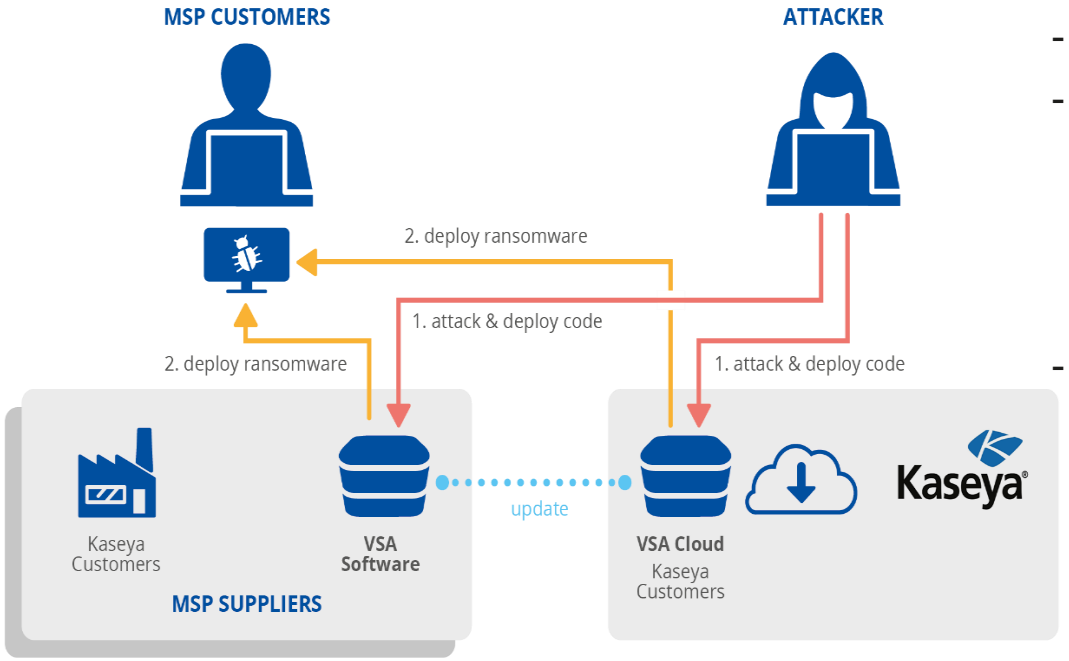


The analysis shows that out of 24 confirmed supply chain attacks:

- 8 reported in 2020 (33%)
- 16 reported from January 2021 to early July 2021 (66%)

Based on this data, the trend forecasts that 2021 may have 4 times more supply chain attacks than 2020.

KASEYA: IT MANAGEMENT SERVICES COMPROMISED WITH RANSOMWARE



- July 2021
- Attackers exploited a zero-day vulnerability in Kaseya's own systems (CVE-2021-30116) 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 to the customers being managed by that VSA CVE-2021-30116, MITRE.

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],	Data, Financial
Malware Infection	

NOT EVERYTHING IS A SUPPLY CHAIN ATTACK

Many traditional software vulnerabilities that were found were reported as a ‘risk’ for future supply chain attacks.

Many of these cases were not supply chain attacks since they did not involve a supplier being compromised.

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.

ENISA Supply Chain Threat Landscape 2021

In some occasions the attackers uploaded malware using similar names to known components/packages in libraries of (open source) software.

KEY FINDINGS

- **More than 50%** of the supply chain attacks were conducted by **state sponsored attackers** and **well-known cybercrime groups**.
- Around **42%** of the attacks were **not attributed** to a particular group.
- Around **62%** of the attacks on customers **took advantage of their trust in their supplier**.
- **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).
- **50% of the attacks** involved infecting the target with **malware.**

KEY FINDINGS (CONT.)

- The majority of the attacks **focused on software**. **Hardware attacks are happening, too**.
- **In 66% of the supply chain attacks, suppliers do not know or are not transparent about how they were compromised**. This may be due to:
  - complexity and sophistication of the attacks
  - lack of maturity in terms of cyber defense in the suppliers
  - slow time to discover the attacks which may hinder investigation efforts.
- **Less than 9% of the compromised customers did not know how the attacks happened.**
- **Not Everything is a Supply Chain Attack.**

RECOMMENDATIONS

Suppliers	Customers
• **Secure development** of products and services that is consistent with commonly accepted security practices • Good practices for **vulnerability management** • Good practices for **patch management**	• Assess the **cybersecurity maturity** of their suppliers • Manage the **supply chain cybersecurity risk** • Manage the **relationship with suppliers**

CONCLUSION

- Supply chain attacks is a **trend** and is **here to stay** and **grow further**.
- An organization could be **vulnerable** to a supply chain attack even **when its own defenses are good**.
- Due to increased interdependencies and complexities, the impact of attacks on suppliers may have **far reaching consequences**.
- The need to act is clear: good practices and coordinated actions are important to reach **a common high level of cybersecurity**.

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 152 31
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu