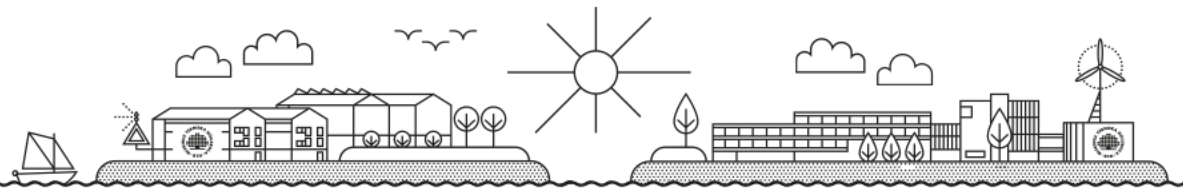
Implementing security compliance requirements for software supply chain security

Feb 22nd, 2023



Supply chain (SC) attacks

Software supply chain attacks are attacks on a target system(s) through the exploitation of the software supply chain of the system(s) (libraries, components, software used in SC, delivery mechanisms).

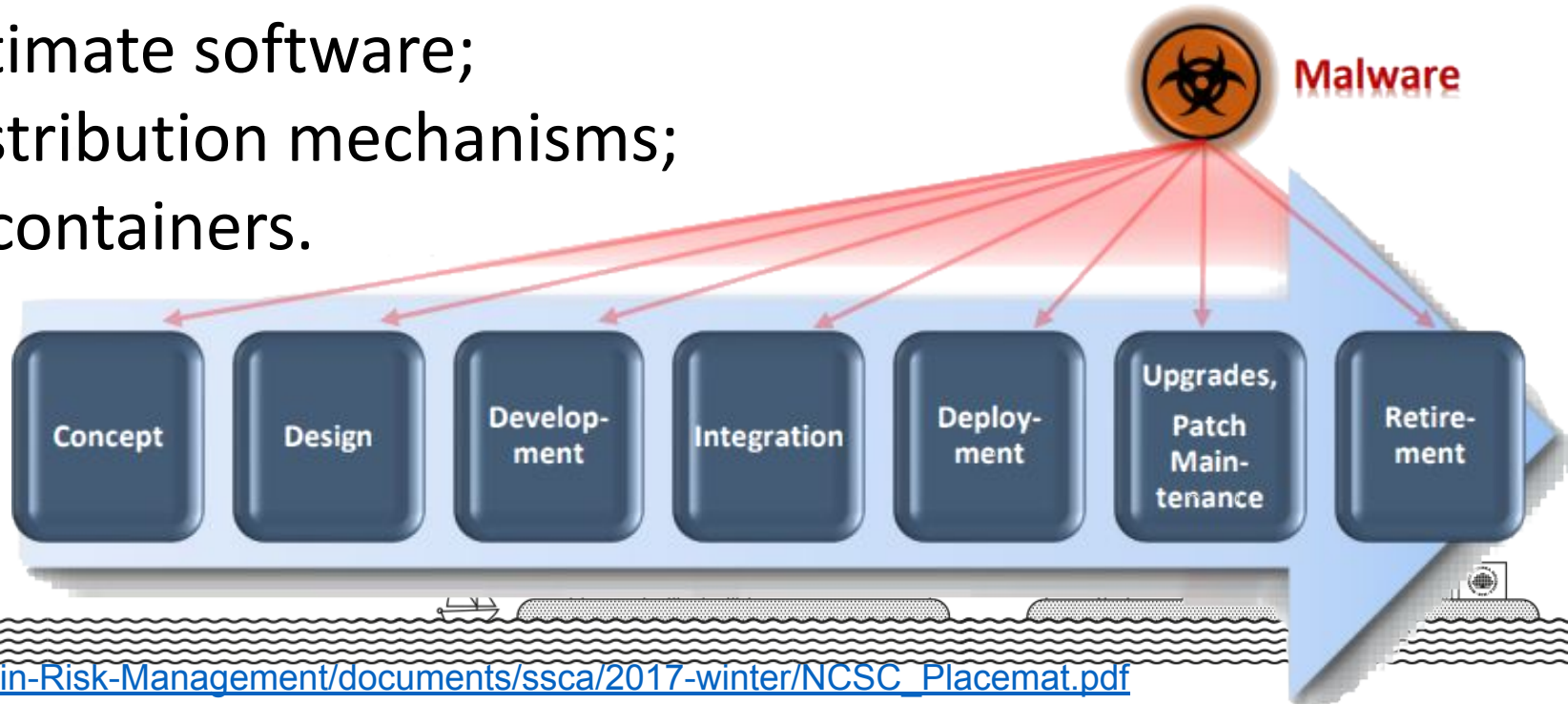
This technique enables cyberattacks of varying scale: from persistent targeted attacks to massive cyberattacks on multiple systems and networks.

Sources:
https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf
https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Types of supply chain attacks

Supply chain compromise can take place at any stage of the supply chain including manipulation/compromise of:

- development tools and environment;
- source code repositories (public or private);
- replacement of legitimate software;
- software update/distribution mechanisms;
- system images and containers.

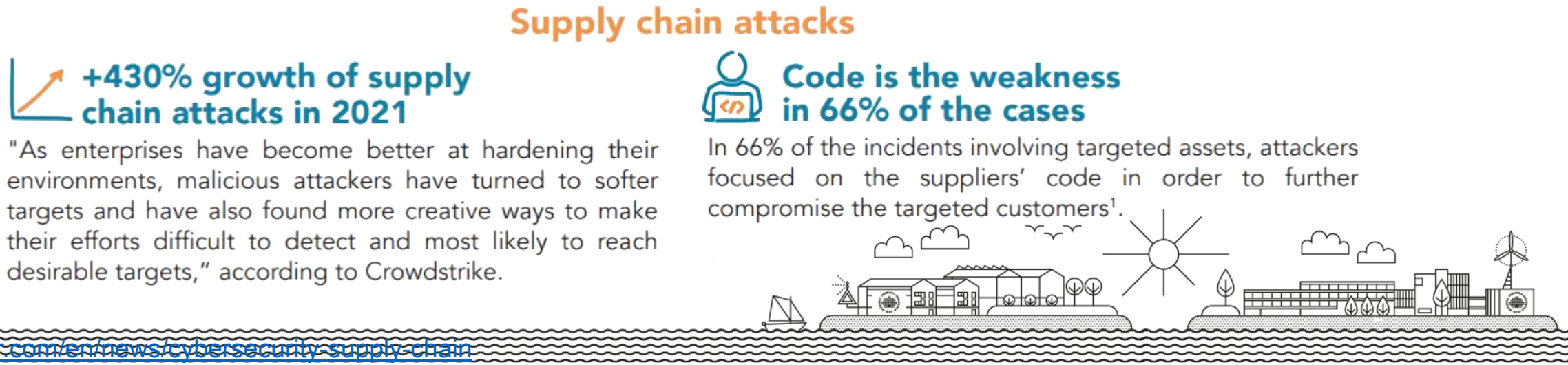


Sources:
https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf

Supply chain attacks statistics

According to Gartner by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chain, a three-fold increase from 2021.

In 66% of the supply chain attacks cases, suppliers did not know, or were not transparent, about how they were compromised.



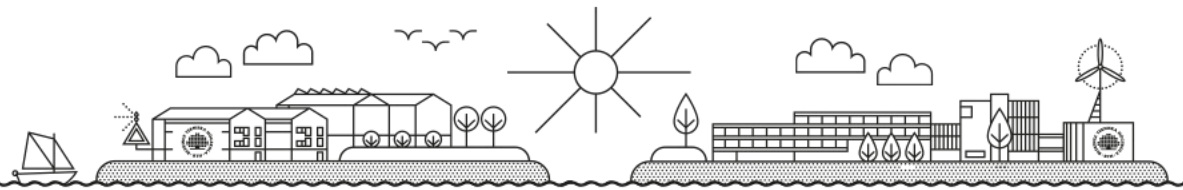
Sources:
https://www.scor.com/en/news/cybersecurity-supply-chain
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Rapid regulatory response

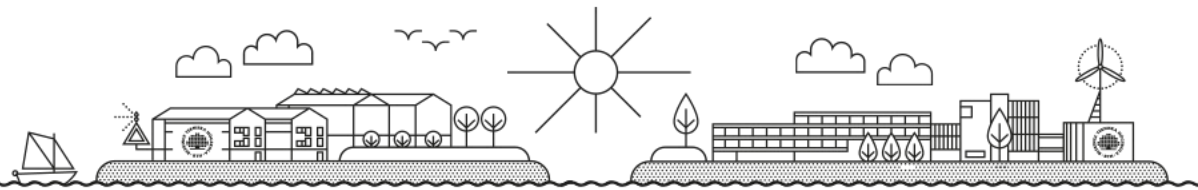
SC cyberattacks are a serious national cybersecurity concern.

Implementation of compliance requirements helps to implement the **minimal security** of the software supply chain as required by regulators and **achieve evident compliance** with such regulations.

Taking a look into existing regulations can help to anticipate future regulatory demands in cybersecurity.



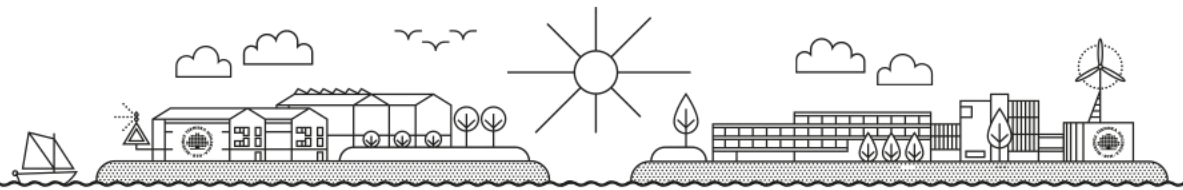
Regulatory requirements



Supply chain attacks: regulatory perspective

“The development of commercial software often lacks **transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors**.”

Software supply chain security "[is] associated with an **enterprise’s decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed**"



European Cyber Resilience Act (CRA)
(proposal)

Mainly targeting to improve cybersecurity by imposing rules on "products with digital elements" in order to assure that such products are "developed in a secure manner and that they have access to **timely security updates** for such products".

Both supply of incorrect, incomplete or misleading information to authorities and non-compliance to the Regulations are subject to administrative fines.

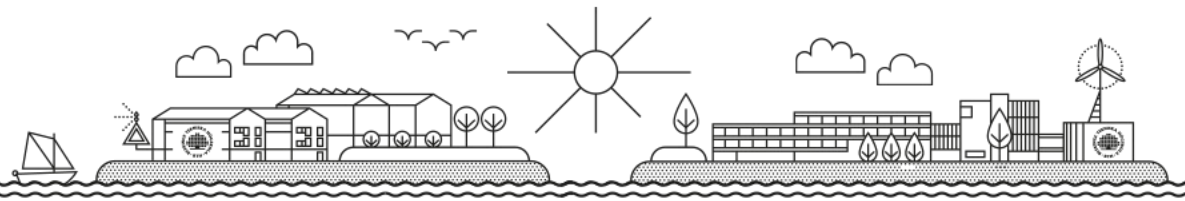
Fines reach **10 000 000 EUR** or **2% of the total worldwide** turnover.

NIS2

Imposes norms on cybersecurity for companies in sectors of high criticality and cybersecurity measures across the EU.

Regulation is mainly focusing on operators of essential services supply chain and theirrelationship with its suppliers in the context of:

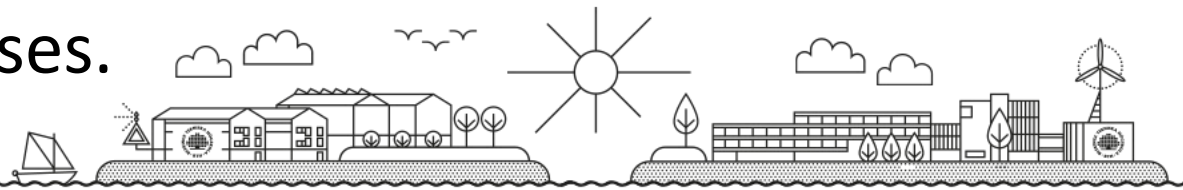
- vulnerabilities affecting third-party products and services;
- appropriate management of supply chain and supplier-related cybersecurity risks.



Executive Order 14028: Improving the Nation's Cybersecurity

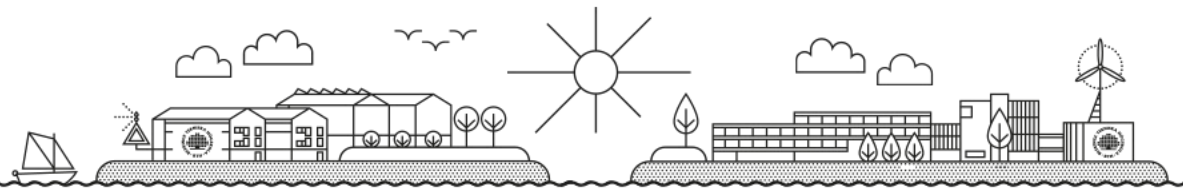
Is focused on cybersecurity of the **Federal Government of the USA** with a special emphasis on “critical software”. The measures for securing software supply chain include:

- secure software development environments;
- automated tools or processes to:
  - maintain trusted source code supply chains;
  - check for known and potential vulnerabilities;
  - remediate vulnerabilities.
- generating and providing, when requested, artifacts of the execution of the tools and processes.



Executive Order 14028: Improving the Nation's Cybersecurity

- maintaining accurate and up-to-date data, provenance of software code or components, and controls on internal and third-party software components, tools, and services present in software development;
- **providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;**
- participating in a vulnerability disclosure program that includes a reporting and disclosure process;
- attesting to conformity with secure software development practices.



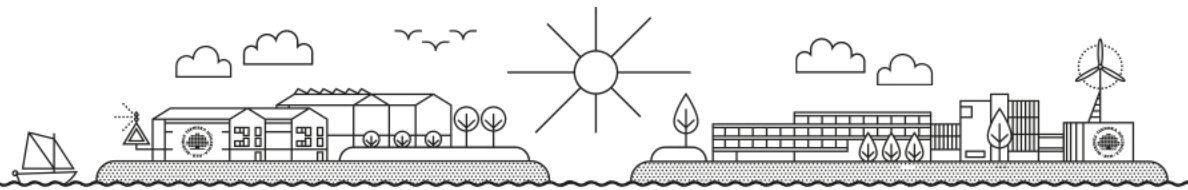
UN Regulation 155 / ISO 21434:2021

UN Regulation 155:

The vehicle manufacturer has taken measures to collect and verify the information required through the supply chain so as to demonstrate that **supplier-related risks are identified and are managed**.

ISO 21434:2021:

Cybersecurity risk management is applied **throughout the supply chain** to support cybersecurity engineering.



Summary on software supply chain security

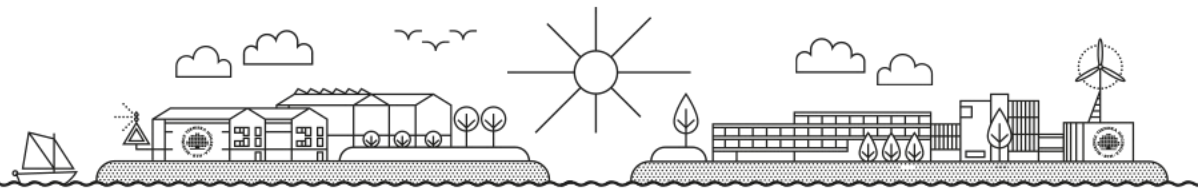
For now, regulations are mainly focused on the SC of “critical software” or software in critical domains.

Compliance requirements evolve around:

- having and providing information;
- risk assessment and risk management,
- baseline supply chain-related security.

One of the important controls suggested in some of the aforementioned regulations is the **software bill of materials (SBOM)**.

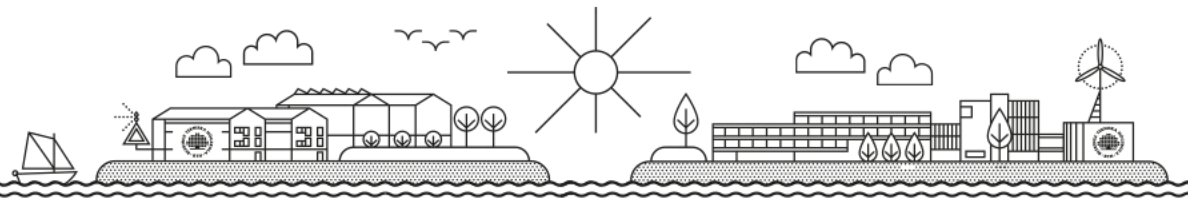
Supply-Chain Attacks



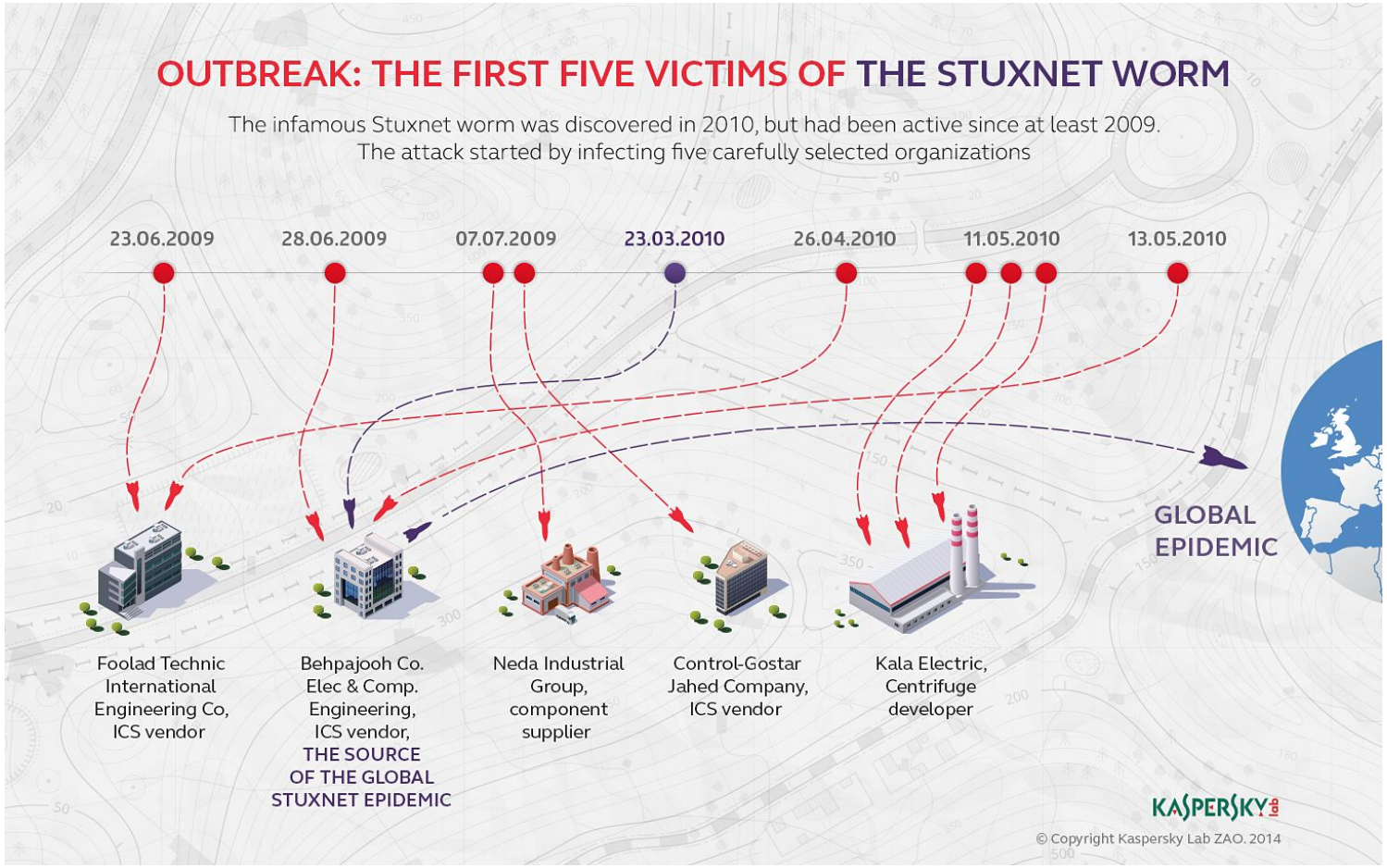
Types of supply-chain attacks

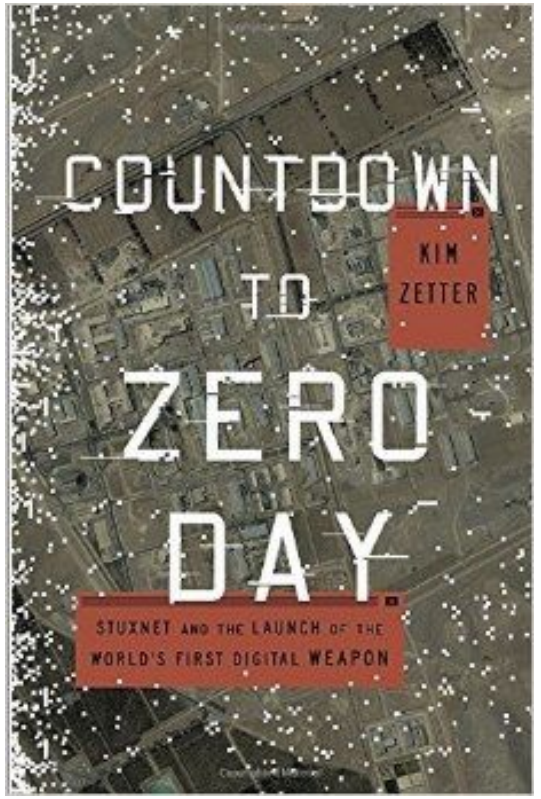
1. Compromised software building tools or update infrastructure
2. Stolen code-sign certificates or signed malicious apps using the identity of dev company
3. Compromised specialized code shipped into hardware or firmware components
4. Pre-installed malware on devices (cameras, USB, phones, etc.)

Source:
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/supply-chain-malware



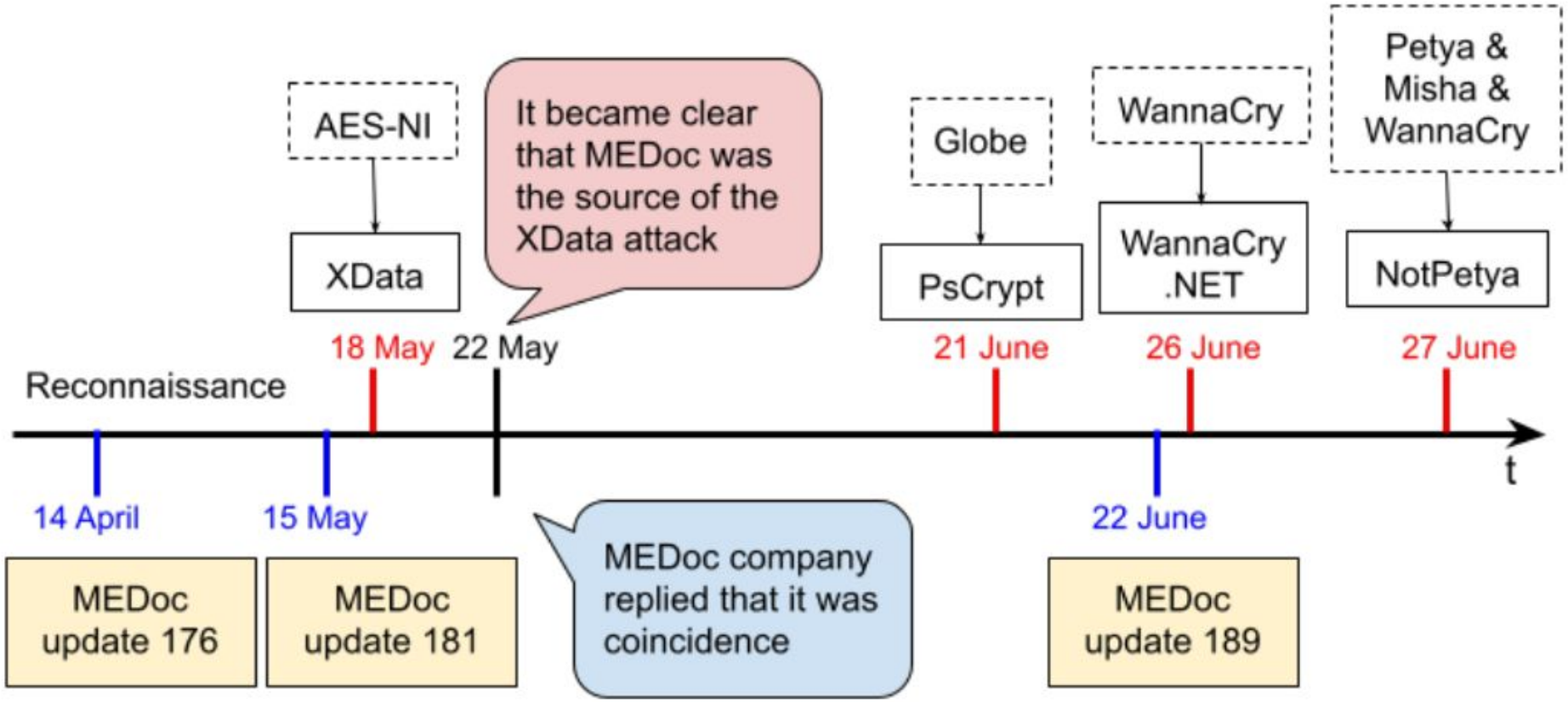
Stuxnet (2010)





Source: https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/

NotPetya via MEDoc (2017)



Solorigate (2020)

Solarigate backdoor in SolarWinds Orion platform reported by FireEye on December 08, 2020

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

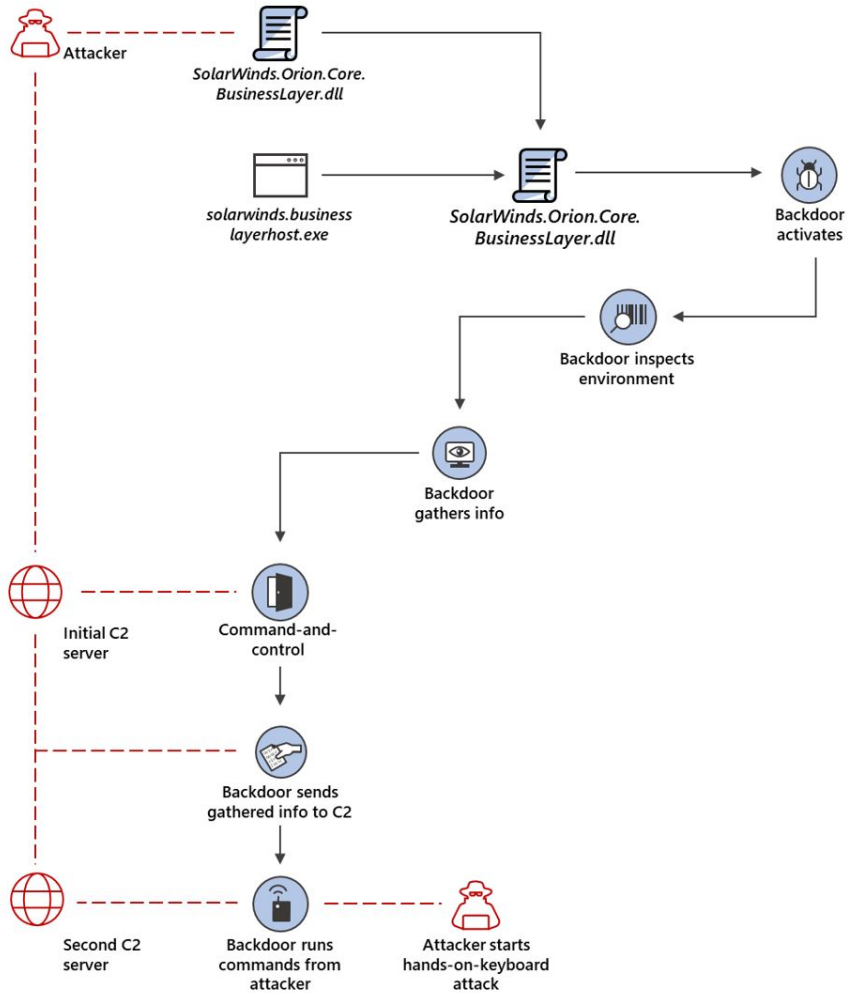
DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

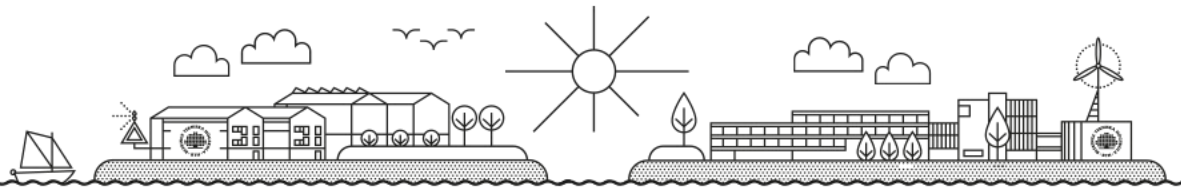
EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



Source:
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

REvil attack via Kaseya VSA (2021)



Happy Blog

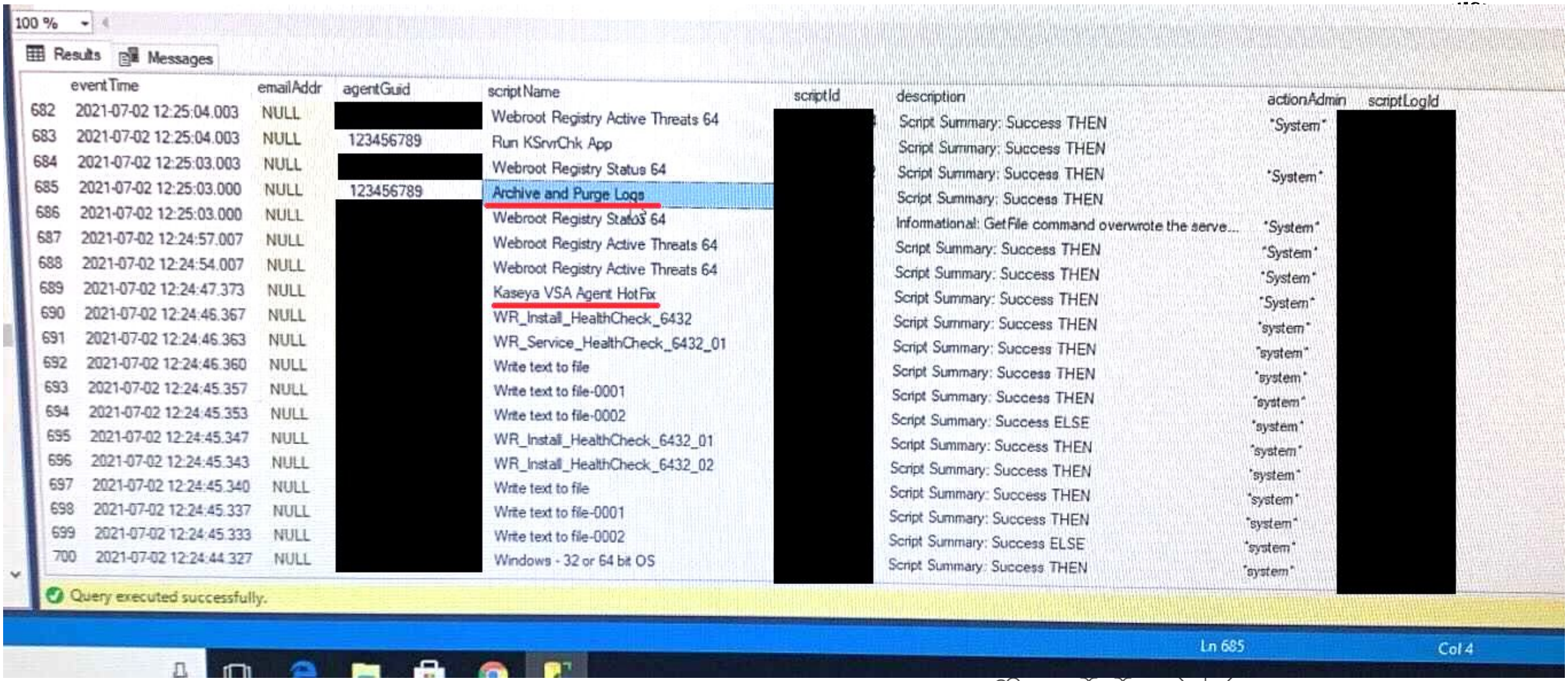
Blog search Search

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

Targets:

- 1000+ organizations
- Norwegian financial software developer Visma, who manages some systems for Swedish supermarket chain Coop. The supermarket chain had to close down its 800 stores for almost a week.

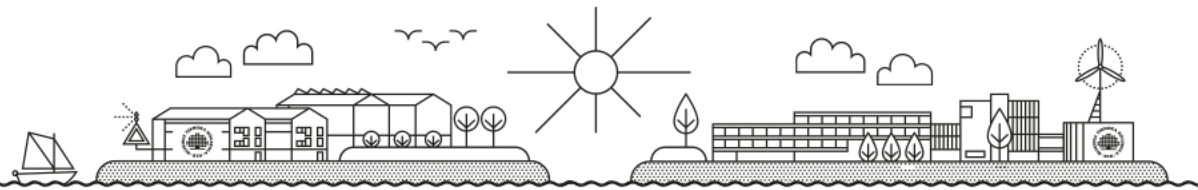


Source: https://twitter.com/KyleHanslovan/status/1411356753720233987

AcidRain (2022)

- Date: 24 Feb 2022
- Targets: Viasat KA-SAT modems
- Discovered by: CERT-UA, SentinelLabs
- Attribution: Sandworm (VPNFilter)
- Platform: Linux and Solaris (ELF 32-bit MIPS)
- Delivery: Supply-chain attack via a misconfigured VPN appliance.
- Destruction: Overwriting data in flash memory on the modems

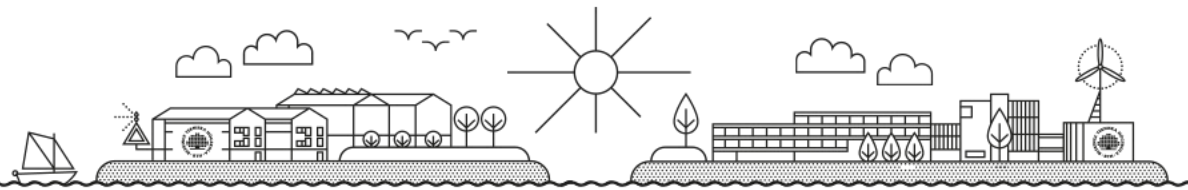
SBOM for software supply chain security



SBOM in software supply chain security

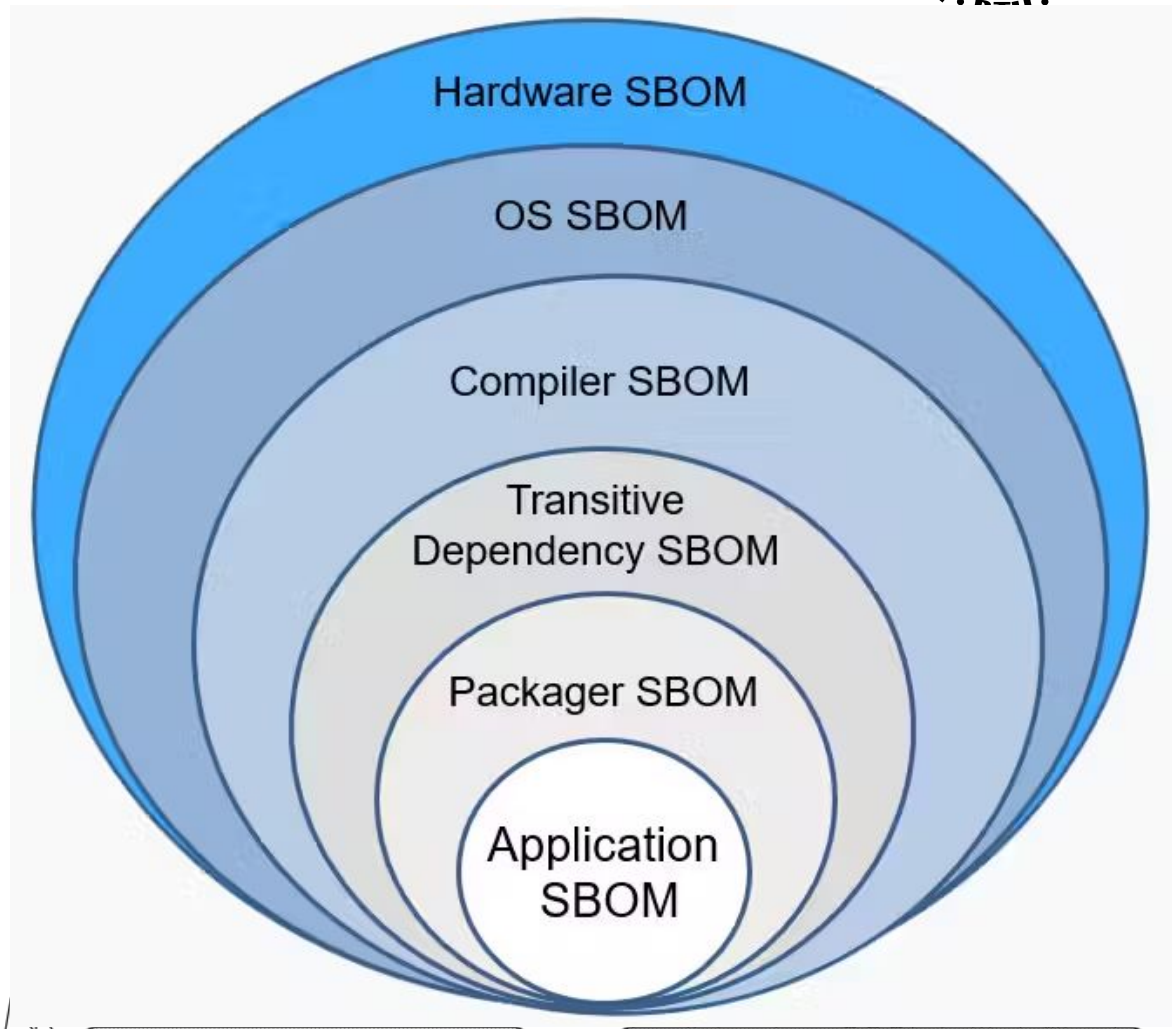
The general vision of regulators is to enable:

- availability of minimal information required for risk management and mitigation, keeping components up to date;
- automation of information exchange and analysis to enable rapid and thorough threat mitigation;
- transparency – availability of SBOM information to all stakeholders;
- responsibility for components/materials maintenance and availability of the required information.



SBOM definition and types

SBOM is a record containing the details and supply chain relationships of various components used in **building software.**



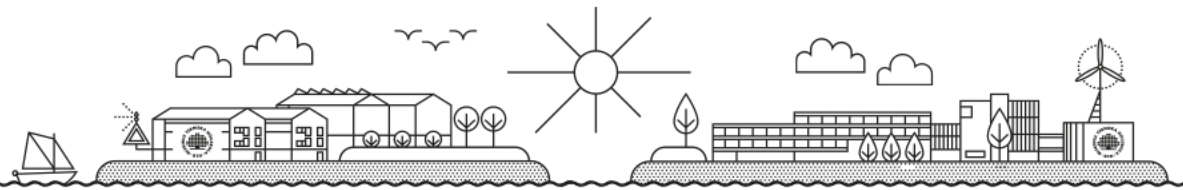
Other types of BOM:
Hardware Bill of Materials (HBOM)
Operations Bill of Materials (OBOM)

Sources:
https://www.deployhub.com/understanding-software-bill-of-materials-sboms/

SBOM Elements

According to Guidelines by the US DoC and NTIA the three categories of minimum elements of SBOM are:

- Data fields and unified structure
- Automation
- Practices and processes



Sources:
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

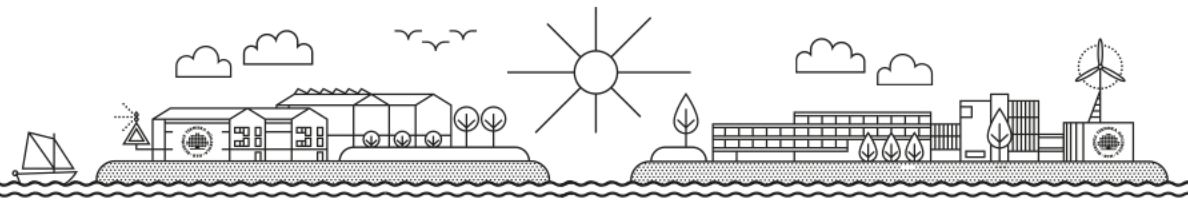
SBOM Elements: Data fields

Data fields:

- Supplier Name
- **Component Name**
- **Version of the Component**
- Other Unique Identifiers
- Dependency Relationship
- Author of SBOM Data
- Timestamp

Recommended:

- **Hash of the Component**
- Lifecycle Phase
- **Other Component Relationships**
- License Information



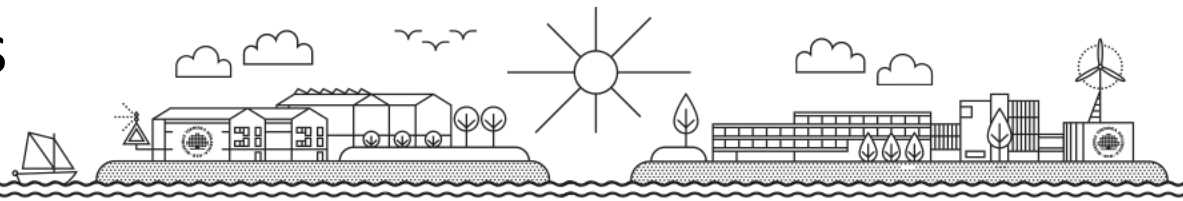
SBOM Elements: Automation

Automatic generation and machine-readability should allow the ability to scale across the software ecosystem.

SBOM data format should be interoperable for the core data fields and use common data syntax.

Support of one of the following data formats:

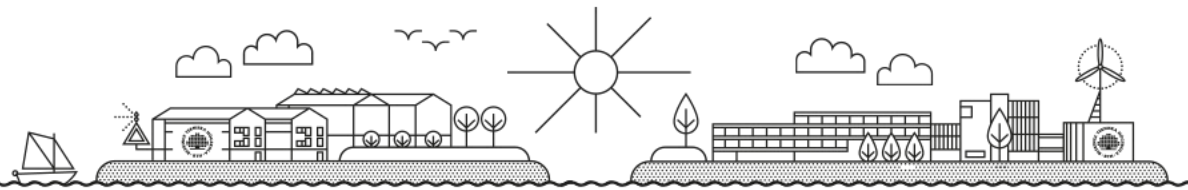
- Software Package Data eXchange (SPDX)
- CycloneDX
- Software Identification (SWID) tags



SBOM Elements: Practices and processes

An SBOM is more than a structured set of data; to integrate it into the operations of the secure development life cycle an organization should follow certain practices and processes that focus on the mechanics of SBOM use.

- Frequency
- Depth
- Known Unknowns
- Distribution and Delivery
- Access Control
- Accommodation of Mistakes

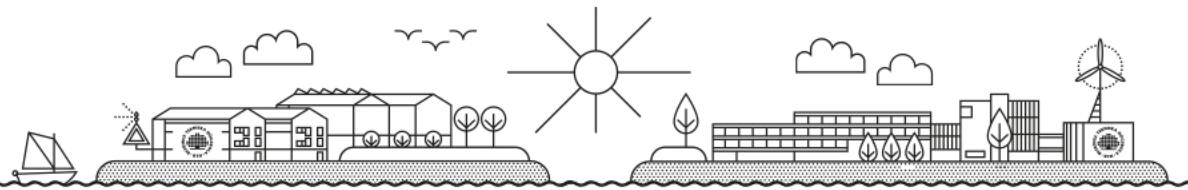


Application of SBOM to mitigate SSC attacks

Vulnerabilities in Kaseya VSA were first discovered on April 1st, 2021. Since then the organization that identified vulnerabilities and Kaseya employees were working to address the vulnerabilities. Still, they didn't manage to do that until July 2nd, 2021.

NotPetya malware used in the global cyberattack in June 2017 was exploiting vulnerabilities EternalBlue and EternalRomance, patches to which were available in March 2017.

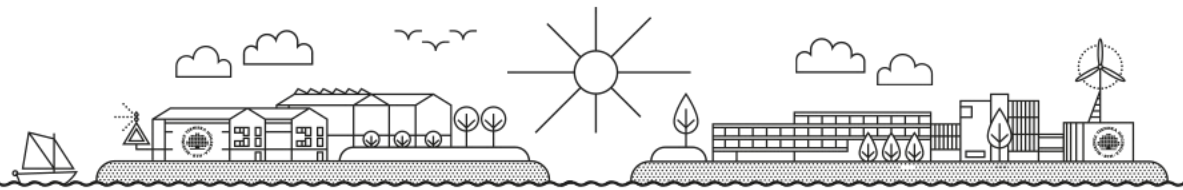
October CMS (CVE-2021-32648) and Log4j (CVE-2021-44228) vulnerabilities patched in 2021, were exploited in attacks on Ukrainian governmental websites in January 2022 [8].



SBOM Business Case

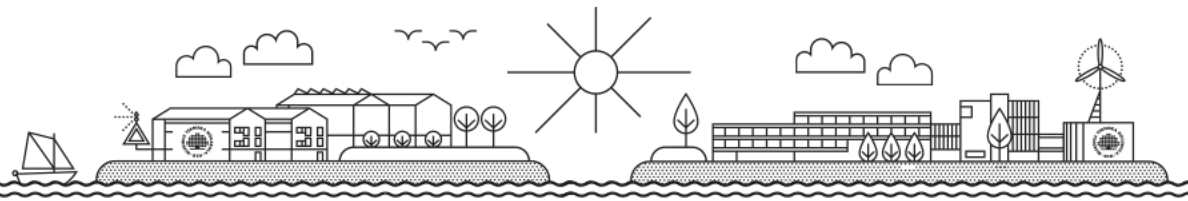
In 2013 Azure and Xbox services were outaged due to digital certificate-related problems.

In 2018 an expired security certificate in the product of one of the large telecommunication equipment manufacturers caused mobile network disruptions in a dozen of countries.



Challenges in SBOM implementation

- Software SC risk management is at the intersection of traditional Supply Chain Risk Management (SCRM) and cybersecurity;
- security concerns due to disclosure of SBOM;
- SBOM for cloud environments SaaSBOM;
- impact on open-source software.



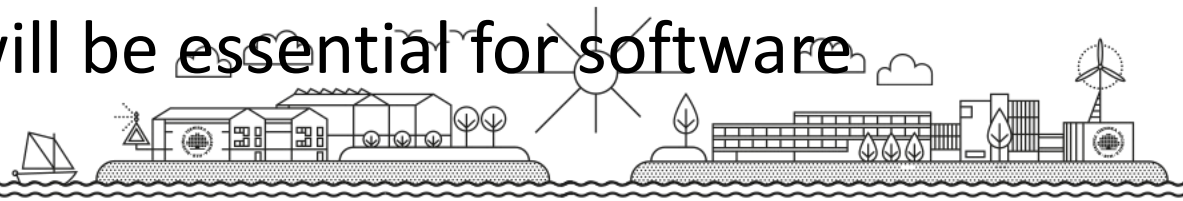
Key Takeaways

The cybersecurity landscape is getting more complex and challenging with the emergence of SC and other types of advanced attacks.

The number of regulations in the cybersecurity domain will continue to grow and will become more stringent in terms of responsibility.

The first step to address SC attacks is to assure the availability of the required data.

Assuring cybersecurity compliance will be essential for software product success.



Upcoming Courses

BLEKINGE INSTITUTE OF TECHNOLOGY

Application for Autumn 2023 Courses is now open

- Applied Case Course in Security (large) 20 credits
- Applied Cryptography 5 credits
- Development Security Operations (DevSecOps) 7.5 credits
- Security for Critical Infrastructure (Operational Technology) 7.5 credits
- Security Inventory for Software Development 3 credits
- Software Security 7.5 credits
- Trusted Systems 7.5 credits
- Web System Security 7.5 credits

All courses are:
- Designed for professionals
- Given Online and flexible
- App 25% Study Pace
- Free of charge, University credits

Questions about Application?

Contact Monique Johansson mow@bth.se or Anna Eriksson aes@bth.se

PRO.M.IS
security built in

Entry Requirements

BLEKINGE INSTITUTE OF TECHNOLOGY

- PROMIS courses requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).
- Even if you don't have the formal academic merits, you might be qualified for the course through validation. See more info on https://promisedu.se/
- **Apply via antagning.se or universityadmission.se**

All courses are:
- Designed for professionals
- Given Online and flexible
- App 25% Study Pace
- Free of charge, University credits

Questions about Application?

Contact Monique Johansson mow@bth.se or Anna Eriksson aes@bth.se

PRO.M.IS
security built in

Save the Date!

Our next Breakfast Seminar is March 22nd

BLEKINGE INSTITUTE OF TECHNOLOGY

"**Cyber Security Certification**" with **Oleksii Baranovskyi**

More details to follow…

Upcoming Security Seminars and Events

Send an email to **Monique Johansson mow@bth.se** to subscribe to our mailing list and stay up to date for PROMIS talks and events

PRO.M.IS
security built in

References

MITRE ATT&CK. Supply Chain Compromise
https://attack.mitre.org/techniques/T1195/
IBM Support. (2017, April 26). Storwize USB Initialization Tool may contain malicious code. Retrieved May 28, 2019.
Schneider Electric. (2018, August 24). Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor. Retrieved May 28, 2019.
https://www.theverge.com/2013/2/22/4019772/xbox-live-and-windows-azure-suffering-from-extended-outages
https://www.theverge.com/2015/11/12/9721108/apple-mac-app-store-bug-security-certificate
https://www.theverge.com/2018/3/7/17092084/oculus-rift-headsets-stopped-working-expired-certificate
https://www.theverge.com/2018/12/7/18130323/ericsson-software-certificate-o2-softbank-uk-japan-smartphone-4g-network-outage

References

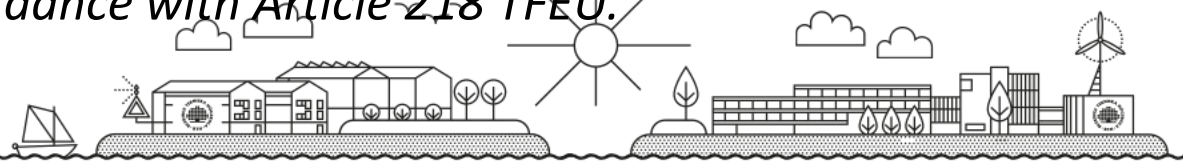
1. https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
2. https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf
3. Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®
4. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
5. https://www.scor.com/en/news/cybersecurity-supply-chain
6. https://www.wired.com/story/revil-ransomware-kaseya-flaw-fix-disclosure-april/
7. https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
8. https://www.securityweek.com/ukraine-attacks-involved-exploitation-log4j-october-cms-vulnerabilities

European Cyber Resilience Act (CRA)

SBOM:
"A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties."

'software bill of materials' means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;

Transnational barriers
"In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment may be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU."



European Cyber Resilience Act (CRA)

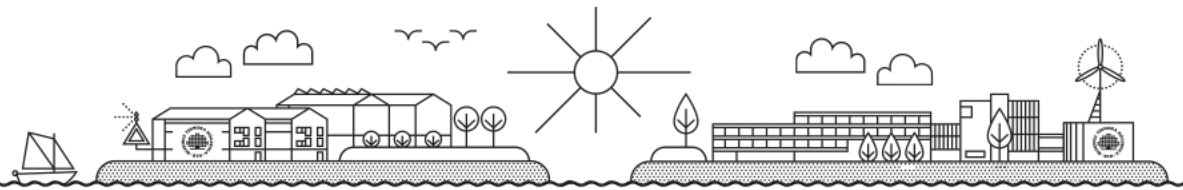
Assessment of products with digital elements which present a significant cybersecurity risk:

"That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken."

Responsibility:

The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

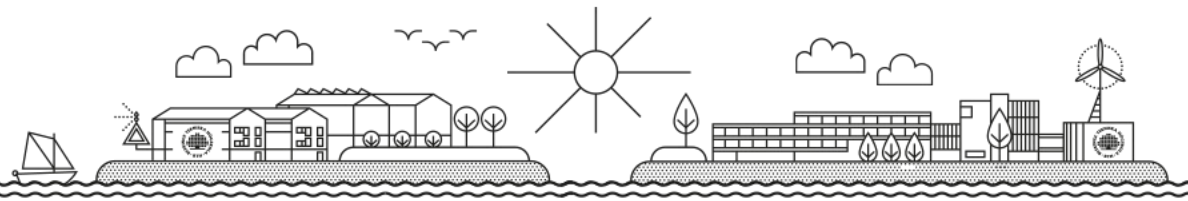


European Cyber Resilience Act (CRA)

Mainly targeting to improve cybersecurity by imposing rules on "products with digital elements"

Notion of supply chain security:
"measures to improve the security of the digital supply chain"

"facilitating the compliance of digital infrastructure providers with the supply chain requirements under the [Directive XXX/XXXX (NIS2)] by ensuring that the products with digital elements that they use for the provision of their services are **developed in a secure manner** and that they have **access to timely security updates for such products**"



NIS2

Imposes norms on how to address the risks related to supply chain by operators of essential services.

Regulation is mainly focusing on "operators of essential services supply chain and its relationship with its suppliers" and considering "vulnerabilities affecting third party products and services".

"To further address key supply chain risks and assist entities operating in sectors covered by this Directive to **appropriately manage supply chain and supplier related cybersecurity risks**, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments ... with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities."