Thematic Workshop 8: Supply Chain Cybersecurity

MARIANTHI THEOCHARIDOU – ENISA & BART VAN RIEL – CAPGEMINI

EMPOWERING EU ISACS CONSORTIUM | NOV 24 2021
Empowering ISACs: Support maturity of existing ISACs and support set-up emerging ISACs

**Goals**
- Support set-up of *emerging* ISACs in the EU
- Support *existing* ISACs to improve maturity
- Support *coordination* between ISACs

**Timelines**
- January 2020
- December 2022

**Activities**
1. Provision of soft support to existing and emerging ISACs
2. Implementation of IT Platforms to support ISACs
3. Organize thematic workshops and conferences for the wider ISAC community
The consortium is currently already supporting a number of European ISAC initiatives. Some examples of our support:

**Stakeholder analysis**
The project performed an analysis of the organisational landscape of an ISAC to determine which categories of stakeholders exist (including [potential] members) to determine how to involve them.

**ISAC promotion and outreach**
The project has helped an ISAC with developing promotional material to initiate (public) outreach, for example to attract new members or create public awareness about the initiative.

**Information-sharing platform**
The project is developing a platform to facilitate information sharing and analysis for multiple EU ISACs to make use of.

**Working Group Efficiency**
The project helps ISACs with organising working groups (teams within an ISAC that work on a specific topic or assignment) efficiently. This involves a ‘best practice’ blueprint and concrete ad hoc advice and support.

**Getting an ISAC started**
In multiple sectors where no European ISAC exists as of yet, the project actively supports ‘founding members’ with their first steps with the establishment of the ISAC.

**Formalisation**
Some ISACs look to formalise the cooperation within an ISAC, for example through documents such as an NDA, Terms of Reference or MoU. The project has supported ISACs with such steps through legal expertise, templates and practical advice.

As you can see, our support activities have different forms: it is not a one-size-fits-all approach.

* Current EU ISACs initiatives we are in contact with and/or supporting
** Sectors in which the project is initiating new EU ISACs

- Energy sector EE-ISAC
- Railway (sub)sector ER-ISAC
- Maritime sector EM-ISAC
- IXP sector PISAX
- Finance sector FI ISAC
- TLD sector
- Healthcare sector
- (drinking) water sector
UNDERSTANDING SUPPLY CHAIN ATTACKS

Marianthi Theocharidou, ENISA
Knowledge and Information Team

etl@enisa.europa.eu

24 | 11 | 2021
ROLE OF ENISA – WHO WE ARE

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.
SUPPLY CHAIN CHALLENGES

• High **complexity**, with **global distribution channels** and multiple, often **hidden to the end user**, **interconnections** and/or **interdependencies**.

• Consequences can be amplified, potentially resulting to a national-wide or even cross-border scale impact.

• **Financially** or **politically motivated attacks**, 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.

*Visibility, Understanding and Control of an organisation along the supply chain*  
(Source: NIST Special Publication 800-161)
• Analysis of 24 supply chain attacks
• Based on publicly reported incidents
• Reporting period: Jan. 2020-July 2021
• Incidents with either regional or global impact
• Taxonomy for supply chain attacks
• Recommendations for suppliers and customers

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:** 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

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attack Techniques Used to Compromise the Supply Chain</strong></td>
<td><strong>Attack Techniques Used to Compromise the Customer</strong></td>
</tr>
<tr>
<td>Malware Infection</td>
<td>Trusted Relationship [T1199]</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Drive-by Compromise [T1199]</td>
</tr>
<tr>
<td>Brute-Force Attack</td>
<td>Phishing [T1565]</td>
</tr>
<tr>
<td>Exploiting Software Vulnerability</td>
<td>Malware Infection</td>
</tr>
<tr>
<td>Exploiting Configuration Vulnerability</td>
<td>Physical Attack or Modification</td>
</tr>
<tr>
<td>Open-Source Intelligence (OSINT)</td>
<td>Counterfeiting</td>
</tr>
<tr>
<td>Pre-existing Software</td>
<td>Data</td>
</tr>
<tr>
<td>Software Libraries</td>
<td>Personal Data</td>
</tr>
<tr>
<td>Code</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>Configurations</td>
<td>Software</td>
</tr>
<tr>
<td>Data</td>
<td>Processes</td>
</tr>
<tr>
<td>Processes</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>Hardware</td>
<td>Financial</td>
</tr>
<tr>
<td>People</td>
<td>People</td>
</tr>
<tr>
<td>Supplier</td>
<td></td>
</tr>
</tbody>
</table>

Supplier Assets: 
- Pre-existing Software
- Software Libraries
- Code
- Configurations
- Data
- Processes
- Hardware
- People
- Supplier

Customer Assets: 
- Data
- Personal Data
- Intellectual Property
- Software
- Processes
- Bandwidth
- Financial
- People
Understanding 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

- 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.

**Understanding Supply Chain Attacks**

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Techniques Used to Compromise the Supply Chain</td>
<td>Attack Techniques Used to Compromise the Customer</td>
</tr>
<tr>
<td>Exploiting Software Vulnerability</td>
<td>Trusted Relationship [T1199], Malware Infection</td>
</tr>
<tr>
<td>Supplier Assets Targeted by the Supply Chain Attack</td>
<td>Customer Assets Targeted by the Supply Chain Attack</td>
</tr>
<tr>
<td>Pre-existing Software</td>
<td>Data, Financial</td>
</tr>
</tbody>
</table>
NOT EVERYTHING IS A SUPPLY CHAIN ATTACK

<table>
<thead>
<tr>
<th>Many traditional software vulnerabilities that were found were reported as a ‘risk’ for future supply chain attacks.</th>
<th>Many of these cases were not supply chain attacks since they did not involve a supplier being compromised.</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>In some occasions the attackers uploaded malware using similar names to known components/packages in libraries of (open source) software.</td>
</tr>
</tbody>
</table>
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
- **Secure development** of products and services that is consistent with commonly accepted security practices
- Good practices for **vulnerability management**
- Good practices for **patch management**

### Customers
- Assess the **cybersecurity maturity** of their suppliers
- Manage the **supply chain cybersecurity risk**
- Manage the **relationship with suppliers**
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.
Prime threats identified (April 2020 to July 2021): the include:

- Ransomware;
- Malware;
- Cryptojacking;
- E-mail related threats;
- Threats against data;
- Threats against availability and integrity;
- Disinformation – misinformation;
- Non-malicious threats;
- Supply-chain attacks
USING THE SOFTWARE BILL OF MATERIALS FOR ENHANCING CYBERSECURITY

ISACs Workshop, November 24th, 2021
Your speakers

Bart van Riel – Enterprise Architect at Capgemini

And I really must credit also:

Allan Friedman – “Doctor SBOM” at CISA
Think about this...

I don’t care what’s inside the software I use!

Because...

What could possibly go wrong?
Wait... What’s an SBOM?

- Bingo Buffer v2.1
  - unknown

- Bob’s Browser v2.2
  - partial

- Acme Application v1.1
  - included in known

- Carol’s Compression Engine v3.1
  - included in root

Supplier Component Version Identifiers Author

Known Unknowns
Wait... What’s an SBOM?

A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory. It is “a formal record containing the details and supply chain relationships of various components used in building software.”
Security Through the Supply Chain

- Quality Assurance
- Security assurance

Generation → Transmission → Distribution → Consumption

SBOM
SBOM isn’t a new concept... even for governments
US Government Engagement

Executive Order 14028 (May 12, 2021) “Improving the Nation’s Cybersecurity”
NCSC-NL Promoting the SBOM

At the forefront of European SBOM initiatives
Study: position, security promise, future possibilities of the SBOM
Possible 1st step towards regulation on European scale

https://english.ncsc.nl/research/research-results/using-the-software-bill-of-materials-for-enhancing-cybersecurity
SBOM from 3 different perspectives

Produce

- Design
- Implement
- Test
- Release
- Maintain

Transparency on Dependencies

Choose

- Requirements
- Initial Selection
- Detailed Assessment
- Choice

SBOM may be a requirement

SBOM used for e.g. security assessment

Operate

- Input for monitoring points
- Input for Asset Management

Continuous Insights
- Monitoring (Learn)
- ITSM (Engage)
- Automation (Deliver)
- Continuous Delivery
- Continuous Agil

Business Value
The 4th perspective: Secure DevOps

DEVOps

Architecture & Design

Test Plans

Implementation

Testing

Release/Feedback from the field

DEVOps

Requirements

Input for Security User Stories

Software stack standards

Endorsed stack components

Test for endorsed components

SBOM Delivered as part of a Release

Findings from the field

Vulnerability Monitoring

SBoM

Deploy

Operate

Release

Monitor

Delivered as part of a Release

Endorsed stack components

Test for endorsed components

Findings from the field

Vulnerability Monitoring
LOTS of SBOM data... so Automate!
Existing solutions – formats and interoperability

**SPDX** is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grass-roots effort includes representatives from more than 20 organizations—software, systems and tool vendors, foundations and systems integrators.

**CycloneDX** is a software bill of materials (SBOM) standard, purpose-built for software security contexts and supply chain component analysis. The specification is maintained by the CycloneDX Core working group, with origins in the OWASP community.

**SWID** tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.
## Existing solutions – formats and interoperability

SPDX is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grassroots effort includes representatives from more than 20 organizations — software, systems and tool vendors, foundations, and systems integrators.

CycloneDX is a software bill of materials (SBOM) standard, purpose-built for software security contexts and supply chain component analysis. The specification is maintained by the CycloneDX Core working group, with origins in the OWASP community.

SWID tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.

<table>
<thead>
<tr>
<th>Field</th>
<th>SPDX</th>
<th>SWID</th>
<th>CycloneDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier</td>
<td>(3.5)</td>
<td>&lt;Entity&gt; @role (softwareCreator/publisher), @name</td>
<td>publisher</td>
</tr>
<tr>
<td>Component</td>
<td>(3.1)</td>
<td>&lt;softwareIdentity&gt; @name</td>
<td>name</td>
</tr>
<tr>
<td>Unique Identifier</td>
<td>(3.2)</td>
<td>&lt;softwareIdentity&gt; @tagID</td>
<td>bom/serialNumber and component/bom-ref</td>
</tr>
<tr>
<td>Version</td>
<td>(3.3)</td>
<td>&lt;softwareIdentity&gt; @version</td>
<td>version</td>
</tr>
<tr>
<td>Component Hash</td>
<td>(3.10)</td>
<td>&lt;Payload&gt;/../&lt;File&gt;@[hash-algorithm]:hash</td>
<td>hash</td>
</tr>
<tr>
<td>Relationship</td>
<td>(7.1)</td>
<td>&lt;Link&gt;@rel, @href</td>
<td>(Nested assembly/subassembly and/or dependency graphs)</td>
</tr>
<tr>
<td>SBOM Author</td>
<td>(2.8)</td>
<td>&lt;Entity&gt; @role (tagCreator), @name</td>
<td>bom-descriptor: metadata/manufacture/contact</td>
</tr>
</tbody>
</table>
# Tooling ecosystem

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Produce</td>
<td>Build</td>
<td>SBOM is automatically created as part of building a software artifact and contains information about the build</td>
</tr>
<tr>
<td></td>
<td>Analyze</td>
<td>Analysis of source or binary files will generate the SBOM by inspection of the artifacts and any associated sources</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td>A tool to assist a person manually entering or editing SBOM data</td>
</tr>
<tr>
<td>Consume</td>
<td>View</td>
<td>Be able to understand the contents in human readable form (e.g., picture, figures, tables, text, etc.). Use to support decision making &amp; business processes</td>
</tr>
<tr>
<td></td>
<td>Diff</td>
<td>Be able to compare multiple SBOMs and clearly see the differences (e.g., comparing two versions of a piece of software)</td>
</tr>
<tr>
<td></td>
<td>Import</td>
<td>Be able to discover, retrieve, and import an SBOM into your system for further processing and analysis</td>
</tr>
<tr>
<td>Transform</td>
<td>Translate</td>
<td>Change from one file type to another file type while preserving the same information</td>
</tr>
<tr>
<td></td>
<td>Merge</td>
<td>Multiple sources of SBOM and other data can be combined together for analysis and audit purposes</td>
</tr>
<tr>
<td></td>
<td>Tool support</td>
<td>Support use in other tools by APIs, object models, libraries, transport, or other reference sources</td>
</tr>
</tbody>
</table>
Who’s doing SBOM already
Vulnerability
Exploitability
eXchange
What makes doing SBOM hard

Legacy Asset Management

Standards Alignment

Data Integrations
SBOM is coming...

Explore how to produce them
Think about how to consume them
Prepare for government drivers

Get involved!
bart.van.riel@capgemini.com
allan.friedman@cisa.dhs.gov
ABOUT CAPGEMINI INVENT

As the digital innovation, consulting and transformation brand of the Capgemini Group, Capgemini Invent helps CxOs envision and build what's next for their organizations. Located in more than 30 offices and 22 creative studios around the world, its 6,000+ strong team combines strategy, technology, data science and creative design with deep industry expertise and insights, to develop new digital solutions and business models of the future.

Capgemini Invent is an integral part of Capgemini, a global leader in consulting, technology services and digital transformation. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion. People matter, results count.

Visit us at www.capgemini.com/invent
Can we help your organization? Let us know!

Contact us:

info@isacs.eu

Empowering EU ISACs Group

Tom van Schie
tom.vanschie@tno.nl

Roeland de Koning
roeland.de.koning@capgemini.com

Upcoming Events

Online Thematic Workshop 7: Cyber Threat Intelligence in the context of ISACs
📅 30/09/2021 - 11:30 - 30/09/2021 - 12:30

2nd Annual Conference
📅 26/10/2021 - 12:45 - 26/10/2021 - 15:30

https://www.isacs.eu/