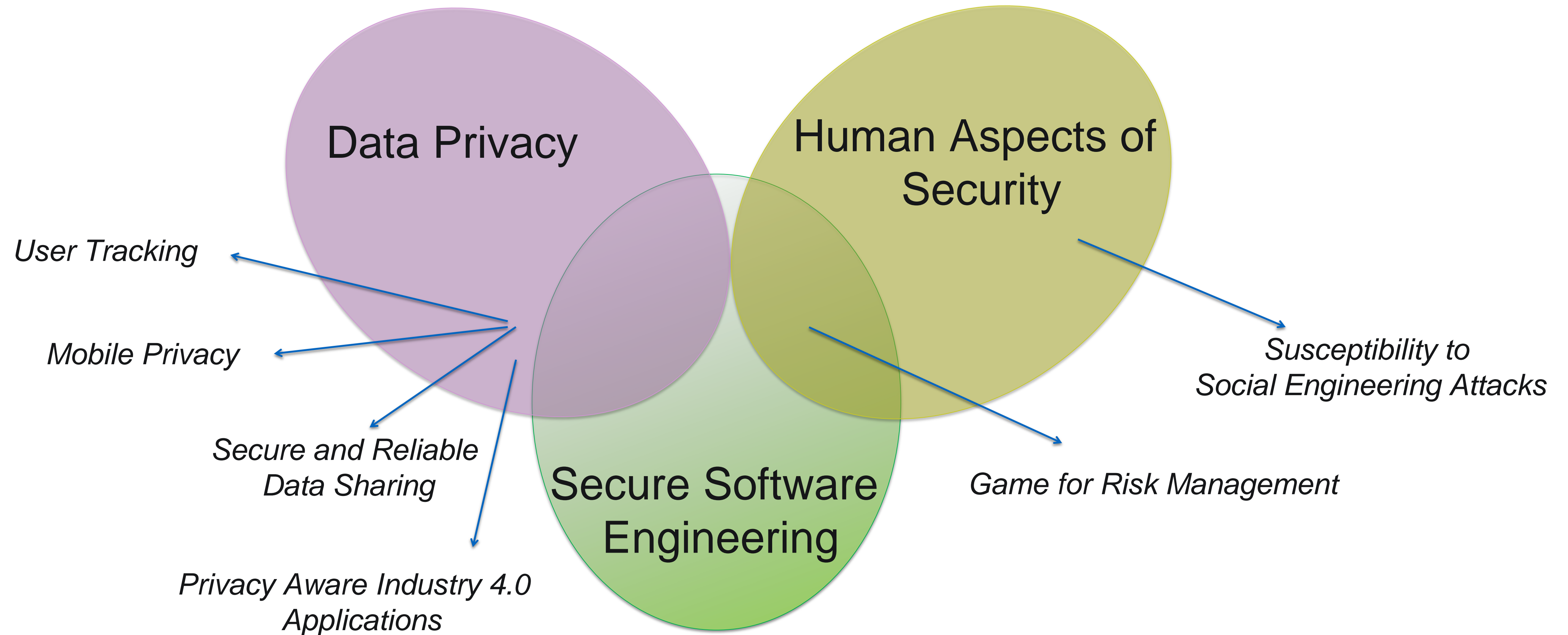


# Fondamenti di Sicurezza e Privacy

## Course Organization

Prof. Federica Paci







# Learning outcomes

- This course aims to give an overview of **cyber security**. The course will equip students with a clear view of the current cyber security landscape considering not only technical measures and defenses, but also the other subject areas that apply, including legal, management, crime, risk, social and human factors.
- At the end of the course, students will have the necessary knowledge and understanding of:
  - the importance of taking a multi-disciplinary approach to cyber security,
  - the cyber threat landscape, both in terms of recent emergent issues and those issues which recur over time,
  - general principles and strategies that can be applied to systems to make them more robust to attack,
  - and issues surrounding privacy, anonymity and pervasive passive monitoring



# Syllabus

- Cybersecurity and cyber security concepts, Cyber threat actors, Threat landscape
- MITRE ATT&ck, Cyberkill chain
- Social Engineering Attacks
- Malware and Ransomware Attacks
- Cyberwar and Attacks to Critical Infrastructures
- Cyber risk management, and threat modeling (STRIDE)
- NIST Framework, Cyber essentials
- User Authentication
- Digital Identity Management
- Access Control
- Introduction to Privacy: notions of privacy, privacy threats
- Privacy threat modeling
- Database privacy: anonymization techniques, differential privacy
- Data protection regulations

# Lectures

- 2 hour on Monday from 10:30 to 12:30
- 2 hours on Friday from 15:30 to 17:30
- Frontal lecture in the classroom
  - The slides will be made available the day before the lecture



# Labs

- 6 laboratory activities on:
  - Threat intelligence: analysis of a cyber attack's techniques using MITRE ATT&ck matrix
    - Computer
  - How to code a malware
    - Windows VM
  - Social Engineering Attacks
    - Kali Linux VM and Amazon Free Tier account
  - Log4j Exploitation
    - Kali Linux VM and Windows VM
  - Password Attacks
    - Kali Linux VM and a vulnerable VM
  - Setting Access Control Policies
    - Computer

# Exam

- Students will be evaluated based on
  - A practical or theoretical project
  - An oral examination on any of the topics taught in the course
- The projects will elaborate on topics taught in the course.
- The project must be done in a group of a maximum of 2 students.
- The students must prepare a written report to present the results of the project.
- During the oral examination, the students will present the project to the teacher, who will ask questions about the project and any of the topics taught during the course.
- At the end of the oral exam, the teacher will propose a final mark.
- The date of the oral examination must be agreed with the teacher during the exam session.



# Theoretical Projects

- Analyze recent cyber attacks
  - Identify the Cyber Kill Chain phases of the attack
  - Identity for each of the phase the techniques leveraged by the attack
  - **Trusted sources:** Fireeye, Symantec, Kaspersky, Wired, CISA
- List of attacks to analyze
  - Kaseya supply chain attack
  - Viasat satellite communication system attack
  - Microsoft Exchange Server Hack 2021
  - Ransomware BianLian 2022



# Practical Project 1

Create a malicious PDF implementing the following features:

- It embeds a Microsoft Word file that contains a macro
- The macro downloads a malware from a C2 server
- It embeds a Javascript code that when a user opens the document saves the embedded Microsoft Word file and executes it
- The Microsoft Word file has to trick the user into enabling the macros



# Practical Project 2

- Code a malware for Windows implementing the following functionalities:
  - Creates a copy of itself on the victim machine
  - Persistence on the machine
    - Modify Windows registries
  - Establish a connection with a C2 server to download a real malware
    - The traffic with the C2 must be encrypted



# Project 3

- Analyze the use of third party trackers
  - You will have to analyze 50 web sites
  - Download the source html of the web sites and identify which third party trackers they use
  - Check that the cookies are not installed on the user browser when the user does not want to be tracked



# Report Structure

Length: maximum 10 pages

Format: IEEE conference template

<https://www.ieee.org/conferences/publishing/templates.html>



# How to communicate with me

- Email: [federicamariafrancesca.paci@univr.it](mailto:federicamariafrancesca.paci@univr.it)
- Office hours: Take appointment via email





# Fondamenti di Sicurezza e Privacy

## Introduction to Cyber Security

Prof. Federica Paci



# Lecture Outline

- What is cyber security?
- Key cyber security properties
- Key cyber security concepts



# Learning outcomes

At the end of this session, you should be able to:

- Define what is cyber security
- Explain key cyber security concepts



# What is cyber security?

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from unauthorized access, harm or misuse.

It's also about preventing unauthorized access to the vast amounts of personal information we store on these devices, and online

# Elements of Cyber Security

Confidentiality

Integrity

Availability

Authenticity

Accountability

Safety



# Cyber security key concepts

## Assets

- Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

# Cyber security key concepts

## Vulnerability

- a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability

## Cyber Threat

- any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

## Attack

- The realization of some specific threat that impacts the confidentiality, integrity, accountability, or availability of a computational resource.



# Cyber security key concepts

**Threat Actor** (synonyms attacker, threat source, threat agent)

- person (or group) seeking to exploit potential vulnerabilities of a system

**Risk**

- the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

**Security controls** (synonyms safeguards or countermeasures)

- the management, operational, and technical controls prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data.



# References

NIST Glossary. Available at <https://csrc.nist.gov/glossary/>





# Fondamenti di Sicurezza e Privacy

## Cyber Threat Actors

Prof. Federica Paci



# Lecture Outline

- Type of threat actors
  - Cyber criminals
  - Hacktivists
  - Nation states
  - Insider Threats



*Who is behind the last cyber attacks ?*



# Who is behind a cyber attacks?

## Cybercriminals

- Interested in illegal profit
- Typical attacks
  - Malware e.g financial trojans
  - Ransomware
  - Data breaches
  - DDoS
- Attack vectors
  - Malware
  - Email
  - Botnet



# Who is behind a cyber attacks?

## Nation State

- Interested in
  - *high quality intelligence*
  - *sabotage activities*
  - *subversion e.g political election*
- Typical attacks
  - Malware
  - Data breaches
  - DDoS
- Attack vectors
  - Use sophisticated malwares and obfuscation techniques
  - Invest in zero-day exploits





# Who is behind a cyber attack?

## Hacktivists

- Motivated by
  - Political views*
  - Cultural/religion belief*
  - National Pride*
  - Terrorist Ideology*
  - Fun*
- Typical attacks
  - Web defacement
  - Leakage of confidential information
  - DDoS
- Attack vectors
  - Exploit kit
  - Email
  - Botnet






# Who is behind a cyber attacks?

## Insider Threats

- Legitimate access to valuable resources
- Intentional
  - Publish information on the web
  - Install a logic bomb
  - Steal and sell information
- Unintentional
  - Accidentally post a classified files
  - Visit websites with malware infecting the enterprise network







# Fondamenti di Sicurezza e Privacy

## Supply Chain Attacks

Prof. Federica Paci



# Lecture Outline

- Supply Chain Attacks
  - Lifecycle
  - Suppliers' and Customers' assets
  - Attack Techniques

# Learning outcomes

At the end of this session, you should be able to:

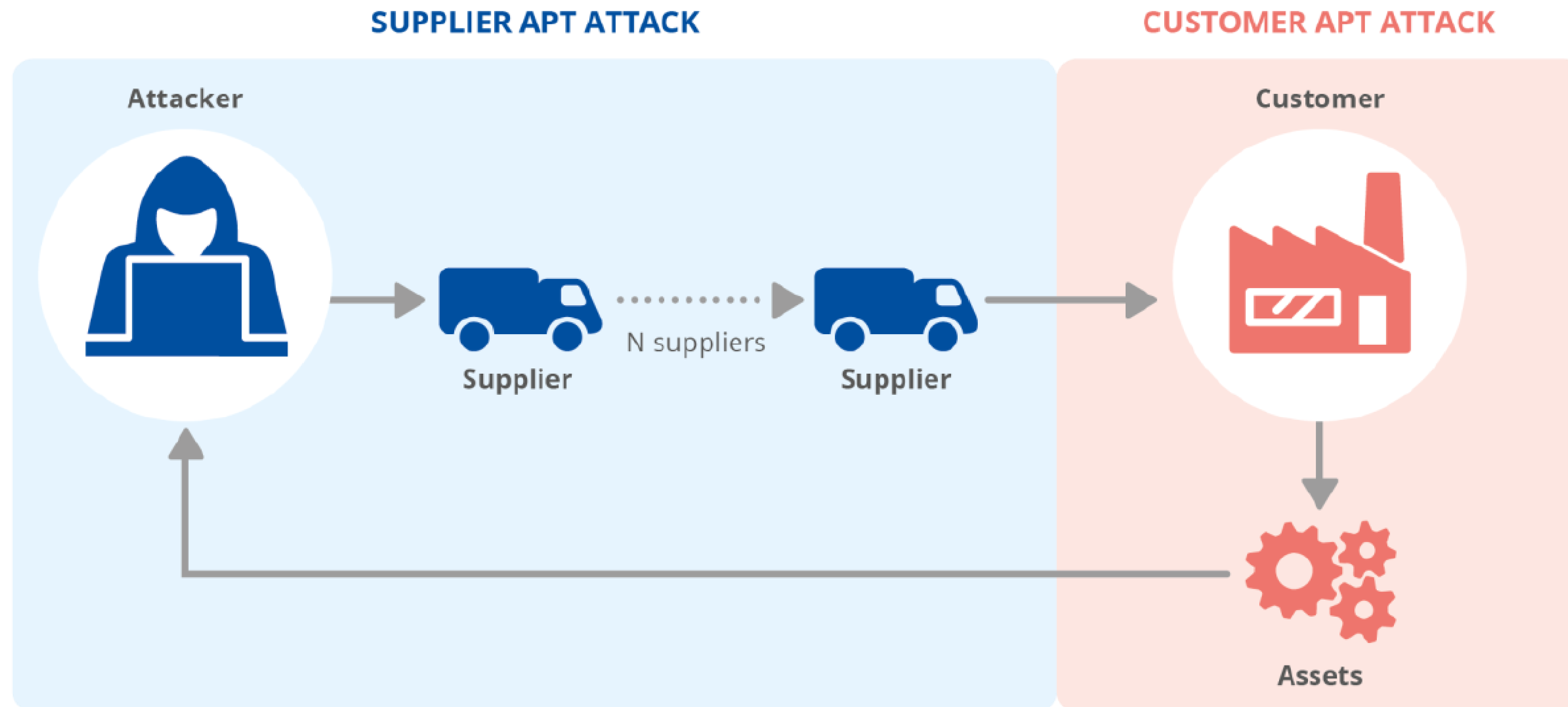
- Learn about supply chain attacks' life cycle
- Learn about supply chain attacks' assets
- Learn about supply chain attackers' techniques



# What is a supply chain?







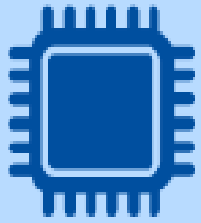

- Supply chain refers to the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product
- There are four key elements in a supply chain:
  - **Supplier:** is an entity that supplies a product or service to another entity
  - **Supplier Assets:** are valuable elements used by the supplier to produce the product or service
  - **Customer:** is the entity that consumes the product or service produced by the supplier
  - **Customer Assets:** are valuable elements owned by the target

# The Life Cycle

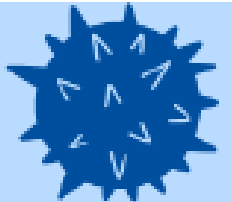


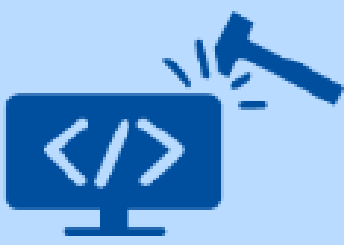








# Supplier Assets

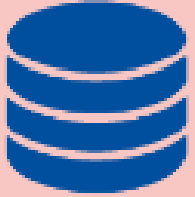

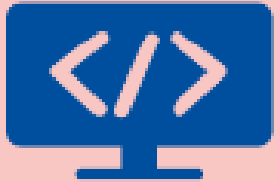

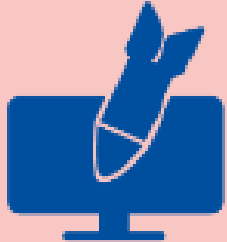


	<b>Pre-existing Software</b>	e.g. software used by the supplier, web servers, applications, databases, monitoring systems, cloud applications, firmware. It does not include software libraries.
	<b>Software Libraries</b>	e.g. third party libraries, software packages installed from third parties such as npm, ruby, etc.
	<b>Code</b>	e.g. source code or software produced by the supplier.
	<b>Configurations</b>	e.g. passwords, API keys, firewall rules, URLs.
	<b>Data</b>	e.g. information about the supplier, values from sensors, certificates, personal data of customers or suppliers themselves, personal data.
	<b>Processes</b>	e.g. updates, backups or validation processes, signing certificates processes.
	<b>Hardware</b>	e.g. hardware produced by the supplier, chips, valves, USBs.
	<b>People</b>	e.g. targeted individuals with access to data, infrastructure, or to other people.

# Supplier Attack Techniques Used

	<b>Malware Infection</b>	e.g. spyware used to steal credentials from employees.
	<b>Social Engineering</b>	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
	<b>Brute-Force Attack</b>	e.g. guessing an SSH password, guessing a web login.
	<b>Exploiting Software Vulnerability</b>	e.g. SQL injection or buffer overflow exploit in an application.
	<b>Exploiting Configuration Vulnerability</b>	e.g. taking advantage of a configuration problem.
	<b>Physical Attack or Modification</b>	e.g. modify hardware, physical intrusion.
	<b>Open-Source Intelligence (OSINT)</b>	e.g. search online for credentials, API keys, usernames.
	<b>Counterfeiting</b>	e.g. imitation of USB with malicious purposes.


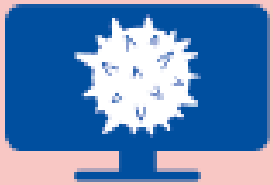

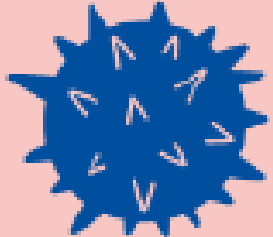




# Customer Assets

	<b>Data</b>	e.g. payment data, video feeds, documents, emails, flight plans, sales data and financial data, intellectual property.
	<b>Personal data</b>	e.g. customer data, employee records, credentials.
	<b>Software</b>	e.g. access to the customer product source code, modification of the software of the customer.
	<b>Processes</b>	e.g. documentation of internal processes of operation and configurations, insertion of new malicious processes, documents of schematics.
	<b>Bandwidth</b>	e.g. use the bandwidth for Distributed Denial of Service (DDoS), send SPAM or to infect others on a large scale.
	<b>Financial</b>	e.g. steal cryptocurrency, hijack bank accounts, money transfers.
	<b>People</b>	e.g. individuals targeted due their position or knowledge.

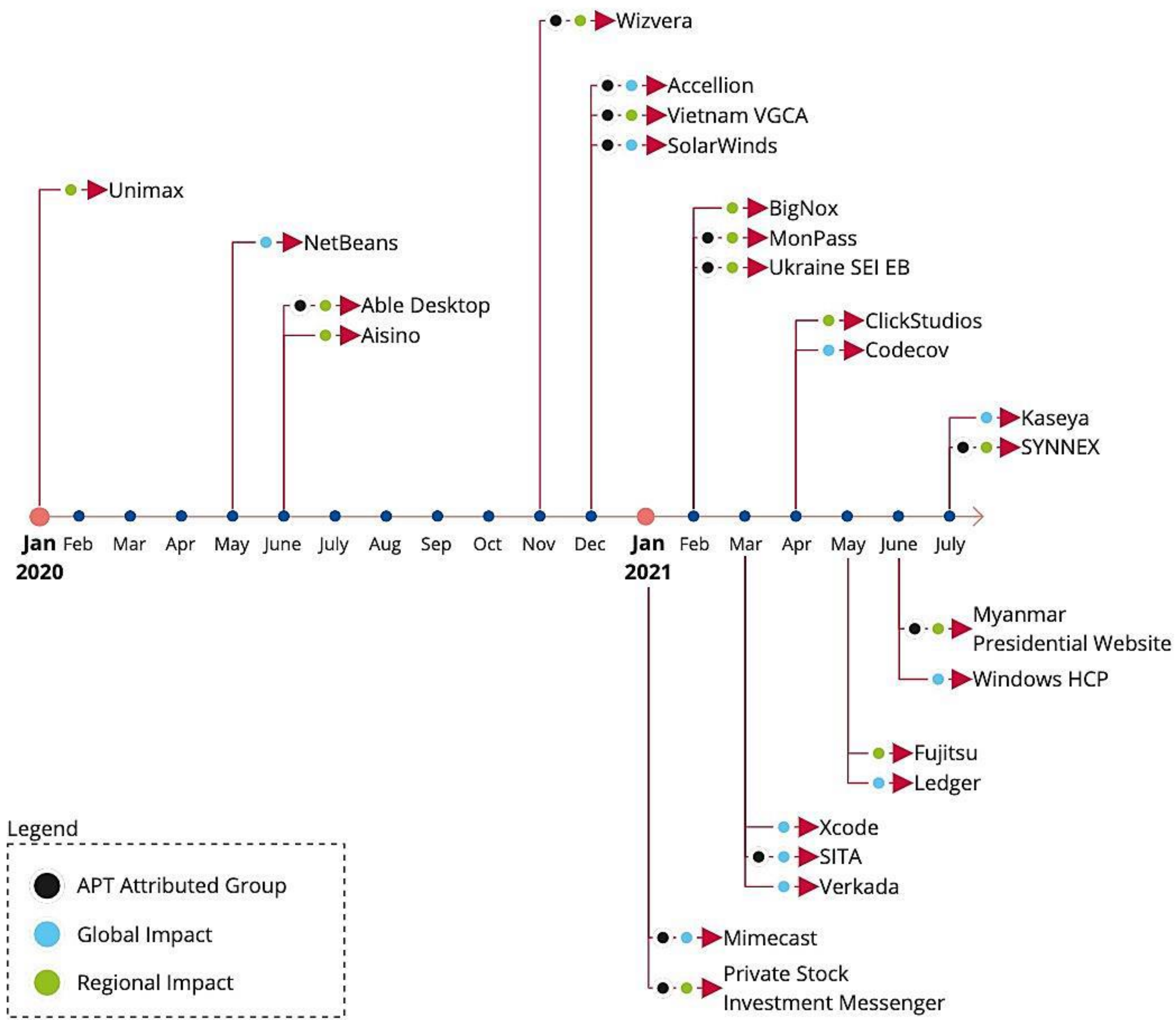


# Customer Attack Techniques

	<b>Trusted Relationship [T1199]</b>	e.g. trust a certificate, trust an automatic update, trust an automatic backup.
	<b>Drive-by Compromise [T1189]</b>	e.g. malicious scripts in a website to infect users with malware.
	<b>Phishing [T1566]</b>	e.g. messages impersonating the supplier, fake update notifications.
	<b>Malware Infection</b>	e.g. Remote Access Trojan (RAT), backdoor, ransomware.
	<b>Physical Attack or Modification</b>	e.g. modify hardware, physical intrusion.
	<b>Counterfeiting</b>	e.g. create a fake USB, modify a motherboard, impersonation of supplier's personnel.

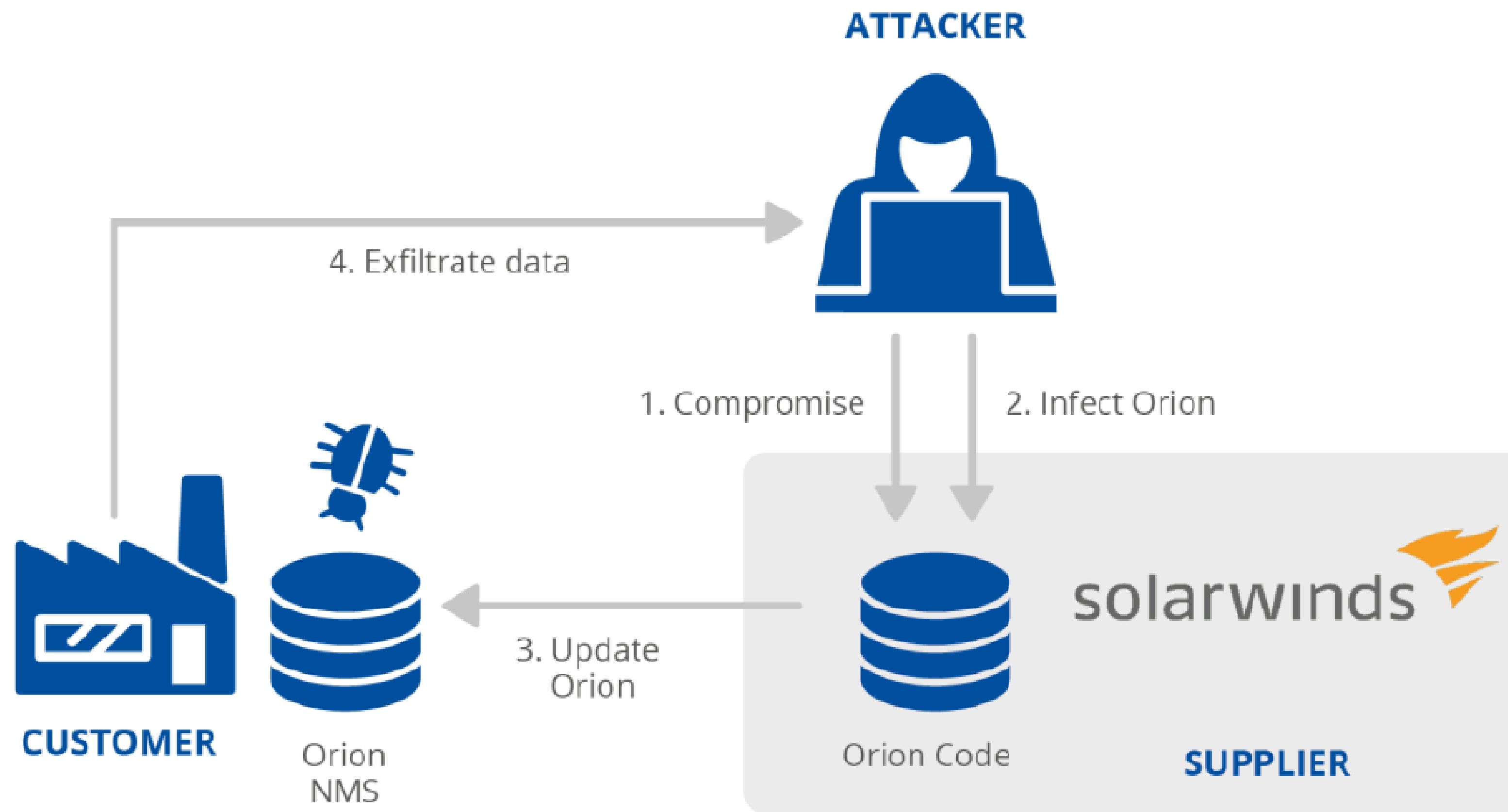


# Attack Timeline





# SolarWinds



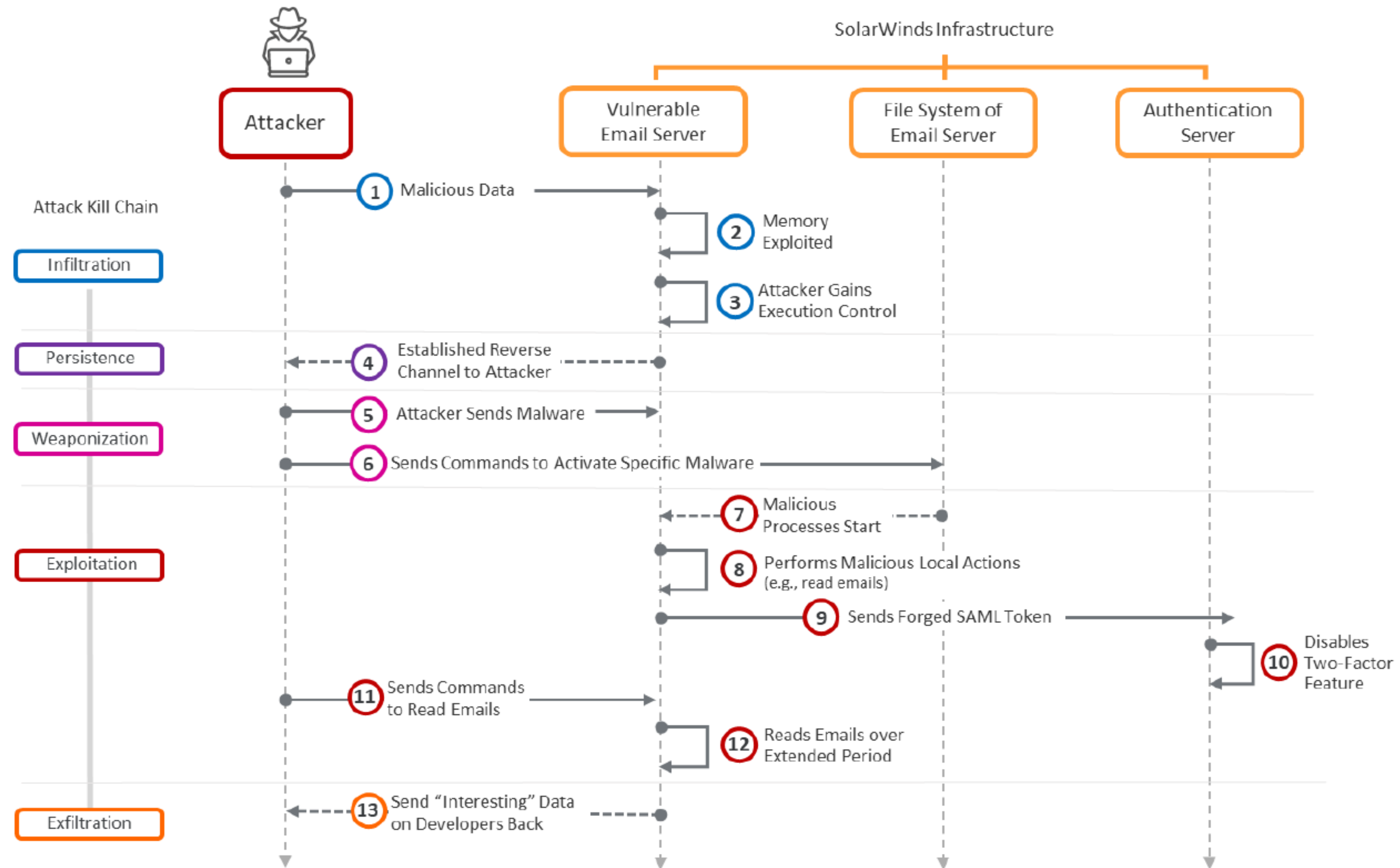
# Phases

Based on the above facts, the attack proceeded through these five stages:

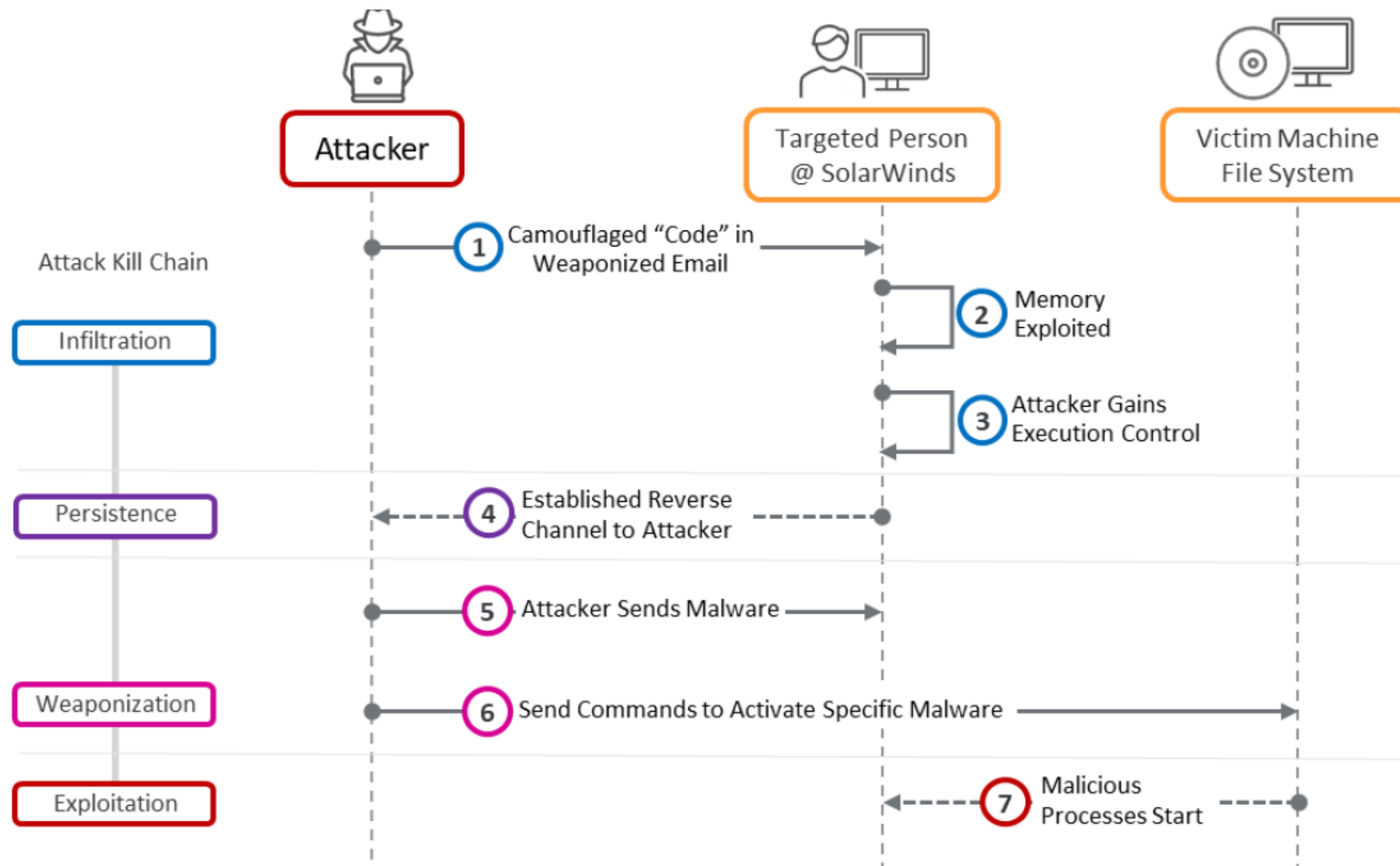
1. **Initial Infiltration:** Potential exploitation of an Authentication Service vulnerability. This allowed the attackers to persist in the victim enterprise and go on to examine email and develop a profile on the developers they needed to target
2. **Reconnaissance:** Launching of spear phishing campaign that targeted the developers of interest
3. **Spear Phishing:** Infecting the local compute instance of the targeted developers
4. **Weaponization** (Insertion of Backdoor): Manipulating the build system to insert their backdoor
5. **Infiltration of Downstream Users:** Abuse trust relationships to penetrate end-user's infrastructure



# Initial Infiltration

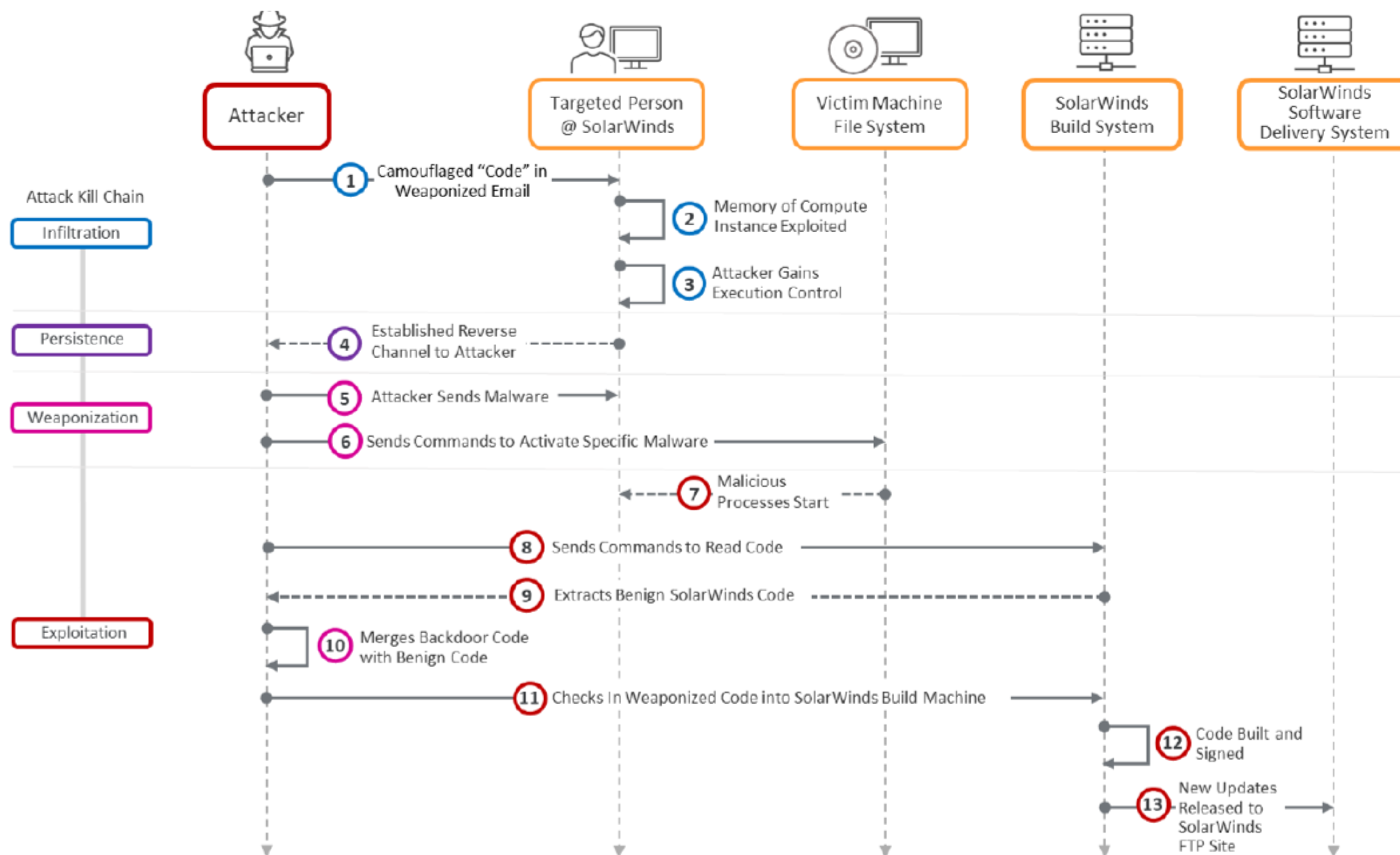


# Reconnaissance & Spear phishing

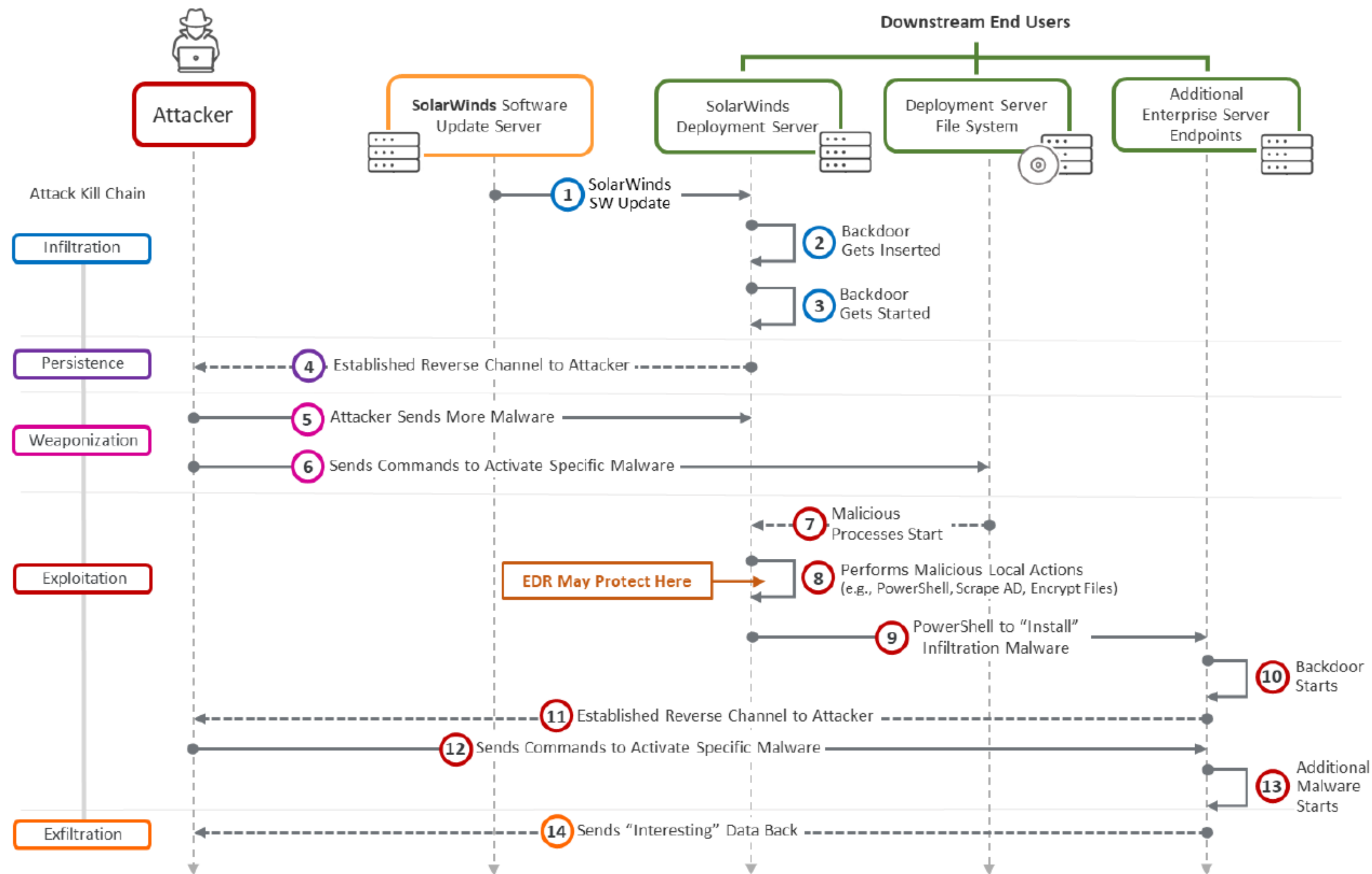




# Weaponization



# Infiltration of Downstream Users





# References

- VIRSEC - Taxonomy of The Attack on SolarWinds and Its Supply Chain
- ENISA – ENISA Threat Landscape for Supply Chain Attacks