Software Supply Chain Attacks

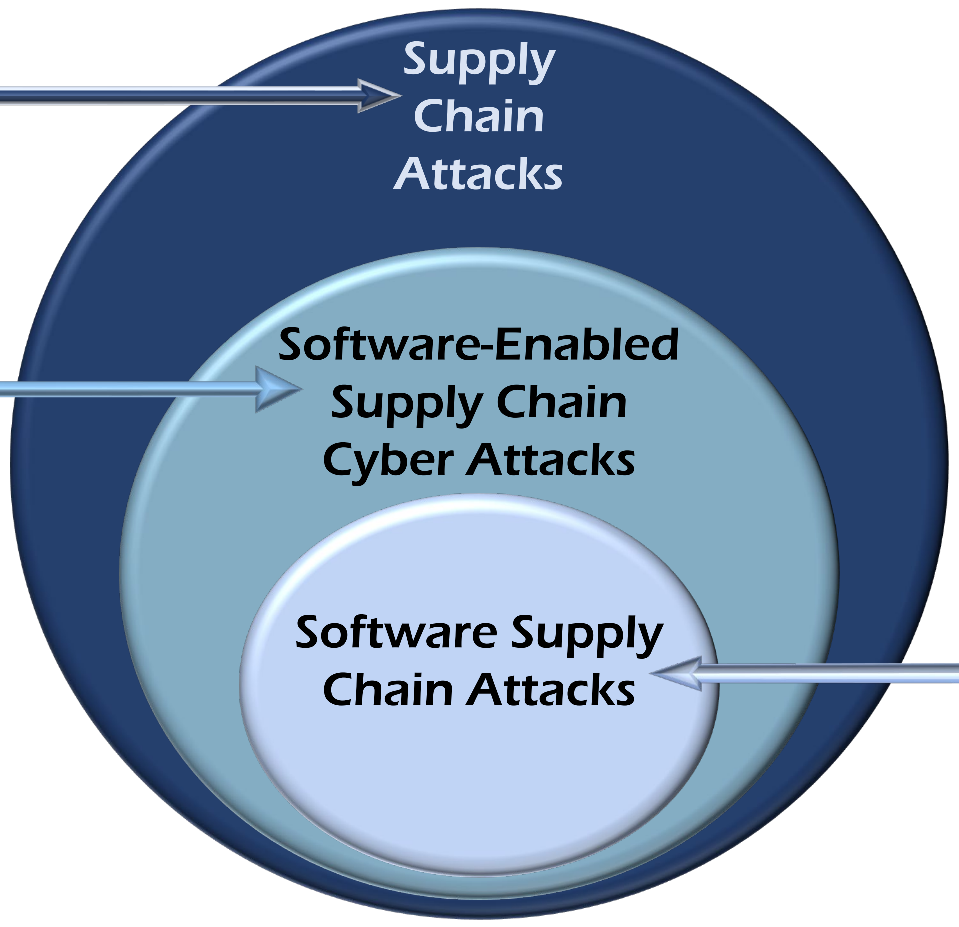
Adversaries may compromise software supply chains via cyber attacks, insider threats, or other malign activities at any stage of a product lifecycle to achieve access, enable espionage, conduct sabotage, or launch follow-on attacks against additional parties.

Supply Chain Attacks

All supply chain attacks combine two or more attacks: a malign actor first attacks at least one supplier within a supply chain and uses that attack as the means for attacking other suppliers or the final customer. Some supply chain attacks use cyber means to target one or more of the resources, processes, developers, or services along a supply chain to gain access to an underlying system or to induce downstream effects that are disruptive or damaging.

Software-Enabled Attacks
(Supply Chain Cyber Attacks)

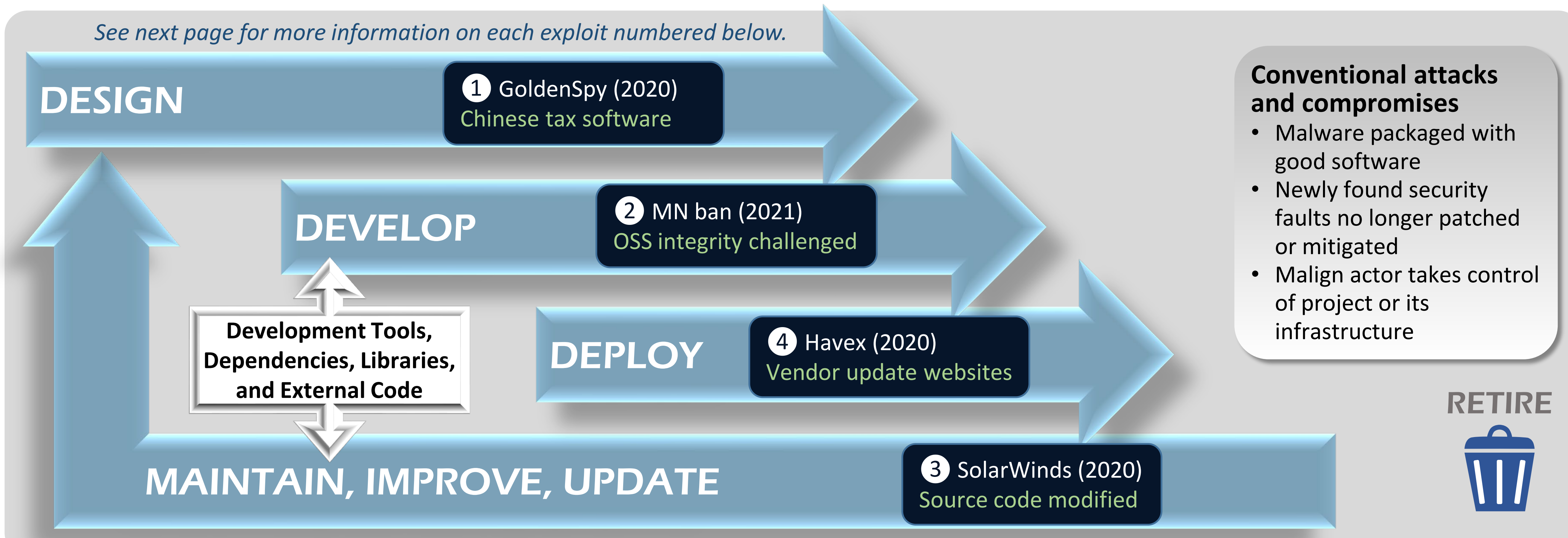
Software-enabled supply chain attacks typically exploit software vulnerabilities (Log4j, for example) to disrupt, disable, or destroy supply chain resources, processes, or services. They include a subset comprised of software supply chain attacks that target the design, development, deployment, or improvement of software itself.


Supply Chain Attacks
Software-Enabled Supply Chain Cyber Attacks
Software Supply Chain Attacks

Software Supply Chain Attacks

Software supply chain attacks are deliberate acts directed against the supply chains of software products themselves. These attacks enable subsequent adversarial actions against users of the software. Malign actors may attempt software supply chain attacks after infiltrating a software developer's networks, systems, personnel, or external resources. By compromising software or its dependencies, malign actors may surveil, disrupt, damage, or otherwise exploit the data or systems of those who use the software. Because these attacks against the supply chain of software are conducted to target the users of the software, software supply chain attacks are a subset of software-enabled supply chain cyber attacks.

See next page for more information on each exploit numbered below.



Conventional attacks and compromises

- Malware packaged with good software
- Newly found security faults no longer patched or mitigated
- Malign actor takes control of project or its infrastructure

Software supply chain attacks are possible through multiple vectors:

- Software supply chain attacks may use complex means to modify the source code of genuine programs by illicitly accessing a developer's infrastructure, but may also exploit the legitimate access possessed by a malicious insider.
- Adversaries may seek to exploit tools, dependencies, shared libraries, and third-party code or compromise the personnel or systems of associated developers or distributors.
- Like all supply chain attacks, software supply chain attacks consist of at least two thrusts: An attack against a supplier that then enables a subsequent attack against another supplier or the final target.
- Using software after it reaches end-of-life exposes users to conventional cyber attacks.

Dated: 21 April 2023

Software Supply Chain Attacks

Adversaries may compromise software supply chains via cyber attacks, insider threats, or other malign activities at any stage of a product lifecycle to achieve access, enable espionage, conduct sabotage, or launch follow-on attacks against additional parties.

Adversarial Objectives

Hackers target software supply chains to gain stealthy and persistent access to secured systems and networks. These attacks enable operations ranging from the targeting of specific victims to indiscriminate attacks on connected networks.

Improved cybersecurity postures across most networks and computers have made software supply chain attack vectors increasingly attractive because many software development and distribution channels lack sufficient protections. Adversarial access accomplished through software supply chain intrusions can be difficult for the software's end users to detect. Cyber operations supported by software supply chain attacks have included criminal activities, targeted information theft, data destruction, economic disruptions, and nation-state espionage.

Software Integrity

Software supply chain attacks are insidious because they erode confidence in the software providers that consumers rely upon for security updates. Contaminating software with malware during the development or deployment stages of the lifecycle makes it difficult to detect. For example, in 2020, security researchers discovered a backdoor dubbed ❶ GoldenSpy in tax software required by foreign companies doing business in China. In other cases, external attackers have hidden malware in unfinished software before developers added digital signatures, thereby imbuing compromised software with a presumption of trustworthiness. In other instances, attackers have injected malicious code through genuine updates and patches for software releases and upgrades, or have compromised servers used for delivering software updates, utilizing them to deliver malware to unsuspecting customers.

Authenticating Software Integrity

- **Code Signing:** Signed code includes a trusted, cryptographically secure indicator that verifies software has been approved by its developer and has not been subsequently modified.
- **Hashing:** Developers distributing software will often provide unique strings of information generated by hashing algorithms. Users can apply the same algorithms to verify software remains in its original state and has not been modified or corrupted**.**

…still subject to exploitation

- Malign actors can steal the cryptographic keys used to generate these security signatures, or compromise the development process before the software is completed, signed, or hashed.

Open-Source Software (OSS)

Open-Source Software (OSS) is widely available under licensing terms that ease its use and distribution. Because the underlying source code for OSS must remain freely available, OSS projects promote transparency and facilitate modifications. Many OSS projects accept contributions and modifications from loosely affiliated, effectively anonymous programmers. Despite concerns about its vulnerabilities, OSS code remains ubiquitous and essential to computing devices and networks worldwide. Easy access to OSS can also expedite the discovery and remediation of vulnerabilities. In 2021, developers of the Linux kernel determined proposed updates provided by University of Minnesota (UMN) researchers deliberately included security flaws. In response, the Linux kernel development team ❷ banned UMN in its entirety from future contributions outright.

The exponential growth of OSS projects steadily expands the potential attack surface, making code audits increasingly challenging. The number of public repositories hosted by popular software development and source code management platform GitHub exploded from 46,000 in February 2009 to more than 200,000,000 by February 2022. Increased corporate codebase contributions and greater funding for audits, eliminating bugs, and supporting developers would enhance the OSS community and its software that saturates all aspects of the modern world .

Attribution

The complexity of software supply chain attacks and the resources necessary to accomplish them often implicate state actors. However, assigning culpability to specific national intelligence services can be challenging.

- In July 2020, a federal grand jury indicted two hackers working with China's Ministry of State Security (MSS) for a global computer intrusion campaign targeting intellectual property and confidential business information.
- In April 2021, the United States announced new economic sanctions directed against Russian technology companies for their role in Russian malicious cyber activities, including the ❸ SolarWinds Orion software supply chain attack. Publicly disclosed in December 2020, the source code compromise of the SolarWinds Orion infrastructure monitoring platform is among the most significant software supply chain attacks impacting the United States to date.
- In March 2022, the Department of Justice unsealed two indictments charging four Russian nationals who worked for the Russian government with orchestrating hacking campaigns that included hiding ❹ Havex malware inside legitimate software updates for industrial control systems used by the energy sector.

Note: The information presented herein is derived from public sources. Please visit https://www.odni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats *for more supply chain information.*

Dated: 21 April 2023