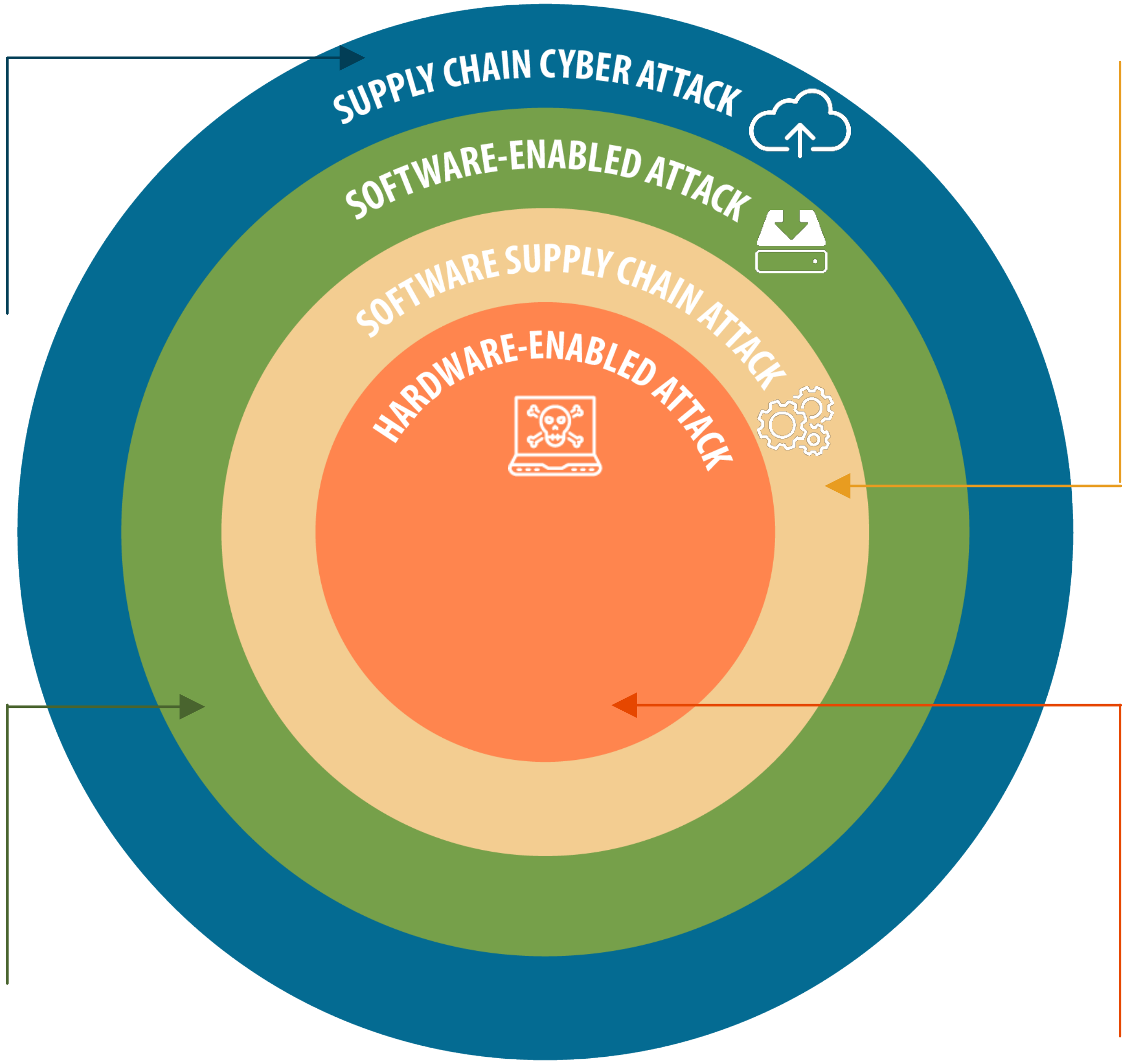
2022-04-01

National Counterintelligence and Security Center

Cyber Attacks on the Information Communications Technology Supply Chain – Defined

What Are the Differences?



SUPPLY CHAIN CYBER ATTACK

Is an attack using cyber means to target one or more of the resources, processes, developers, or services of a supply chain and thereby achieves access to the underlying system or induces effects that are disruptive or damaging.

Software-Enabled Attack

Software-Enabled Supply Chain Attacks typically exploit software vulnerabilities to disrupt, disable, or destroy supply chain resources, processes, or services. These are distinct from the Software Supply Chain Attack subset that targets the design, development, delivery, or improvement of software itself.

Software Supply Chain Attack

A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system. Software Supply Chain Attacks are a subset of Supply Chain Cyber Attacks. They are attacks against the supply chain of piece of software itself.

Hardware-Enabled Attack

By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system. Hardware backdoors may be inserted into various devices, such as servers, workstations, network infrastructure, or peripherals.

Note: Information contained herein represents the most reliable sources found in the public domain for this topic. When available, documents were used from the Cybersecurity and Information Security Agency, the National Institute of Standards and Technology, and other recognized, authoritative, commercial sources. Additional details are available at the following resources:

- Defending Against Software Supply Chain Attacks; https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
- NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- MITRE ATT&CK T1195 - https://attack.mitre.org/techniques/T1195

2022-04-01

National Counterintelligence and Security Center

Attack with Software or Attack on Software?

Software-Enabled Attack

Log4j is an open-source logging utility discovered in 2021 to contain a remote-code execution (RCE) vulnerability. The default configuration of Log4j2 allows attackers to coax the program into loading and running malware of the attacker's choosing. Designated LOG4SHELL (CVE-2021-44228), the ease of creating exploits coupled with widespread use of Log4j makes LOG4SHELL one of the most serious cyber vulnerabilities ever discovered.

Log4j
2021

LOG4J

V.

Software Supply Chain Attack

Russia's Foreign Intelligence Service (SVR) exploited access to SolarWinds' software development operations to modify SolarWinds' source code for its Orion network management software. SVR inserted malicious code in an automatic software security update impacting 18,000 government and private users. SVR used the code to conduct malicious follow-on activity, including installing malware for an espionage campaign against targeted U.S. federal agencies and 100 private-sector companies.

SolarWinds
2020

solarwinds

A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system, like the SolarWinds software supply chain attack. In contrast, software-enabled supply chain attacks use an existing software vulnerability to exploit the customer's data or system, like the LOG4SHELL vulnerability. Either way, software attacks or attacks with software leave an organization exposed to malicious cyber activities including cyber espionage and IP theft. For additional information on how to defend against these attacks, please see Defending Against Software Supply Chain Attacks (April 2021), a Joint publication by Department of Homeland Security (DHS) Cyberspace and Infrastructure Security Agency (CISA) & Department of Commerce National Institute of Standards and Technology (NIST).