Supply Chain Attacks

Overview:

Supply chain attacks have become a major cybersecurity threat, targeting vulnerabilities in complex networks of interconnected businesses and vendors. Attackers exploit these vulnerabilities to compromise legitimate software, networks, and hardware, often with devastating consequences.

statistics

The global annual cost of software supply chain attacks is expected to reach $138 billion by 2031, up from $46 billion in 2023.
Software Supply Chain Attacks To Cost The World $60 Billion By 2025.

Prevalence:
98% of organizations experienced data breaches through third-party vendors in 2023.
The mean number of supply chain breaches rose from 3.29 incidents in 2022 to 4.16 incidents in 2023.

Impact:
The Royal Mail ransomware attack in 2023 crippled postal delivery for over a month.
The MOVEit attack exposed sensitive data from numerous organizations.
The 3CX attack compromised endpoint clients with malicious code.

reference:
Notable Recent Supply Chain Attacks:
https://cyberint.com/platform/supply-chain-intelligence/
Supply chain trends, critical infrastructure & cyber security in 2024:
https://www.thefastmode.com/market-trends/33799-5-cybersecurity-trends-for-2024-according-to-ntt
Is Software Supply Chain The Biggest Security Threat Of 2024?:
https://accelerationeconomy.com/cybersecurity/why-and-how-the-software-supply-chain-is-increasingly-under-threat/