

A Brief History of Supply Chain Attacks in the News





Here's a quick
breakdown of the most
impactful supply chain
attacks over the last
decade or so.





2011

RSA Security

Threat actors compromised RSA's "seed warehouse" for SecurID tokens and gained access to other systems leveraging the tokens.



2013

Target

Hackers compromised Target's server and placed malware on POS devices across their entire store network.



MARCH 2017

CCleaner

Attackers breached Piriform via stolen TeamViewer credentials. ShadowPad malware was used to infect software distribution systems.



2019

ASUSTek Computer

ASUS Live Update Utility service delivered malware to 1000s of customers and impacted up to 500,000 computers.



DECEMBER 2020

SolarWinds

SUNBURST malicious code was deployed by Solar Winds official updates, impacting 18,000+ customers.



JULY 2021

Kaseya

Kaseya VSA software was used to deliver ransomware, compromising approximately 1,500 customers. Russian-linked REvil took credit demanding a \$70M ransom.



Learn More at s1.ai

