Supply Chain Attack

The attackers insert malware in the update process of one of your key enterprise management tools. This gives them direct access to the heart of your infrastructure.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

SUNBURST
SUPERNOVA

https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers

https://www.wired.com/story/russia-solarwinds-hack-roundup

Backdoors™ & Breaches

INITIAL COMPROMISE

Created by: BLACK HILLS | Information Security