Veille technologique : Cyberattaque SolarWinds (Sunburst)

En décembre 2020, l'éditeur américain SolarWinds a révélé avoir été victime d'une cyberattaque majeure ciblant son logiciel de supervision Orion. Les attaquants, liés au groupe étatique russe APT29, ont compromis l'environnement de développement de SolarWinds et injecté un malware nommé Sunburst dans des mises à jour officielles, signées et distribuées à plus de 18 000 organisations dans le monde.

Une fois installé, le malware restait discret plusieurs jours avant d'établir une communication chiffrée avec des serveurs de commande. Il permettait ensuite vol de données, exécution de commandes et infiltration de réseaux gouvernementaux américains, d'entreprises technologiques et de structures critiques. L'opération visait l'espionnage à grande échelle via la compromission de la chaîne d'approvisionnement logicielle.

Cette attaque a souligné la vulnérabilité des environnements de build, l'importance de la vérification des mises à jour logicielles et la nécessité d'une meilleure transparence sur les composants logiciels (ex. SBOM). Elle reste aujourd'hui l'une des attaques de supply-chain les plus marquantes de la décennie.

https://www.solarwinds.com/sa-overview/securityadvisory

https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-005/