ZERO TRUST ARCHITECTURE

BeCode - El Khattouti Bilalle

SolarWinds

Société

américaine spécialisé dans le développement de logiciel permettant la gestion des réseaux, systèmes et infrastructure informatique.

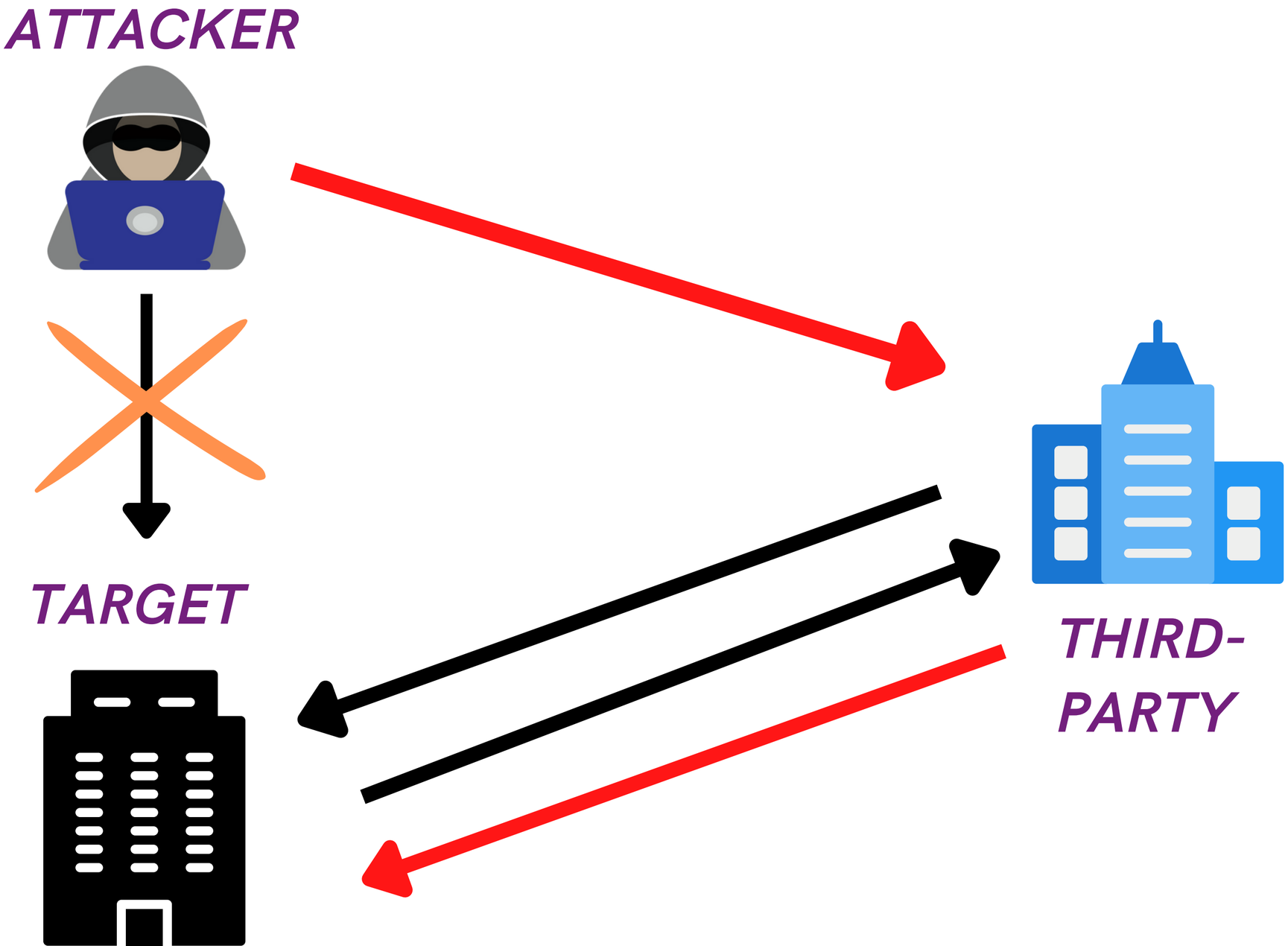
Cyberattaque

découverte en décembre 2020.
 Les hackers on utilisé l'exploit Sunburst : contamine les victimes avec une mise à jour du software Orion. Ce dernier permet le monitoring et parfois même l'accès à des routers, firewalls, etc.

Collaborant

avec 425 des 500 plus grosses entreprises des Etats-Unis, les 10 plus gros Telecom et notamment des organismes d'états.

Supply Chain Attack



Protéger

Protéger

Protéger

Protéger

Protéger

Protéger

Zero Trust

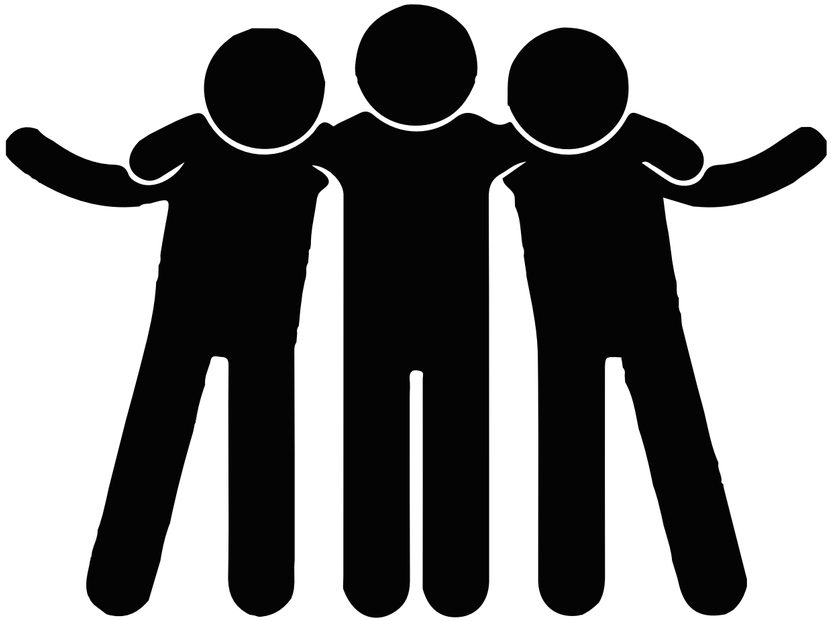
"Never trust, always verify"

Ne pas faire confiance en nos dispositifs de sécurité

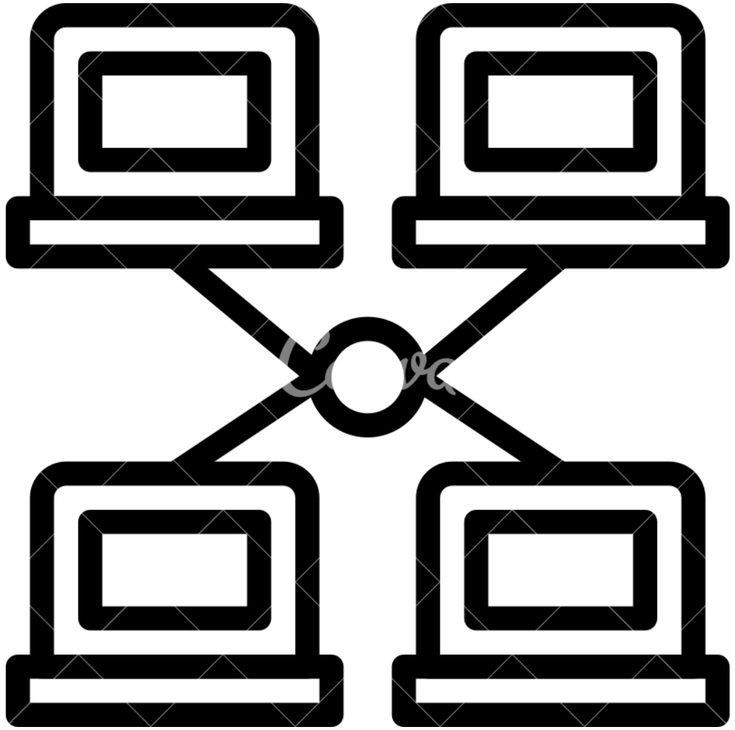
Contexte en évolution : cloud (hybrid/full), télétravail, etc.

Zero Trust

"Never trust, always verify"



≠



Zero Trust Principles

Secure access

- Identifié, autorisé, vérifier
- Considérer chaque utilisateur, machine ou app comme potentiellement dangereux

Log everything

- Tout le trafic doit être enregistré sous forme de log et inspecté à différents moments

Zero Trust Principles

Assume breach

- Considérer que le danger est déjà présent

Verify then trust

- Vérifier le plus souvent possible

Least privilege

- Donner les accès minimaux à un compte qui lui permettent de faire son travail

SolarWinds + Zero Trust = ?

La stratégie ou le modèle zero trust n'est pas, comme on peut s'y attendre, une solution miracle mais aurait permis de réduire l'impact.

Stratégie marketing ?

En tout cas, ce modèle se popularise avec de grands noms comme IBM, Cloudflare ou Microsoft.

solarwinds123

Thanks !

LUKE, I AM YOUR FATHER
I WANT TO BELIEVE
YOU BUT: ZERO TRUST MODEL
imgflip.com

I SEE SECURITY RISKS
EVERYWHERE

Ressources

- https://www.securityroundtable.org/the-solarwinds-hack-why-we-need-zero-trust-more-than-ever/
- https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
- https://www.tcg.com/blog/the-solarwinds-hack-and-zero-trust-architecture/
- https://www.wsj.com/articles/solarwinds-microsoft-hacks-prompt-focus-on-zero-trust-security-11619429402
- https://info.techdata.com/rs/946-OMQ-360/images/Preserve%20customer%20privacy.pdf
- https://www.youtube.com/watch?v=yn6CPQ9RioA
- https://www.youtube.com/watch?v=lT11tGaEC3s
- https://www.extremetech.com/computing/318430-security-researcher-solarwinds123-password-left-firm-vulnerable-in-2019