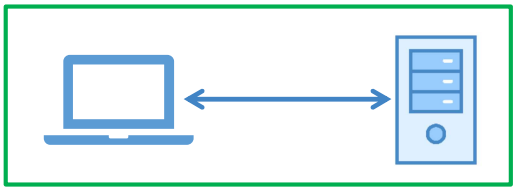
Sécurité des Réseaux

Dr Salim Benayoune

Contenu

- Introduction à la sécurité des SI
  - Notions de base et définitions
- La sécurité des réseaux
  - Les attaques sur les réseaux
  - La méthodologie d'attaque réseau
- Sécurisation des réseaux
  - Parefeux et Architecture sécurisée
  - Proxy et IDS
  - Les VPN
- La sécurité des systèmes
  - Normes et durcissement
  - Les malwares et les techniques virales

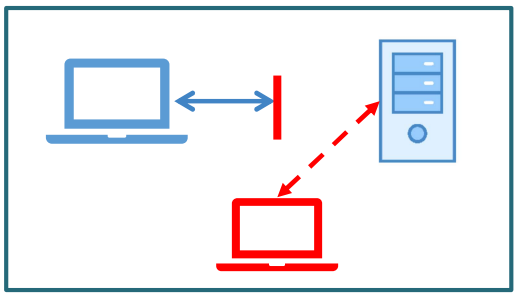
Les attaques réseaux



Connexion Sécurisée

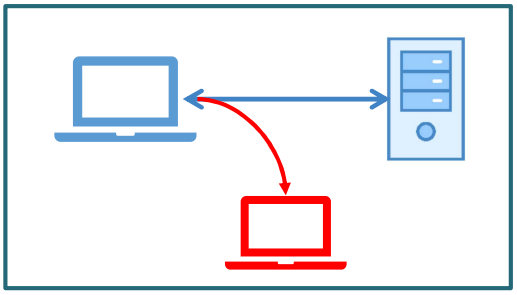
Interruption

Disponibilité

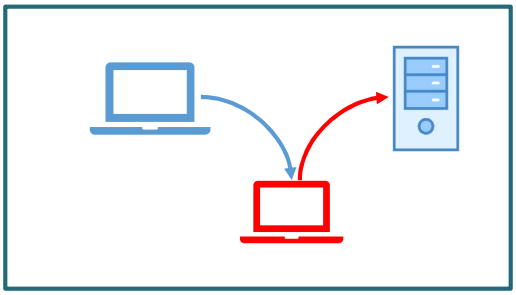


Interception

Confidentialité

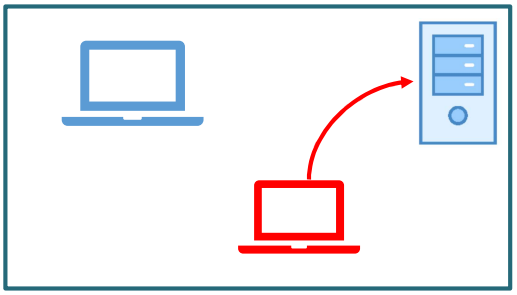


Intégrité



Modification

Authenticité



Fabrication

Les attaques réseaux : classification

Attaques

Passives

Actives

Ecoute

Analyse du trafic

Mascarade

Rejeu

Déni de Service

Modification de message

Les attaques réseaux : Ecoute sur réseaux sans fil

- Canal sans fil en diffusion
- Nécessite un matériel spécial :

  - **ALFA NETWORK AWUS1900**

- Utiliser WPA2 ou WPA3

Les attaques réseaux : Ecoute sur réseaux filaires

- **Les switchs ne font pas de diffusion pour le trafic unicast**
- **Solutions pour capturer le trafic :**
  - **MAC spoofing** (outil macchanger)
  - **ARP spoofing** ou **ARP cache poisoning** : envoi de messages ARP falsifiés afin de changer la table ARP ou MAC du switch, voire même le routage.
  - **MAC flooding** : transformer le **switch** en **hub**
  - Changement frauduleux de la configuration du commutateur
  - **STP attack**

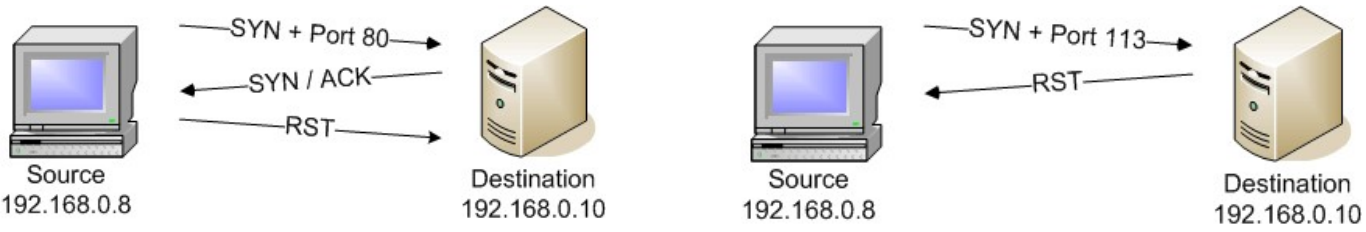
```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

Les attaques réseaux : Techniques de Scan

- Envoyez le paquet SYN et attendez la réponse :
  - SYN+ACK
    - Le port est ouvert
    - Envoyer RST pour fermer la connection
  - RST
    - Le port est fermé



  - Avantage : ne crée jamais une connexion TCP, donc moins susceptibles d'être enregistrées ou bloquées
  - Inconvénient : nécessite un privilège root (**Raw socket**)

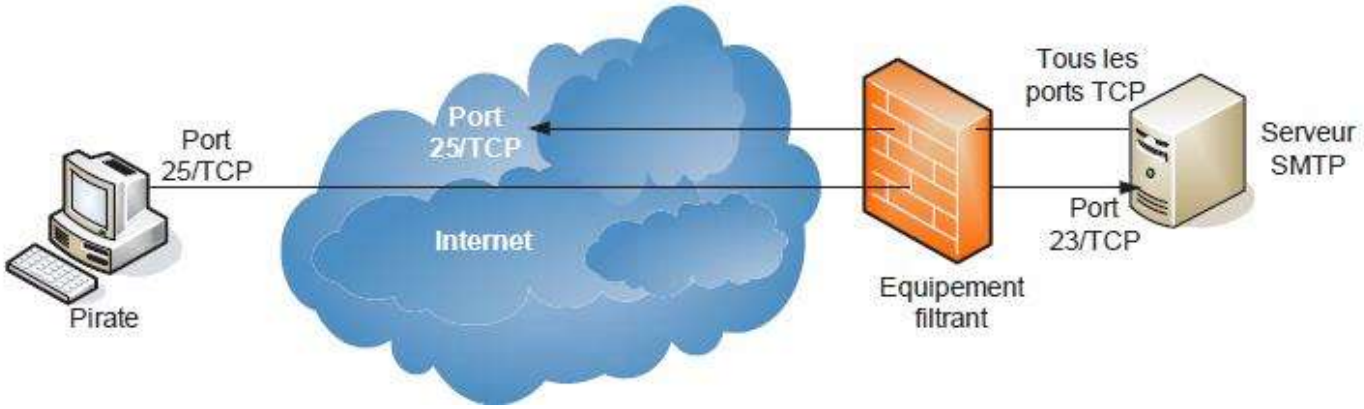
Les attaques réseaux : Techniques de Scan

1. TCP connect() scan
2. TCP SYN scan
3. TCP FIN scan
4. TCP Xmas scan
5. TCP Null scan
6. TCP ACK scan
7. Fragmentation Scan
8. FTP bounce scan
9. Idle Scan
10. UDP scan

Exercice : Comparer ces différentes techniques

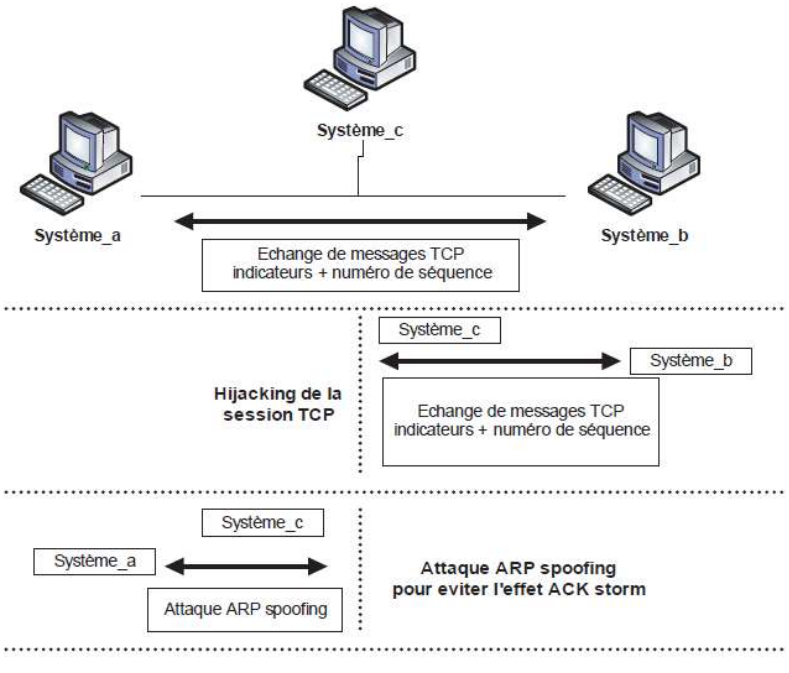
Les attaques réseaux : Techniques de Scan

- Traversée des équipements filtrants :
  - Fragmentation des paquets
  - Modification du port source



Les attaques réseaux : Mascarade (Spoofing)

- **Attaques permettant d'interférer avec une session réseau :** exploitant les faiblesses des mécanismes d'authentification
  - Vol de session TCP, token PHP, … etc

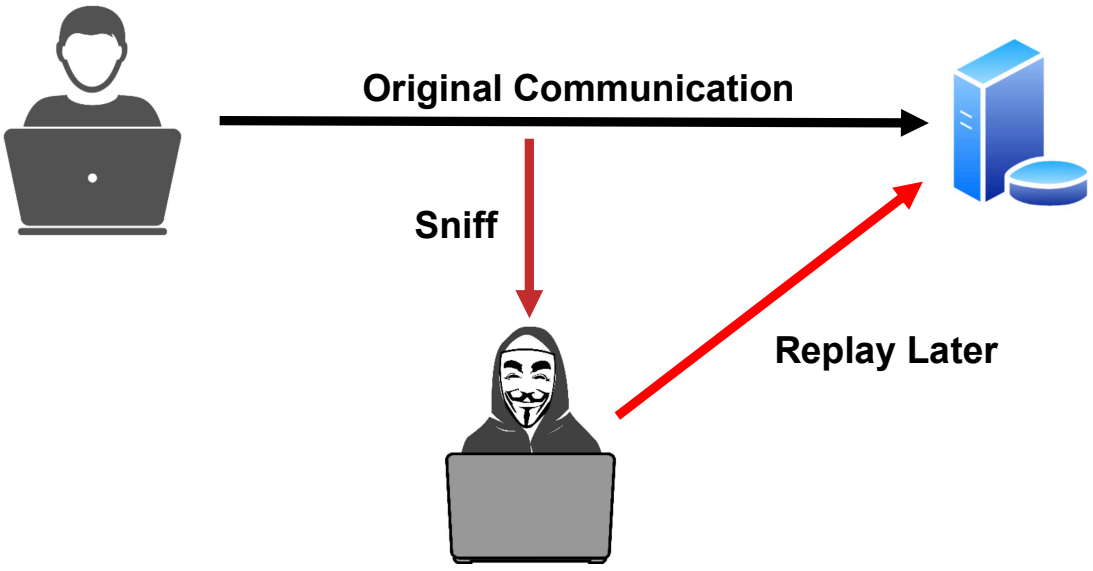


Les attaques réseaux : Mascarade

- Exemple : Attaque Kevin Mittnick (1994)

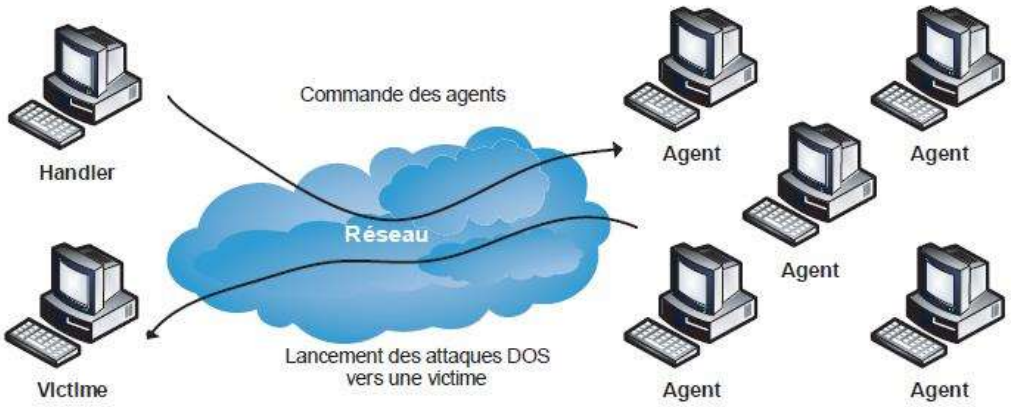
- **Exercice : Expliquer le déroulement de cette attaque**

Les attaques réseaux : Replay



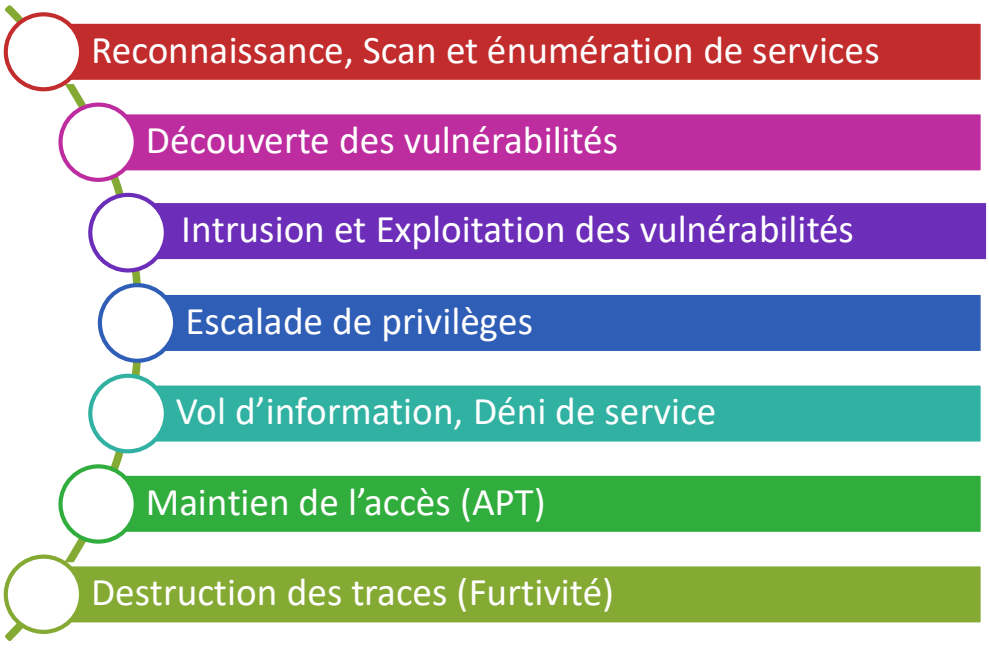
Les attaques réseaux : DoS

- **Attaques permettant de mettre le réseau en déni de service :**
  - Attaque par inondation (ping, SYN)
  - Attaque sur DNS
  - Distributed Denial of Service : DDoS



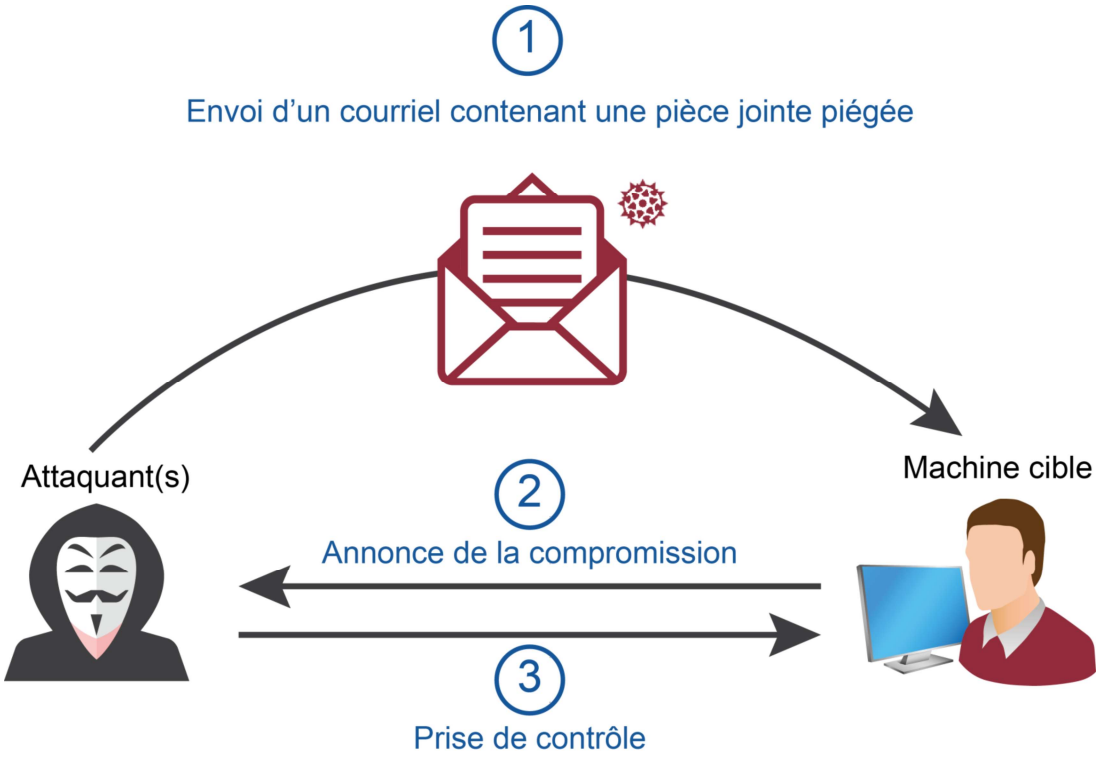
Les attaques réseaux

- Démarche de l'attaquant

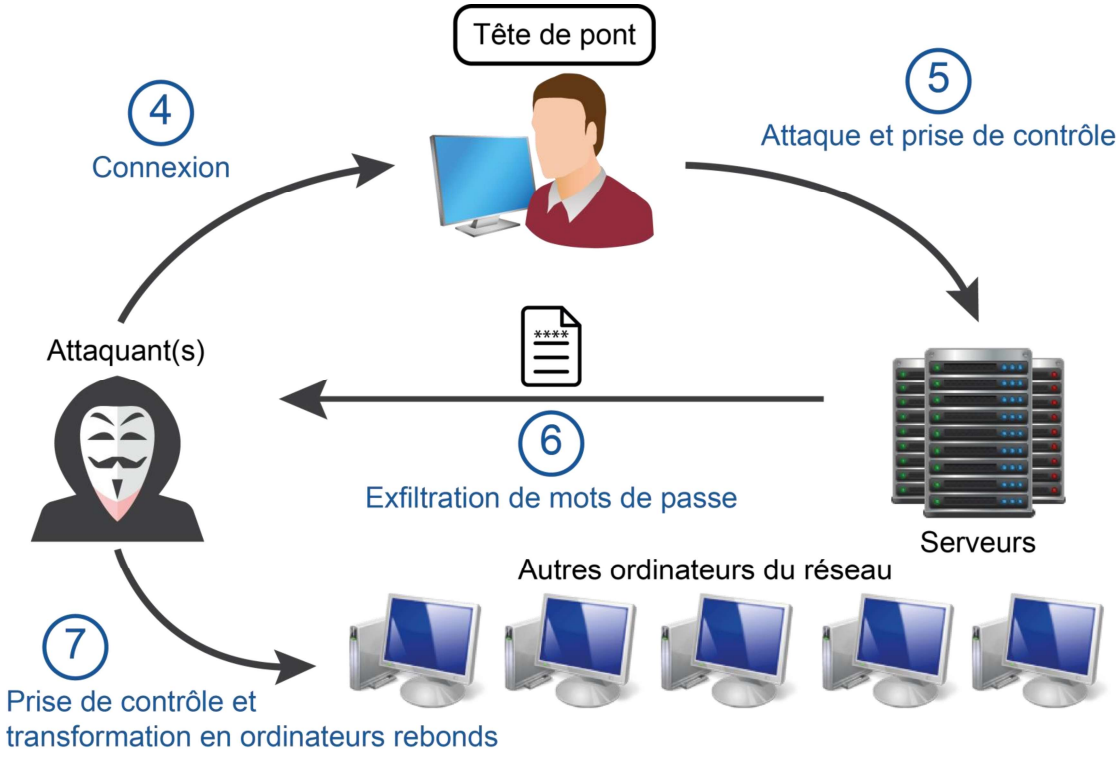


Les attaques réseaux : APT

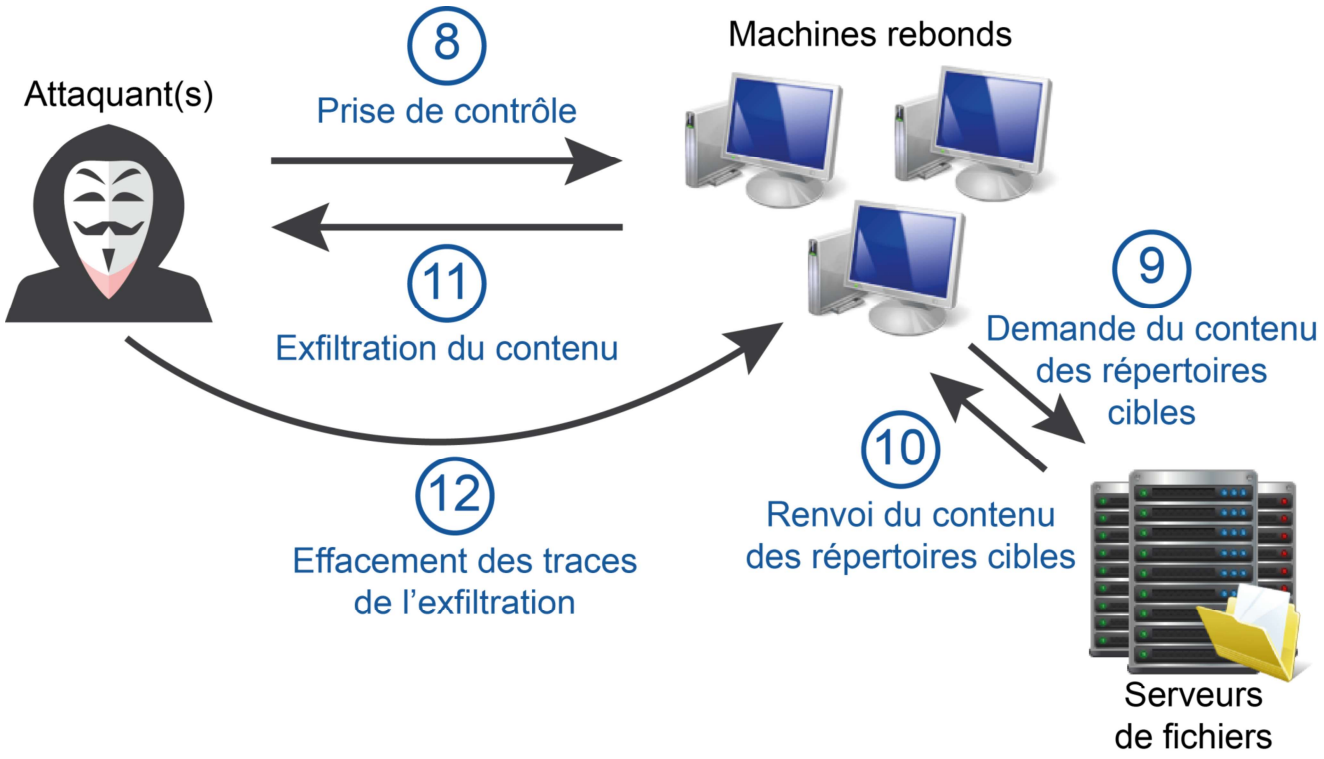
APT: Advanced Persistent Threat



Les attaques réseaux : APT



Les attaques réseaux : APT



Supply Chain Attack

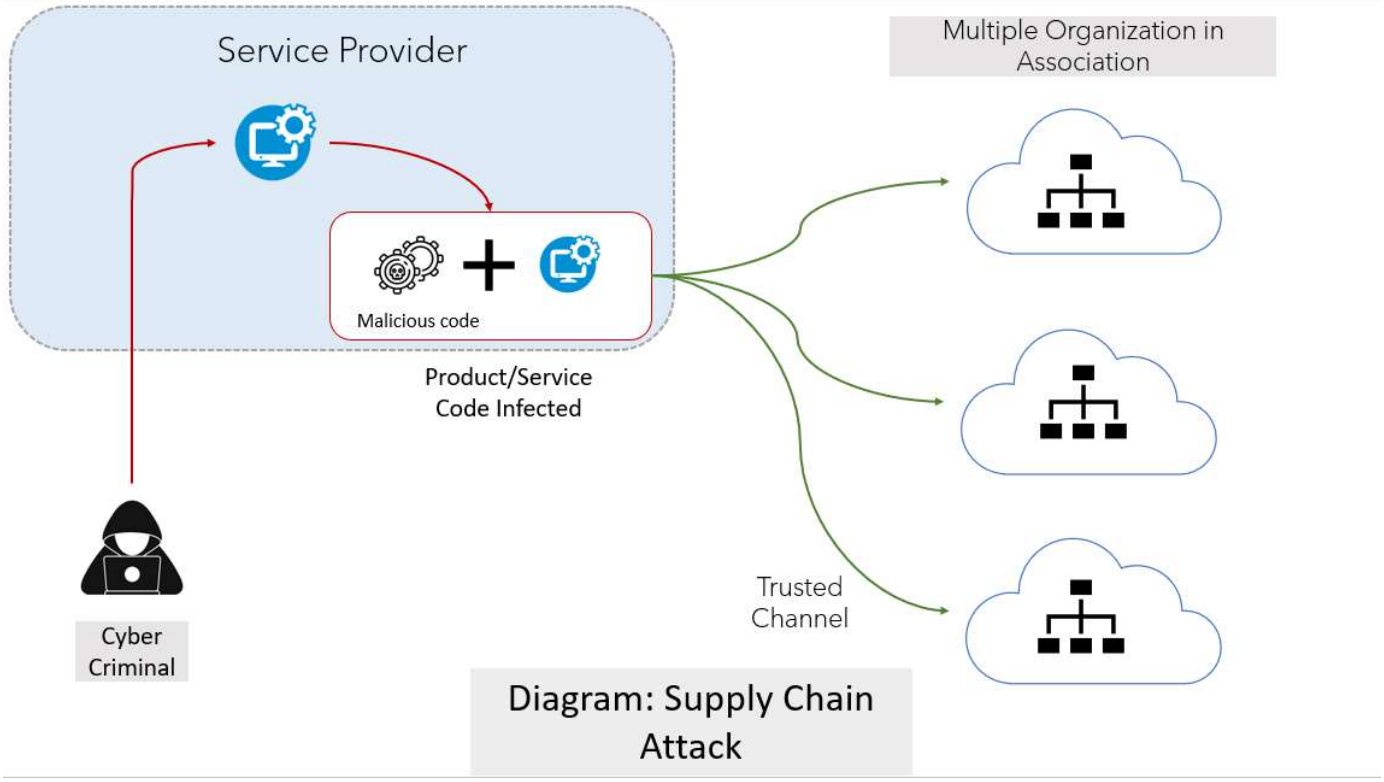


Diagram: Supply Chain Attack

Attaques et outils