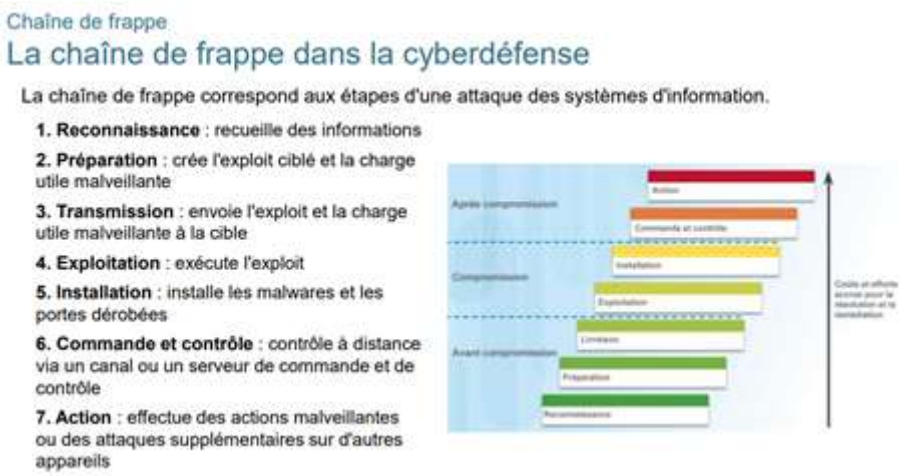
Cyber kill chain model

Cyber kill chain est un modèle de sécurité qui décrit les phases d'une cyberattaque. Une chaîne de destruction couvre toutes les étapes d'une violation de réseau, de la planification et de l'espionnage précoces à l'objectif final du pirate.

Comprendre les étapes d'une attaque permet aux entreprises de planifier les tactiques de prévention et de détection des intrus malveillants.



Le terme *« chaîne de destruction »* a une origine militaire. Le concept original définissait la structure d'une opération militaire et comprenait :

- L'identification de la cible.
- L'envoi de la force vers la cible.
- L'ordre de frapper la cible.
- L'élimination de la cible.

Les étapes d'une Chaîne De Destruction Cybernétique

Les sept phases de la cyber kill chain sont les différentes étapes d'une attaque réussie. Une équipe de sécurité a une chance d'arrêter les attaquants à chaque étape, mais une entreprise devrait idéalement identifier et arrêter les menaces dans la première moitié de la chaîne de cyber-attaque.

1. Étape 1 : Reconnaissance

L'attaquant recueille les informations nécessaires lors de l'étape de reconnaissance. Les pirates sélectionnent la victime, mènent des recherches approfondies sur l'entreprise et recherchent les points faibles du réseau cible.

Il existe deux types de reconnaissance :

- **Reconnaissance passive :** un pirate recherche des informations sans interagir avec la cible. La victime n'a aucun moyen de connaître ou d'enregistrer l'activité de l'agresseur.
- **Reconnaissance active :** un pirate obtient un accès non autorisé au réseau et interagit directement avec le système pour recueillir des informations.

Au cours de cette étape, les attaquants évaluent les aspects suivants d'un système :

- Vulnérabilités de sécurité et points faibles.
- La possibilité d'employer un complice initié.
- Outils, appareils, protocoles de vérification et hiérarchie des utilisateurs.

Elle fait appel à de nombreuses techniques et à des outils différents, ainsi qu'à des fonctions de navigation Web courantes, comme les :

- Moteurs de recherche
- Archives Web
- Services cloud publics
- Registres de noms de domaine
- Commandes WHOIS
- Renifleurs de paquets (Wireshark, tcpdump, WinDump, etc.)
- Mappages réseau (nmap)
- Commandes DIG, Ping
- Scanners de ports (Zenmap, scanner de ports TCP, etc.)

Mesures défensives pour la phase de reconnaissance :

- Installez des pare-feux pour renforcer la sécurité du périmètre.
- Surveillez les points d'entrée et les journaux des visiteurs pour détecter tout comportement suspect.
- Assurez-vous que les employés signalent les e-mails, appels et messages suspects sur les réseaux sociaux.
- Donner la priorité à la protection des individus et des systèmes qui sont des cibles privilégiées pour la reconnaissance.
- Limitez la quantité de données d'entreprise accessibles au public.

2. Étape 2 : Militarisation

L’équipe d’attaquants a trouvé un point faible dans le système et sait créer un point d’entrée. L’équipe criminelle conçoit maintenant un virus ou un ver pour cibler la faiblesse. Si les attaquants trouvent un exploit zero-day, ils travaillent généralement rapidement avant que la victime ne découvre et ne corrige la vulnérabilité.

Une fois que le logiciel malveillant est prêt, les pirates placent généralement le logiciel malveillant dans des documents ordinaires tels qu’un fichier PDF ou un fichier Office.

Les vecteurs d'attaque les plus courants sont les suivants :

- Identifiants volés ou avec un niveau de sécurité faible
- Services d'accès à distance (RDP, SSH, VPN)
- Employés négligents
- Attaques internes
- Chiffrement faible ou inexistant
- Mauvaise configuration du système
- Relations de confiance entre les appareils/systèmes
- Phishing (social engineering)
- Attaques par déni de service
- Attaques de type « Man-in-the-middle » (MITM)
- Chevaux de Troie (trojans)
- Attaques par injection SQL

Mesures défensives pour la phase de militarisation :

- Organisez une formation de sensibilisation à la sécurité pour aider les employés à reconnaître les tests de militarisation.
- Analysez les artefacts de logiciels malveillants pour vérifier les chronologies suspectes et les similitudes.
- Construire des outils de détection pour les militariseurs (outils automatisés qui associent les logiciels malveillants aux exploits).

3. Étape 3 : Livraison

Les criminels lancent l'attaque dans l'environnement cible. Les méthodes d'infection varient, mais les techniques les plus courantes sont :

- Périphériques USB infectés.
- Exploiter une faille matérielle ou logicielle.
- Comptes d'utilisateurs compromis.
- Un téléchargement intempestif qui installe des logiciels malveillants en plus d'un programme normal.
- Piratage direct via un port ouvert ou un autre point d'accès externe.

Le but de cette étape est de percer le système et de s'implanter en silence. Une tactique populaire consiste à lancer une attaque DDoS simultanée pour distraire les défenseurs et infecter le réseau sans alarmer les contrôles de sécurité.

Mesures défensives pour la phase de livraison :

- Protégez-vous des attaques de phishing.
- Utilisez les outils de gestion des correctifs.
- Signalez et examinez les modifications apportées aux fichiers et aux dossiers grâce à la surveillance de l'intégrité des fichiers (FIM).
- Surveillez les comportements étranges des utilisateurs, tels que les horaires ou les emplacements de connexion impairs.
- Exécutez des tests d'intrusion pour identifier les risques et les points faibles de manière proactive.

4. Étape 4 : Installation

Des logiciels malveillants se trouvent à l'intérieur du système et les administrateurs ne sont pas conscients de la menace. La quatrième étape de la cyber kill chain est l'installation du malware sur le réseau.

Une fois le logiciel malveillant installé, les intrus accèdent au réseau (c'est-à-dire une porte dérobée). Désormais, avec un accès ouvert, les intrus sont libres de :

- Installez les outils nécessaires.
- Modifier les certificats de sécurité.
- Créez des fichiers de script.
- Recherchez d'autres vulnérabilités pour mieux prendre pied avant de lancer l'attaque principale.

Garder leur présence secrète est essentiel pour les attaquants. Les intrus effacent généralement les fichiers et les métadonnées, écrasent les données avec de faux horodatages et modifient les documents pour qu'ils ne soient pas détectés.

Mesures défensives pour la phase d'installation :

- Maintenez les appareils à jour.
- Utilisez un logiciel antivirus.
- Configurez un système de détection d'intrusion basé sur l'hôte pour alerter ou bloquer les chemins d'installation courants.
- Effectuez une analyse régulière des vulnérabilités.

5. Étape 5 : Mouvement Latéral

Les intrus se déplacent latéralement vers d'autres systèmes et comptes sur le réseau. L'objectif est d'obtenir des autorisations plus élevées et d'atteindre plus de données. Les techniques standard au cours de cette étape sont :

- Exploiter les vulnérabilités des mots de passe.
- Extraction des identifiants.
- Cibler d'autres vulnérabilités du système.

Mesures défensives pour la phase de mouvement latéral :

- Mettez en œuvre la sécurité Zero Trust pour limiter la portée des comptes et des programmes compromis.
- Utilisez la segmentation du réseau pour isoler les systèmes individuels.

- Éliminer l'utilisation de comptes partagés.
- Appliquez les meilleures pratiques de sécurité des mots de passe.
- Auditez toutes les activités suspectes des utilisateurs privilégiés.

6. Étape 6 : Commandement Et Contrôle (C2)

Les logiciels malveillants complexes de niveau APT nécessitent une interaction manuelle pour fonctionner, de sorte que les attaquants ont besoin d'un accès au clavier à l'environnement cible. La dernière étape avant la phase d'exécution consiste à établir un canal de commande et de contrôle (C2) avec un serveur externe.

Les pirates atteignent généralement C2 via une balise sur un chemin de réseau externe. Les balises sont généralement

Si l'exfiltration de données est l'objectif de l'attaque, les intrus commencent à placer les données cibles dans des paquets pendant la phase C2. Un emplacement typique pour les bundles de données est une partie du réseau avec peu ou pas d'activité ou de trafic.

Mesures défensives pour la phase de commandement et de contrôle :

- Recherchez les infrastructures C2 lors de l'analyse des logiciels malveillants.
- Demander des proxys pour tous les types de trafic (
- Analysez en permanence les menaces.
- Réglez les systèmes de détection d'intrusion pour alerter sur tous les nouveaux programmes contactant le réseau.

La détection et la réponse gérées (MDR) offrent l'agilité nécessaire pour identifier et réagir aux cybermenaces en temps réel.

7. Étape 7 : Exécution

Les intrus prennent des mesures pour atteindre le but de l'attaque. Les objectifs varient, mais les buts les plus courants sont :

- Cryptage des données.
- Exfiltration de données.
- Destruction de données.

Juste avant le début d'une attaque, les intrus couvrent leurs traces en semant le chaos sur le réseau. L'objectif est de semer la confusion et de ralentir l'équipe de sécurité et d'investigation en :

- Effacement des journaux pour masquer l'activité.
- Suppression de fichiers et de métadonnées.
- Écraser les données avec des horodatages incorrects et des informations trompeuses.
- Modification des données vitales pour qu'elles paraissent normales même en cas d'attaque.

Certains criminels lancent également une autre attaque DDoS pour distraire les contrôles de sécurité lors de l'extraction des données.

Mesures défensives pour la phase d'exécution :

- Créez un manuel de réponse aux incidents qui décrit un plan de communication clair et une évaluation des dommages en cas d'attaque.
- Utilisez des outils pour détecter les signes d'exfiltration de données en cours.
- Exécutez des réponses immédiates des analystes à toutes les alertes.

Exemple De Cyber Kill Chain

L'exemple de cyber kill chain ci-dessous montre les différentes étapes auxquelles une équipe de sécurité peut détecter et empêcher une attaque de ransomware personnalisée :

- **Étape 1 :** Les pirates effectuent des opérations de reconnaissance pour trouver une faiblesse dans le système cible.
- **Étape 2 :** Les criminels créent un programme d'exploit ransomware et le placent dans une pièce jointe à un e-mail. Les pirates envoient alors un e-mail de phishing à un ou plusieurs employés.
- **Étape 3 :** Un utilisateur commet l'erreur d'ouvrir et d'exécuter le programme à partir de la boîte de réception.
- **Étape 4 :** Ransomware s'installe sur le réseau cible et crée une porte dérobée.
- **Étape 5 :** Le programme appelle l'infrastructure malveillante et informe l'attaquant de la réussite de l'infection.
- **Étape 6 :** Les intrus se déplacent latéralement dans le système pour trouver des données sensibles.
- **Étape 7 :** Les attaquants obtiennent le contrôle et le commandement et commencent à chiffrer les fichiers cibles.