Cryptojacking

1. Définition du Cryptojacking

Le **cryptojacking** est une cyberattaque dans laquelle un attaquant utilise de manière frauduleuse les ressources informatiques d'une victime (ordinateur, smartphone, serveur ou autre appareil connecté) pour miner des cryptomonnaies. Cette activité est effectuée à l'insu de la victime et consomme de l'énergie ainsi que des ressources matérielles, entraînant des ralentissements des systèmes, une augmentation des coûts et une usure prématurée des équipements.

2. Fonctionnement du Cryptojacking

1. **Infection par Logiciel Malveillant**
    - L'attaquant distribue un malware de cryptominage via des emails de phishing, des sites compromis ou des logiciels infectés.
    - Une fois installé, le malware utilise le processeur ou la carte graphique de l'appareil infecté pour miner des cryptomonnaies comme Bitcoin ou Monero.
2. **Scripts dans le Navigateur**
    - Certains attaquants injectent des scripts de cryptominage dans des pages web. Lorsqu'un utilisateur visite le site, le script utilise les ressources de son appareil pour miner, jusqu'à ce qu'il ferme la page.

3. Impacts du Cryptojacking

1. **Performance Dégradée**
    - Les appareils touchés fonctionnent plus lentement, car leurs ressources sont monopolisées par le processus de minage.
2. **Usure Matérielle**
    - Une utilisation intensive et continue des ressources matérielles (CPU, GPU) peut réduire la durée de vie des équipements.
3. **Consommation d'Énergie Élevée**
    - Les appareils affectés consomment davantage d'énergie, entraînant une augmentation des coûts d'électricité, particulièrement pour les entreprises.
4. **Risque de Surcharge**
    - Dans les environnements critiques (comme les serveurs), l'excès de charge peut provoquer des interruptions de service.

4. Exemple Concret : CoinHive

- **Contexte** : CoinHive était un script légitime permettant de miner la cryptomonnaie Monero via des navigateurs web.
- **Problème** : Des attaquants ont détourné cette technologie en l'intégrant à des sites web compromis, sans le consentement des visiteurs.
- **Impact** : Des milliers de sites web ont été utilisés comme plateformes de cryptominage à l'insu des utilisateurs.

5. Détection des Signes de Cryptojacking

1. **Ralentissements Inexpliqués**
    - Les ordinateurs ou appareils fonctionnent plus lentement que d'habitude, même lorsqu'ils ne sont pas utilisés intensivement.
2. **Augmentation de la Température**
    - Les ventilateurs des appareils tournent fréquemment à pleine vitesse, indiquant une charge importante sur le processeur.
3. **Consommation Électrique Élevée**
    - Les factures d'électricité augmentent sans explication apparente.
4. **Processus Inconnus**
    - Surveillance des tâches révèle des processus inhabituels utilisant beaucoup de ressources.

6. Solutions pour Se Protéger Contre le Cryptojacking

1. **Installer un Antivirus et Antimalware**
    - Utilisez des logiciels de sécurité capables de détecter et de bloquer les scripts et malwares de cryptominage.
2. **Bloqueurs de Scripts dans le Navigateur**
    - Installez des extensions comme NoScript ou minerBlock pour empêcher l'exécution de scripts de minage dans les navigateurs.
3. **Mises à Jour Régulières**
    - Maintenez les systèmes, logiciels et navigateurs à jour pour combler les failles de sécurité.
4. **Éducation des Utilisateurs**
    - Sensibilisez les employés et utilisateurs aux dangers des emails de phishing et des téléchargements non vérifiés.
5. **Surveillance des Performances**
    - Utilisez des outils de surveillance pour détecter des pics anormaux de consommation de ressources.
6. **Segmentation du Réseau**

- Isolez les appareils critiques pour minimiser les impacts en cas d'infection.

7. **Filtrage du Contenu Web**
    - Configurez des solutions de filtrage pour bloquer les sites web connus pour contenir des scripts de cryptominage.

7. Conclusion

Le cryptojacking représente une menace émergente qui exploite les ressources des victimes à des fins lucratives, sans qu'elles en aient connaissance. Bien que les attaques ne visent pas directement à voler des données, elles peuvent causer des dommages économiques importants et dégrader les performances des systèmes. Une combinaison de technologies de sécurité, de pratiques rigoureuses et de sensibilisation peut aider à prévenir ces attaques. **La vigilance et la proactivité sont essentielles pour maintenir la sécurité de vos systèmes.**