Anatomie d'une attaque Atomic Stealer

Découvrez comment Atomic Stealer s'appuie sur l'ingénierie sociale pour dérober des identifiants et compromettre les systèmes.

1

Reconnaissance

Les acteurs malveillants recueillent des informations sur les cibles pour préparer leur attaque.

EXEMPLE : des campagnes d'ingénierie sociale identifient et profilent les victimes.

2

Armement

Les outils d'attaque sont développés à partir des renseignements collectés, puis empaquetés.

EXEMPLE : du code malveillant est intégré dans une application d'apparence légitime.

3

Livraison

L'application malveillante est diffusée via des canaux destinés à tromper les utilisateurs.

EXEMPLE : des publicités sponsorisées incitent les utilisateurs à télécharger une fausse application.

4

Exploitation

Une notification falsifiée invite l'utilisateur à révéler ses identifiants.

EXEMPLE : une fausse notification de mise à jour enregistre des identifiants et des données sensibles.

5

Installation

Les mécanismes de persistance pérennisent l'accès après la compromission initiale.

EXEMPLE : une porte dérobée permet aux pirates de continuer à accéder à l'appareil.

6

Commande et contrôle (C2)

Les identifiants volés sont utilisés pour accéder à d'autres systèmes et données.

EXEMPLE : les adversaires utilisent le C2 pour étendre leur emprise et se déplacer dans le réseau.

7

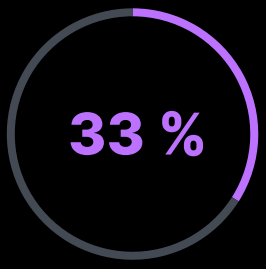
Passage à l'action

Les attaquants profitent de cet accès pour mener à bien une campagne de compromission plus vaste.

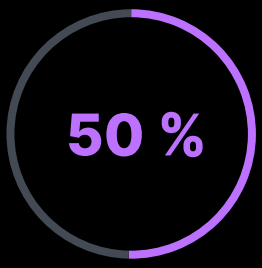
EXEMPLE : prise de contrôle de comptes, mouvement latéral, vol de données et extorsion.

jamf

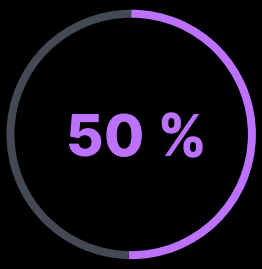
L'importance de l'AMOS



logiciels malveillants liés aux infostealers



attaques basées sur les chevaux de Troie



des menaces échappent à la détection

SOURCE : **Jamf Security 360, Rapport annuel 2026 sur les tendances Mac.**

Obtenir le livre blanc