Projet Big-Brogger

Tom Dejardin
Yohan Bordes

Sommaire

- Contexte et Problématique
- Objectifs du projet
- Originalité et positionnement
- Fonctionnement du Module
- Analyse critique des résultats
- Conclusion

Contexte et problématique

Vous avez trouvé une vulnérabilité sur une machine puis utilisé un module d'exploitation metasploit pour en prendre le contrôle.

Comment récupérer les mots de passes de l'utilisateurs en toute discrétion ?

Objectifs du projet

Objectif Principal: Capturer efficacement les saisies au clavier sur les systèmes Windows compromis

- Développer un module de post-exploitation pour metasploit
- Assurer la fiabilité et la discrétion du module
- Enregistrer les données capturées de manière fiable

Originalité du module

Simplicité et Efficacité

« Big Brogger » se distingue par sa simplicité et son efficacité dans la capture des saisies au clavier sur les systèmes Windows compromis.

Approche Légère

Contrairement à d'autres modules plus complexes, « BigBrogger » offre une solution légère et facile à utiliser pour la post-exploitation

Fonctionnalités Essentielles

Le module se concentre sur les fonctionnalités essentielles pour la capture des saisies au clavier, offrant ainsi une solution pratique et fonctionnelle.

Fonctionnement du Module

Migration vers explorer.exe :

Le module migre vers le processus Explorer.exe pour une persistance accrue et une dissimulation efficace

Démarrage du keylogger :

Le module démarre le keylogger en utilisant la fonction keyscan_start pour capturer les saisies au clavier..

Capture et enregistrement des saisies :

Les saisies au clavier sont récupérées à l'aide de la fonction keyscan_dump et sont enregistrées dans un fichier spécifié par l'utilisateur, le cas échéant.

Migration vers PowerShell:

Enfin, le module migre vers un processus PowerShell existant ou en crée un nouveau pour éviter la détection et la réponse des défenses de sécurité.

Analyse critique des résultats

Conclusion