Projet : développement d'un module metasploit

- Tom Dejardin
- Yohan Bordes

Présentation

Le module "Big Brogger" a été développé par Yohan Bordes et Tom Dejardin dans le cadre d'un projet de sécurité informatique. Il vise à capturer toutes les saisies au clavier sur un système Windows compromis. Cela permet aux opérateurs de sécurité de recueillir des informations sensibles telles que les mots de passe, les commandes exécutées et d'autres données importantes. L'intérêt de ce module réside dans sa capacité à fournir un accès furtif aux informations confidentielles sans éveiller les soupçons de l'utilisateur cible.

Originalité du Module et Positionnement

Le module "Big Brogger" se distingue par sa simplicité et son efficacité. Bien que son envergure soit modeste, il offre une solution pratique et fonctionnelle pour la capture des saisies au clavier sur les systèmes Windows compromis. Comparé à d'autres modules plus complexes offrant des fonctionnalités similaires, telles que la capture de frappes et la migration de processus, "Big Brogger" se positionne comme une option légère et facile à utiliser.

Dans l'écosystème Metasploit, il existe plusieurs modules proposant des fonctionnalités similaires, mais souvent plus élaborées. Par exemple :

- **keylogger.rb :** Ce module offre une gamme étendue de fonctionnalités pour la capture des saisies au clavier, y compris la prise en charge de différentes plates-formes et la personnalisation avancée des options. En comparaison, "Big Brogger" offre une approche plus simplifiée et centrée sur les besoins fondamentaux de capture des saisies au clavier sur les systèmes Windows.

Malgré sa taille modeste, "Big Brogger" trouve sa place dans le paysage des modules Metasploit en offrant une solution légère et facile à utiliser pour la capture des saisies au clavier sur les systèmes Windows compromis. Son positionnement réside dans sa simplicité et sa fonctionnalité, en fournissant une option pratique pour les opérateurs de sécurité confrontés à de tels scénarios d'attaque.

Description de la Machine Cible

La machine cible est une machine virtuelle Windows 10 Professionnel. Notre projet consiste en un module de post-exploitation, donc nous ne nous intéresserons pas à l'exploitation de failles, mais plutôt à l'utilisation de notre module **big-brogger**. Par conséquent, nous avons spécifiquement configuré la machine pour qu'elle soit vulnérable au module de post exploitation psexec.

Voici un aperçu détaillé de ses caractéristiques :

- **Système d'Exploitation :** Windows 10 Professionnel
- **Protection Antivirus :** Windows Defender Real-Time Protection est définitivement désactivé pour permettre l'exécution sans entraves du module Big Brogger.

- **Configuration du Contrôle des Comptes Utilisateurs (UAC) :** Le contrôle des comptes utilisateurs (UAC) est configuré de sorte à être désactivé pour une utilisation optimale du module.
- **Configuration Réseau :** La machine est configurée avec une adresse IP accessible depuis le réseau local pour pouvoir ainsi transmettre le key-logger depuis la machine de l'attaquant.

Une machine cible déjà configuré est présente sur ce lien. Si vous désirez en créer une vous même, veuillez à suivre les instructions inscrite dans le fichier readme.md

Cette machine cible est utilisée pour la démonstration de l'utilisation du module "Big Brogger" dans un environnement de test contrôlé.

Fonctionnement du Module

Le module "Big Brogger" fonctionne en plusieurs étapes :

1. **Migration vers explorer.exe :** Le module migre vers le processus Explorer.exe pour une persistance accrue et une dissimulation efficace.

2. **Démarrage du keylogger :** Le module démarre le keylogger en utilisant la fonction keyscan_start pour capturer les saisies au clavier.

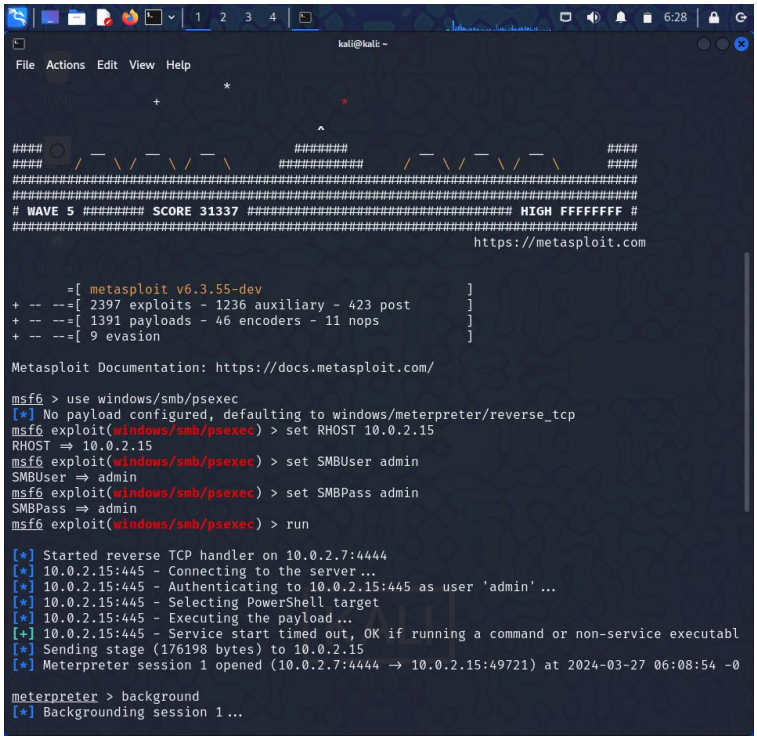
3. **Capture et enregistrement des saisies :** Les saisies au clavier sont récupérées à l'aide de la fonction keyscan_dump et sont enregistrées dans un fichier spécifié par l'`utilisateur,` le cas échéant.

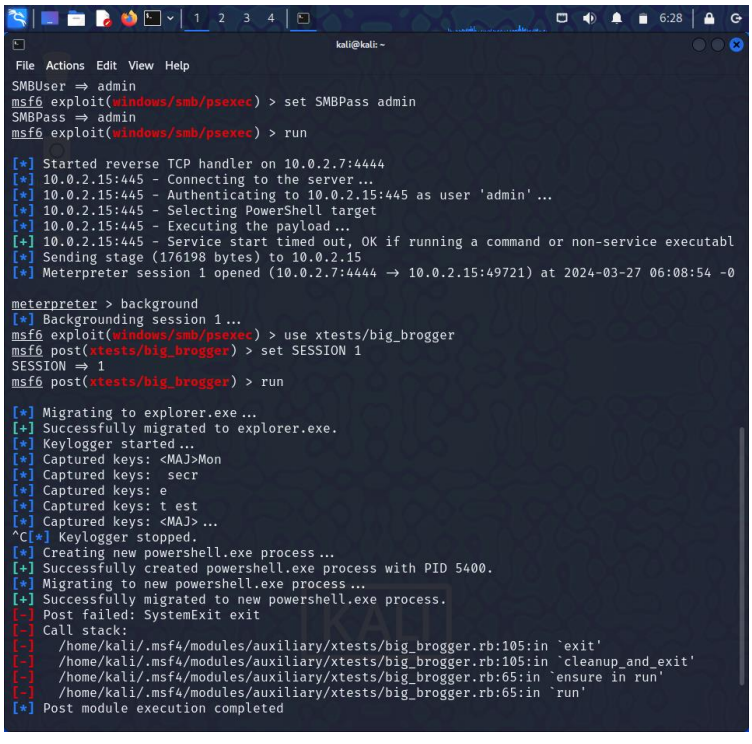
4. **Migration vers PowerShell :** Enfin, le module migre vers un processus PowerShell existant ou en crée un nouveau pour éviter la détection et la réponse des défenses de sécurité.

Démonstration

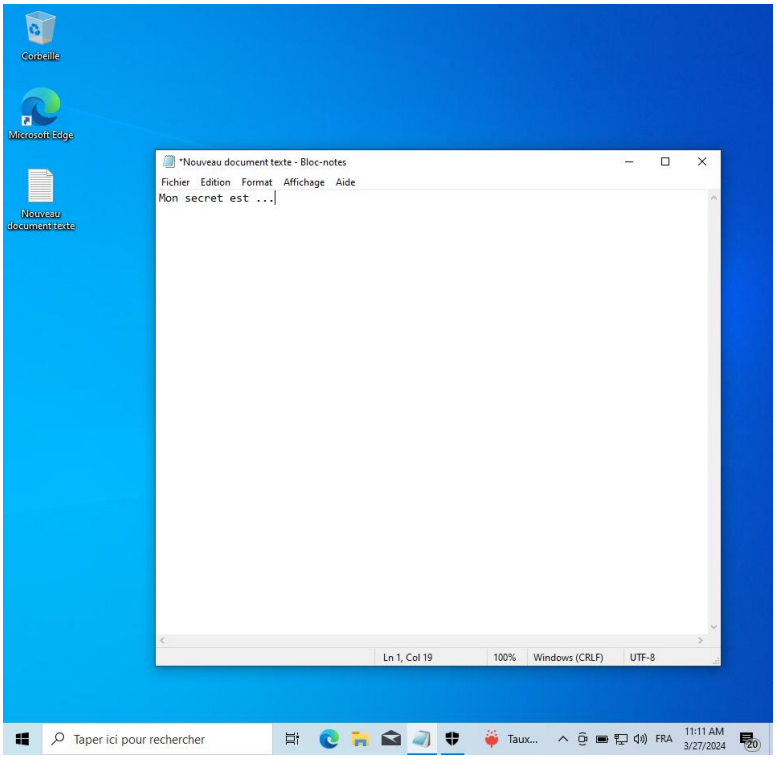
Ceci est un module de post-exploitation, donc vous devrez obtenir l'accès à la machine Windows. Vous pouvez le faire de n'importe quelle manière, mais nous utiliserons `windows/smb/psexec` dans Metasploit pour la démonstration.

Tout d'abord, utilisez psexec pour obtenir une session avec un identifiant valide et mettez en arrière-plan la session Meterpreter et exécuter le keylogger :





En ayant écrit quelque chose dans la machine Windows :



Analyse Critique des Résultats

L'analyse du module "Big Brogger" met en lumière plusieurs aspects importants. Tout d'abord, il a démontré une efficacité notable dans la capture des saisies au clavier sur les systèmes Windows cibles. Les données collectées ont été enregistrées de manière fiable, ce qui permet aux opérateurs de sécurité d'accéder à des informations sensibles telles que les mots de passe et les commandes exécutées.

Cependant, malgré sa discrétion relative, il est important de reconnaître que le module n'est pas à l'abri d'une détection par certains outils de sécurité. Sa discrétion peut être compromise par divers facteurs, notamment les configurations de sécurité de la machine cible et la vigilance des utilisateurs.

Par ailleurs, le module présente certaines limitations, notamment sa dépendance à l'égard de Meterpreter et sa compatibilité limitée avec d'autres types de sessions. De plus, bien qu'il puisse capturer les saisies au clavier, il ne garantit pas la capture de toutes les interactions utilisateur, telles que l'utilisation de la souris.

Pour améliorer le module, plusieurs fonctionnalités pourraient être ajoutées, notamment :

- **Filtrage des Frappes Clavier par Application :** Le module pourrait être mis à jour pour filtrer les frappes clavier par application, permettant ainsi de capturer uniquement les frappes clavier des applications spécifiques.
- **Enregistrement des Informations Supplémentaires :** Il serait judicieux d'ajouter la possibilité d'enregistrer des informations supplémentaires en plus des frappes clavier, telles que l'horodatage, le nom d'utilisateur et l'adresse IP de la machine compromise.
- **Fonctionnalité d'Exfiltration :** Le module pourrait être mis à jour pour exfiltrer les données capturées vers un serveur distant, garantissant ainsi la collecte des données même en cas de perte de connexion à la machine compromise.

En outre, des améliorations en termes de fiabilité et de robustesse pourraient être apportées, notamment en renforçant la gestion des erreurs et en effectuant davantage de tests pour garantir le bon fonctionnement du module. En ce qui concerne la sécurité, des efforts pour éviter la détection par les logiciels antivirus et les outils de sécurité, ainsi que pour chiffrer les données capturées, pourraient également être envisagés.

Conclusion

Le module "Big Brogger" offre une solution pratique pour la capture des saisies au clavier sur les systèmes Windows compromis. Malgré quelques limites, il reste un outil utile et fonctionnel. Des améliorations futures pourraient renforcer son efficacité et sa robustesse dans des environnements variés.