Livre blanc

Partie 1

Stratégies et Techniques pour échapper aux Antivirus modernes et contourner les EDR

NBS System
Groupe CELESTE

SOMMAIRE

1. CONTEXTE ET PÉRIMÈTRE DES EDR ET ANTIVIRUS

Les **EDR (Endpoint Detection and Response)** et les **antivirus** sont des outils de sécurité essentiels pour protéger les systèmes informatiques contre les attaques malveillantes.

Cependant, ces outils ne sont pas infaillibles et peuvent être contournés par des attaquants expérimentés. Les missions de **pentest** sont des exercices visant à évaluer la sécurité d'un système informatique en testant sa vulnérabilité aux attaques.

Dans le cadre de ces missions, nous utilisons souvent des techniques de contournement des antivirus et des EDR pour évaluer leur efficacité et mettre en évidence les points faibles du système de sécurité.

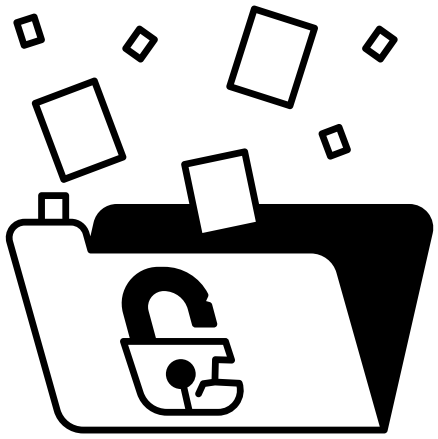
Ce livre blanc explore ces différentes techniques utilisées dans les missions de test d'intrusion, en mettant en évidence leurs avantages et leurs limites. Le livre blanc sera découpée en trois parties.

2. OBJECTIFS ET MÉTHODOLOGIE

Notre projet vise à développer des techniques d'évasion avancées pour contourner les antivirus et les EDR. L'objectif principal de ce projet est d'optimiser nos **tests d'intrusion internes** pour nos clients, qui utilisent des solutions de sécurité avancées telles que les EDR pour renforcer leur environnement **Active Directory**.

Ce projet nous permettra de contourner les solutions de sécurité qui peuvent bloquer certaines activités malveillantes, assurant ainsi le succès de notre mission visant à obtenir les droits d'administrateur du domaine.

Par exemple, lors d'un pentest interne pour un client, nous pourrions utiliser cette approche pour développer une charge utile exécutable capable d'extraire les informations sensibles stockées dans la **mémoire LSASS** sans être détectée par les solutions de sécurité.



2. OBJECTIFS ET MÉTHODOLOGIE

Le **Local Security Authority Server Service (LSASS)** est un processus du système d'exploitation Windows responsable de l'authentification des utilisateurs : il vérifie les mots de passe, gère les changements de mots de passe, crée les tokens d'accès des processus utilisateurs, etc.

Ce processus est lancé au démarrage du système d'exploitation par le compte NT AUTHORITY/SYSTEM. En 2007, il a été découvert que les mots de passe des utilisateurs se trouvaient en clair dans la mémoire du processus LSASS.exe.

Cela signifie que si un attaquant parvenait à compromettre une machine Windows, il pourrait accéder aux mots de passe des utilisateurs connectés depuis le dernier redémarrage de la machine.

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

Pour comprendre comment les antivirus et les solutions EDR fonctionnent, il est important de se familiariser avec les méthodes qu'ils utilisent pour détecter et neutraliser les menaces.

Les antivirus utilisent généralement des bases de données de signatures pour identifier les logiciels malveillants connus, ainsi que des techniques de détection comportementale pour identifier les comportements suspects des programmes en cours d'exécution.

Les solutions EDR, quant à elles, surveillent les activités du système et des utilisateurs en temps réel, en utilisant des techniques de détection comportementale avancées pour identifier les comportements anormaux.

Dans les prochaines parties, nous explorerons plus en détail les méthodes de détection utilisées par les antivirus et les solutions EDR, ainsi que les avantages et les limites de chaque type de logiciel de sécurité.

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

A. PRINCIPE DE FONCTIONNEMENT DES ANTIVIRUS

Afin de mettre au point des techniques d'évasion efficaces, il est essentiel de bien comprendre le fonctionnement des antivirus. Pour cela, nous avons consacré une part importante de notre temps à étudier les techniques de détection des antivirus, notamment les algorithmes de signature et l'analyse dynamique.

Cela nous a permis de mieux comprendre les mécanismes de détection et les limites des solutions de sécurité actuelles. Voici les principes fondamentaux du fonctionnement des antivirus :

Analyse statique des signatures :

L'analyse de signature est basée sur une liste noire de méthodes et de séquences d'octets. Lorsqu'un nouveau malware est détecté par un analyste, une signature spécifique est créée pour celui-ci.

La signature peut être basée sur un code ou des données spécifiques (par exemple, en utilisant une chaîne de caractères ou un prototype de fonction).

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

Très souvent, les signatures sont construites sur les premiers octets exécutables d'un fichier malveillant. L'antivirus contient des millions de signatures dans sa base de données, qui sont comparées aux séquences d’octets des fichiers suspects afin de détecter une correspondance.

Les premiers antivirus utilisaient cette méthode, mais elle est encore efficace aujourd'hui en combinaison avec l'analyse dynamique. Le plus gros problème avec l'analyse basée sur les signatures est qu’elle ne peut pas être utilisée pour détecter de nouveaux logiciels malveillants.

Pour contourner l'analyse basée sur la signature, il nous suffit donc de créer un nouveau code ou de modifier considérablement le code existant pour contourner la signature actuelle.

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

Analyse dynamique :

De nos jours, de plus en plus d'antivirus reposent sur une approche dynamique. Lorsqu'un fichier exécutable est analysé, il est lancé pendant une courte durée dans une machine virtuelle (bac à sable).

Combiné à la vérification des signatures, il peut détecter les logiciels malveillants inconnus, même ceux qui reposent sur le chiffrement. En effet, l'analyse dynamique est une fonctionnalité complexe capable d'analyser des millions de fichiers, de les exécuter dans un environnement émulé et de vérifier toutes les signatures. Cependant, elle a aussi quelques limitations :

- L'analyse est trop rapide, l'antivirus a donc une limite par rapport au nombre d'opérations qu'il peut effectuer pour chaque analyse.

- L'environnement étant émulé, les spécifications de l'appareil et l'environnement du malware sont inconnus.

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

B. Principe de fonctionnement des EDR

Pourquoi un EDR ?

Les solutions EDR sont devenues un élément essentiel de la sécurité des entreprises. Elles permettent de surveiller les activités des points finaux (postes de travail, serveurs, etc.) en temps réel et de détecter les comportements anormaux grâce à des algorithmes avancés. Elles sont particulièrement efficaces pour contrer les menaces avancées qui échappent aux antivirus traditionnels.

Comment fonctionne un EDR ?

Les EDR visent à détecter et à répondre aux menaces avancées qui ciblent les endpoints, c'est-à-dire les terminaux (ordinateurs, téléphones, tablettes, etc.) qui sont utilisés pour accéder aux systèmes d'information d'une entreprise.

Voici le principe de fonctionnement d'un EDR

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

Collecte de données

L'EDR collecte des données à partir des points finaux, telles que les événements système, les fichiers, les journaux d'application, les connexions réseau, les processus en cours d'exécution, etc. Ces données sont collectées en temps réel pour fournir une vue en temps réel de l'état des points finaux.

Analyse des données

L'EDR utilise des algorithmes d'analyse pour détecter les comportements malveillants. Ces algorithmes sont basés sur des modèles de comportement normaux, de sorte que toute activité qui s'écarte de ces modèles est considérée comme suspecte. Ils utilisent également des bases de données de signatures de virus et de logiciels malveillants pour identifier les menaces connues.

Alertes

Lorsqu'une activité suspecte est détectée, l'EDR génère une alerte pour informer les équipes de sécurité. Les alertes peuvent être déclenchées par des événements tels que l'ouverture d'un fichier malveillant, la tentative d'exécution d'une commande dangereuse, la modification des paramètres système, etc. Les alertes sont généralement classées en fonction de leur niveau de gravité.

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

Investigation

Les équipes de sécurité enquêtent sur les alertes pour déterminer si elles sont réellement malveillantes ou non. Les EDRs fournissent des outils d'investigation pour aider les équipes de sécurité à recueillir des preuves, à examiner les fichiers, à analyser les connexions réseau, à suivre les processus en cours d'exécution, etc.

Réponse à incident

Si une menace est confirmée, l'EDR déclenche une réponse automatique ou manuelle pour neutraliser la menace. Les réponses peuvent inclure l'isolation de l'Endpoint, la suppression du fichier malveillant, la fermeture des connexions réseau suspectes, la restauration du système à un état antérieur, etc.

Rapports

L'EDR génère des rapports pour fournir une vue d'ensemble de l'activité de sécurité, y compris le nombre d'alertes générées, le temps de réponse moyen, le nombre de menaces confirmées, etc. Ces rapports peuvent être utilisés pour surveiller l'efficacité de la sécurité et pour identifier les zones à risque.

3. FONCTIONNEMENT DES ANTIVIRUS ET EDR

Quel est le meilleur EDR ?

La sélection du meilleur EDR dépend des besoins spécifiques de chaque organisation. Parmi les solutions EDR les plus populaires, on trouve SentinelOne, Cortex, CrowdStrike et bien d'autres. Ces produits de sécurité se distinguent par leurs fonctionnalités avancées, leur capacité à détecter les programmes malveillants, et leur efficacité à répondre aux incidents en temps réel.

Dans les sections à venir, nous fournirons une explication détaillée sur les techniques avancées employées par les EDRs.

EN RÉSUMÉ

En résumé, l'EDR est une solution de sécurité qui collecte et analyse des données à partir des points finaux pour détecter les menaces avancées et y répondre de manière rapide et efficace.

Les EDRs sont devenus un élément essentiel de la sécurité des entreprises, en particulier dans un contexte où les attaques informatiques sont de plus en plus sophistiquées et ciblées. Pour les professionnels de la sécurité informatique, il est crucial de comprendre les mécanismes de fonctionnement des EDR et des antivirus afin de développer des stratégies de défense et des stratégies de contournement efficaces.