STAGE - 2027

Étude de la couverture EDR : de la source de télémétrie à sa suppression

fenrisk

PARIS | MARSEILLE

Stage Étude de la couverture EDR

Objectifs

L'objectif du stage est l'étude de la couverture des solutions EDR (Endpoint Detection and Response) et de leurs mécanismes de télémétrie sur Windows. Le stagiaire devra effectuer un état de l'art des mécanismes de collecte et des techniques permettant de dégrader ou de supprimer les différents signaux observables par un EDR. Il devra dans un premier temps étudier un agent EDR afin de cartographier ses différentes sources de télémétrie : hooks user-mode, callbacks kernel, minifilters, ETW-TI, AMSI, etc.

Il devra ensuite mettre en place un banc de test reproductible permettant de corréler différentes actions d'attaque avec les signaux effectivement observables par l'EDR, puis mesurer la dégradation de cette télémétrie face à différentes familles de techniques d'évasion.

Le stagiaire devra enfin identifier les artefacts résiduels permettant de concevoir de nouvelles techniques de détection et d'évaluer les mécanismes d'auto-protection de l'agent. Il s'agit d'un projet de recherche qui nécessite donc de l'initiative, de l'autonomie et une forte capacité d'expérimentation.

Résultats attendus

Le stage a pour objectif de produire des résultats parmi les suivants :

- Une cartographie des différentes sources de télémétrie d'un agent EDR ;
- Un banc de test reproductible permettant d'évaluer la couverture d'un EDR ;
- Une matrice de couverture mettant en relation les TTP étudiées et les sources de télémétrie disponibles ;
- Une méthodologie de mesure de la visibilité d'un EDR face aux différentes techniques d'évasion ;
- Une analyse de techniques telles que l'unhooking, le call stack spoofing, l'obfuscation mémoire ou la réduction des signaux réseau ;
- Des heuristiques et signatures de détection basées sur les artefacts résiduels identifiés ;

- Une checklist d'audit de la sécurité et de l'auto-protection d'un agent EDR ;
- Un article de blog ou une publication portant sur le sujet ;
- Des outils d'automatisation permettant de rejouer les expérimentations et de comparer les résultats entre différentes versions d'un produit ;
- L'identification et, le cas échéant, la divulgation coordonnée de vulnérabilités affectant l'agent étudié.

Compétences attendues

- Connaissances et intérêt pour la sécurité des systèmes Windows et des endpoints ;
- Intérêt pour le pentest, la sécurité offensive et les techniques d'évasion ;
- Connaissances d'ETW, des syscalls et des mécanismes de télémétrie Windows ;
- Bon niveau en C/C++ ;
- Des connaissances en IPC et en développement ou analyse de drivers Windows seraient appréciées ;
- Bon niveau rédactionnel en français et anglais ;
- Autonomie et capacité à travailler en télétravail ;
- Être force de proposition et d'initiative.

Conditions

- Gratification brute de 1800€/mois ;
- En télétravail ;
- Un profil habilitable ;
- Les expérimentations liées aux techniques d'évasion seront réalisées dans un environnement de laboratoire isolé et contrôlé ;
- Il est attendu que le stage débouche sur un CDI d'auditeur en sécurité.

Comment postuler

Contactez apply@fenrisk.com en joignant :

- Votre CV ;
- Une présentation de votre parcours et de vos attentes ;
- Vos coordonnées.