TRAVAUX PATIQUES : ANALYSE DE RAM

Ressources :

- Volatility
- Mitre Att&ck
- Virus Total

Scénario :

En tant qu'enquêteur judiciaire dans une grande institution financière, votre SIEM a signalé une activité inhabituelle sur un poste de travail interne ayant accès à des données financières sensibles, ce qui indique une violation potentielle. Avec un vidage de la mémoire de la machine compromise, votre tâche consiste à analyser les indicateurs de compromission, à retracer l'origine de l'anomalie et à contenir l'incident tout en évaluant sa portée.

Questions :

1) L'identification du nom du processus malveillant permet de comprendre la nature de l'attaque. Quel est le nom du processus malveillant ?
2) Connaître l'identifiant du processus parent (PPID) du processus malveillant permet de retracer la hiérarchie des processus et de comprendre le déroulement de l'attaque. Quel est le PID parent du processus malveillant ?
3) Il est essentiel de déterminer le nom du fichier utilisé par le logiciel malveillant pour exécuter la charge utile de deuxième étape afin d'identifier les activités malveillantes ultérieures. Quel est le nom du fichier utilisé par le logiciel malveillant pour exécuter la charge utile de deuxième étape ?
4) L'identification du répertoire partagé sur le serveur distant permet de tracer les ressources ciblées par l'attaquant. Quel est le nom du répertoire partagé auquel on accède sur le serveur distant ?
5) Quel est l'identifiant de la sous-technique MITRE utilisé par le logiciel malveillant pour exécuter la charge utile de la deuxième étape ?
6) L'identification du nom d'utilisateur sous lequel le processus malveillant s'exécute permet d'évaluer le compte compromis et son impact potentiel. Quel est le nom d'utilisateur sous lequel le processus malveillant s'exécute ?
7) Il est essentiel de connaître le nom de la famille de logiciels malveillants pour établir une corrélation entre l'attaque et les menaces connues et mettre au point des défenses appropriées. Quel est le nom de la famille de logiciels malveillants ?