

Pourquoi votre réponse consiste-t-elle à suspendre les programmes ?

Les criminels ont appris qu'en opérant uniquement en mémoire, à l'aide de techniques telles que l'injection de processus, ils bénéficient de divers avantages :

1. Prise de contrôle de l'identité d'un utilisateur pour ce programme.
2. Évasion des contrôles de gestion des identités.
3. Évasion des règles de pare-feu basées sur les applications et des listes blanches.
4. Évasion des outils de prévention des pertes de données sur les serveurs.
5. Suppression de presque toutes les preuves en mémoire lorsque le processus est arrêté.
6. Suppression de presque toutes les preuves en mémoire une fois l'ordinateur redémarré.

En suspendant les programmes sous le contrôle de l'attaquant, les preuves sont figées dans le temps.

L'attaquant est également figé.

Les preuves sont disponibles pour les outils d'investigation numérique dans le cadre d'un processus d'enquête.

Si l'organisation n'est pas équipée pour effectuer une investigation numérique à ce moment-là, un simple redémarrage par l'attaquant ramènera le système à un état sain. Forcer l'arrêt du programme suspendu, puis le redémarrer, a généralement également l'effet souhaité.