

¿Por qué responden suspendiendo los programas?

Los delincuentes han aprendido que operar únicamente en memoria, utilizando técnicas como la inyección de procesos, proporciona una variedad de ventajas:

1. Asumir el control de la identidad de un usuario para ese programa.
2. Evasión de las verificaciones de gestión de identidad.
3. Evasión de las reglas de firewall basadas en aplicaciones y de las listas blancas.
4. Evasión de las herramientas de prevención de pérdida de datos en los servidores.
5. Eliminación de casi toda la evidencia en memoria cuando se elimina el proceso.
6. Eliminación de casi toda la evidencia en memoria una vez que se reinicia el equipo.

Al suspender los programas bajo el control del atacante, la evidencia queda congelada en el tiempo.

El atacante también queda congelado.

La evidencia está disponible para las herramientas forenses como parte de un proceso de investigación.

Si la organización no está equipada para realizar análisis forenses en ese momento, un simple reinicio por parte del atacante devolverá el sistema a un estado saludable. Forzar la finalización del programa suspendido y reiniciarlo, por lo general, también produce el efecto deseado.

Revision #1

Created 2026-07-24 01:47:18 UTC by Dennis Underwood

Updated 2026-07-24 01:47:18 UTC by Dennis Underwood