

Warum reagieren Sie mit dem Anhalten von Programmen?

Kriminelle haben gelernt, dass das ausschließliche Operieren im Arbeitsspeicher – unter Einsatz von Techniken wie Prozessinjektion – eine Reihe von Vorteilen bietet:

1. Übernahme der Identität eines Benutzers für dieses Programm.
2. Umgehung von Identitätsmanagement-Prüfungen.
3. Umgehung von anwendungsbasierten Firewall-Regeln und Whitelists.
4. Umgehung von Data-Loss-Prevention-Tools auf Servern.
5. Löschung nahezu aller im Arbeitsspeicher befindlichen Beweise, wenn der Prozess beendet wird.
6. Löschung nahezu aller im Arbeitsspeicher befindlichen Beweise nach einem Neustart des Computers.

Durch das Anhalten der vom Angreifer kontrollierten Programme werden die Beweise quasi eingefroren.

Auch der Angreifer wird dadurch eingefroren.

Die Beweise stehen forensischen Tools im Rahmen eines Untersuchungsprozesses zur Verfügung.

Ist die Organisation zu diesem Zeitpunkt nicht in der Lage, forensische Analysen durchzuführen, versetzt ein einfacher Neustart durch den Angreifer das System wieder in einen unbedenklichen Zustand. Ein erzwungenes Beenden des angehaltenen Programms und dessen Neustart hat in der Regel ebenfalls den gewünschten Effekt.

Revision #1

Created 2026-07-24 04:33:04 UTC by Dennis Underwood

Updated 2026-07-24 04:33:05 UTC by Dennis Underwood