_General

Created by Dennis Underwood on May 18, 2022

Criminals have learned that operating in memory only, using techniques such as process injection, provide a variety of advantages:

1. Assuming control of a user’s identity for that program.
2. Evasion from identity management checks.
3. Evasion from application-based firewall rules and whitelists.
4. Evasion from data loss prevention tools on servers.
5. Deletion of almost all in-memory evidence when the process is killed.
6. Deletion of almost all in-memory evidence once the computer is rebooted.

By suspending the programs under control of the attacker, evidence is frozen in time.

The attacker is also frozen.

Evidence is available for forensic tools as part of an investigation process.

If the organization is not equipped to perform forensics at the time, a simple reboot by the attacker will bring the system back to a healthy state. Force killing the suspending program, and restarting it, usually also has the desired effect.

Revision #1
Created 2026-05-18 20:27:13 UTC by Dennis Underwood
Updated 2026-05-18 20:27:13 UTC by Dennis Underwood