Memory Modification

Created by Kyle Nehman, last modified on Oct 19, 2022

What is memory modification?

Memory modification, as Cyber Crucible use the term, is when the executable sections of a process' memory have been modified in abnormal ways. The normal execution of a given process, without outside tampering, does not trigger these modification – they are separate from normal ‘volatile memory’ operations within a process.

A common technique of memory modification is process hollowing, where an attacker will start a victim process on the machine, often starting in a suspended state, and change the executable code to actually execute the code of some other program.

Relevant MITRE tactics:

- MITRE T1055 - Process injection, usually used to run malicious code in a target process while allowing the original process to continue.
- MITRE T1055-12 - Process injection by replacing code in a process, typically before it begins execution.
- MITRE T1559 - Inter-Process communication can provide control over the target process from the injector once the injection is complete.
- MITRE T1548 - Abusing elevation control can allow a process that would not normally have higher privileges be escalated to gain access to protected data.

What are the consequences?

Memory modifications can have very similar consequence to other process injection techniques, but is even more evasive. Since there is no remote thread creations, or external functions called, it can often be very difficult to detect memory modifications at all, even harder to attribute them to any particular process.

A process that has modified memory can be forced to carry out malicious activity that it otherwise would not have. No process with executable memory that has been tampered with should be trusted, as it is not a normal occurrence for inter-process communications or interactions.

What does Cyber Crucible do?

Cyber Crucible monitors the state of a process' memory throughout its lifecycle. If the memory is deemed to be tampered with, then the process is flagged and considered untrusted. At the time of an extortion event occurring, the memory is snapshotted to be provided during potential IR investigations.

The snapshotted memory contains the original, untampered, executable memory, and any “diffs”, with their offsets within the process' memory. Analysis of these memory dumps can be challenging, but can provide strong evidence towards the behaviors of the malicious code.

How do I tell?

Cyber Crucible Indicates Responses with Modified Memory

Cyber Crucible Indicates Responses with Modified Memory

Modified memory is harder and more ephemeral to track down than other methods of process injection. Instead, we provide a quick boolean value to see that the modification occurred, and from there analyzing the actual memory diffs require some deeper diving.

Some raw memory

Some raw memory

Disassembled memory

Disassembled memory

Collecting the memory is just step one, even after disassembly the code can be very obfuscated and hard to read. The good news is that we have lots to go off of for this analysis when we have the original memory, associated metadata, the original executable, and the modified executable instructions themselves.

1. yes, 2.

Example Scenarios:

- [Training Scenario - Memory Modification]

Revision #4
Created 2026-05-18 20:29:17 UTC by Dennis Underwood
Updated 2026-06-19 06:06:40 UTC by Aaron Birmbaum