Memory Injection Prevention

Minerva Anti-Evasion Platform blocks attempts by fileless malware and other stealthy malicious software to hide in a legitimate process, preventing malicious programs from gaining a foothold on the endpoint.

Memory Injection Threats

Attackers are evasive, constantly looking for new and improved methods to hide their malicious code and to inconspicuously blend into legitimate applications. One frequently used method of executing this kind of attacks is called “Memory Injection”. Attackers take their malicious memory and inject it into legitimate applications or OS processes, making it difficult to detect and analyze.

Memory injection can also be used to bypass restrictions such as Windows and firewall access rules by impersonating a benign process.

Memory Tampering

Attackers can access other processes’ memory space to view or manipulate its data. This ability is often exploited to steal sensitive data such as credit cards, banking information, passwords or any other data.

Our Solution

Minerva offers a unique solution that prevents and mitigates memory injection attacks, stopping evasive malware and denying malicious access to your sensitive data.
Better Prevention

Preventing malware from blending into legitimate application and OS processes »
Ensuring smooth and un-tampered execution.

Preventing process impersonation attempts »
Enforcing security restrictions.

Preventing fileless memory attacks »
Protecting legitimate process's memory space.

Preventing Man In The Browser (MITB) attacks »
Denying malicious code injections on any browser.

Preventing malicious access to sensitive processes’ memory »
Protecting Point of Sale and custom in-house applications, denying access to memory, credit card and other sensitive data.

Enterprise-Grade Features

**Increased detection rate**
- Reporting and integrating prevention data with already installed tools such as: AV, Sandbox, and SIEM

**Easy deployment**
- No reboots required
- No configuration needed
- No prerequisites

**Faster and easier Incident Response process**
- Automatically saves and submits captured malicious code for analysis
- Easy integration with cloud and reputation tools
- No false positives

**Reduced Operational Cost**
- Stop chasing and replacing - Keep your traditional security tools in place
- No signatures needed
- Offline operation mode

**Forensics Data Capture**
- Attack timeline discovery
- Activity snapshot