# TTP Detail – T1055.011

## TTP Information

Name: Extra Window Memory Injection

Description: Adversaries may inject malicious code into process via Extra Window Memory (EWM) in order to evade process-based defenses as well as possibly elevate privileges. EWM injection is a method of executing arbitrary code in the address space of a separate live process.

Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data).(Citation: Microsoft Window Classes) Registration of new windows classes can include a request for up to 40 bytes of EWM to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value. (Citation: Microsoft GetWindowLong function) (Citation: Microsoft SetWindowLong function)

Although small, the EWM is large enough to store a 32-bit pointer and is often used to point to a windows procedure. Malware may possibly utilize this memory location in part of an attack chain that includes writing code to shared sections of the process’s memory, placing a pointer to the code in EWM, then invoking execution by returning execution control to the address in the process’s EWM.

Execution granted through EWM injection may allow access to both the target process's memory and possibly elevated privileges. Writing payloads to shared sections also avoids the use of highly monitored API calls such as <code>WriteProcessMemory</code> and <code>CreateRemoteThread</code>.(Citation: Elastic Process Injection July 2017) More sophisticated malware samples may also potentially bypass protection mechanisms such as data execution prevention (DEP) by triggering a combination of windows procedures and other system functions that will rewrite the malicious payload inside an executable portion of the target process. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via EWM injection may also evade detection from security products since the execution is masked under a legitimate process.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: privilege-escalation

## Malware

* Epic
* Power Loader