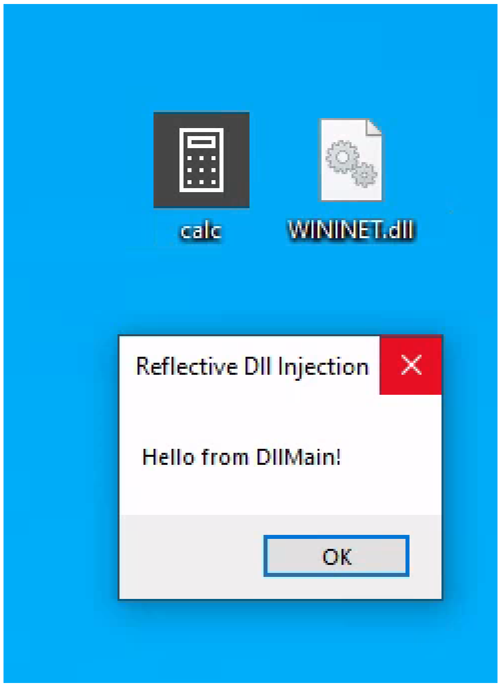
DLL Hijacking: Simulation and Detection with Sysmon and Event Viewer

Replicate the DLL hijacking attack and Find the SHA256 hash of the malicious WININET.dll.

Simulating the attack

1. Moving the calc.exe and the reflective_dll.x64.dll from System 32 to Desktop (to a writable directory).And rename the reflective_dll.x64.dll to WININET.dll
2. Instead of the Calculator application, a MessageBox is displayed.

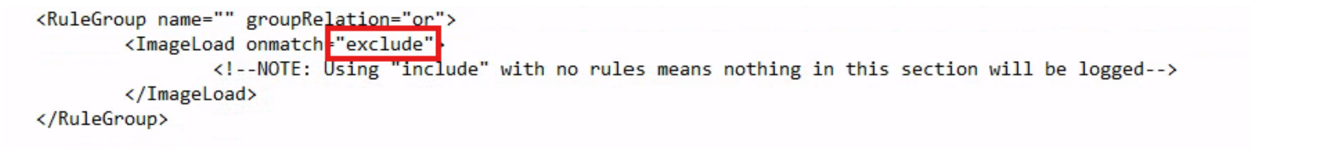


Reflective Dll Injection

Hello from DllMain!

DLL Hijacking is Successful !!!

In the case of detecting DLL hijacks, In sysmonconfig-export.xml, we change the "include" to "exclude" to ensure that nothing is excluded, allowing us to capture the necessary data .



```
<RuleGroup name="" groupRelation="or">
        <ImageLoad onmatch="exclude">
                <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
        </ImageLoad>
</RuleGroup>
```

Detecting the Attack with Sysmon

1.