**Exploit Steps for Windows:**

Note: victim-process would be calculator. So that process name would be running as win32calc.exe in Win2019/2016 probes and will be running as calc.exe in windows 2012 R2 probe )

**Prerequisite:**

- Create a process profile as a full scan with LM enabled, RMP enabled, enable 'Allow Microsoft signed files' and disable 'Auto whitelist'

- Do publish with simple whitelist

- Enable Detect mode

- RDP to the probe

1. **Process Hollowing attack (V2-19742 – the issue fixed in next build)**

- Open a command prompt

- Execute the following command from command prompt

- Make sure if incident receives with type as Process Monitoring and Memory Integrity

Command : ProcessHollowing2.exe xbin.exe SleepingBinary5sec.exe

Text

Description automatically generated

1. **PE Injection attack.**

- Open a command prompt

- Launch any process (ex: calc.exe)

- Execute the following command from command prompt

- Make sure if incident receives with type as Process Monitoring and Memory Integrity

Command: pe-injection.exe calc.exe

Text

Description automatically generated

**3. Reflective DLL injection.**

**-** Open a command prompt

- Launch any process (ex: calc.exe)

- Execute the following command from command prompt

- Make sure if incident receives with type as Process Monitoring and Memory Integrity

Command: inject.x64.exe <pid of calc.exe>

**ex: inject.x64.exe 5572**

Text

Description automatically generated

**4. Early Bird attack.** Provide the name of the victim process

- Open a command prompt

- Launch any process (ex: calc.exe)

- Execute the following command from command prompt

- Make sure if incident receives with type as Process Monitoring and Memory Integrity

Text

Description automatically generated

**5. Process Doppelganging**

- Open a command prompt

- Launch any process (ex: calc.exe)

- Execute the following command from command prompt

- Make sure if incident receives with type as Process Monitoring and Memory Integrity

Text

Description automatically generated with medium confidence

**6. Powershell Injection: (Pre-requisites – have to install PowerShell ver 2 as mentioned below)**

- Open powershell.exe

- On powershell, run the following command

Step1: Open calc.exe

Step2:

PS D:\Malware\Executables> Powershell.exe -Version 2

Windows PowerShell

Copyright (C) 2009 Microsoft Corporation. All rights reserved.

Step3:

PS D:\Malware\Executables> Import-Module .\Invoke-Shellcode.ps1

Step4:

PS D:\Malware\Executables> Invoke-Shellcode -ProcessId <pid of calc.exe>

ex:

PS D:\Malware\Executables> Invoke-Shellcode -ProcessId 2800

Graphical user interface, application

Description automatically generated

Text

Description automatically generated