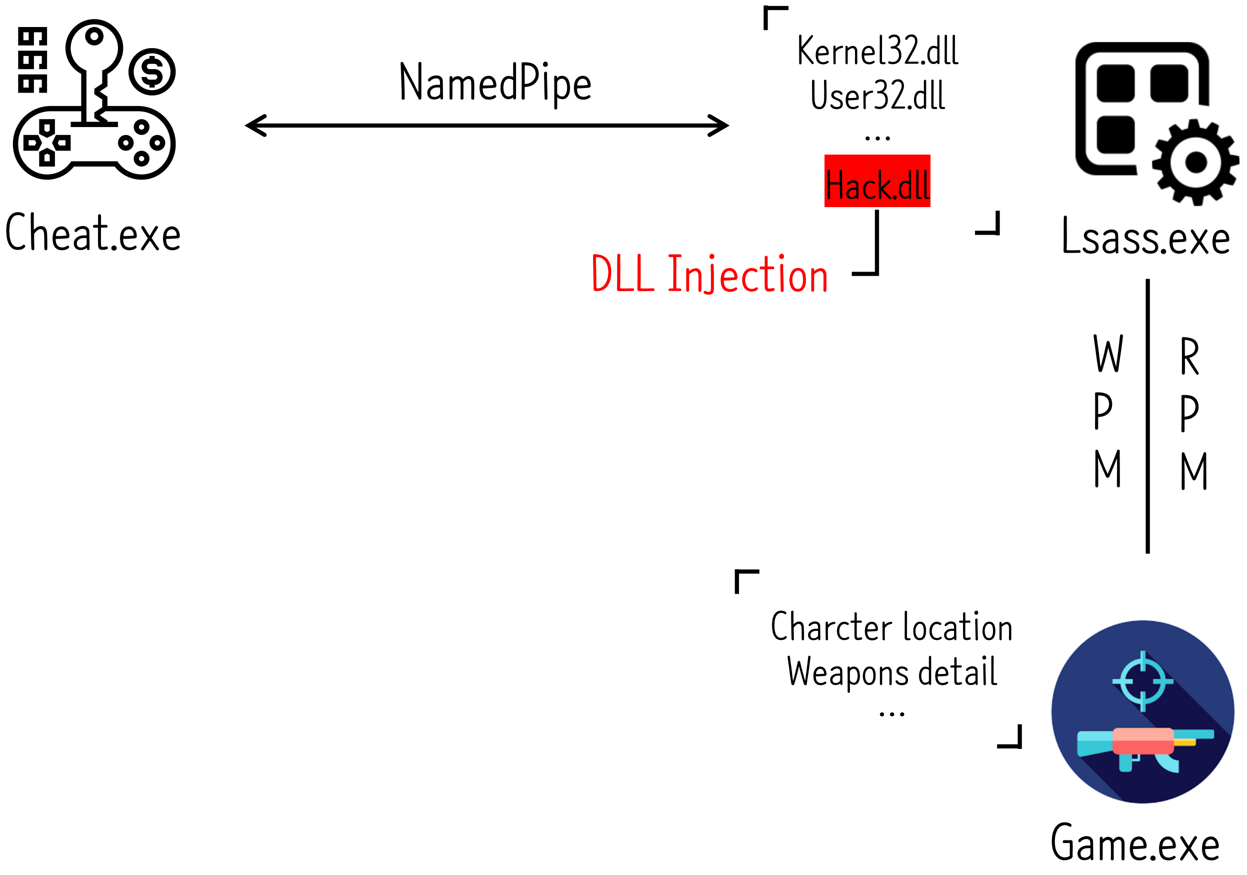
# Thanks harakirinox

ULTIMATE
Handle hijacking

Handle Hijacking



Cheat.exe

NamedPipe

Kernel32.dll
User32.dll
...
Hack.dll

DLL Injection

Lsass.exe

WPM

RPM

Charcter location
Weapons detail
...

Game.exe

AC detection vector

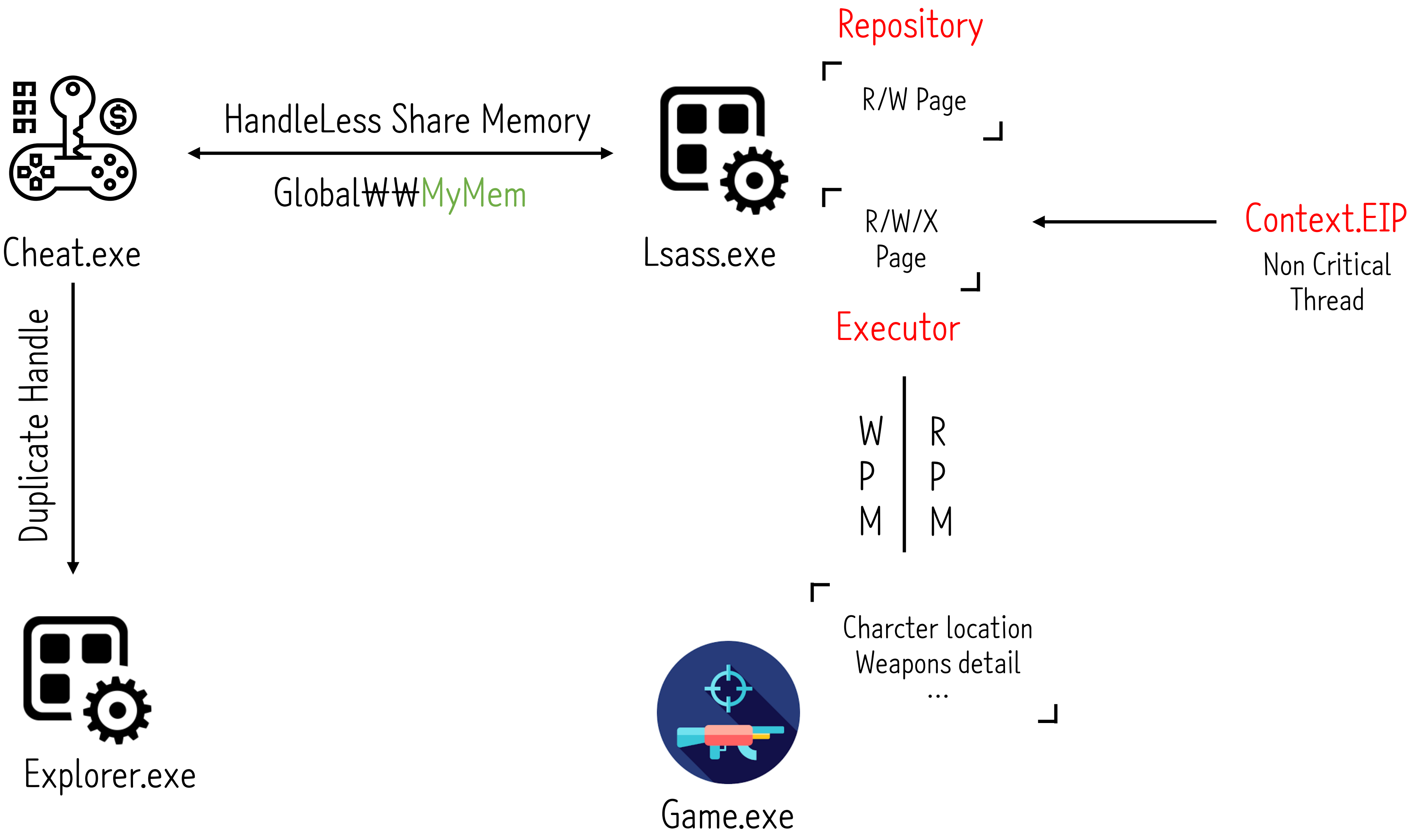
Handle

Memory Section (Executable)

Thread

Injection

ultimate handle hijacking



Cheat.exe

HandleLess Share Memory

Global₩₩MyMem

Lsass.exe

Repository

R/W Page

R/W/X Page

Executor

Context.EIP

Non Critical Thread

Duplicate Handle

Explorer.exe

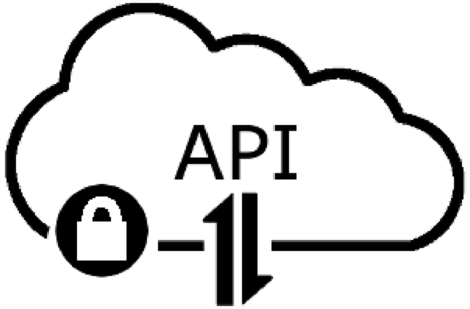
WPM

RPM

Charcter location
Weapons detail
...

Game.exe

Anyhow Keyword is 'reuse'



# Share Memory

CreateFileMapping, OpenFileMapping, MapViewOfFile

# Thread Control

SuspendThread, GetThreadContext, SetThreadContext, ResumeThread

# Read Memory Section

VirtualQueryEx

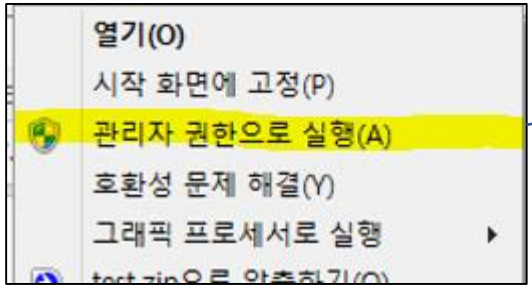
# Get Thread Information

CreateToolhelp32Snapshot, Thread32First, Thread32Next, NtQueryInformationThread, EnumProcessModules, GetModuleFileNameEx, GetModuleInformation

# Handle copy

DuplicateHandle

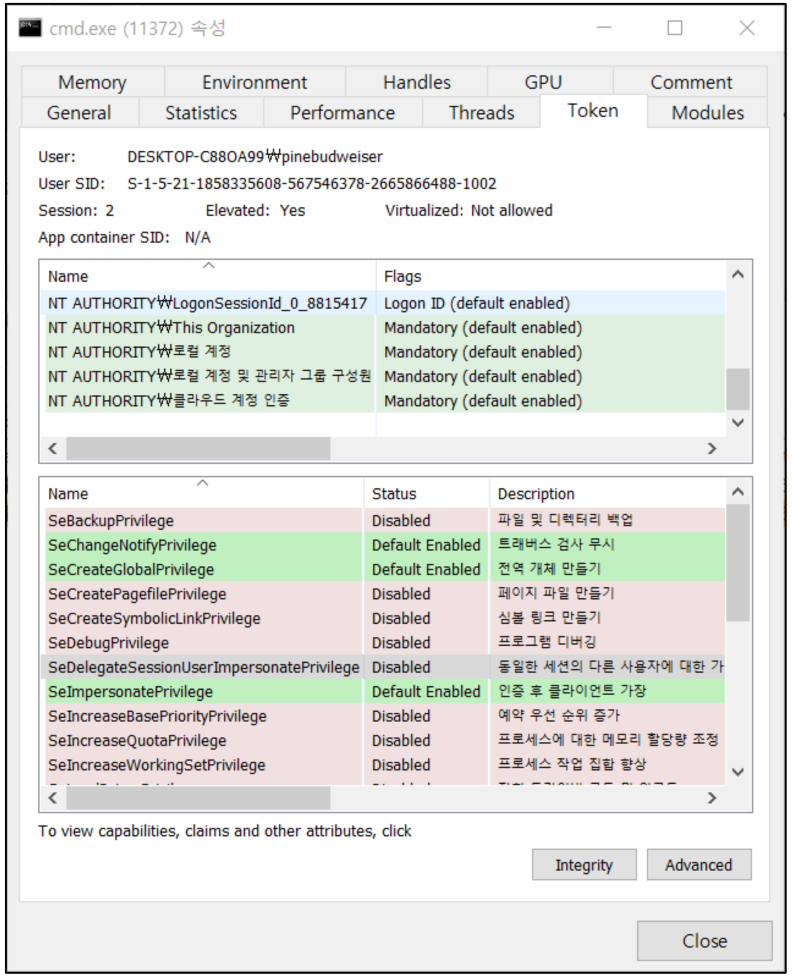
Wait! We don't know windows authority



이 녀석..!

에러의 주범!

windows authority

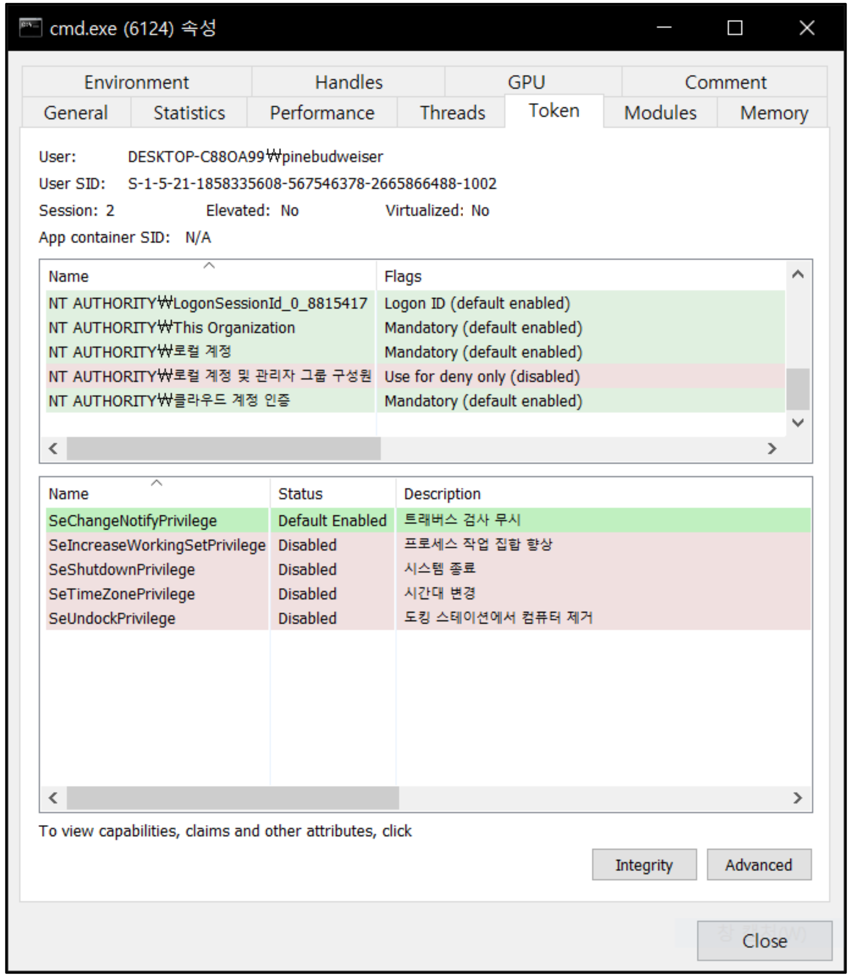


User: DESKTOP-C88OA99₩pinebudweiser
User SID: S-1-5-21-1858335608-567546378-2665866488-1002
Session: 2 Elevated: Yes Virtualized: Not allowed
App container SID: N/A

Name	Flags
NT AUTHORITY₩LogonSessionId_0_8815417	Logon ID (default enabled)
NT AUTHORITY₩This Organization	Mandatory (default enabled)
NT AUTHORITY₩로컬 계정	Mandatory (default enabled)
NT AUTHORITY₩로컬 계정 및 관리자 그룹 구성원	Mandatory (default enabled)
NT AUTHORITY₩클라우드 계정 인증	Mandatory (default enabled)

Name	Status	Description
SeBackupPrivilege	Disabled	파일 및 디렉터리 백업
SeChangeNotifyPrivilege	Default Enabled	트래버스 검사 무시
SeCreateGlobalPrivilege	Default Enabled	전역 개체 만들기
SeCreatePagefilePrivilege	Disabled	페이지 파일 만들기
SeCreateSymbolicLinkPrivilege	Disabled	심볼 링크 만들기
SeDebugPrivilege	Disabled	프로그램 디버깅
SeDelegateSessionUserImpersonatePrivilege	Disabled	동일한 세션의 다른 사용자에 대한 가
SeImpersonatePrivilege	Default Enabled	인증 후 클라이언트 가장
SeIncreaseBasePriorityPrivilege	Disabled	예약 우선 순위 증가
SeIncreaseQuotaPrivilege	Disabled	프로세스에 대한 메모리 할당량 조정
SeIncreaseWorkingSetPrivilege	Disabled	프로세스 작업 집합 향상

To view capabilities, claims and other attributes, click



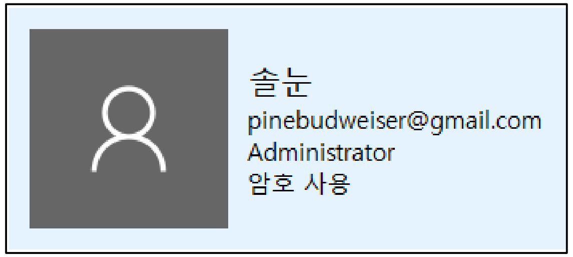
User: DESKTOP-C88OA99₩pinebudweiser
User SID: S-1-5-21-1858335608-567546378-2665866488-1002
Session: 2 Elevated: No Virtualized: No
App container SID: N/A

Name	Flags
NT AUTHORITY₩LogonSessionId_0_8815417	Logon ID (default enabled)
NT AUTHORITY₩This Organization	Mandatory (default enabled)
NT AUTHORITY₩로컬 계정	Mandatory (default enabled)
NT AUTHORITY₩로컬 계정 및 관리자 그룹 구성원	Use for deny only (disabled)
NT AUTHORITY₩클라우드 계정 인증	Mandatory (default enabled)

Name	Status	Description
SeChangeNotifyPrivilege	Default Enabled	트래버스 검사 무시
SeIncreaseWorkingSetPrivilege	Disabled	프로세스 작업 집합 향상
SeShutdownPrivilege	Disabled	시스템 종료
SeTimeZonePrivilege	Disabled	시간대 변경
SeUndockPrivilege	Disabled	도킹 스테이션에서 컴퓨터 제거

To view capabilities, claims and other attributes, click

windows authority



솔눈
pinebudweiser@gmail.com
Administrator
암호 사용

Login Success

Admin Token

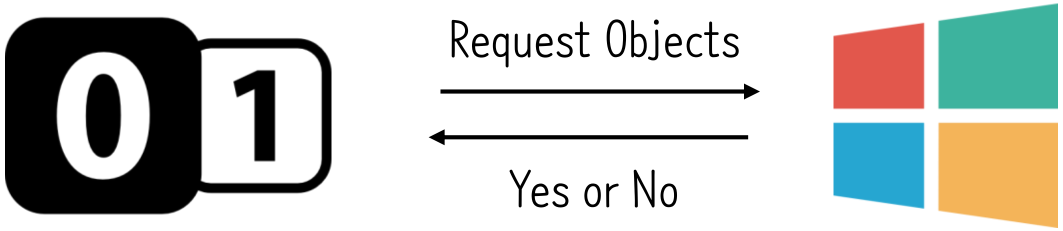
windows authority

Copy admin token

#Privileges
- [+] SeDebugPrivilege
- [+] ···
- [+] SeShutdownPrivilege

#LUID
- [+] LowPart
- [+] HighPart

#Attributes
- [+] SE_PRIVILEGE_ENABLED_BY_DEFAULT
- [+] SE_PRIVILEGE_ENABLED
- [+] SE_PRIVILEGE_REMOVED
- [+] SE_PRIVILEGE_USED_FOR_ACCESS



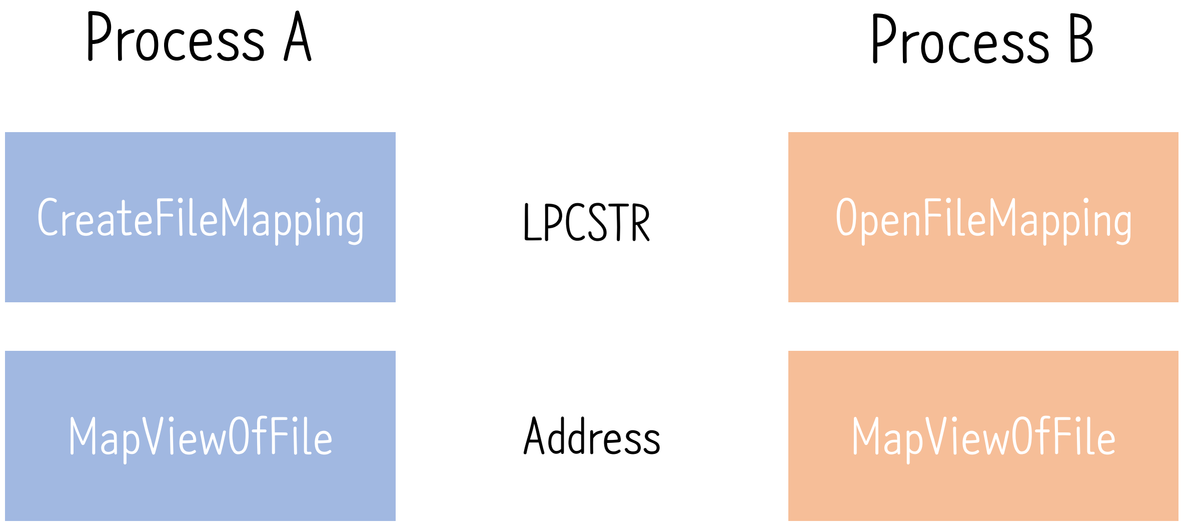
Request Objects

Yes or No

Process.exe

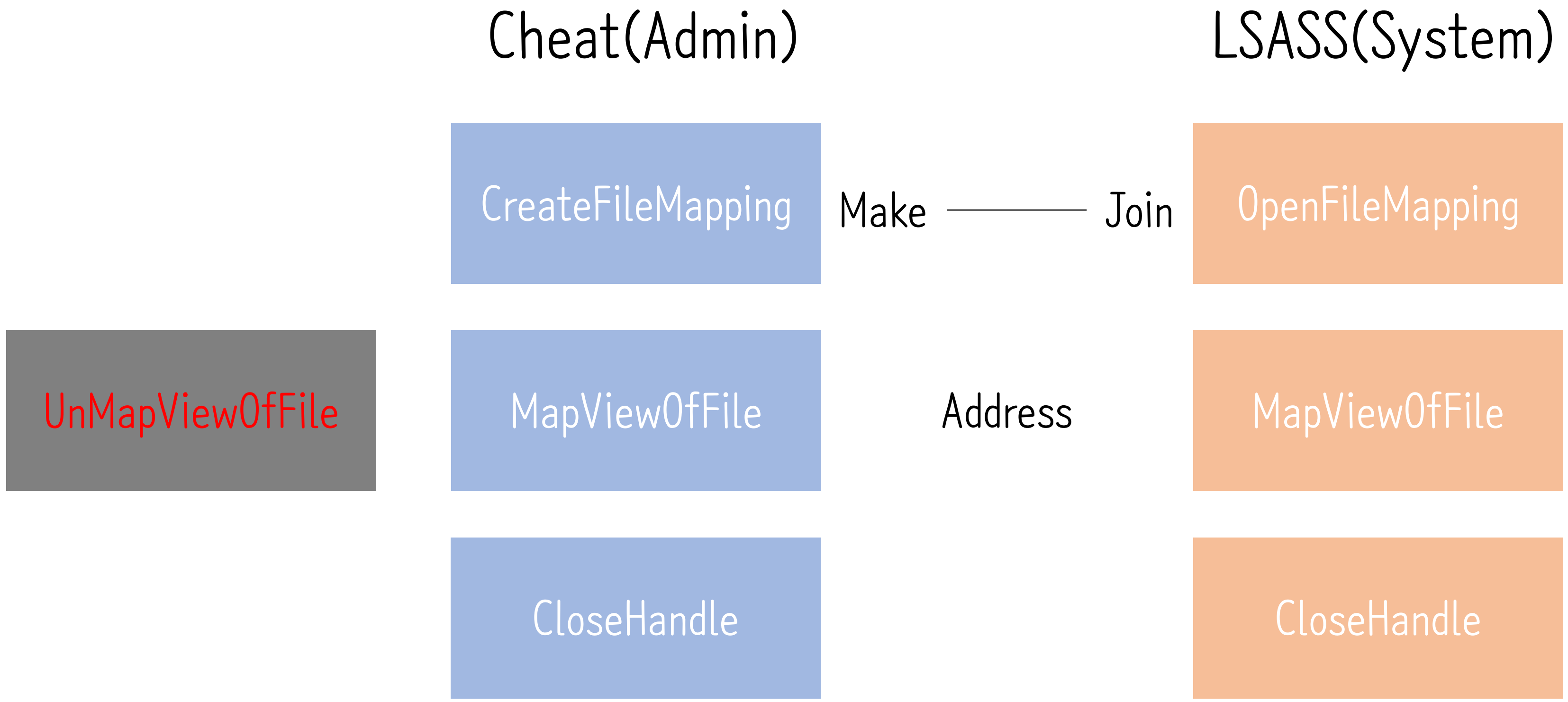
Window

Share Memory



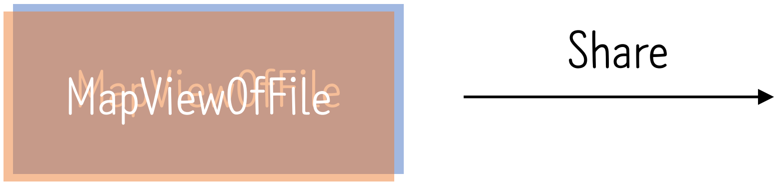
Process A		Process B
CreateFileMapping	LPCSTR	OpenFileMapping
MapViewOfFile	Address	MapViewOfFile

Share Memory



	Cheat(Admin)		LSASS(System)
	CreateFileMapping	Make —— Join	OpenFileMapping
UnMapViewOfFile	MapViewOfFile	Address	MapViewOfFile
	CloseHandle		CloseHandle

Share Memory

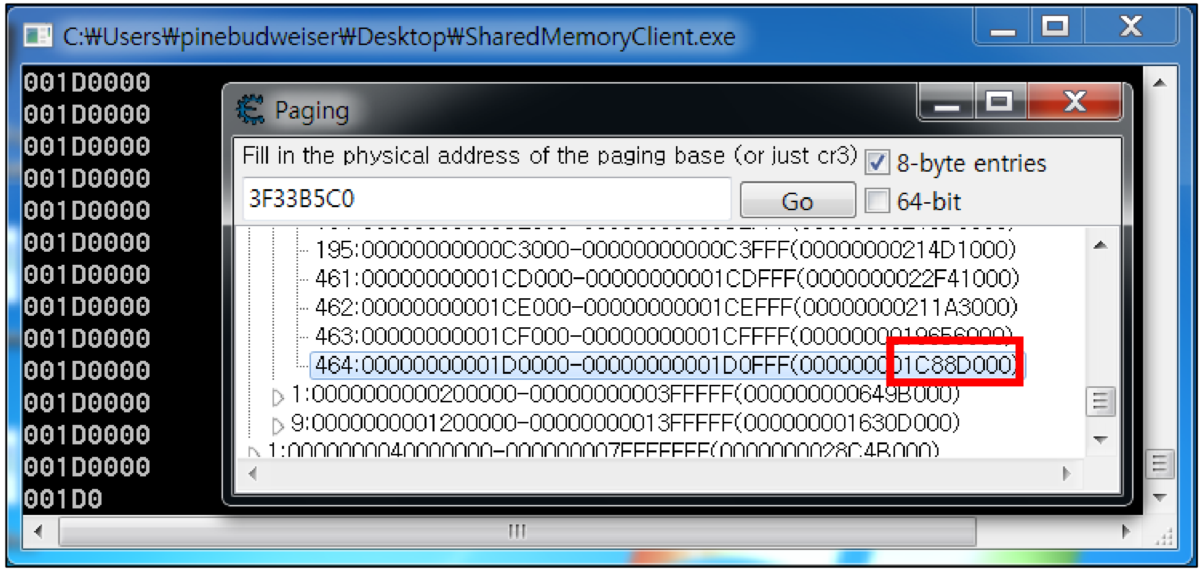


MapViewOfFile

Share

플레이어의 X, Y, Z 좌표(정보)
RPM, WPM의 읽어올 버퍼 주소
…
명령 코드

Share Memory



C:₩Users₩pinebudweiser₩Desktop₩SharedMemoryClient.exe

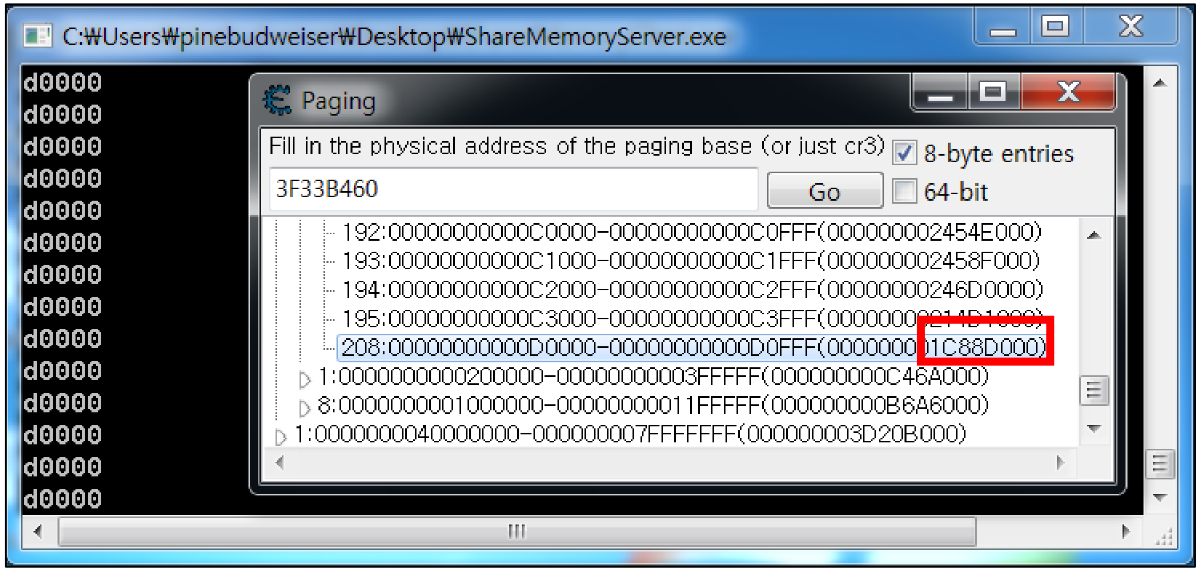
```
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0000
001D0
```

Paging

Fill in the physical address of the paging base (or just cr3) ☑ 8-byte entries

3F33B5C0 Go ☐ 64-bit

```
      195:00000000000C3000-00000000000C3FFF(00000000214D1000)
      461:00000000001CD000-00000000001CDFFF(0000000022F41000)
      462:00000000001CE000-00000000001CEFFF(00000000211A3000)
      463:00000000001CF000-00000000001CFFFF(0000000019656000)
      464:00000000001D0000-00000000001D0FFF(000000001C88D000)
    ▷ 1:0000000000200000-00000000003FFFFF(00000000649B000)
    ▷ 9:0000000001200000-00000000013FFFFF(000000001630D000)
  ▷ 1:0000000040000000-000000007FFFFFFF(0000000028C4B000)
```



C:₩Users₩pinebudweiser₩Desktop₩ShareMemoryServer.exe

```
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
d0000
```

Paging

Fill in the physical address of the paging base (or just cr3) ☑ 8-byte entries

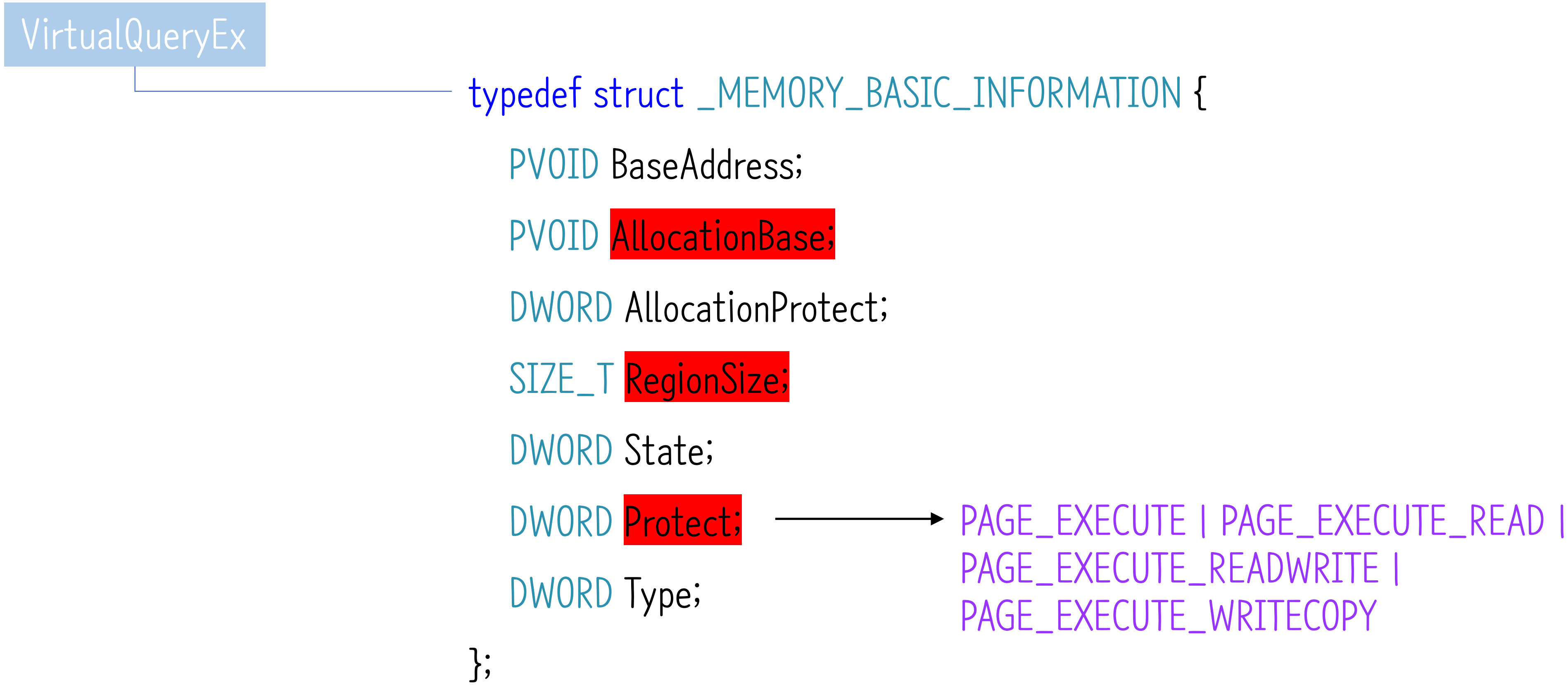
3F33B460 Go ☐ 64-bit

```
      192:00000000000C0000-00000000000C0FFF(000000002454E000)
      193:00000000000C1000-00000000000C1FFF(000000002458F000)
      194:00000000000C2000-00000000000C2FFF(00000000246D0000)
      195:00000000000C3000-00000000000C3FFF(00000000214D1000)
      208:00000000000D0000-00000000000D0FFF(000000001C88D000)
    ▷ 1:0000000000200000-00000000003FFFFF(00000000C46A000)
    ▷ 8:0000000001000000-00000000011FFFFF(00000000B6A6000)
  ▷ 1:0000000040000000-000000007FFFFFFF(000000003D20B000)
```

같은 하늘~ 같은 시간~ 같은 곳에서~

- 가상메모리는 주소는 다르지만 `물리메모리`에서 같은 공간에 매핑 되어있다 -

Reading Memory Section

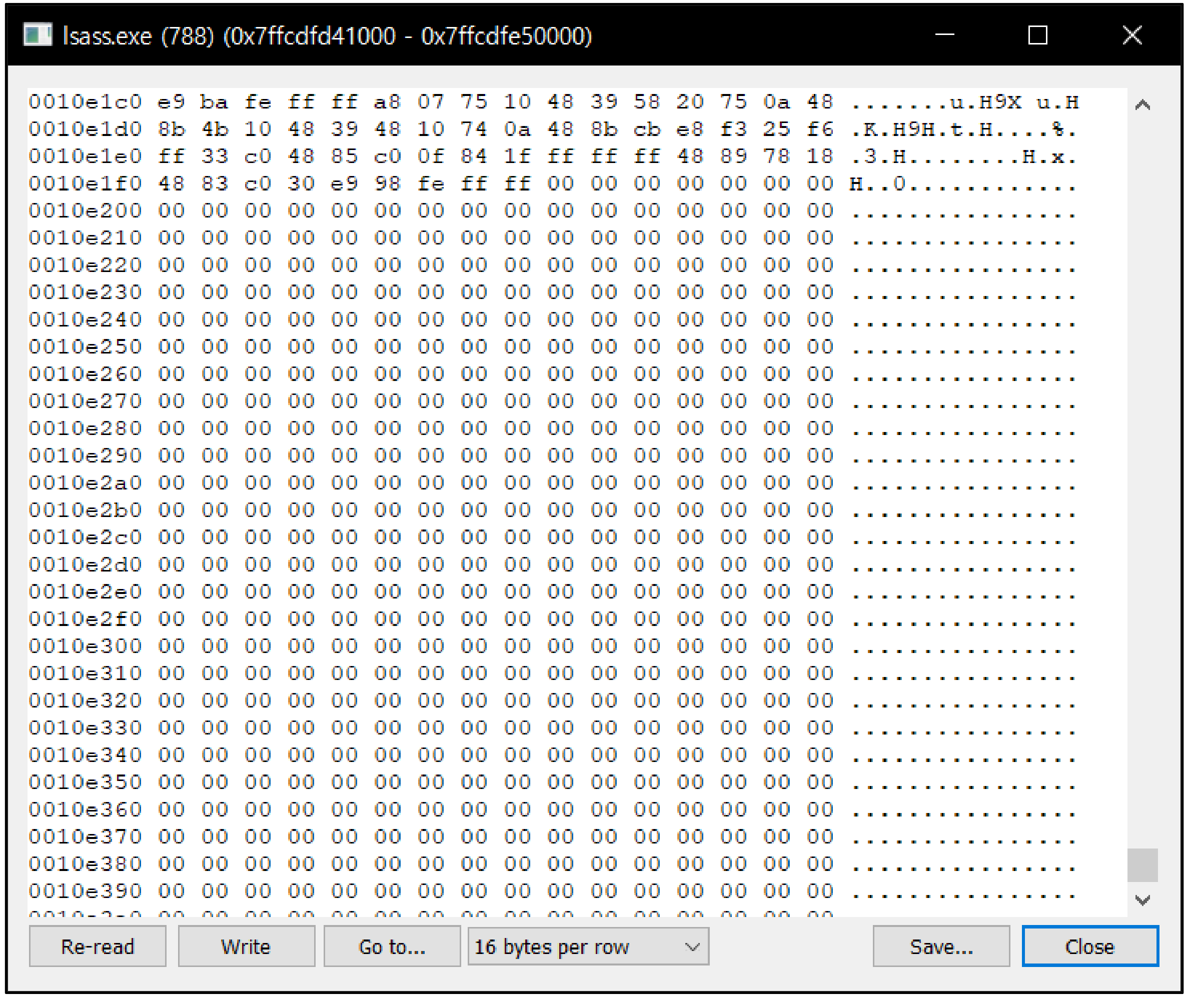


VirtualQueryEx

```
typedef struct _MEMORY_BASIC_INFORMATION {
    PVOID BaseAddress;
    PVOID AllocationBase;
    DWORD AllocationProtect;
    SIZE_T RegionSize;
    DWORD State;
    DWORD Protect;
    DWORD Type;
};
```

PAGE_EXECUTE | PAGE_EXECUTE_READ |
PAGE_EXECUTE_READWRITE |
PAGE_EXECUTE_WRITECOPY

Reading Memory Section



lsass.exe (788) (0x7ffcdfd41000 - 0x7ffcdfe50000)

```
0010e1c0 e9 ba fe ff ff a8 07 75 10 48 39 58 20 75 0a 48 .......u.H9X u.H
0010e1d0 8b 4b 10 48 39 48 10 74 0a 48 8b cb e8 f3 25 f6 .K.H9H.t.H....%.
0010e1e0 ff 33 c0 48 85 c0 0f 84 1f ff ff ff 48 89 78 18 .3.H........H.x.
0010e1f0 48 83 c0 30 e9 98 fe ff ff 00 00 00 00 00 00 00 H..0............
0010e200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e2a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e2b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e2c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e2d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e2e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e2f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010e390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

메모리 페이지는
4K 단위로 할당

Spinlock

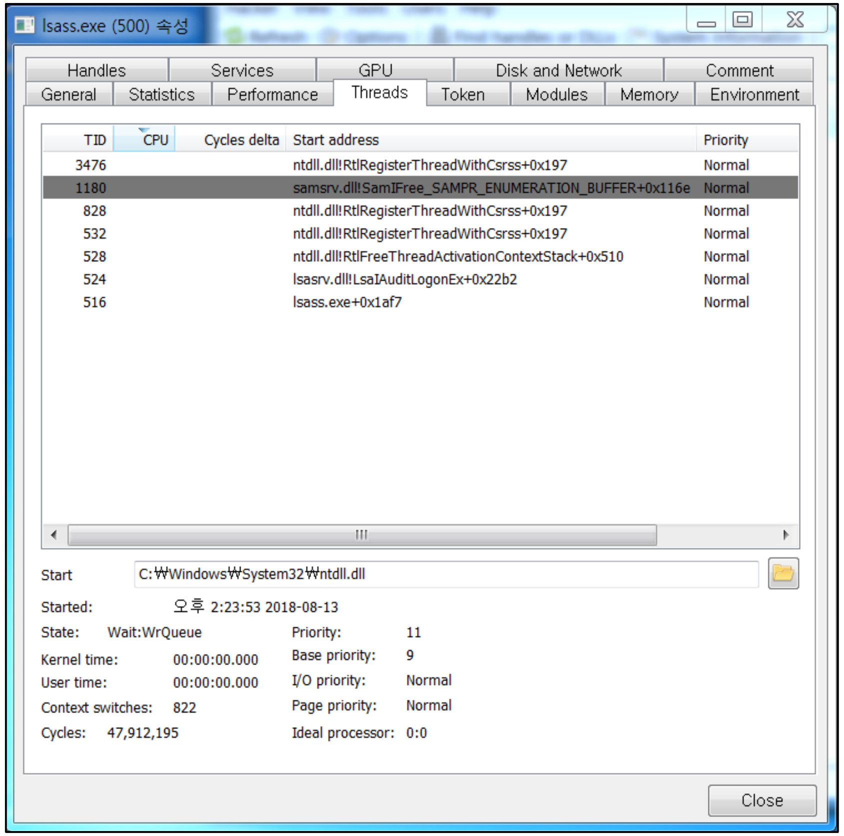
```
SpinLock:
        repe nop
        cmp bl, [sharemem address]
        jne SpinLock
        ret
```

Upgrade?

```
SpinLock:
        repe nop
        xor eax,eax
        mov eax, [sharemem_rpm]
        cmp eax, 1 // on
        jne IsEnd
        push 0
        push [sharemem_size]
        push [sharemem_buffer]
        push [sharemem_target_mem]
        call ReadProcessMemory
IsEnd:
        cmp bl, [spinlock on]
        jne SpinLock
        ret
```

Spin lock need another flow

Find non critical thread



TID	CPU	Cycles delta	Start address	Priority
3476			ntdll.dll!RtlRegisterThreadWithCsrss+0x197	Normal
1180			samsrv.dll!SamIFree_SAMPR_ENUMERATION_BUFFER+0x116e	Normal
828			ntdll.dll!RtlRegisterThreadWithCsrss+0x197	Normal
532			ntdll.dll!RtlRegisterThreadWithCsrss+0x197	Normal
528			ntdll.dll!RtlFreeThreadActivationContextStack+0x510	Normal
524			lsasrv.dll!LsaIAuditLogonEx+0x22b2	Normal
516			lsass.exe+0x1af7	Normal

Start C:₩Windows₩System32₩ntdll.dll

Started: 오후 2:23:53 2018-08-13

State: Wait:WrQueue

Kernel time: 00:00:00.000

User time: 00:00:00.000

Context switches: 822

Cycles: 47,912,195

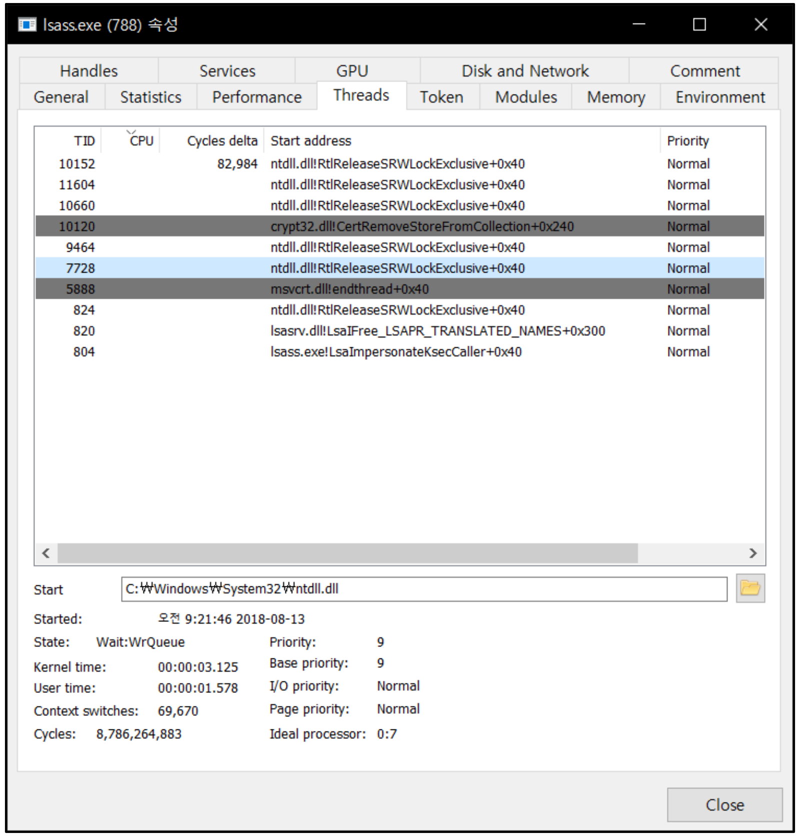
Priority: 11

Base priority: 9

I/O priority: Normal

Page priority: Normal

Ideal processor: 0:0



TID	CPU	Cycles delta	Start address	Priority
10152		82,984	ntdll.dll!RtlReleaseSRWLockExclusive+0x40	Normal
11604			ntdll.dll!RtlReleaseSRWLockExclusive+0x40	Normal
10660			ntdll.dll!RtlReleaseSRWLockExclusive+0x40	Normal
10120			crypt32.dll!CertRemoveStoreFromCollection+0x240	Normal
9464			ntdll.dll!RtlReleaseSRWLockExclusive+0x40	Normal
7728			ntdll.dll!RtlReleaseSRWLockExclusive+0x40	Normal
5888			msvcrt.dll!endthread+0x40	Normal
824			ntdll.dll!RtlReleaseSRWLockExclusive+0x40	Normal
820			lsasrv.dll!LsaIFree_LSAPR_TRANSLATED_NAMES+0x300	Normal
804			lsass.exe!LsaImpersonateKsecCaller+0x40	Normal

Start C:₩Windows₩System32₩ntdll.dll

Started: 오전 9:21:46 2018-08-13

State: Wait:WrQueue

Kernel time: 00:00:03.125

User time: 00:00:01.578

Context switches: 69,670

Cycles: 8,786,264,883

Priority: 9

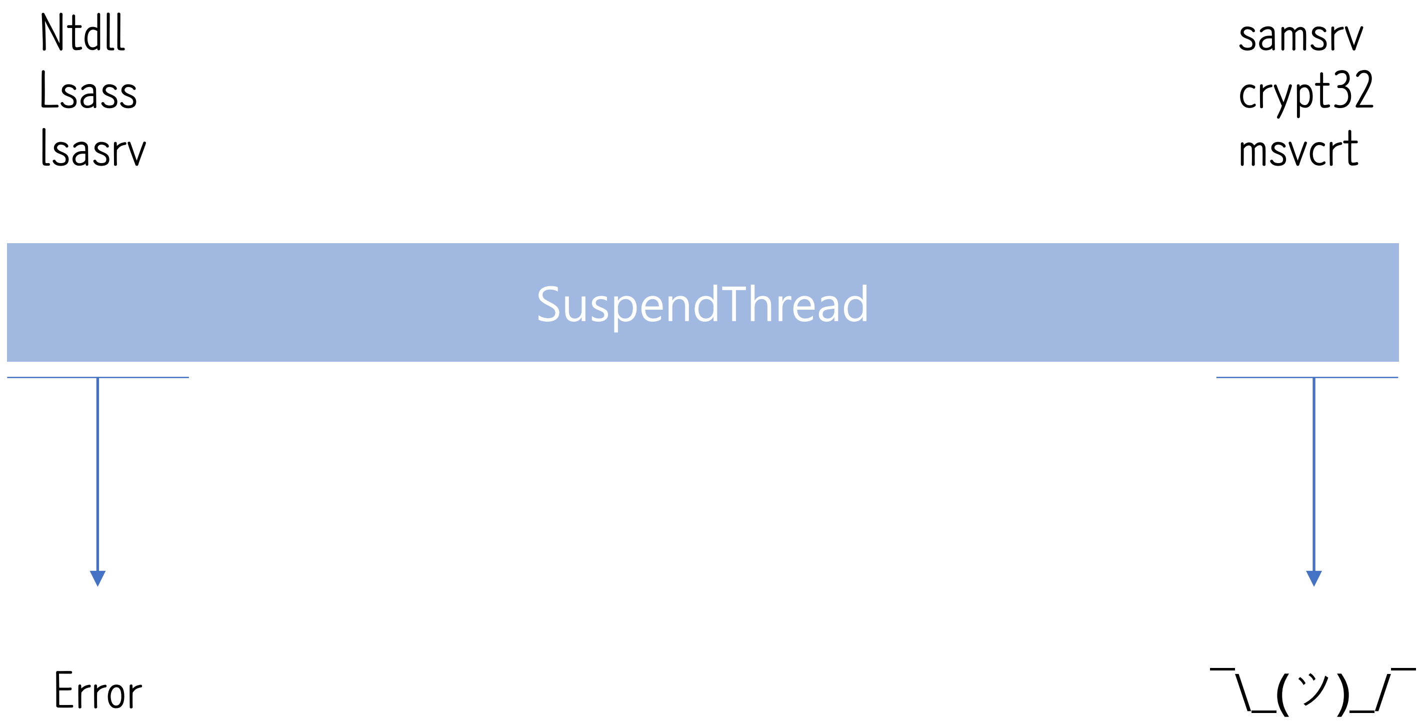
Base priority: 9

I/O priority: Normal

Page priority: Normal

Ideal processor: 0:7

Find non critical thread



Ntdll
Lsass
lsasrv

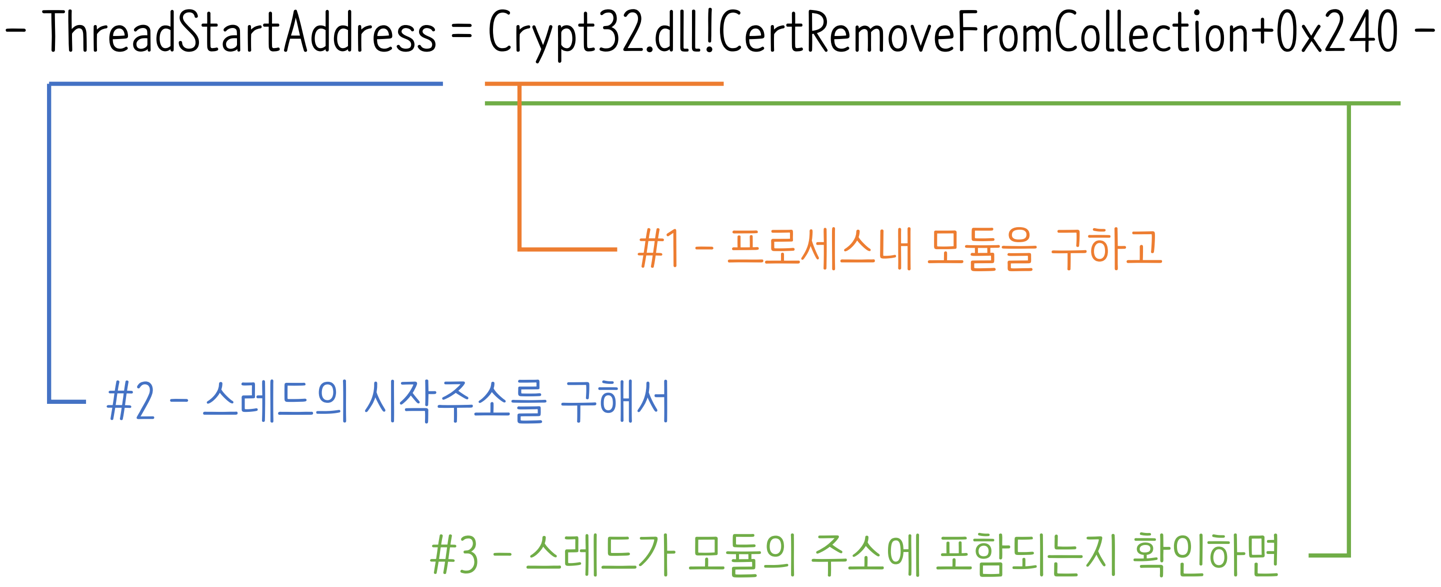
samsrv
crypt32
msvcrt

SuspendThread

Error

¯_(ツ)_/¯

StartAddress and Module



- ThreadStartAddress = Crypt32.dll!CertRemoveFromCollection+0x240 -

#1 - 프로세스내 모듈을 구하고

#2 - 스레드의 시작주소를 구해서

#3 - 스레드가 모듈의 주소에 포함되는지 확인하면

미리 알아 둔 탈취해도 되는 스레드임을 알 수 있다!

Find Thread Information

#ToolHelp Library

CreateToolhelp32Snapshot

Thread32First

Thread32Next

```
typedef struct tagTHREADENTRY32
{
    DWORD   dwSize;
    DWORD   cntUsage;
    DWORD   th32ThreadID;       // this thread
    DWORD   th32OwnerProcessID; // Process this thread is associated with
    LONG    tpBasePri;
    LONG    tpDeltaPri;
    DWORD   dwFlags;
} THREADENTRY32;
```

- NtQueryInformationThread(handle, info_class, info, size info, ret length)

```
NtQueryInformationThread(hThread, (THREADINFOCLASS)ThreadQuerySetWin32StartAddress, &StartAddress,
sizeof(StartAddress), NULL)
```

Find Thread Information

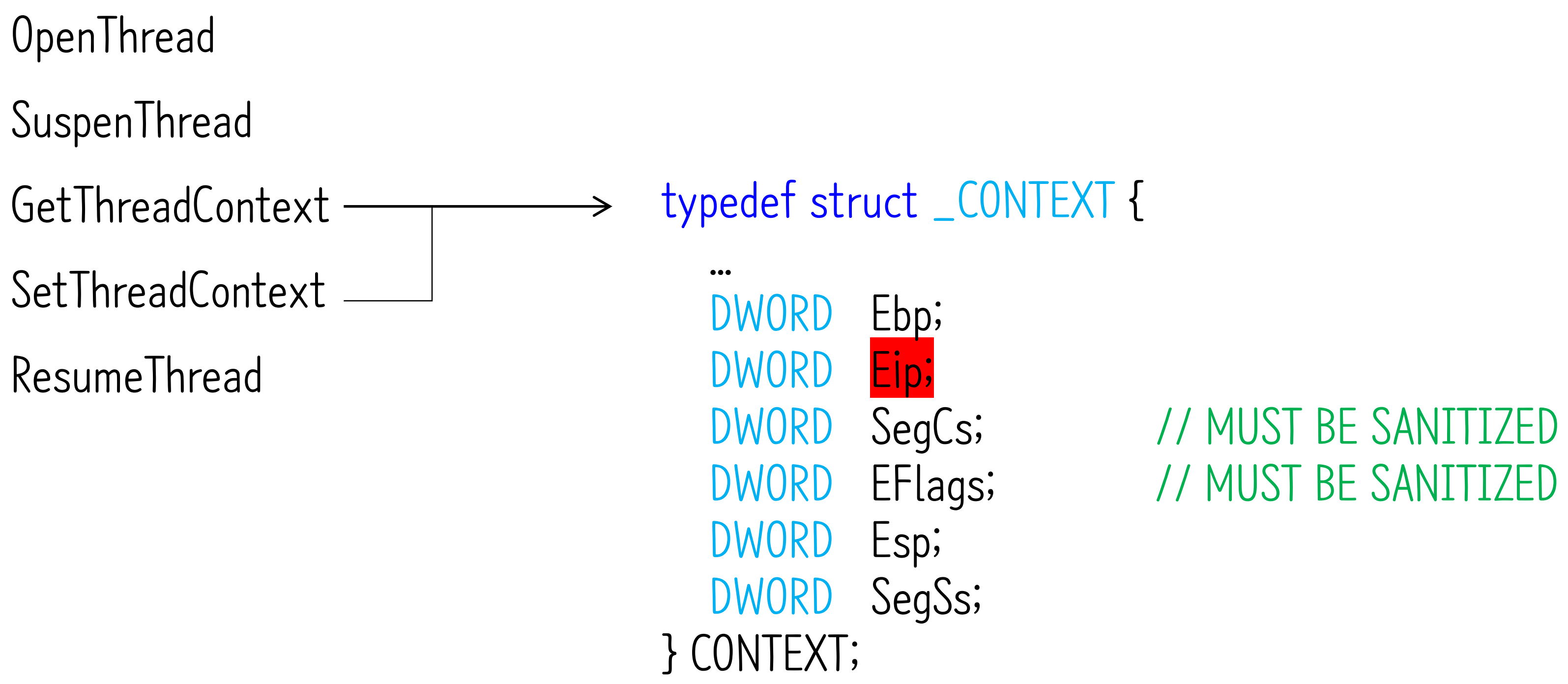
#EnumProcessModules

GetModuleFileNameEx → “C:₩Windows₩SYSTEM32₩ntdll.dll”

GetModuleInformation →

```
typedef struct _MODULEINFO {
    LPVOID lpBaseOfDll;
    DWORD SizeOfImage;
    LPVOID EntryPoint;
} MODULEINFO, *LPMODULEINFO;
```

Change EIP



OpenThread

SuspenThread

GetThreadContext

SetThreadContext

ResumeThread

```
typedef struct _CONTEXT {
    ...
    DWORD   Ebp;
    DWORD   Eip;
    DWORD   SegCs;          // MUST BE SANITIZED
    DWORD   EFlags;         // MUST BE SANITIZED
    DWORD   Esp;
    DWORD   SegSs;
} CONTEXT;
```

Do you have any questions?