HANDLE

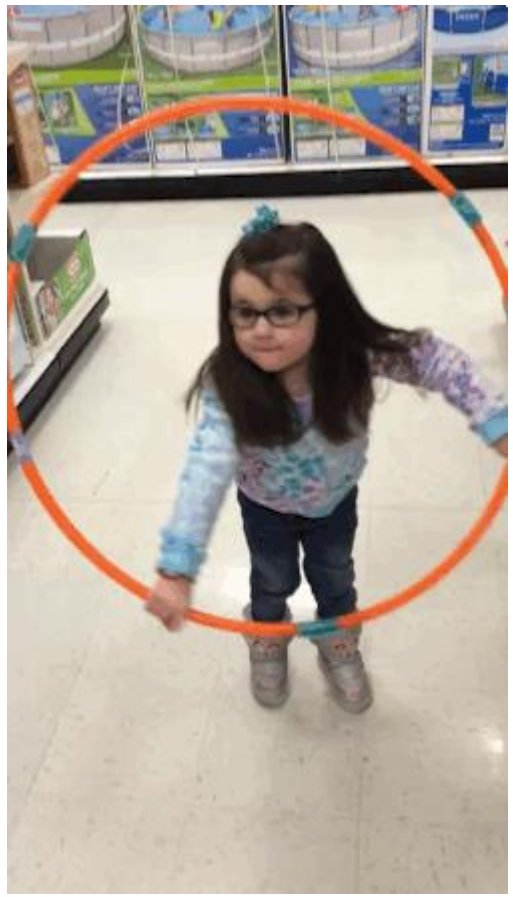
→ Hijacking

Proof of Concept

Thanks harakrinox

18.07.19 #pinebudweiser

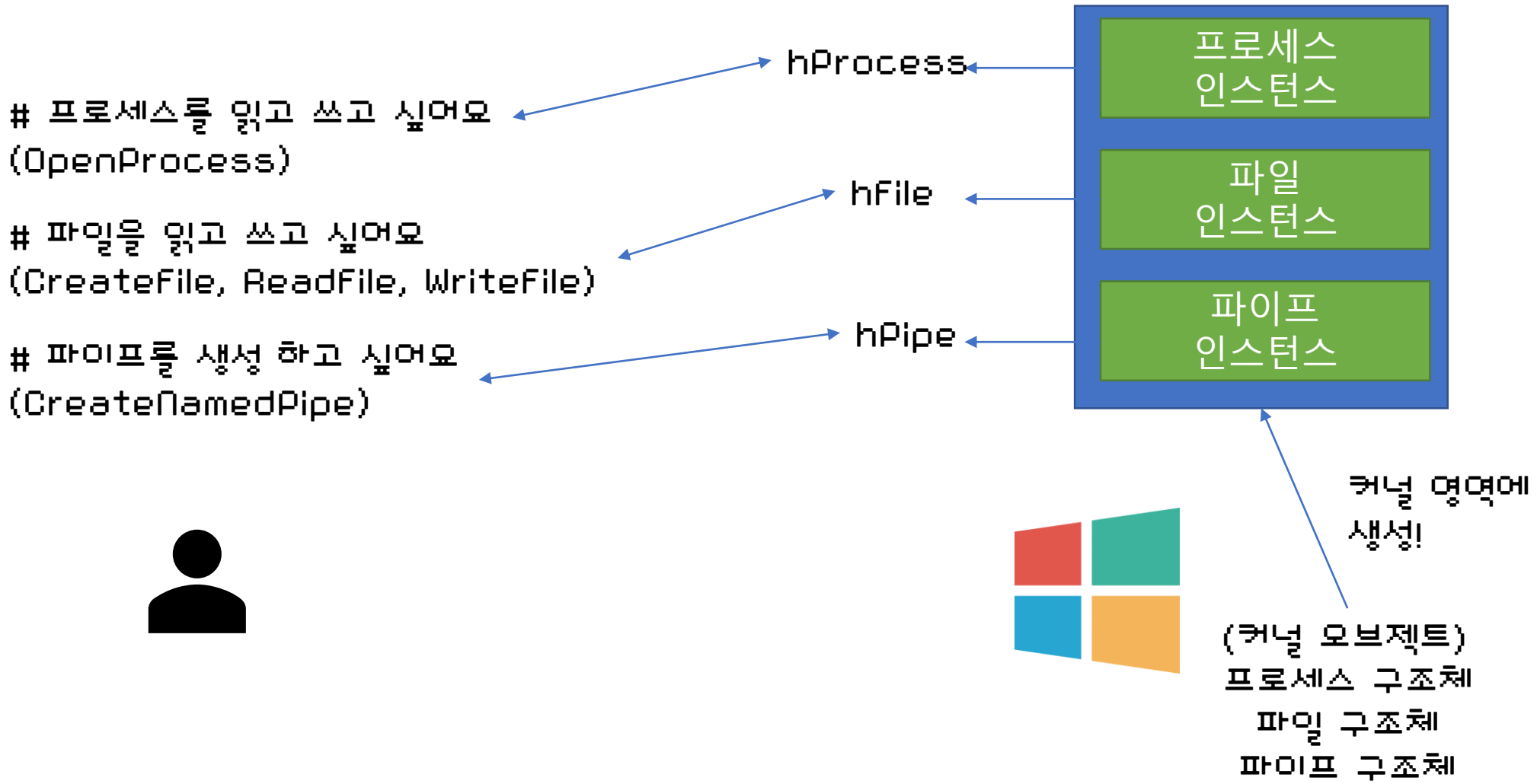
핸들이란?



핸들

- 4Byte의 정수 값
- 커널 객체에 접근 하기 위한 방법
- 열고 나선? 닫아 줘야 함!

잘 모르겠는 걸요?


프로세스를 읽고 쓰고 싶어요
(OpenProcess)
파일을 읽고 쓰고 싶어요
(CreateFile, ReadFile, WriteFile)
파이프를 생성 하고 싶어요
(CreateNamedPipe)
hProcess
hFile
hPipe
프로세스
인스턴스
파일
인스턴스
파이프
인스턴스
커널 영역에
생성!
(커널 오브젝트)
프로세스 구조체
파일 구조체
파이프 구조체

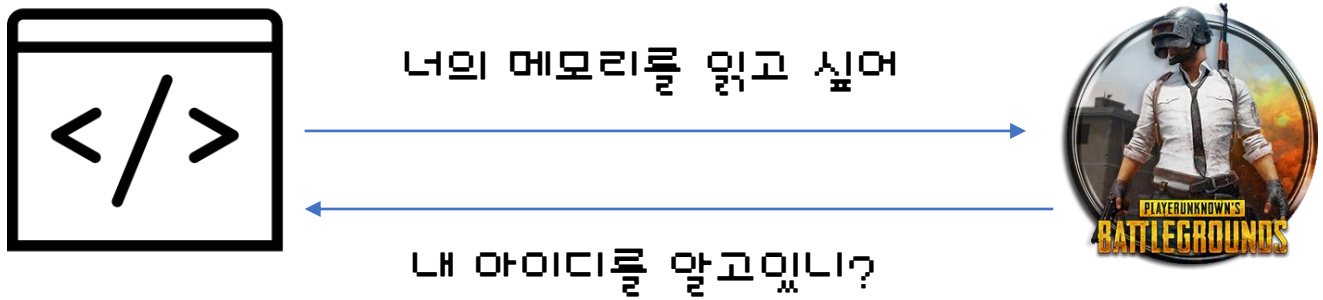
하이재킹

“

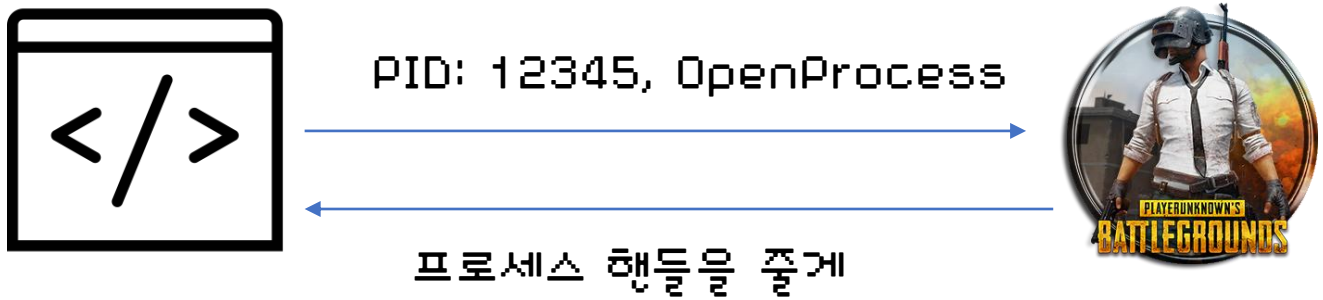
”

사용하던 리소스를 훔쳐서 사용 하는 것

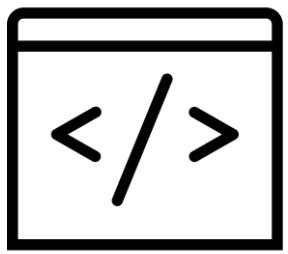
왜 이게 우회법이죠?



왜 이게 우회법이죠?


PID: 12345, OpenProcess
프로세스 핸들을 줄게
PLAYERUNKNOWN'S
BATTLEGROUNDS

왜 이게 우회법이죠?



PID: 12345, OpenProcess

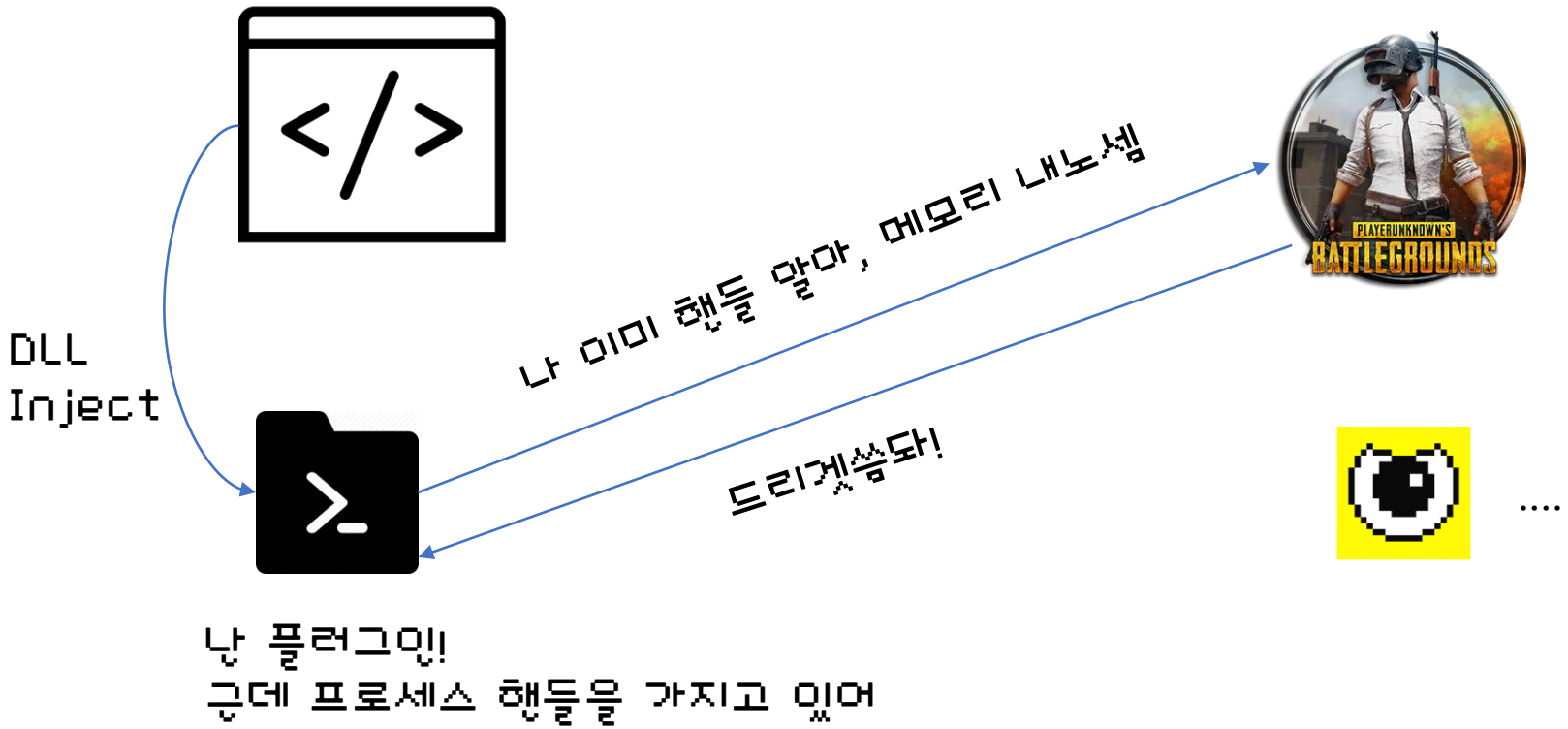
~~프로세스 핸들을 줄게~~

이쉑히 수상한데?
함 지켜보자

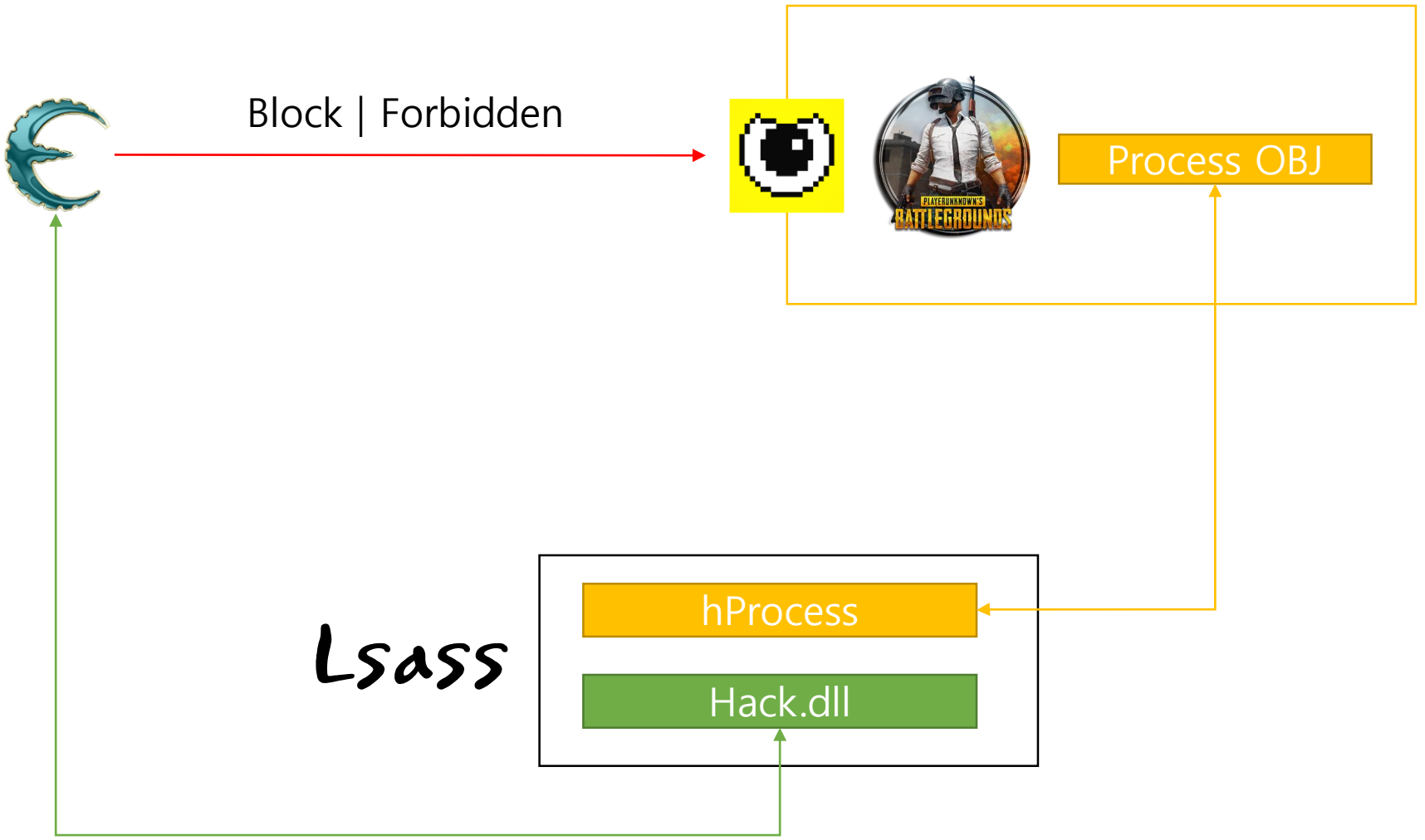
왜 이게 우회법이죠?

You have been banned

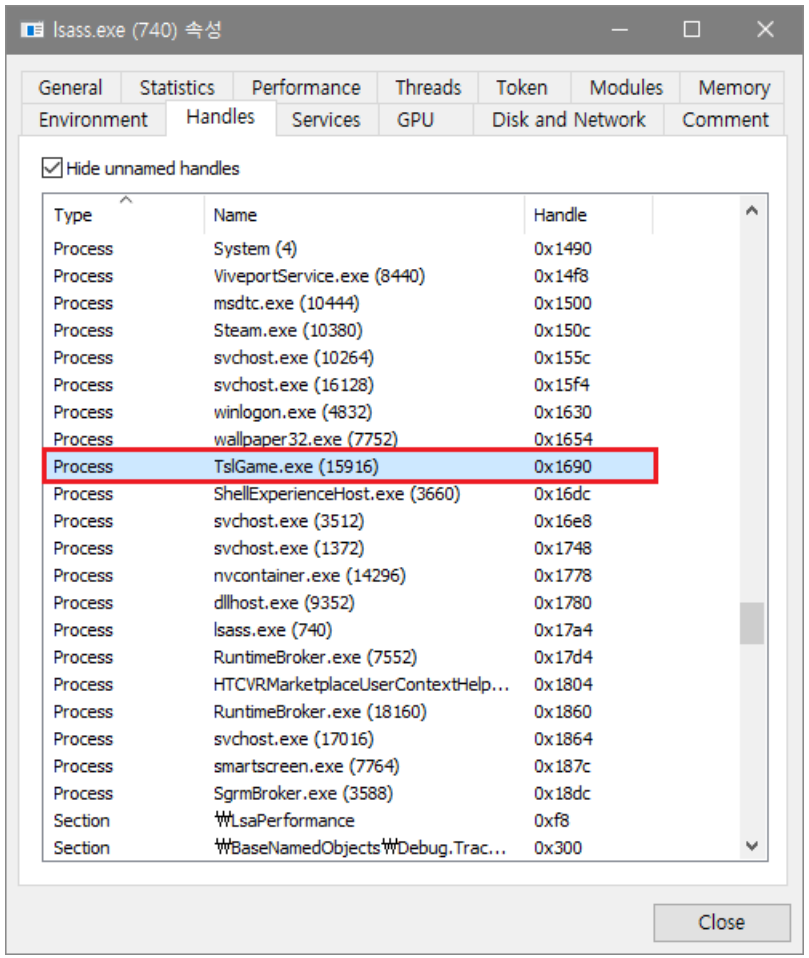
왜 이게 우회법이죠?


DLL
Inject
나 이미 핸들 말야, 메모리 내노셈
드리겟씀돠!
PLAYERUNKNOWN'S
BATTLEGROUNDS
....
난 플러그인!
근데 프로세스 핸들을 가지고 있어

Concept



Check

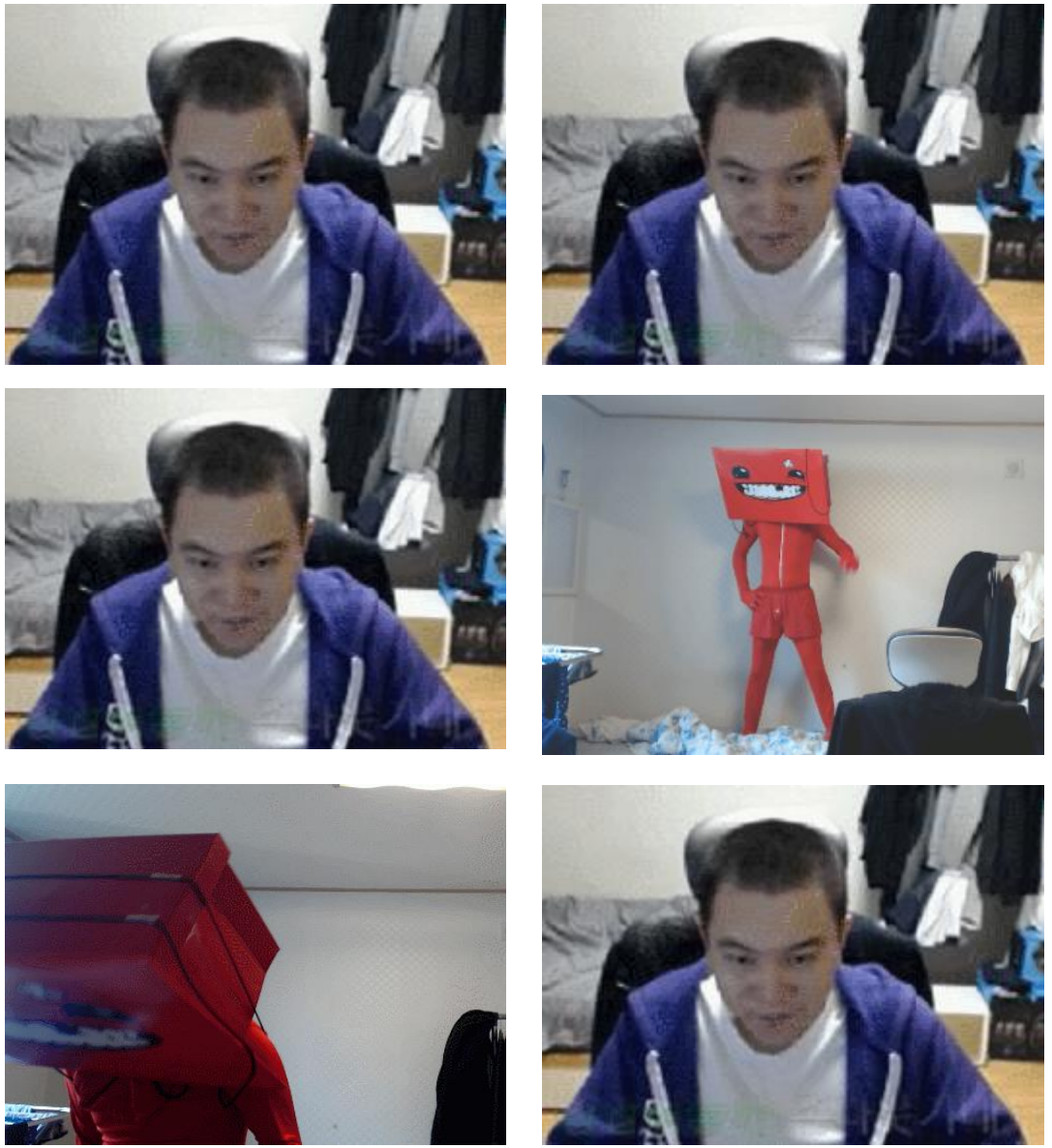

lsass.exe (740) 속성
General
Statistics
Performance
Threads
Token
Modules
Memory
Environment
Handles
Services
GPU
Disk and Network
Comment
Hide unnamed handles
Type
Name
Handle
Process System (4) 0x1490
Process ViveportService.exe (8440) 0x14f8
Process msdtc.exe (10444) 0x1500
Process Steam.exe (10380) 0x150c
Process svchost.exe (10264) 0x155c
Process svchost.exe (16128) 0x15f4
Process winlogon.exe (4832) 0x1630
Process wallpaper32.exe (7752) 0x1654
Process TslGame.exe (15916) 0x1690
Process ShellExperienceHost.exe (3660) 0x16dc
Process svchost.exe (3512) 0x16e8
Process svchost.exe (1372) 0x1748
Process nvcontainer.exe (14296) 0x1778
Process dllhost.exe (9352) 0x1780
Process lsass.exe (740) 0x17a4
Process RuntimeBroker.exe (7552) 0x17d4
Process HTCVRMarketplaceUserContextHelp... 0x1804
Process RuntimeBroker.exe (18160) 0x1860
Process svchost.exe (17016) 0x1864
Process smartscreen.exe (7764) 0x187c
Process SgrmBroker.exe (3588) 0x18dc
Section ₩LsaPerformance 0xf8
Section ₩BaseNamedObjects₩Debug.Trac... 0x300
Close

프로세스간 통신(IPC)

- File
- Anonymous Pipe
- Named Pipe
- Socket
- Shared Memory
- Memory Mapped File
- Windows Message

프로세스간 통신(IPC)

- File
- Anonymous Pipe
- Named Pipe
- Socket
- Shared Memory
- Memory Mapped File
- Windows Message



파이프 |

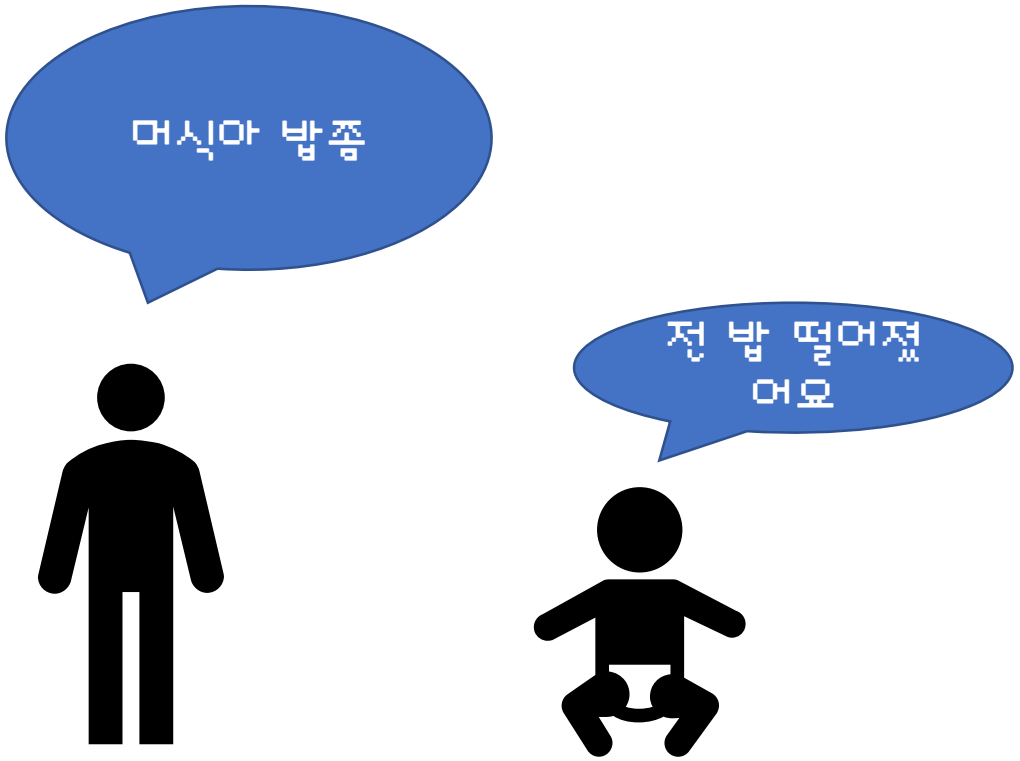
이름 없는 파이프와 이름 있는 파이프로 나뉨

이름 없는 파이프

- 프로세스간 관계가 있어야함
Ex) 부모-자식 프로세스

- 읽기, 쓰기용 핸들이 따로 있음

이름 있는 파이프



- 프로세스간 관계 필요 없음
- 양방향 통신 가능
- Byte형, Message형 전송 방식이 있음
- 파이프 이름은 ₩₩.₩pipe₩pipename 규칙을 따름

테스트 프로그램

Target Process

varInt
varString

Pipe Server

OpenProcess
CreateNamedPipe
ConnectNamedPipe
Read/WriteFile

Pipe Client

CreateFile
Read/WriteFile

Show you

Next week

Lsass가 뭔데 프로세스의 핸들을 가지고 있나요?
윈도우 10에 적용된 PPL(Protected Process Light)
난 C++을 시러해, 근데 써야 될 거같은데?(코드 수정)