










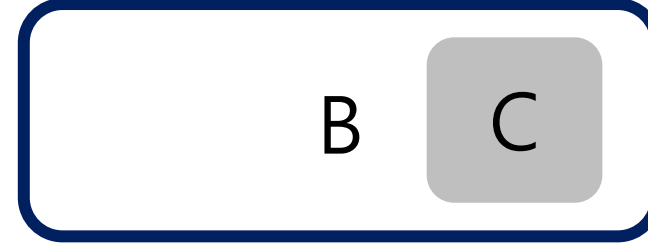
SCP 이다영

DLL Injection

DLL이란?

-  aadcloudap.dll
-  aadjcsp.dll
-  aadtb.dll
-  aadWamExtension.dll
-  AarSvc.dll
-  AboutSettingsHandlers.dll
-  AboveLockAppHost.dll
-  accessibilitycpl.dll
-  accountaccessor.dll

DLL이란?



C가 필요한 프로그램이 100개이고 100개의 프로그램을 동시에 돌린다면?

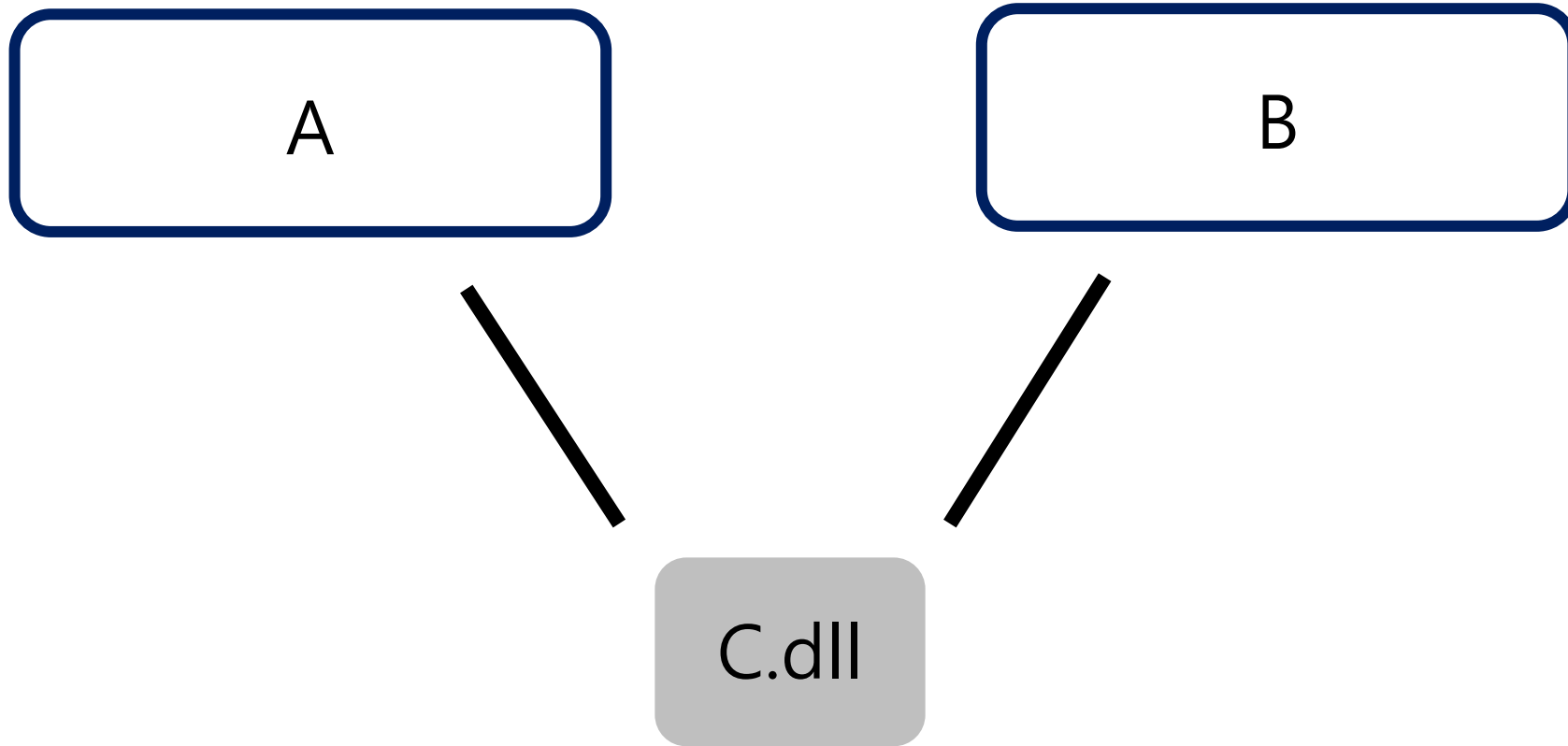
-> C가 들어간 프로그램이 100개이고, C 100개가 동시 실행 될 것



DLL(Dynamic Link Library)

: 동적 링크 라이브러리

DLL 인젝션이란?



-> 사용자가 원하는 동작을 하도록 DLL을 만든 뒤,
인젝션(삽입) 하여 프로그램이 원하는 동작을 하도록 만들 수 있다

=> DLL 인젝션

DLL 인젝션이란?

└─ 프로세스에서 DLL을 로드하는데 사용되는 함수

다른 프로세스에게 `LoadLibrary()` API를 스스로 호출하도록
명령하여 사용자가 원하는 DLL을 로딩하는 것

DLL 인젝션 기법을 통해 할 수 있는 것



API 후킹, 프로그램 기능 개선 및 버그 패치 등



notepad.exe



myhack.dll



index.html

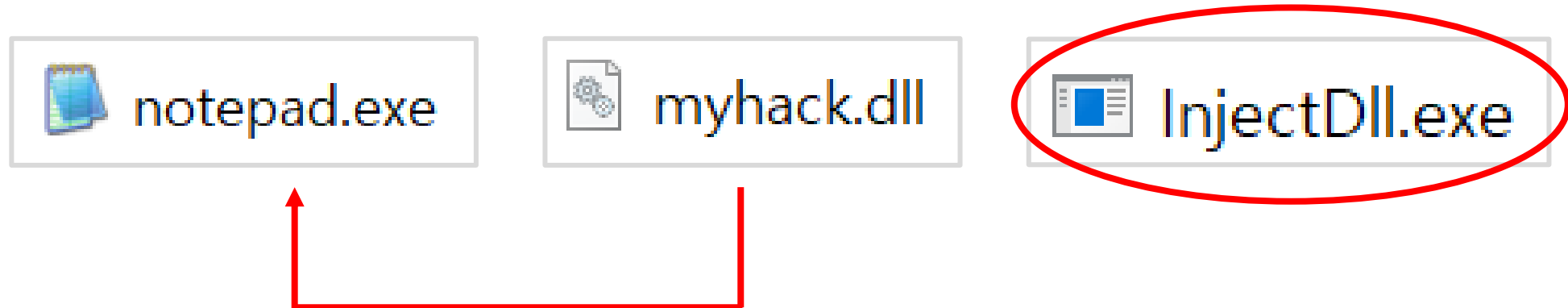
myhack.dll은 notepad.exe 프로세스에 이미 로딩된 DLL들(kernel32.dll, user32.dll 등)과 마찬가지로 notepad.exe 프로세스 메모리에 대한
정당한 접근 권한을 가진다

-> 사용자가 원하는 어떤 일이라도 수행할 수 있다



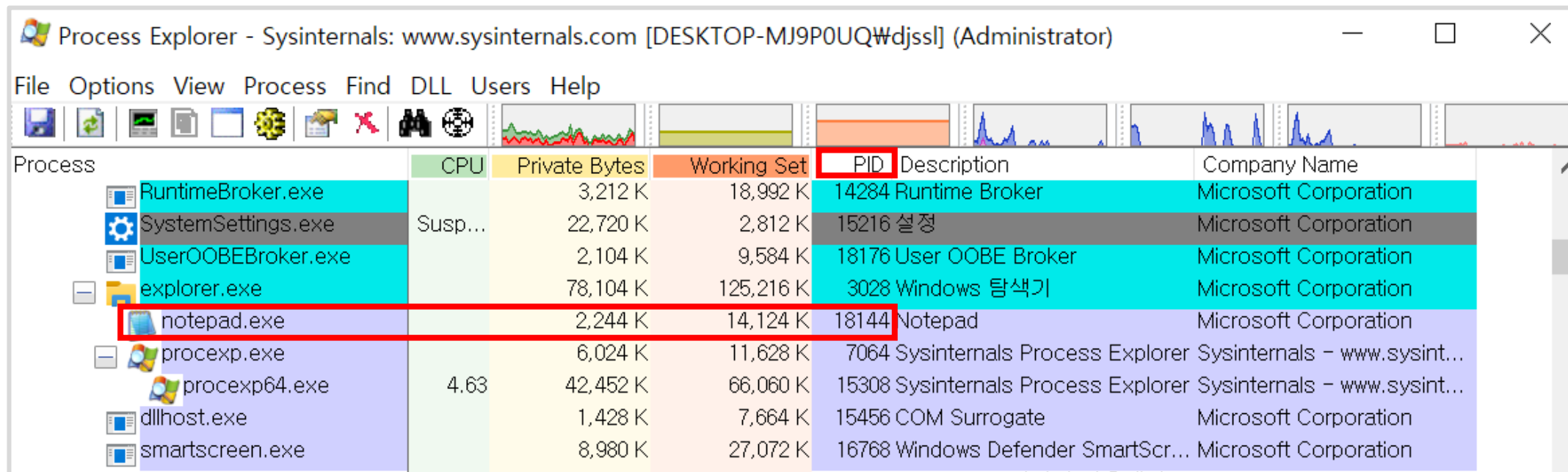
DLL 인젝션 구현 방법

1. 원격 스레드 생성(CreateRemoteThread() API)
2. 레지스트리 이용(AppInit_DLLs 값)



원격 스크린 생성

notepad.exe 프로그램 실행



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-MJ9P0UQWdjssl] (Administrator)

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
RuntimeBroker.exe		3,212 K	18,992 K	14284	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	22,720 K	2,812 K	15216	설정	Microsoft Corporation
UserOOBEBroker.exe		2,104 K	9,584 K	18176	User OOBEBroker	Microsoft Corporation
explorer.exe		78,104 K	125,216 K	3028	Windows 탐색기	Microsoft Corporation
notepad.exe		2,244 K	14,124 K	18144	Notepad	Microsoft Corporation
procexp.exe		6,024 K	11,628 K	7064	Sysinternals Process Explorer	Sysinternals - www.sysint...
procexp64.exe	4.63	42,452 K	66,060 K	15308	Sysinternals Process Explorer	Sysinternals - www.sysint...
dllhost.exe		1,428 K	7,664 K	15456	COM Surrogate	Microsoft Corporation
smartscreen.exe		8,980 K	27,072 K	16768	Windows Defender SmartScr...	Microsoft Corporation

PID(Process ID): 각 프로세스나 서비스를 식별하기 위해 할당한 번호
notepad.exe의 PID: 18144

원격 스레드 생성





myhack.dll 인젝션

```
C:\Users\djssl\Desktop\test>injectDll.exe 18144 C:\Users\djssl\Desktop\test\myhack.dll  
InjectDll("C:\Users\djssl\Desktop\test\myhack.dll") success!!!
```




notepad.exe에 myhack.dll 인젝션 성공

원격 스레드 생성

myhack.dll 인젝션

	notepad.exe	< 0.01	2,880 K	18,684 K	18144 Notepad	Microsoft Corporation
	procexp.exe		5,888 K	10,532 K	7064 Sysinternals Process Explorer	Sysinternals - www.sysint...
	procexp64.exe	3.13	42,268 K	44,932 K	15308 Sysinternals Process Explorer	Sysinternals - www.sysint...
	dllhost.exe		1,508 K	7,440 K	15456 COM Surrogate	Microsoft Corporation
Name	Description	Company Name		Path		
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation		C:\Windows\SysWOW64\msvcrt.dll		
mswsock.dll	Microsoft Windows Sockets 2.0 S...	Microsoft Corporation		C:\Windows\SysWOW64\mswsock.dll		
mswsock.dll.mui	Microsoft Windows 소켓 2.0 서비...	Microsoft Corporation		C:\Program Files\WindowsApps\Microsoft.LanguageEx...		
myhack.dll				C:\Users\djss\Desktop\test\myhack.dll		
notepad.exe	Notepad	Microsoft Corporation		C:\Users\djss\Downloads\실습예제\02_PE_File_Form...		
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation		C:\Windows\SysWOW64\nsi.dll		
ntdll.dll	NT 계층 DLL	Microsoft Corporation		C:\Windows\SysWOW64\ntdll.dll		

myhack.dll 인젝션

> 바탕 화면 > test	
이름	
	index.html
	InjectDll.exe
	myhack.dll

원격 스레드 생성

myhack.dll 코드 분석

```
29  BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
30  {
31      HANDLE hThread = NULL;
32
33      g_hMod = (HMODULE)hinstDLL;
34
35      switch( fdwReason )
36      {
37          case DLL_PROCESS_ATTACH :
38              OutputDebugString(L"<myhack.dll> Injection!!!");
39              hThread = CreateThread(NULL, 0, ThreadProc, NULL, 0, NULL);
40              CloseHandle(hThread);
41              break;
42      }
43
44      return TRUE;
45  }
```

myhack.dll 코드 분석

```
1  #include "windows.h"
2  #include "tchar.h"
3
4  #pragma comment(lib, "urlmon.lib")
5
6  #define DEF_URL      (L"http://www.naver.com/index.html")
7  #define DEF_FILE_NAME (L"index.html")
8
9  HMODULE g_hMod = NULL;
10
11 DWORD WINAPI ThreadProc(LPVOID IParam)
12 {
13     TCHAR szPath[_MAX_PATH] = {0,};
14
15     if( !GetModuleFileName( g_hMod, szPath, MAX_PATH ) )
16         return FALSE;
17
18     TCHAR *p = _tcsrchr( szPath, 'W' );
19     if( !p )
20         return FALSE;
21
22     _tscpy_s(p+1, _MAX_PATH, DEF_FILE_NAME);
23
24     URLDownloadToFile(NULL, DEF_URL, szPath, 0, NULL);
25
26     return 0;
27 }
```

코드 요약

1. notepad.exe 프로세스에 myhack.dll 인젝션
2. DllMain() 함수 호출
3. ThreadProc() 함수 실행
4. URLDownloadToFile() 함수 실행
5. Index.html 파일 다운

InjectDll.exe 코드 분석

다른 프로세스에게 스레드를 실행시키는 함수

```
79      hThread = CreateRemoteThread(hProcess, NULL, 0, pThreadProc, pRemoteBuf, 0, NULL);
80      WaitForSingleObject(hThread, INFINITE);
81
82      CloseHandle(hThread);
83      CloseHandle(hProcess);
84
85      return TRUE;
86  }
```


현재 자신을 로딩한 프로세스 이름이
notepad.exe와 같다면
IE를 숨김모드로 실행시켜 index.html에 접속



레지스트리 이용

- Windows 10에서는 사용할 수 없는 방법

user32.dll의 특별한 기능을 이용하여
DLL을 인젝션 하는 방법



Applnit_DLLs

: Windows 운영체제에서 기본으로 제공하는 레지스트리 키



user32.dll은 자신이 로드되는 시점에 Applnit_DLLs에 등록된
DLL을 자동으로 Load 해주기 때문에 불특정 프로세스에
DLL injection이 가능하게 됨

레지스트리 이용

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

	이름	종류	데이터
SecEdit	(기본값)	REG_SZ	mnmsrvc
Sensor	Applnit_DLLs	REG_SZ	C:\myhack2.dll
SoftwareProtectionPlatform	DdeSendTimeout	REG_DWORD	0x00000000 (0)
SPP	DesktopHeapLo...	REG_DWORD	0x00000001 (1)
SRUM	DeviceNotSelect...	REG_SZ	15
Superfetch	DwmInputUsesI...	REG_DWORD	0x00000001 (1)
Svchost	EnableDwmInpu...	REG_DWORD	0x00000007 (7)
SystemRestore	GDIProcessHand...	REG_DWORD	0x00002710 (10000)
TileDataModel	IconServiceLib	REG_SZ	IconCodecService.dll
Time Zones	LoadApplnit_DLLs	REG_DWORD	0x00000001 (1)
TokenBroker	NaturalInputHan...	REG_SZ	Ninput.dll
Tracing	ShutdownWarni...	REG_DWORD	0xffffffff (4294967295)
UAC			
UnattendSettings			

user32.dll이 로딩된 프로세스에 DLL을 인젝션
-> 거의 모든 프로세스



정상적인 프로세스(winlogon.exe, services.exe, svchost.exe, explorer.exe) 등에 몰래 숨어들어가 백도어 포트(Backdoor port)를 열어서 외부에서 접속을 시도하거나, 키로깅 기능으로 사용자의 개인 정보를 훔치는 등의 악의적인 짓 수행



감사합니다 😊