



DLL Injection

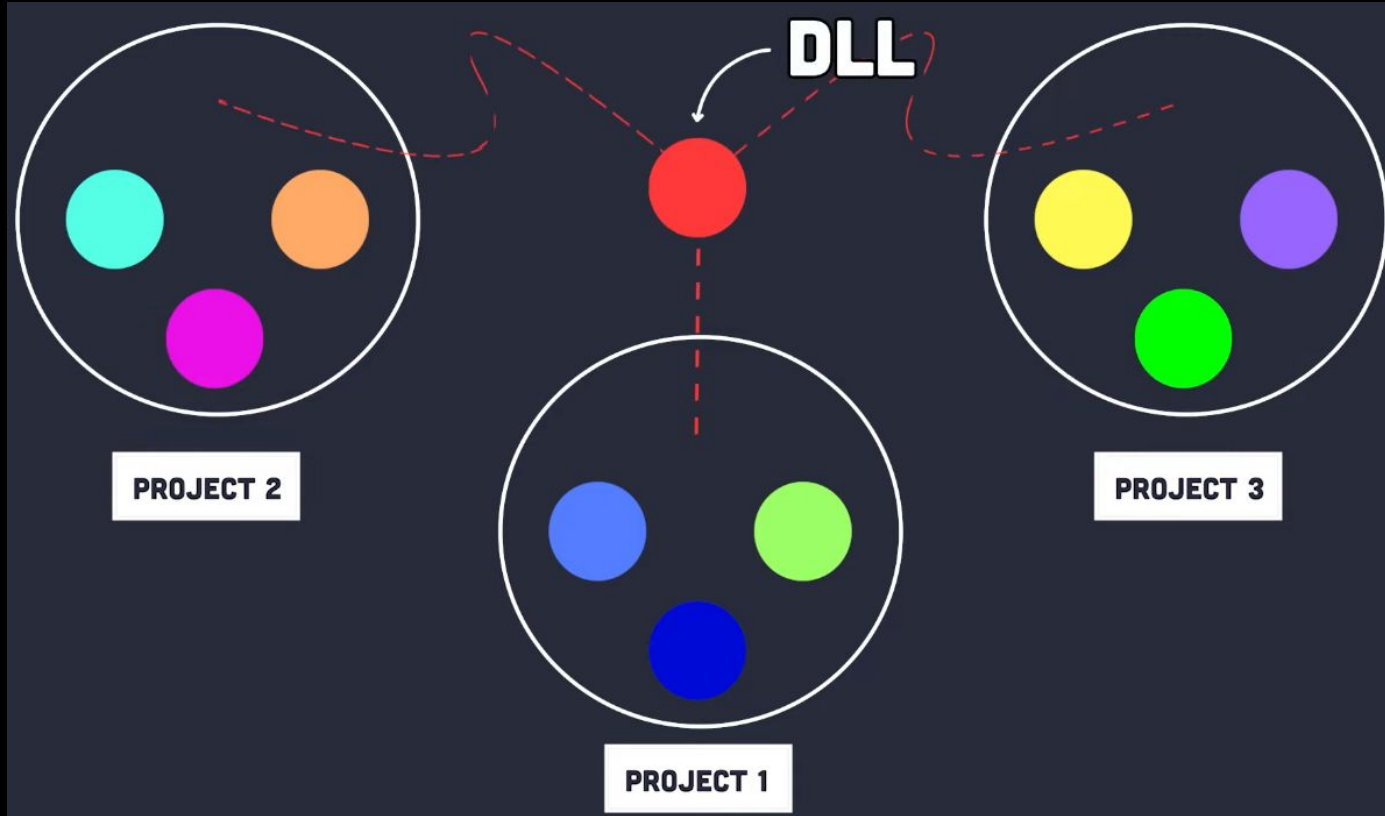


# O que são DLLs?

# O que são DLLs?

- Dynamic Link Library (Biblioteca de Link Dinâmico)
- Contém código, dados ou recursos (ícones, imagens)
- Acesso compartilhado
- No passado, solução para falta de memória (evita duplicação)
- É um PE (Portable Executable, permite execução)
- Apenas para Windows

# O que são DLLs?



# O que são DLLs?

01 MALICIOUS\_DLL.dll

Offset	Hex	Decoded Text
00000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	M Z
00000010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	@ .
00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000030	00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 00	
00000040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	! . L ! T h
00000050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	i s p r o g r a m c a n n o
00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t b e r u n i n D O S
00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	m o d e . . . \$ . . .
00000080	50 45 00 00 4C 01 0E 00 1F 9B D4 68 00 4C 00 00	P E . . L . . h . L .
00000090	43 01 00 00 E0 00 06 21 0B 01 02 1C 00 0C 00 00	C . . ! . .
000000A0	00 24 00 00 00 02 00 00 60 10 00 00 00 10 00 00	\$ .
000000B0	00 20 00 00 00 00 90 6E 00 10 00 00 00 02 00 00	n . . .
000000C0	04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00	

**Header DOS (Magic numbers)**

**Decoded Text**

**Assinatura (PE)**

**Arquitetura (x86)**

**Em 0x3C, ponteiro para header PE**

**Indica que é DLL**





# APIs do Windows

# APIs do Windows

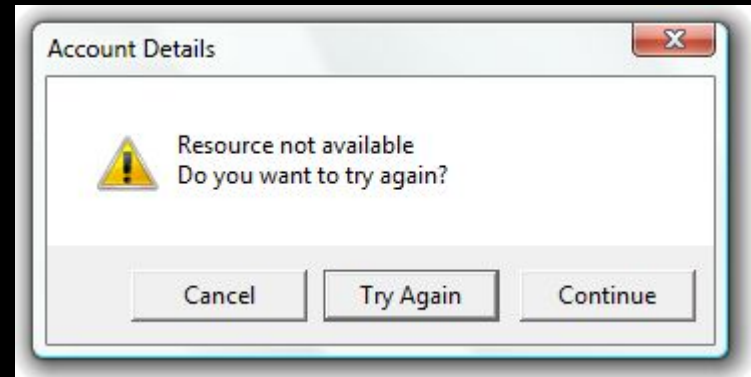
- Conjunto de funções que facilitam uso dos recursos do SO
- Apps não possuem acesso direto a processador/memória, deve ser feito via APIs

# APIs do Windows



```
#include <windows.h>

int main(void) {
    MessageBox(
        NULL,
        (LPCWSTR)L"Resource not available\nDo you want to try again?",
        (LPCWSTR)L"Account Details",
        MB_ICONWARNING | MB_CANCELTRYCONTINUE | MB_DEFBUTTON2
    );
}
```





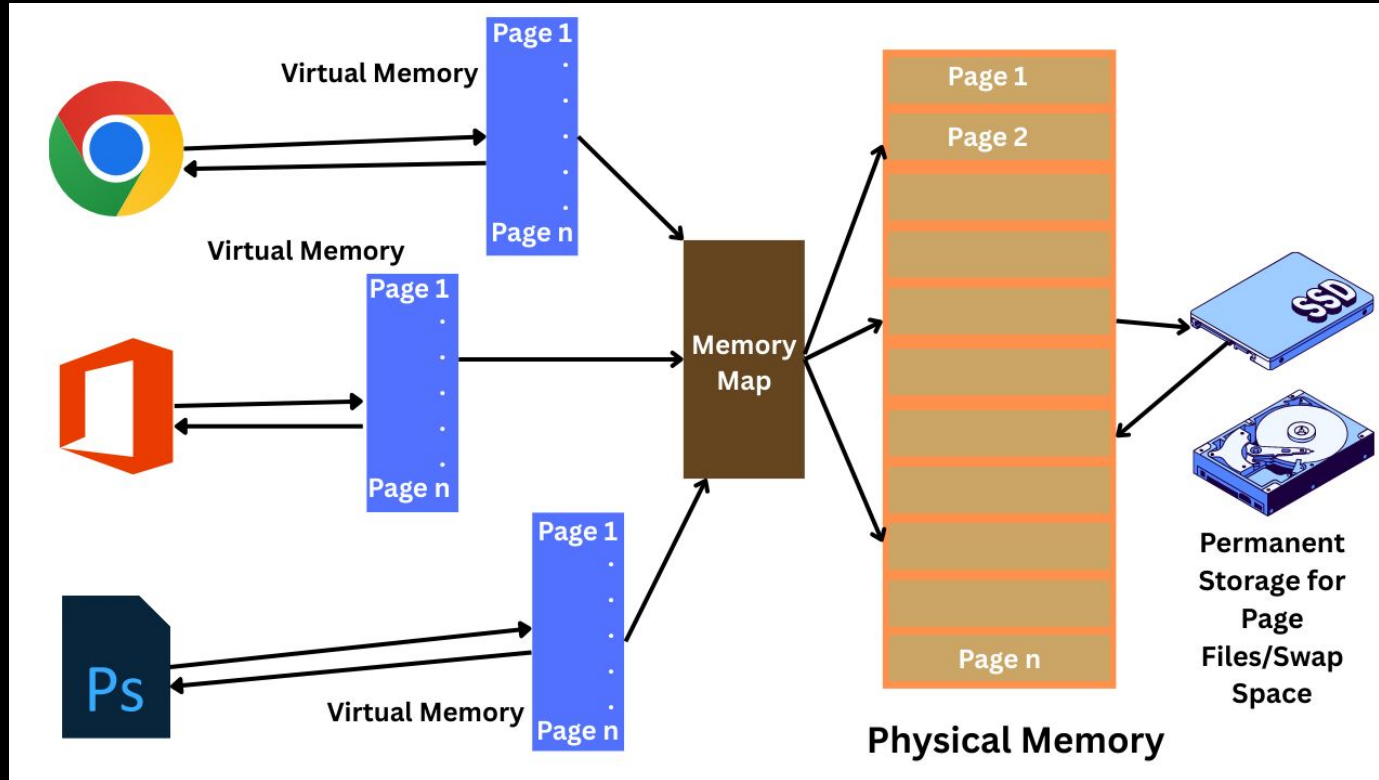


# Memória Virtual

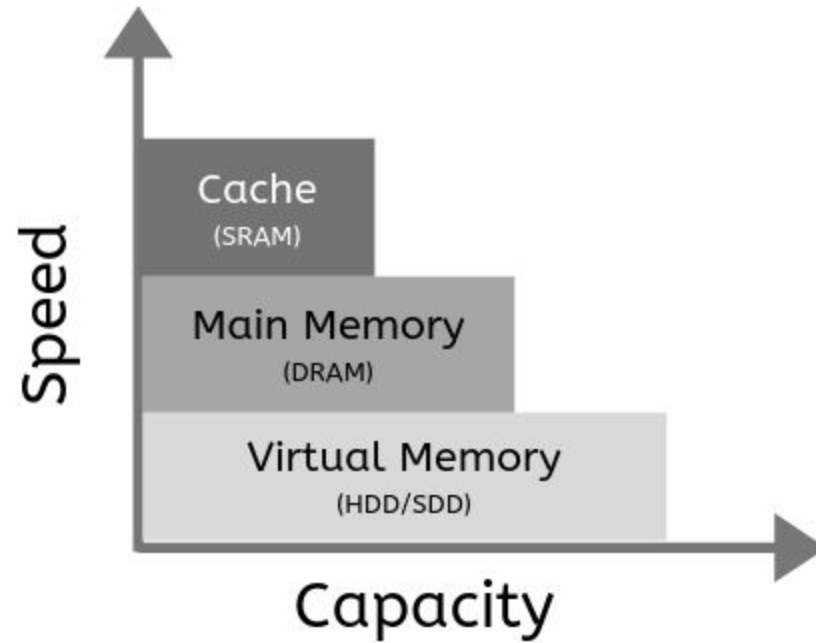
# Memória Virtual

- Técnica que permite executar programas que precisam de mais memória do que o disponível
- Gerenciado pelo SO
- Dados na RAM que não são usados com frequência são jogados temporariamente no HD/SSD, como arquivos de paginação (pagefile.sys)
- Arquivos de paginação são gerenciados como (memória a mais), e recuperados/armazenados conforme necessidade
- A memória virtual contém tanto RAM quanto HD/SSD

# Memória Virtual



# Memória Virtual





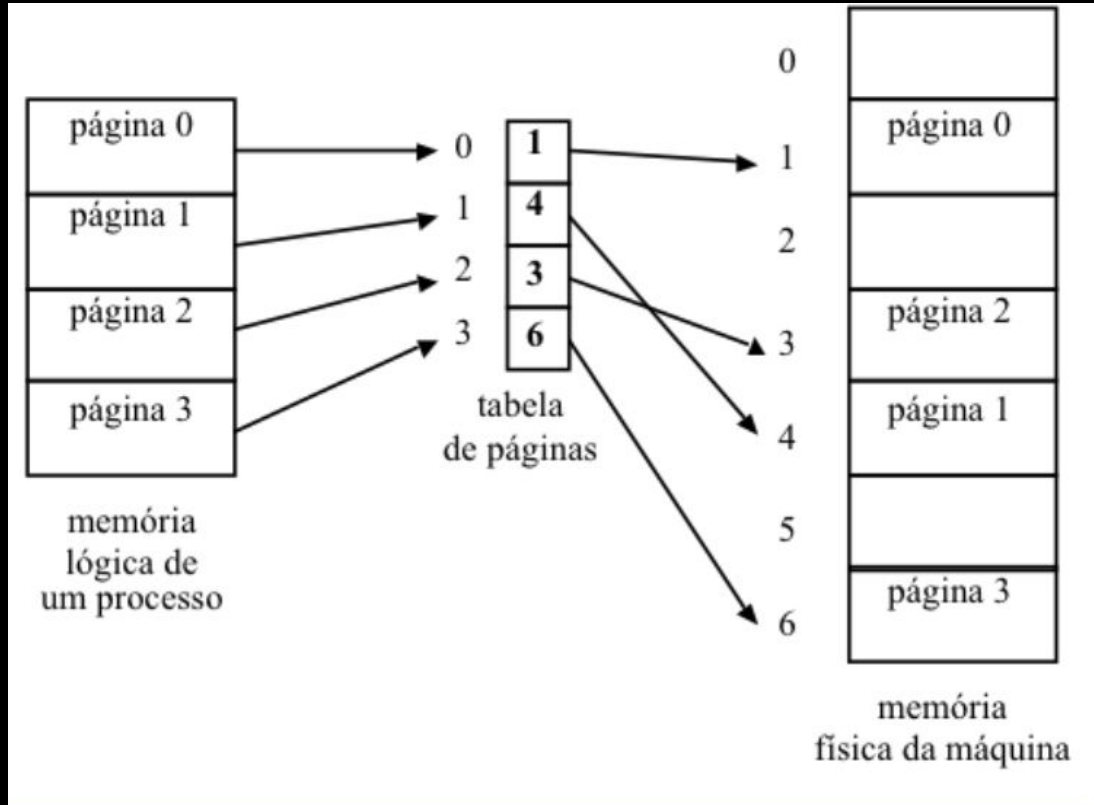
# Paginação

# Paginação

- Técnica de gerenciamento de memória
- Memória dividida em pedaços do mesmo tamanho (cerca de 4Kb), tanto na RAM (frames) quanto na memória virtual (páginas)
- Programa não precisa ser encaixado na RAM, está espalhado
- Cada processo tem sua própria tabela de páginas (mapa de páginas e frames). Assim, um processo não pode acessar memória de outro processo



# Memória Virtual





# Process Address Space

# Process Address Space

- Região de memória virtual alocada para cada processo rodando na máquina
- Windows implementa isolamento por padrão. Processos podem apenas acessar seu próprio espaço de memória.

# Process Address Space

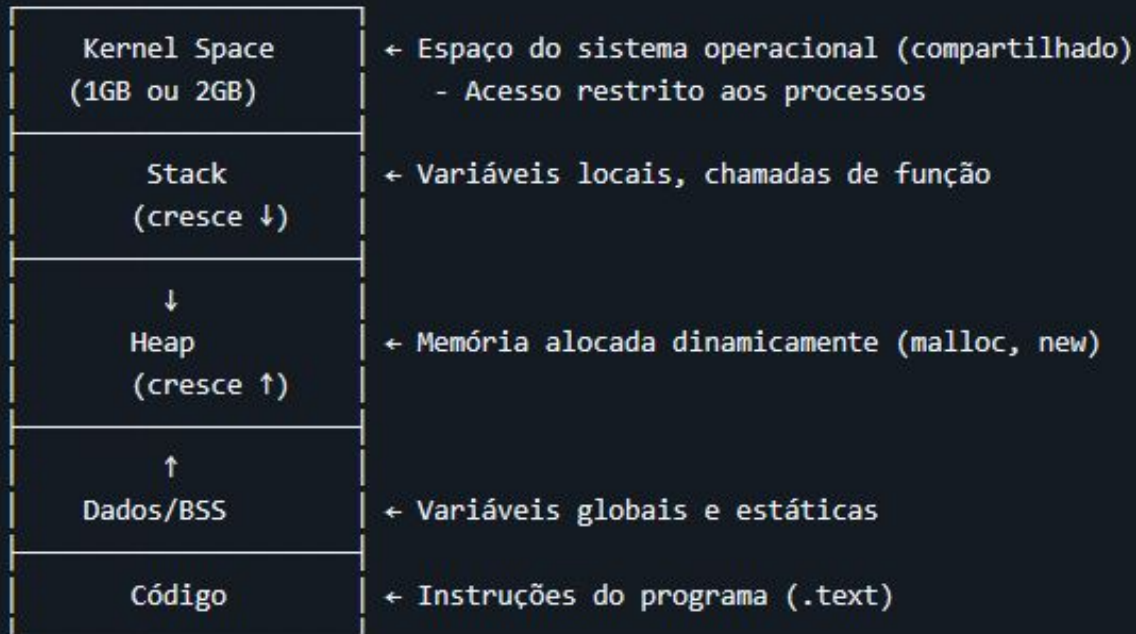


Processo A (Word):	Processo B (Excel):	Memória Física (RAM):
0x00000000-0x0000FFFF	0x00000000-0x0000FFFF	Processo A - Página 0
0x00010000-0x0001FFFF	0x00010000-0x0001FFFF	Processo B - Página 0
0x00020000-0x0002FFFF	0x00020000-0x0002FFFF	Processo A - Página 1
...	...	Processo B - Página 1
0x7FFFFFFF-0xFFFFFFFF	0x7FFFFFFF-0xFFFFFFFF	...

# Process Address Space



Endereço Alto (0xFFFFFFFF)



Endereço Baixo (0x00000000)



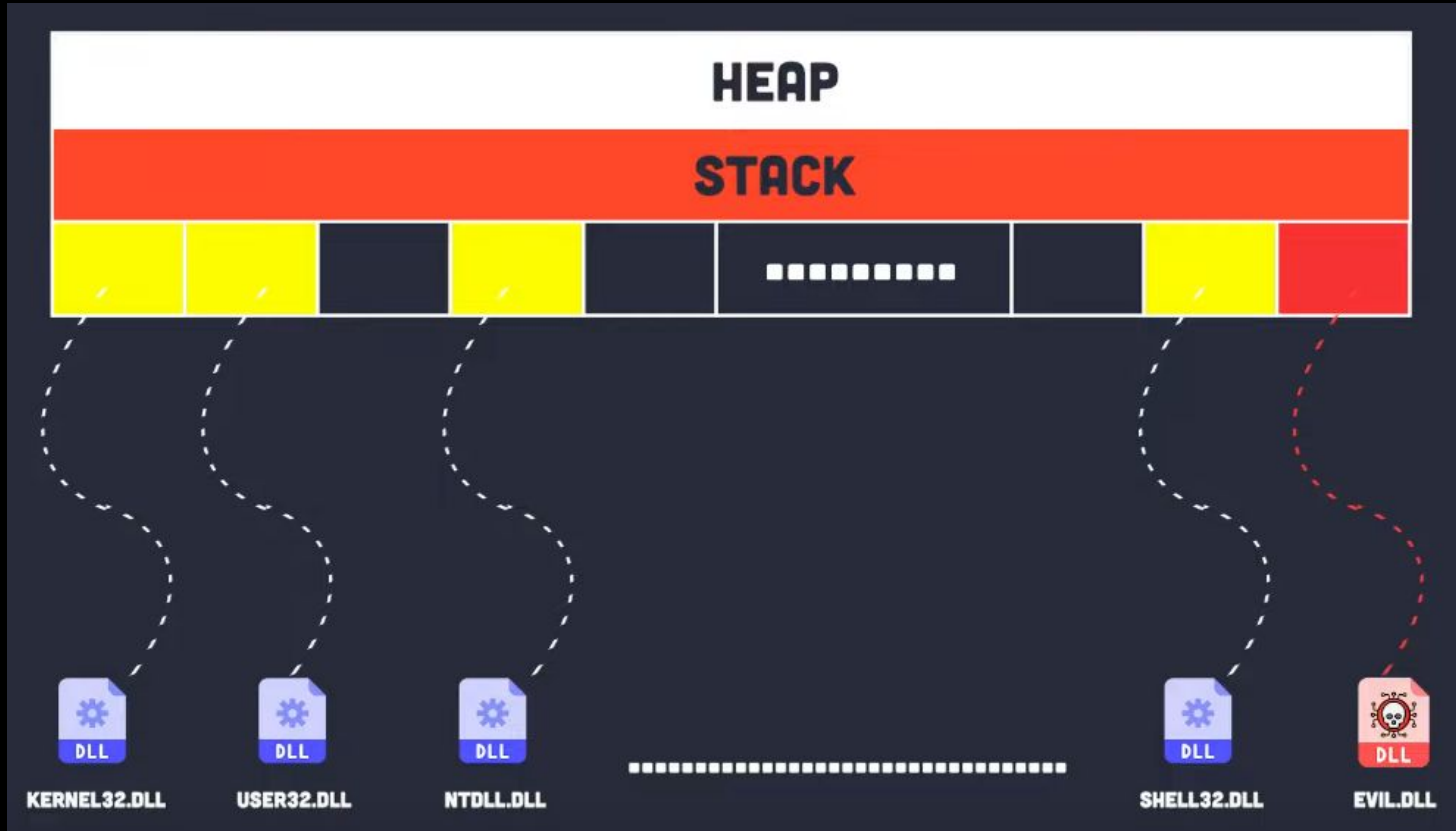
# DLL Injection



# DLL Injection

- Método de injeção de código, onde um processo (injetor) manipula outro processo ativo para carregar uma DLL dentro dele
- DLL injetada ganha acesso completo ao espaço de memória do processo alvo, inclusive a recursos e privilégios
- É difícil de detectar, consegue evadir antivírus, não é notado pelo usuário, herda os privilégios do processo alvo, e pode ler dados da região de memória do processo alvo (como cookies, senhas, tokens de sessão)

# DLL Injection



# GANESH

Grupo de Extensão em Segurança  
da Informação



@ganeshICMC



@ganeshicmc

Contato:

ganesh@icmc.usp.br

<https://ganesh.icmc.usp.br>

