malicious process

LoadLibrary(filename)

myInjectDll()
{
}

kernel32.dll

LoadLibrary(filename)

Internet Explorer process
malicious process

LoadLibrary(filename)

myInjectDll()
{
    h=OpenProcess(,,proc_id)
}

Internet Explorer process

LoadLibrary(filename)

kernel32.dll

LoadLibrary(filename)
LoadLibrary(filename)

myInjectDll()
{
    h=OpenProcess,,,,proc_id
    addr = VirtualAllocEx(h,,, size,,)
}

malicious process

kernel32.dll

LoadLibrary(filename)

Internet Explorer process
malicious process

myInjectDll()
{
    h=OpenProcess,,,proc_id
    addr = VirtualAllocEx(h,, size,,,)
}

Internet Explorer process

kernel32.dll

LoadLibrary(filename)

LoadLibrary(filename)

0x4000
myInjectDll()
{
    h=OpenProcess(,,proc_id)
    addr = VirtualAllocEx(h,, size,,)
    WriteProcessMem(h,addr,buf,size,...)
}

malicious process
malicious process

```
myInjectDll()
{
    h=OpenProcess(,,proc_id)
    addr = VirtualAllocEx(h,, size,,)
    WriteProcessMem(h,addr,buf,size,...)
}
```

Internet Explorer process

kernel32.dll

```
LoadLibrary(filename)
```

```
LoadLibrary(filename)
```

```
0x4000
```

```
“evil.dll”
```
myInjectDll()
{
    h=OpenProcess(,,proc_id)
    addr = VirtualAllocEx(h,, size,,)
    WriteProcessMem(h,addr,buf,size,...)
    CreateRemoteThread(h,,start,param,...)
}

malicious process

Internet Explorer process

LoadLibrary(filename)

kernel32.dll

LoadLibrary(filename)

0x4000

“evil.dll”
LoadLibrary(filename)

myInjectDll()
{
    h=OpenProcess(,,proc_id)
    addr = VirtualAllocEx(h,, size,,)
    WriteProcessMem(h,addr,buf,size,...)
    CreateRemoteThread(h,,start,param,...)
}

malicious process

Internet Explorer process

kernel32.dll

LoadLibrary(filename)

0x4000

“evil.dll”

LoadLibrary(“evil.dll”)