NANOSEC

RE:HACK
re:search + re:scrutiny + re:educate

Cyber security Workshop

Revisiting PE and Process Injections

Special thanks to

NANOSEC

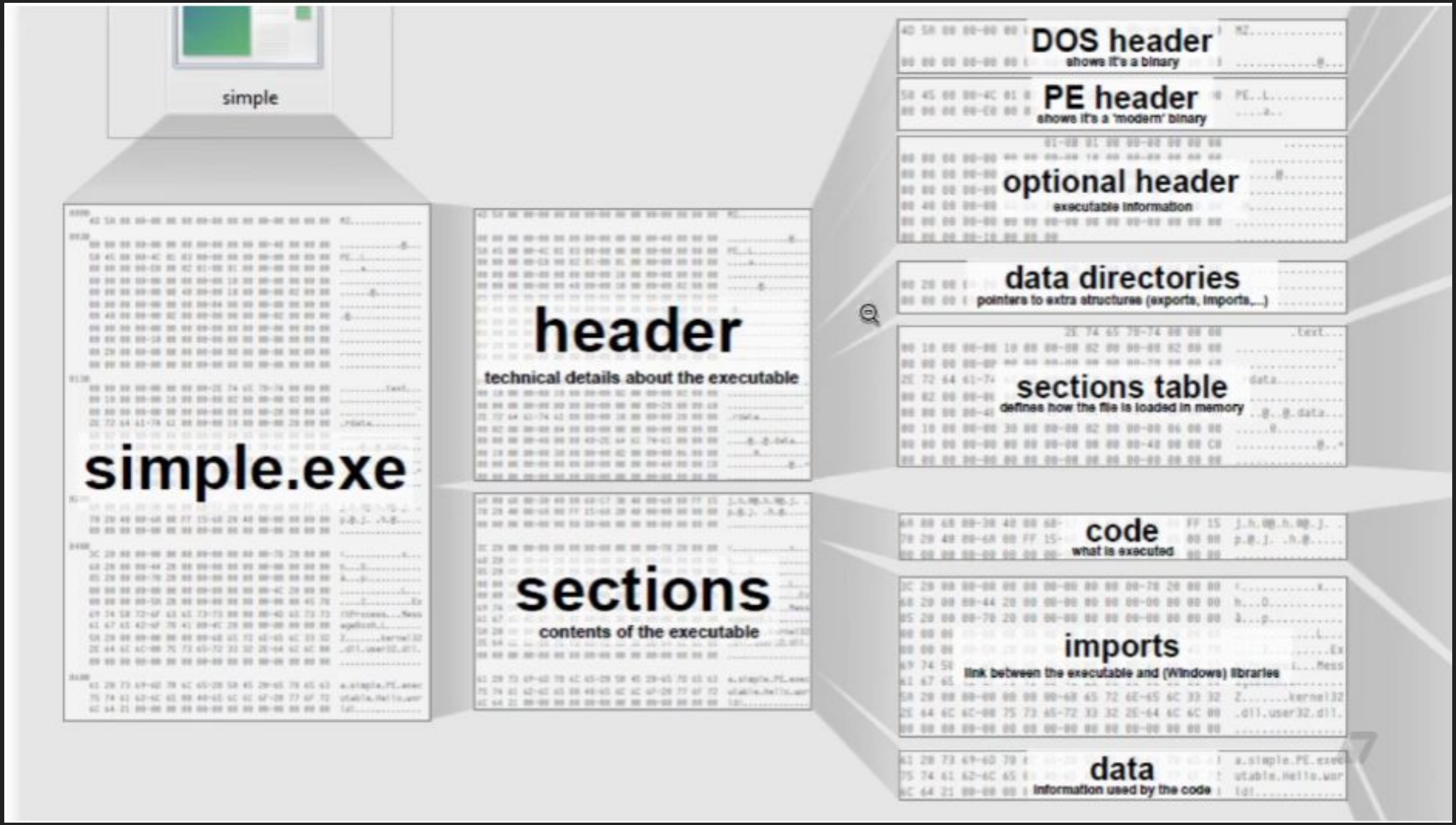
RE:HACK
re:search + re:scrutiny + re:educate

Introduction

Disclaimer

All the information are provided for free and can't be distributed without the permission of the organisers. Any attendees that using the materials for gaining self profit is not allowed and an action will be taken

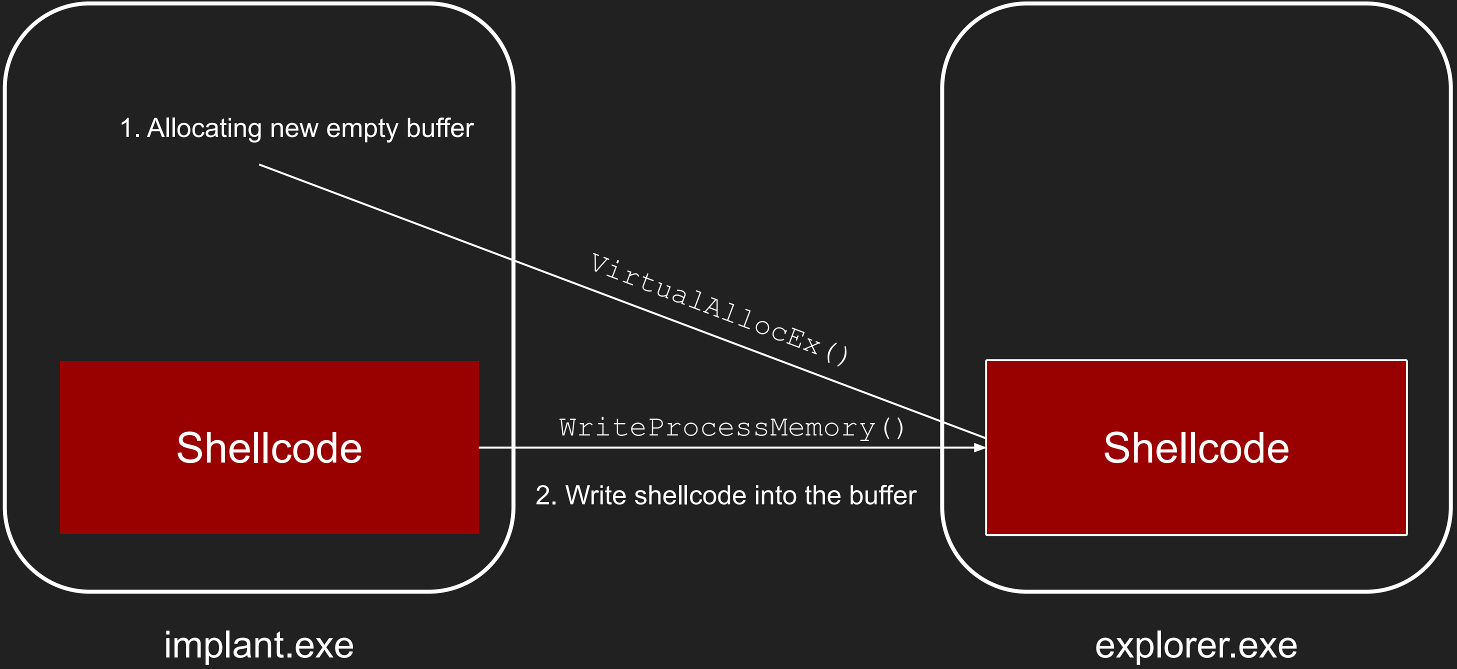
PE Structure


simple
simple.exe
header
technical details about the executable
sections
contents of the executable
DOS header
shows it's a binary
PE header
shows it's a 'modern' binary
optional header
executable information
data directories
pointers to extra structures (exports, imports,...)
sections table
defines how the file is loaded in memory
code
what is executed
imports
link between the executable and (Windows) libraries
data
information used by the code

4 Process Injections

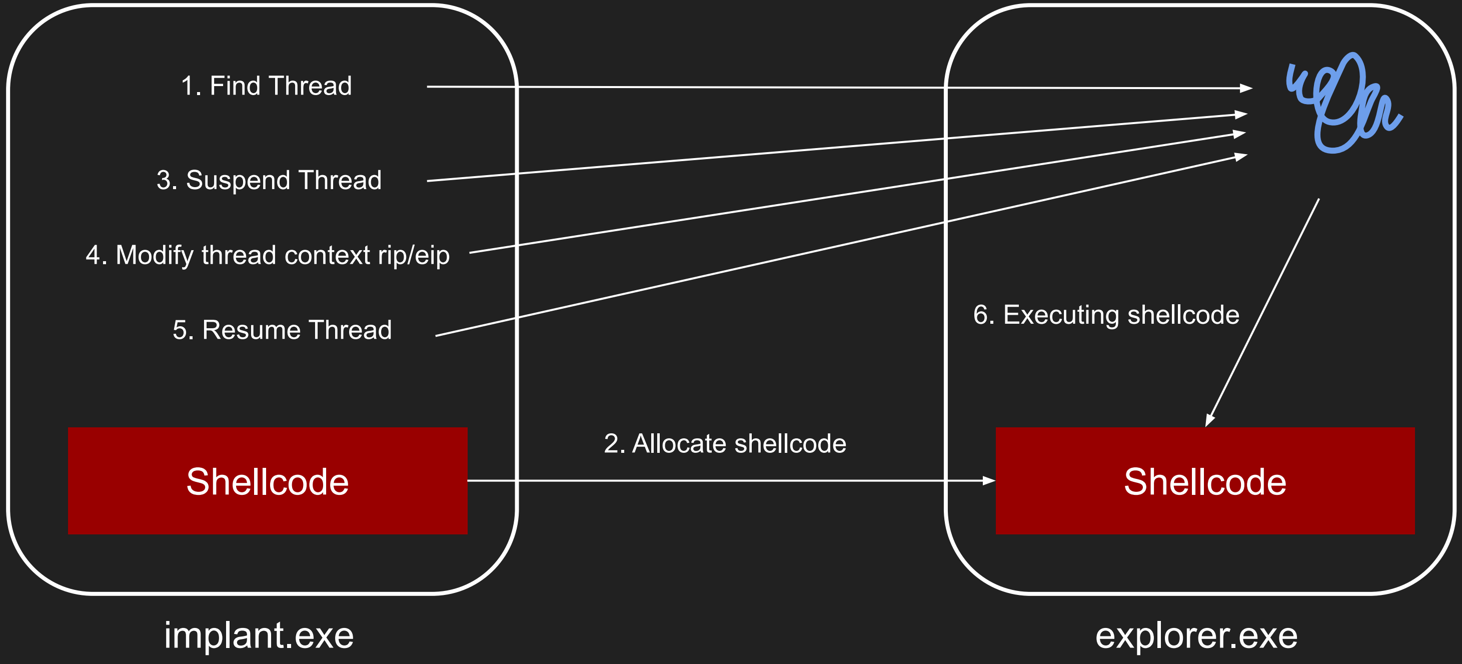
1. Classic

Create a new memory region to store shellcode in a remote process



2. Thread Context

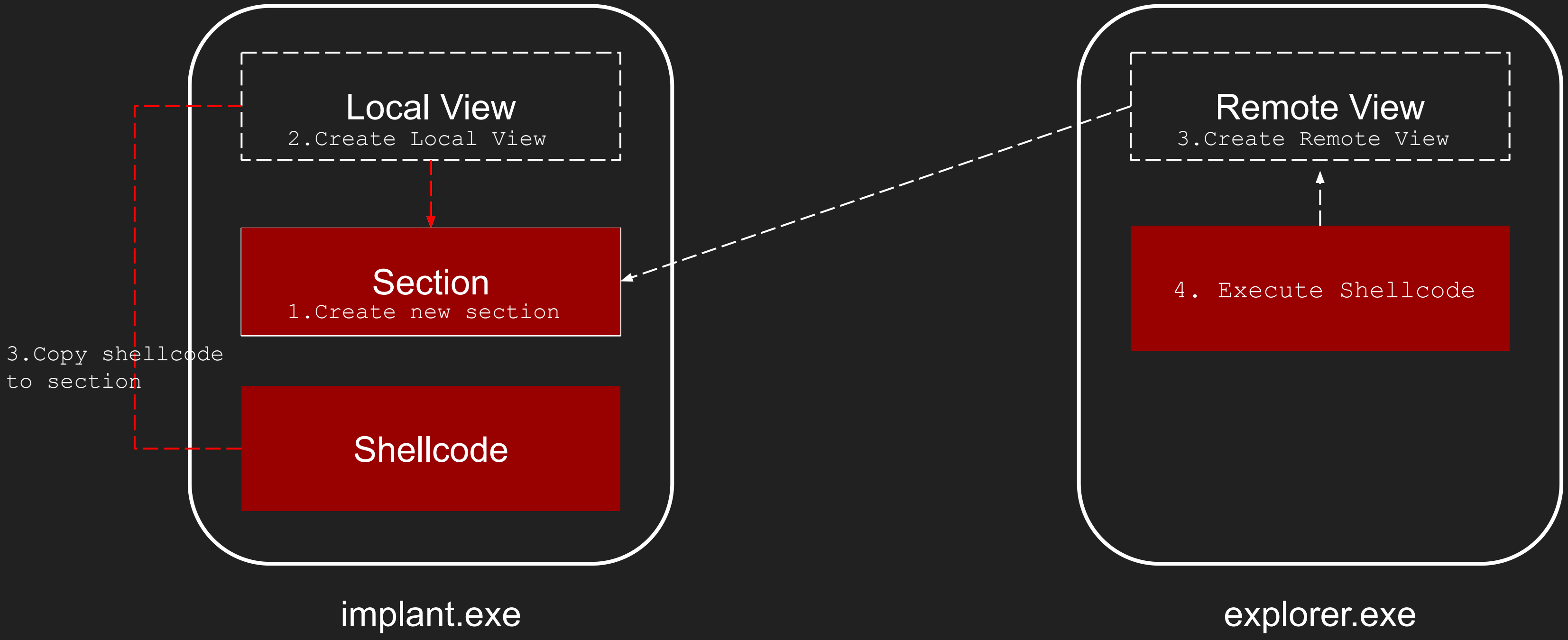
Find usable thread in remote process and points to our shellcode



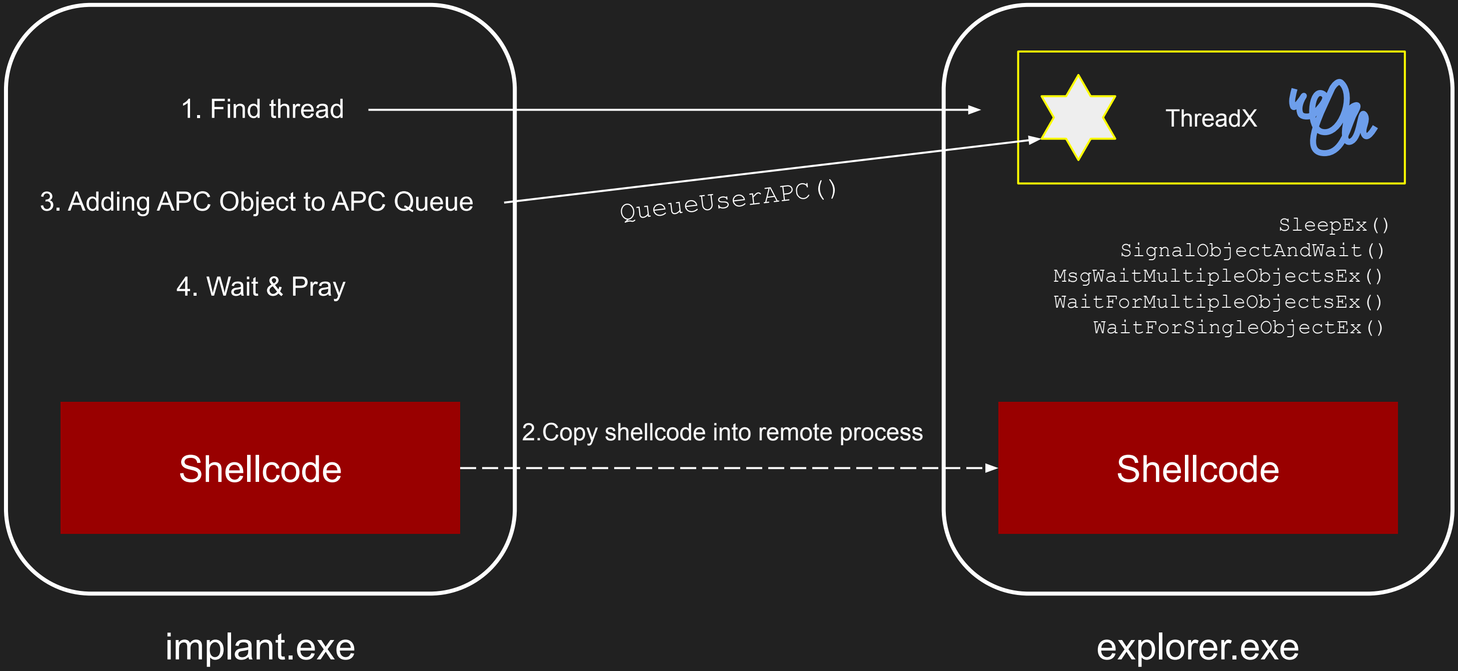
5 minutes 🍵 break

3. MapView

Creating inter-process section views. The remote process has access to view our shellcode



4. Asynchronous Procedure Calls (APC)



1. Find thread

3. Adding APC Object to APC Queue

4. Wait & Pray

Shellcode

implant.exe

2.Copy shellcode into remote process

`QueueUserAPC()`

ThreadX

```
SleepEx()
SignalObjectAndWait()
MsgWaitMultipleObjectsEx()
WaitForMultipleObjectsEx()
WaitForSingleObjectEx()
```

Shellcode

explorer.exe

QnA

Thank you!