HACK & BEER//2023

Curitiba – 04/OUT/2023

Organizadores

HDTEC Solution provider

SEC4US

Patrocinador

2EN VIA

Bypassing AV/EDR using Windows In/Direct System Call

Helvio Junior (M4v3r1ck)

Pesquisador de segurança e Co-Fundador da Sec4US

2023 Curitiba

Agenda

- Whoami (or not)
- Injeção de processo
- Anéis de proteção (protection rings)
- APIs e como são utilizadas
- Como as camadas de defesa AV, EDR ... functionam
- Direct System Calls
- Event Tracing for Windows
- Indirect System Calls

! (whoami)

O que eu não sou!

- Dono do conhecimento (tenho diversas lacunas e falhas)
- Deus do código (sei desenvolver, mas longe de seguir as melhores práticas)
- White hat (ataco somente quando tenho autorização)

AQUELA GAMBIARRA BÁSICA... ATIVANDO O MODO MACGYVER

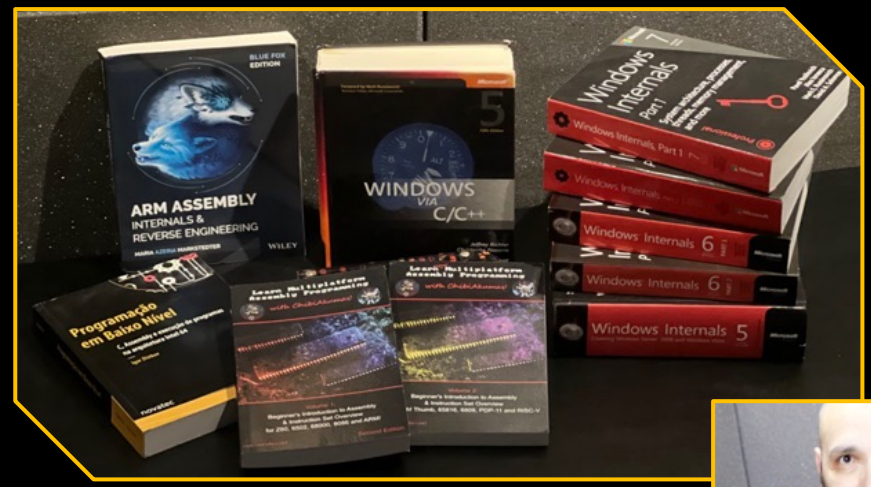
Whoami

A la macgyver specialist

ping -t specialist

Whoami

- Helvio Junior (M4v3r1ck)
- Primeiro OSCE3 da América Latina
- Em preparação para OSEE
- Foco de estudo e pesquisa:
  - Low Level Security
  - Buffer Overflow
  - Shellcoding
  - Criação de Malware
  - Bypass de AV/EDR
  - Mobile e etc...
- CEO da Sec4US Treinamentos
- https://github.com/helviojunior/



OFFENSIVE SECURITY OSCE³

OSEP OSED OSWE OSCE OSCP eCXD eMAPT

HACK & BEER// 2023 Curitiba

Motivação

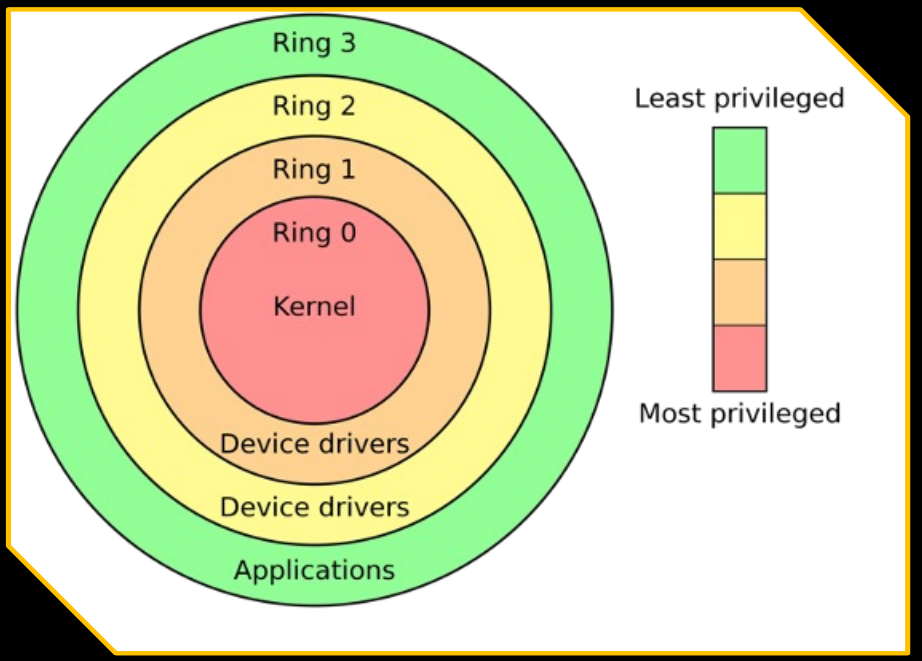
- Muitos acreditam, tenho a solução X, que é líder do Gartner, então estou 100% protegido.
- Não existe uma bala de prata
- Bypass/contorno das camadas de defesa
- FUD - Fully UnDetectable
- FUD é quando o seu código não é detectado por nenhuma camada/ferramenta de defesa
- Importante ser 100% FUD em relação ao seu alvo

Motivação

- Soluções de defesa (mesmo as ditas NextGeneration) ainda trabalham muito com padrões e ainda não estão maduras o suficiente para conter ataques e ameaças sofisticadas
- O Direct e Indirect Syscall, apesar de conhecido, realiza o bypass de muitas ferramentas famosas no mercado

Protection Rings

- Do ponto de vista de segurança existem os anéis de proteção (protection rings)
- Objetiva criar mecanismos de proteção contra falhas e ações maliciosas
- Para o nosso fosse de hoje, o principal objetivo é proteger as áreas críticas do SO das aplicações executadas pelo usuário
- Ring 3 (user mode/user land): Acesso restrito aos recursos, solicita acesso controlado ao recurso via API
- Ring 0 (kernel mode): Possui acesso direto aos recursos como memória, CPU, sistema e etc



API

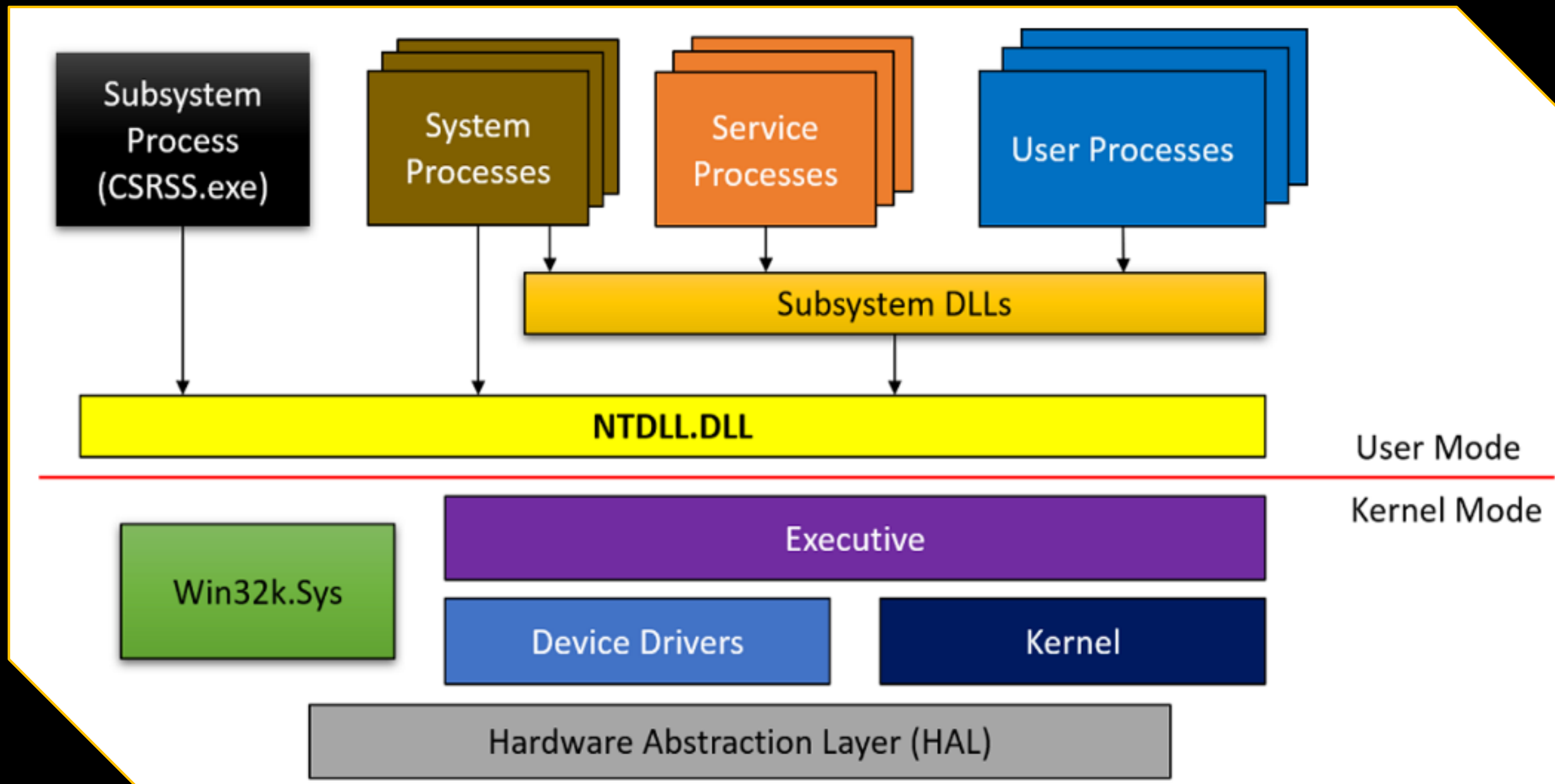
- API é um acrônimo para Application Programming Interface (Interface de programação de Aplicativos). API é um conjunto de métodos de comunicação entre vários componentes de software.

- A Microsoft, por exemplo, define Windows API como “A interface de programação do sistema com centenas de funções executáveis”. Na pratica tudo que realizamos no Windows (abrir arquivo, acesso de leitura ou escrita em arquivos, acessar a rede, entre outros) são realizados através das APIs do Windows. O mesmo ocorre em outros sistemas (incluindo sistemas operacionais como Linux, iOS, Android e etc...).

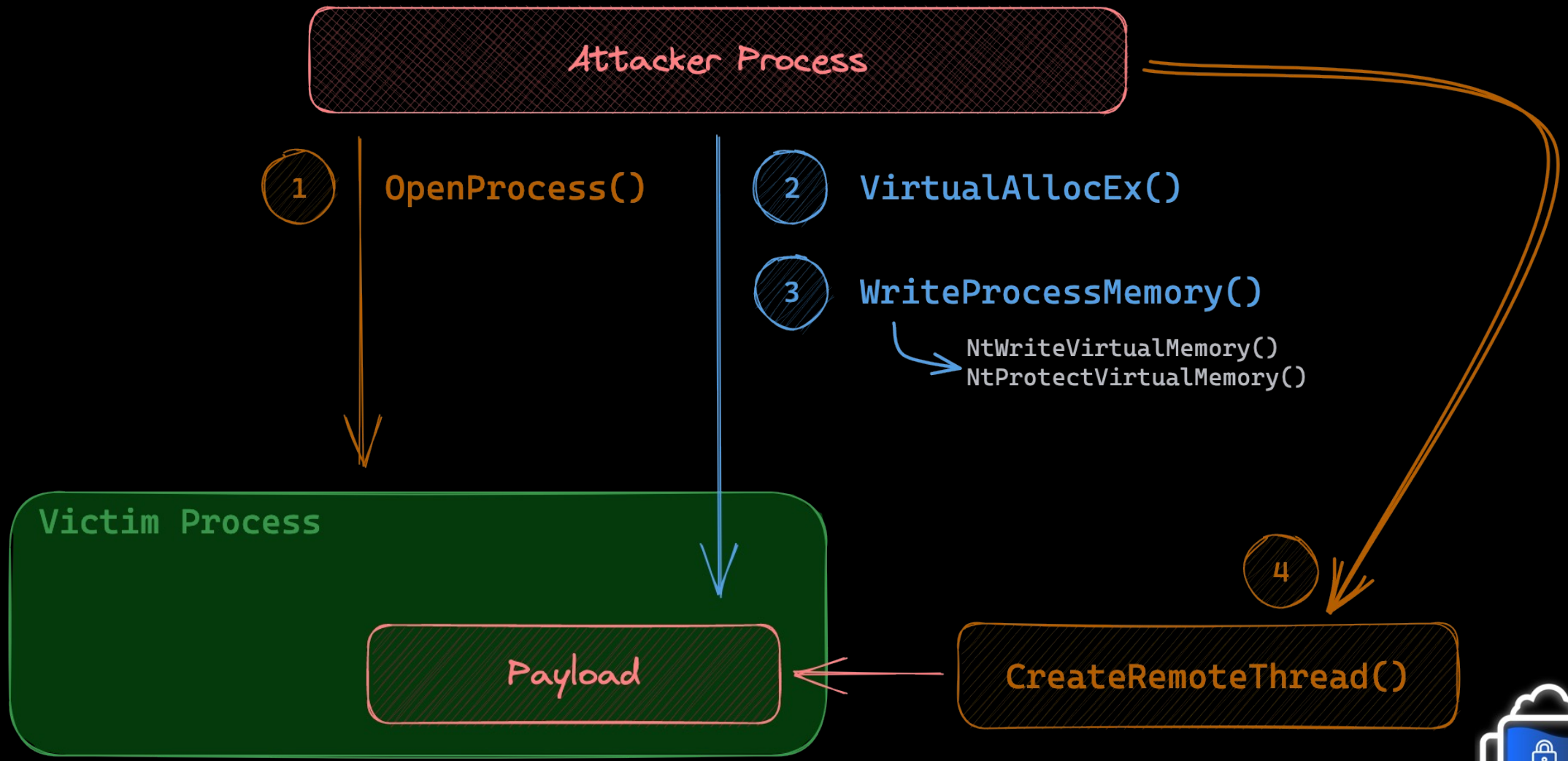
API

- As principais funções de uma API são:
  - Expor os métodos para que outros aplicativos o utilizem;
  - Padronizar a forma de chamada da API e seus métodos;
  - Abstrair sua implementação interna, de forma que caso haja mudanças em sua implementação os outros softwares não precisam ser alterados;
- Qualquer software (inclusive sistemas operacionais) podem deter API para que outros softwares se integrem com o mesmo

Windows APIs

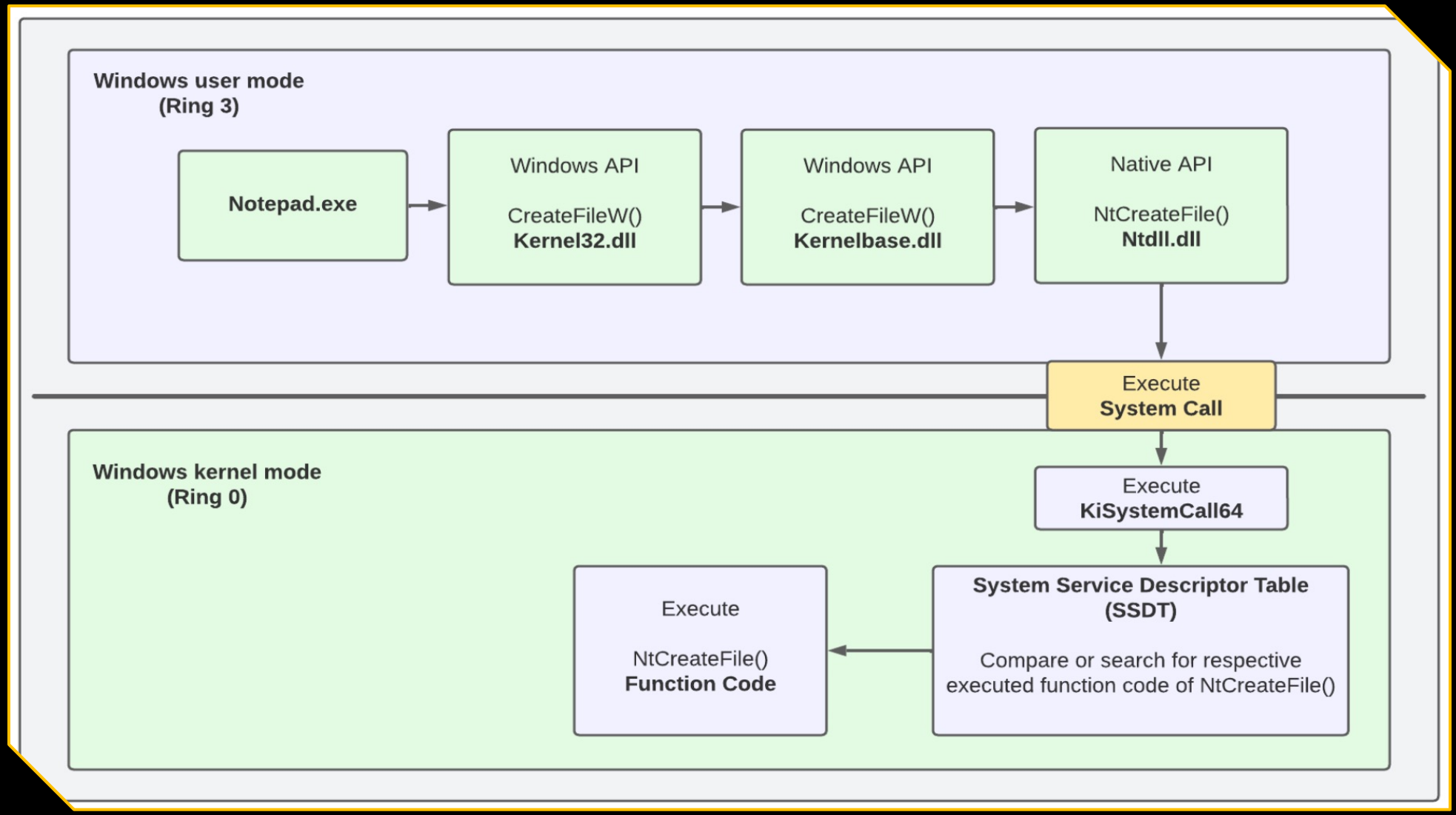


O ataque – Process Injection



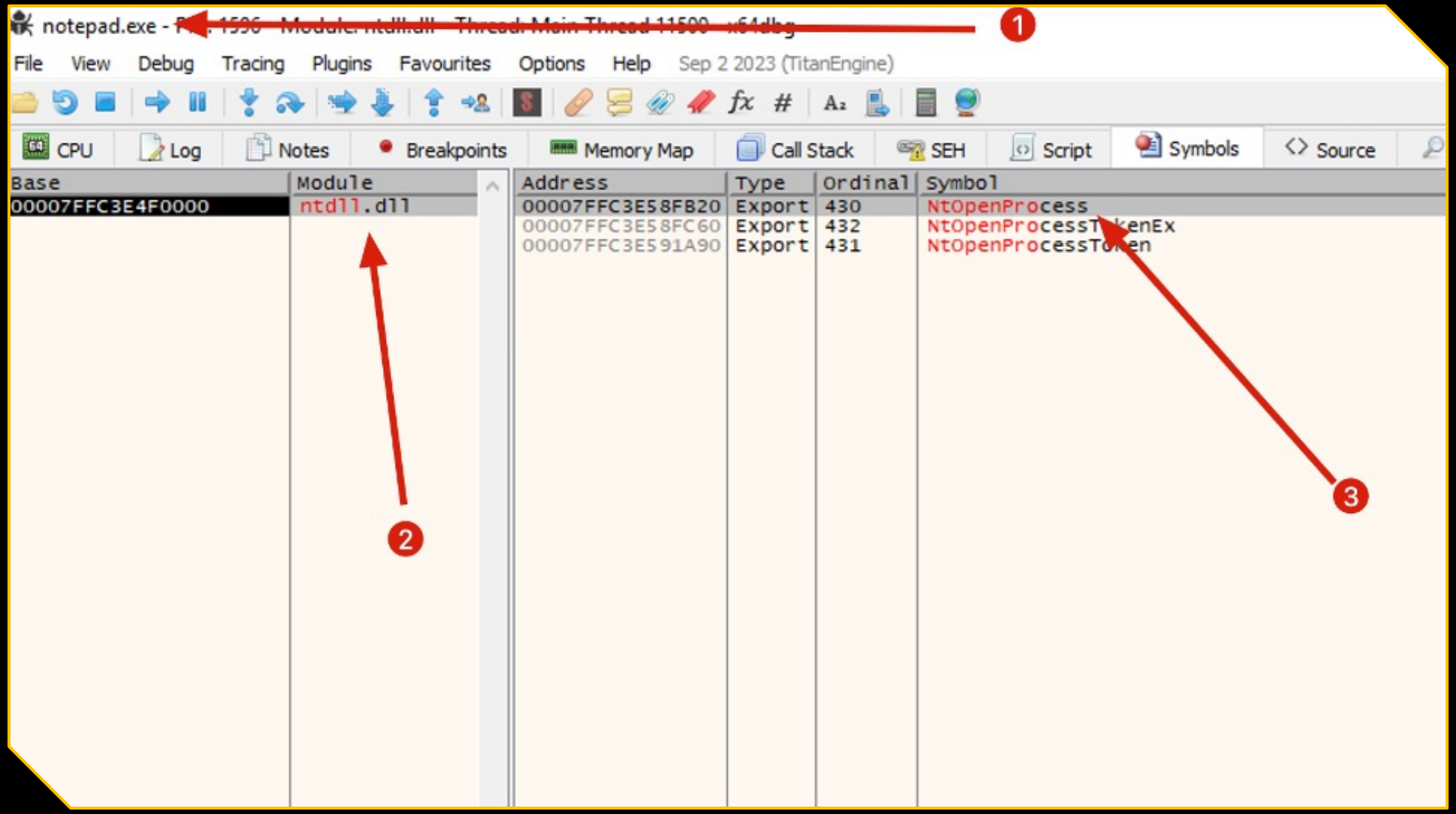
HACK & BEER
2023 Curitiba

Windows APIs

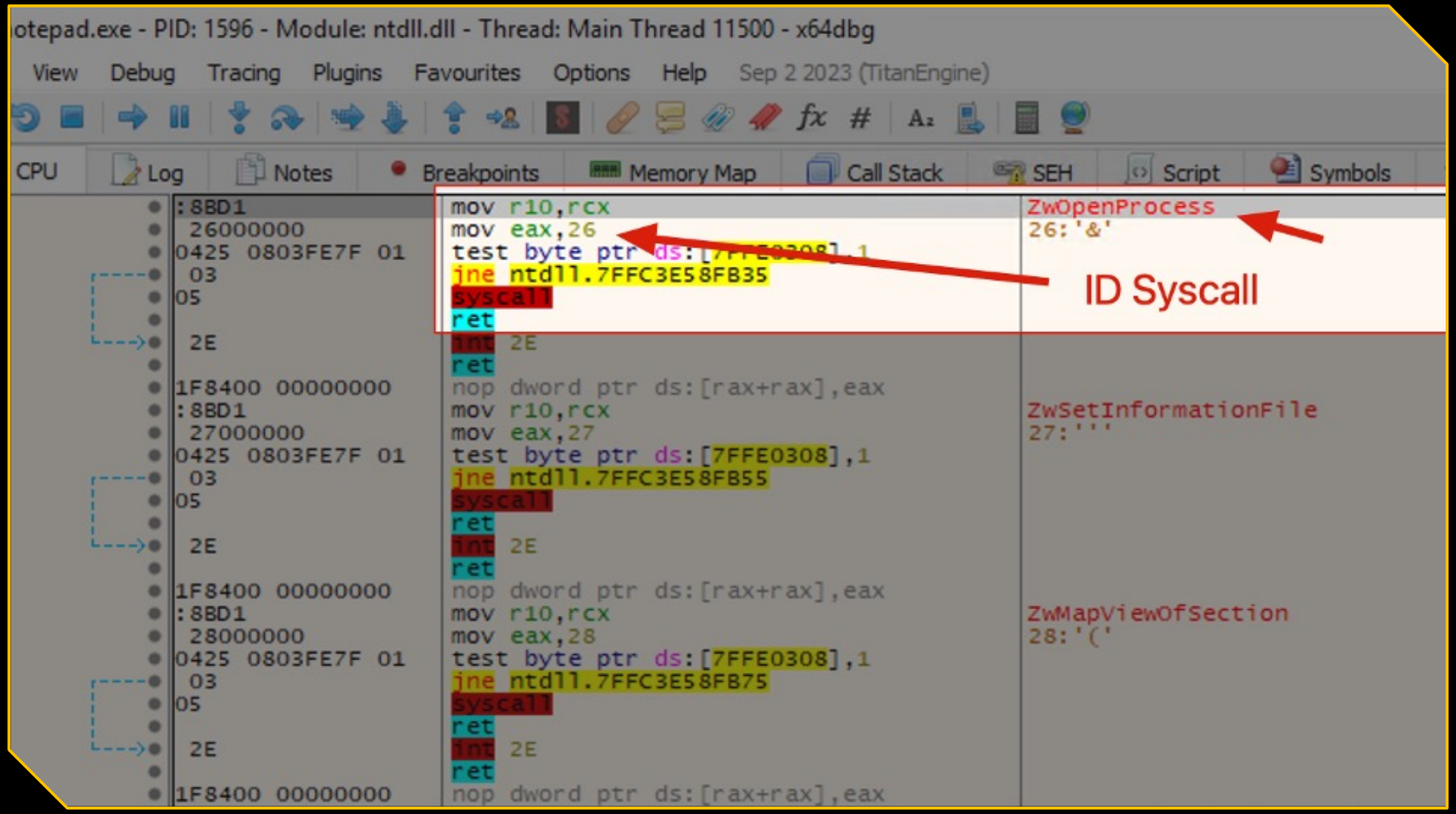


HACK & BEER
2023 Curitiba

Unhooked API



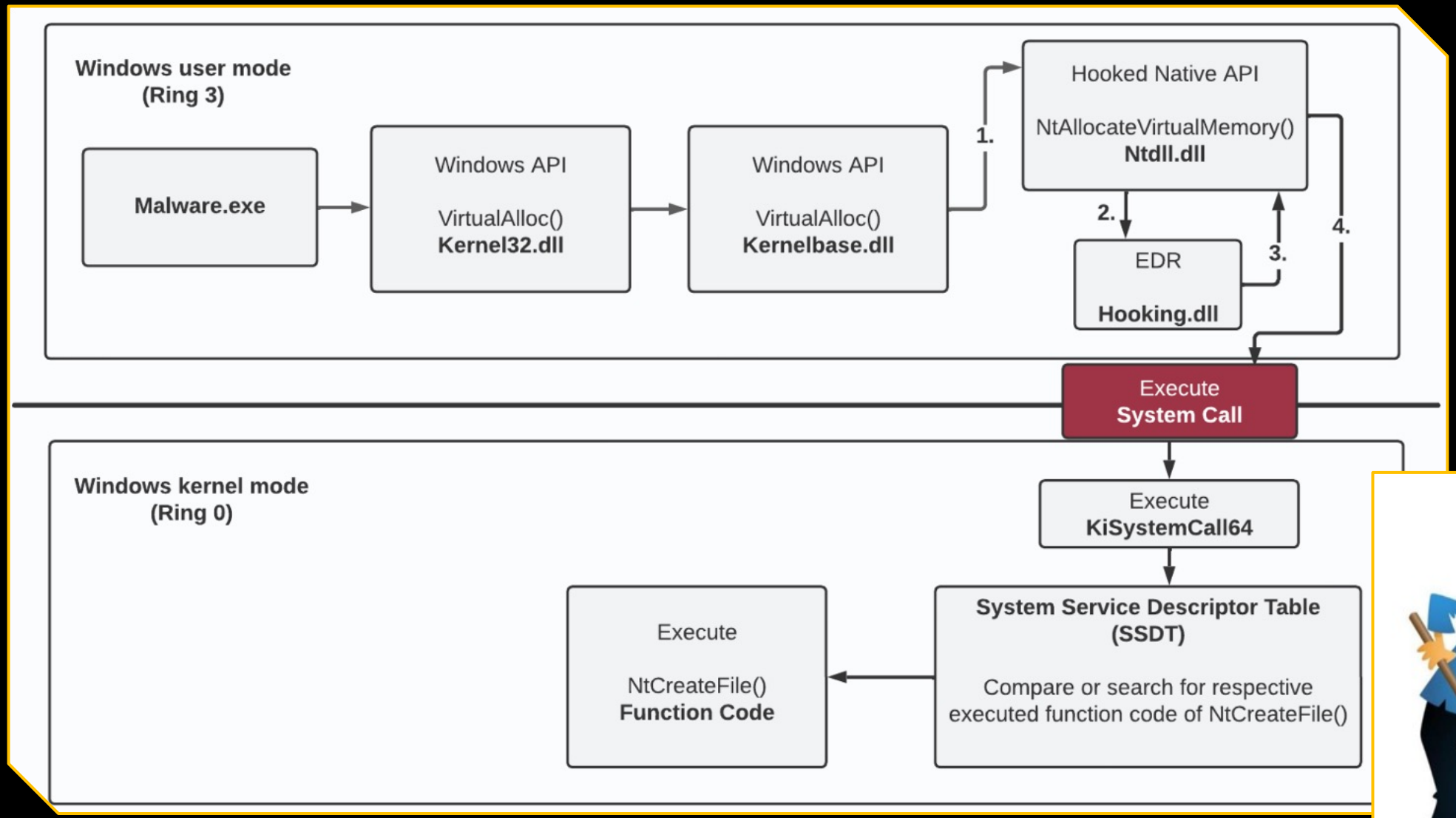
Unhooked API



HACK & BEER

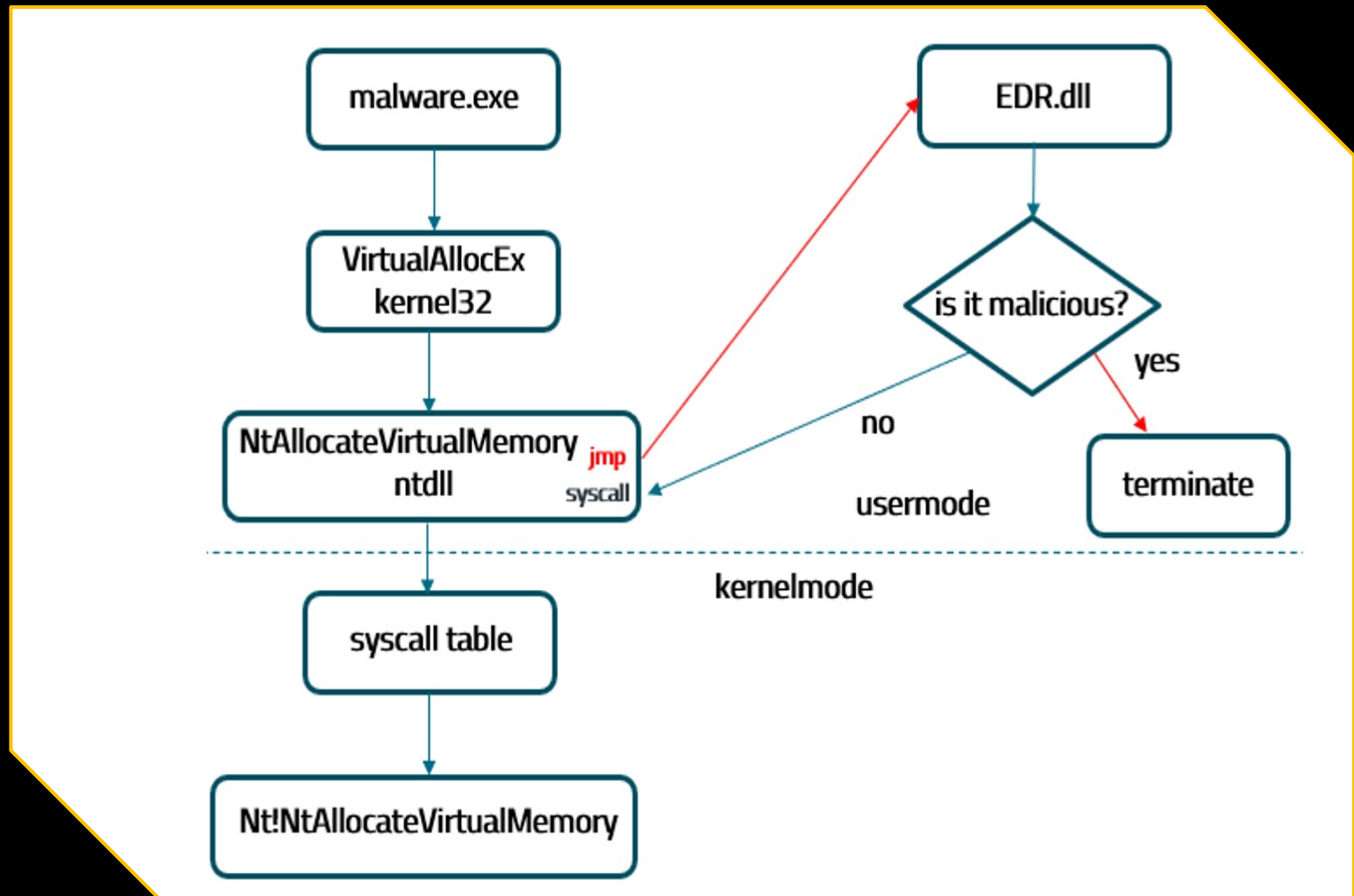
2023 Curitiba

Overview EDR



Overview EDR - Hooking

- Injeta sua própria DLL na aplicação
- Intercepta a chamada da API
- Encaminha a requisição para o código do EDR
- Analisa a requisição e resposta



Hooked API

Process Hacker [MSEDGEWIN10\IEUser]

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information notep

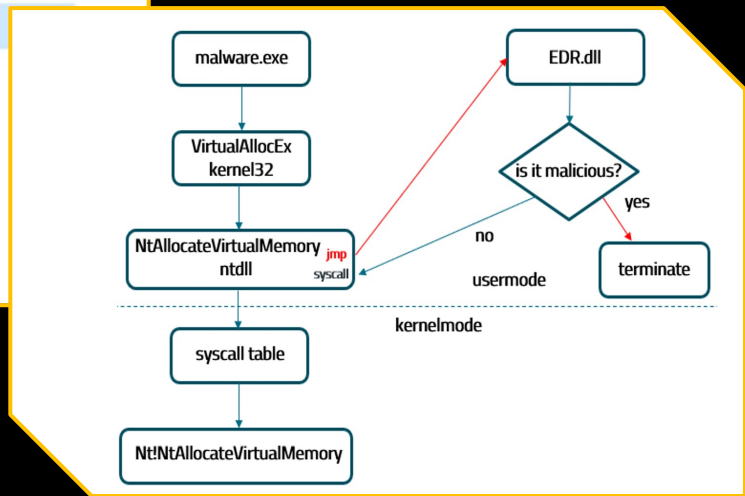
Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
notepad.exe	496	0.02		5.41 MB	MSEDGEWIN10\IEUser	Notepad

notepad.exe (496) Properties

General Statistics Performance Threads Token Modules Memory Environment Handles GPU Comment

Name	Base address	Size	Description
notepad.exe	**0x7ff610050000**	**268 kB**	**Notepad**
advapi32.dll	0x7ffc3c900000	652 kB	Advanced Windows 32 Base API
atcuf64.dll	0x7ffbf1d50000	1.35 MB	Bitdefender Active Threat Control Usermode Filter
bcrypt.dll	0x7ffc3a930000	152 kB	Windows Cryptographic Primitives Library
bcryptprimitives...	0x7ffc3b6a0000	504 kB	Windows Cryptographic Primitives Library
bdhkm64.dll	0x7ffbf1eb0000	852 kB	BitDefender Hooking DLL
cfgmgr32.dll	0x7ffc3aa80000	296 kB	Configuration Manager DLL
clbcatq.dll	0x7ffc3beb0000	648 kB	COM+ Configuration Catalog



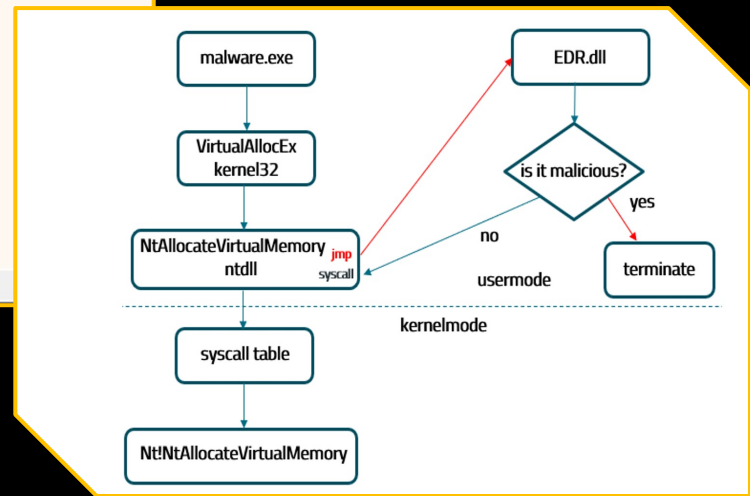
Hooked API

notepad.exe - PID: 8004 - Module: ntdll.dll - Thread: Main Thread 8488 - x64dbg

File View Debug Tracing Plugins Favourites Options Help Sep 2 2023 (TitanEngine)

CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threa

```
00007FFEDE5AF800  4C:8BD1          mov r10,rcx                          ZwQueryInformationThread
00007FFEDE5AF803  B8 25000000      mov eax,25                           Unhooked
00007FFEDE5AF808  F60425 0803FE7F 01  test byte ptr ds:[7FFE0308],1
00007FFEDE5AF810  75 03            jne ntdll.7FFEDE5AF815
00007FFEDE5AF812  0F05             syscall
00007FFEDE5AF814  C3               ret
00007FFEDE5AF815  CD 2E            int 2E
00007FFEDE5AF817  C3               ret
00007FFEDE5AF818  0F1F8400 00000000  nop dword ptr ds:[rax+rax],eax
00007FFEDE5AF820  E9 D6091500      jmp 7FFEDE7004FB                     ZwOpenProcess
00007FFEDE5AF825  CC               int3                                 Hooked
00007FFEDE5AF826  CC               int3                                 ID 26
00007FFEDE5AF827  CC               int3
00007FFEDE5AF828  F60425 0803FE7F 01  test byte ptr ds:[7FFE0308],1
00007FFEDE5AF830  75 03            jne ntdll.7FFEDE5AF835
00007FFEDE5AF832  0F05             syscall
00007FFEDE5AF834  C3               ret
00007FFEDE5AF835  CD 2E            int 2E
00007FFEDE5AF837  C3               ret
00007FFEDE5AF838  0F1F8400 00000000  nop dword ptr ds:[rax+rax],eax
00007FFEDE5AF840  4C:8BD1          mov r10,rcx                          ZwSetInformationFile
00007FFEDE5AF843  B8 27000000      mov eax,27                           Unhooked
00007FFEDE5AF848  F60425 0803FE7F 01  test byte ptr ds:[7FFE0308],1
00007FFEDE5AF850  75 03            jne ntdll.7FFEDE5AF855
00007FFEDE5AF852  0F05             syscall
00007FFEDE5AF854  C3               ret
00007FFEDE5AF855  CD 2E            int 2E
00007FFEDE5AF857  C3               ret
00007FFEDE5AF858  0F1F8400 00000000  nop dword ptr ds:[rax+rax],eax
00007FFEDE5AF860  E9 2E0B1500      jmp 7FFEDE700693                     ZwMapViewOfSection
00007FFEDE5AF865  CC               int3
00007FFEDE5AF866  CC               int3
00007FFEDE5AF867  CC               int3
00007FFEDE5AF868  F60425 0803FE7F 01  test byte ptr ds:[7FFE0308],1
00007FFEDE5AF870  75 03            jne ntdll.7FFEDE5AF875
00007FFEDE5AF872  0F05             syscall
00007FFEDE5AF874  C3               ret
00007FFEDE5AF875  CD 2E            int 2E
```



E agora?

HACK & BEER//
2023 Curitiba

Direct System Call

Windows user mode
(Ring 3)

Malware.exe

mov r10, rcx
mov eax, SSN
syscall
return

Windows API

CreateFileW()
Kernel32.dll

Windows API

CreateFileW()
Kernelbase.dll

Native API

NtCreateFile()
Ntdll.dll

Windows kernel mode
(Ring 0)

Execute
KiSystemCall64

System Service Descriptor Table (SSDT)

Compare or search for respective executed function code of NtCreateFile()

Execute

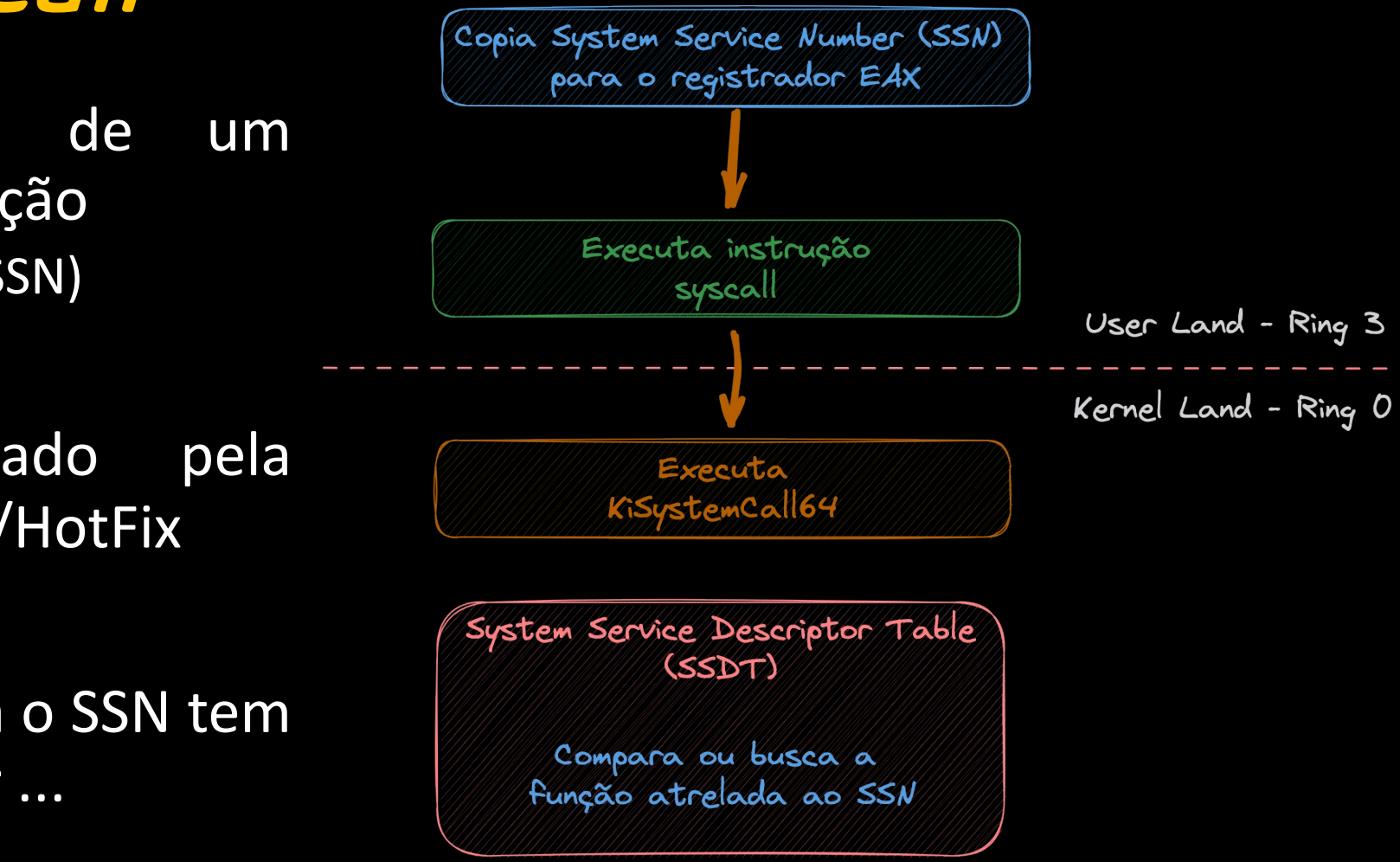
NtCreateFile()
Function Code

Direct System Call

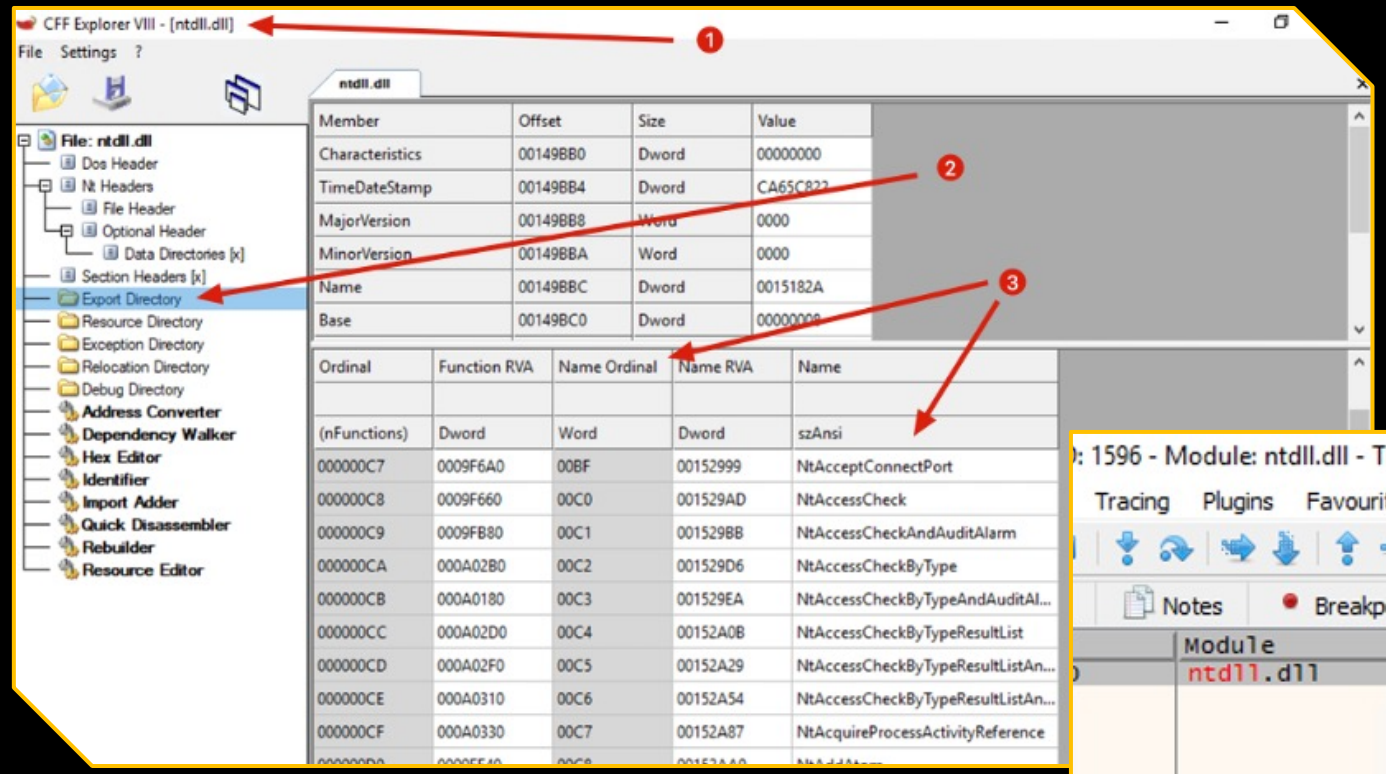
- System Call depende de um IDentificador de cada função
  - System Service Number (SSN)

- O SSN é randomizado pela Microsoft a cada Release/HotFix

- Então, se tem uma tabela o SSN tem que estar em algum lugar ...

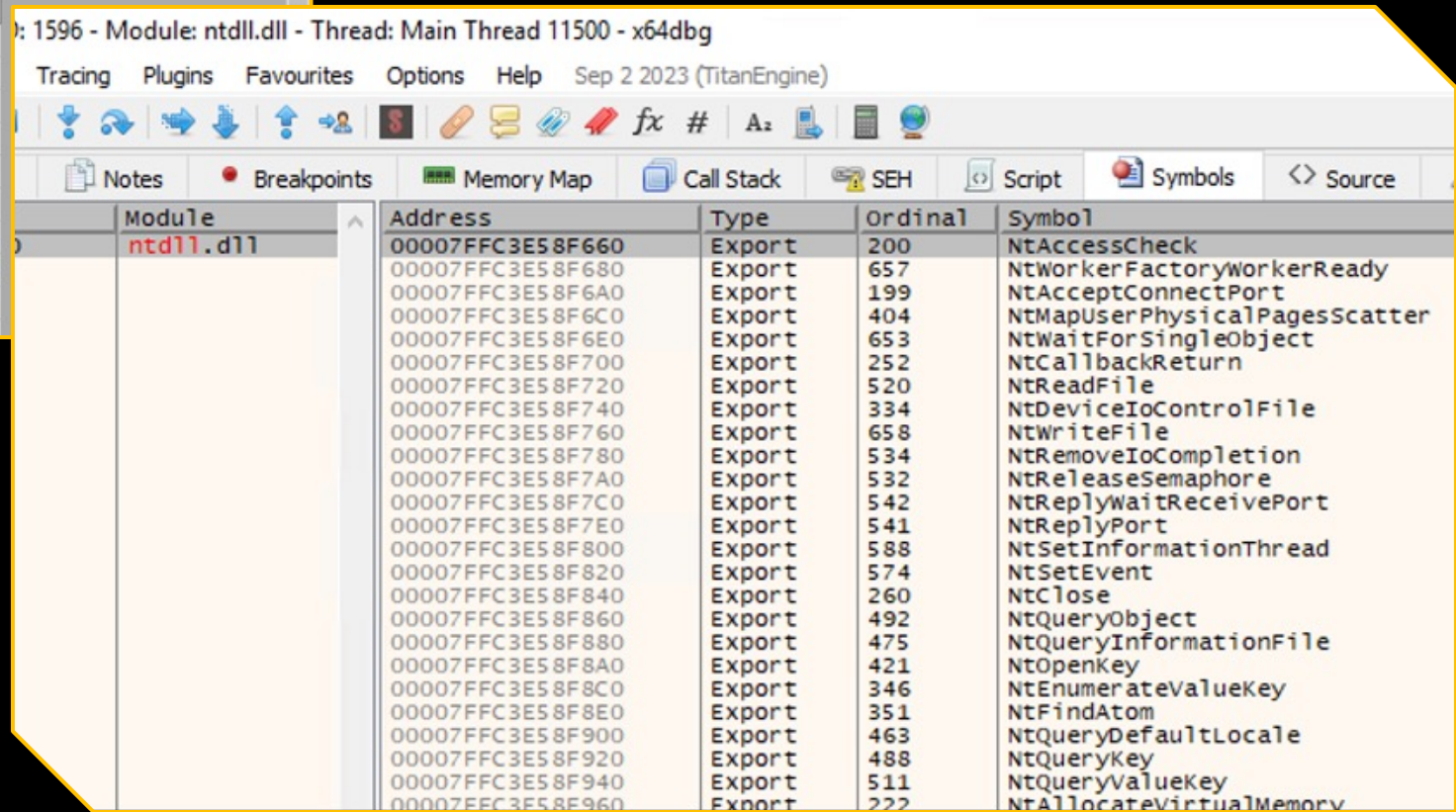


Export Address Table

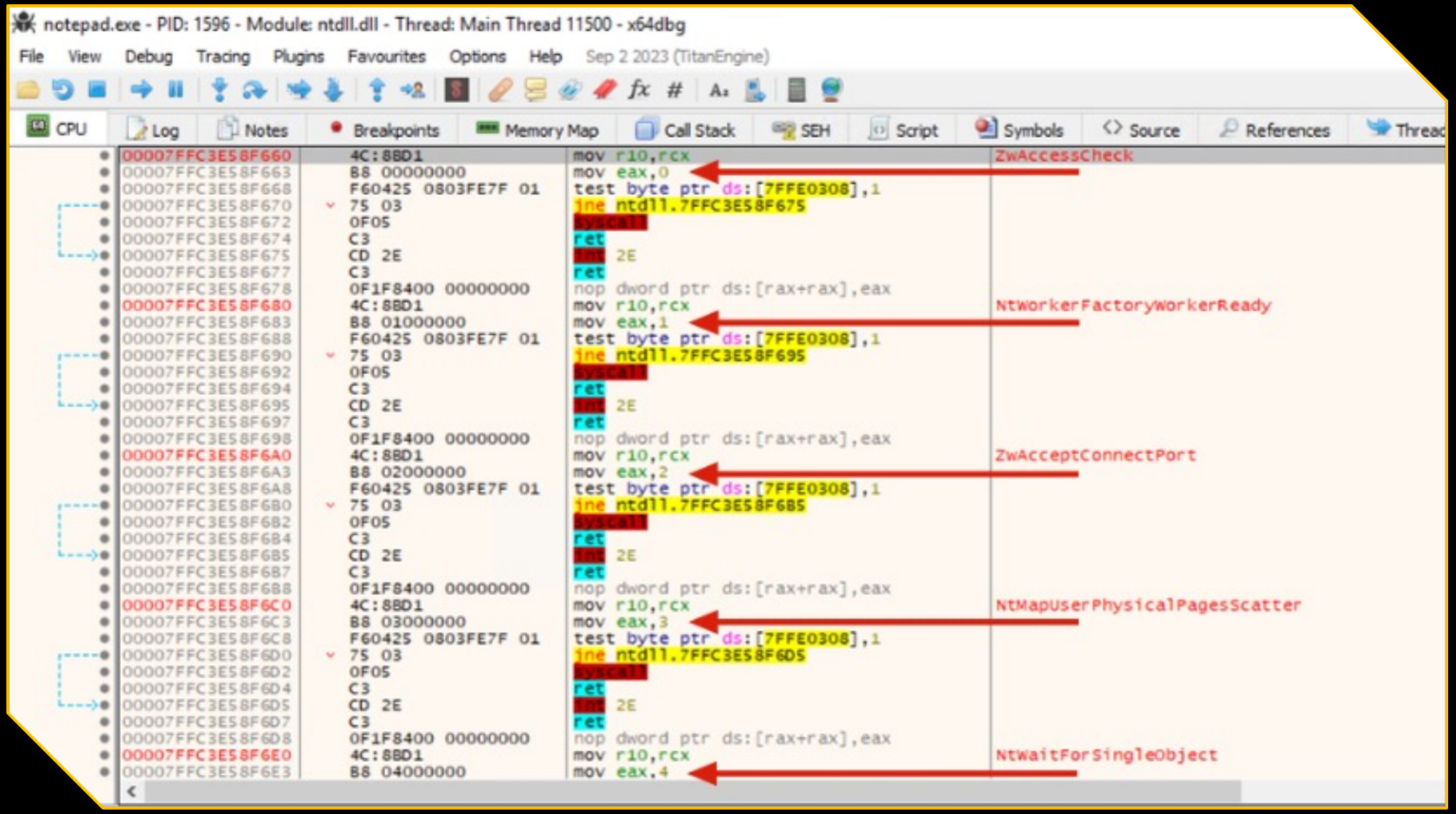


Exportação ordenada pelo nome

Exportação ordenada pelo endereço de memória

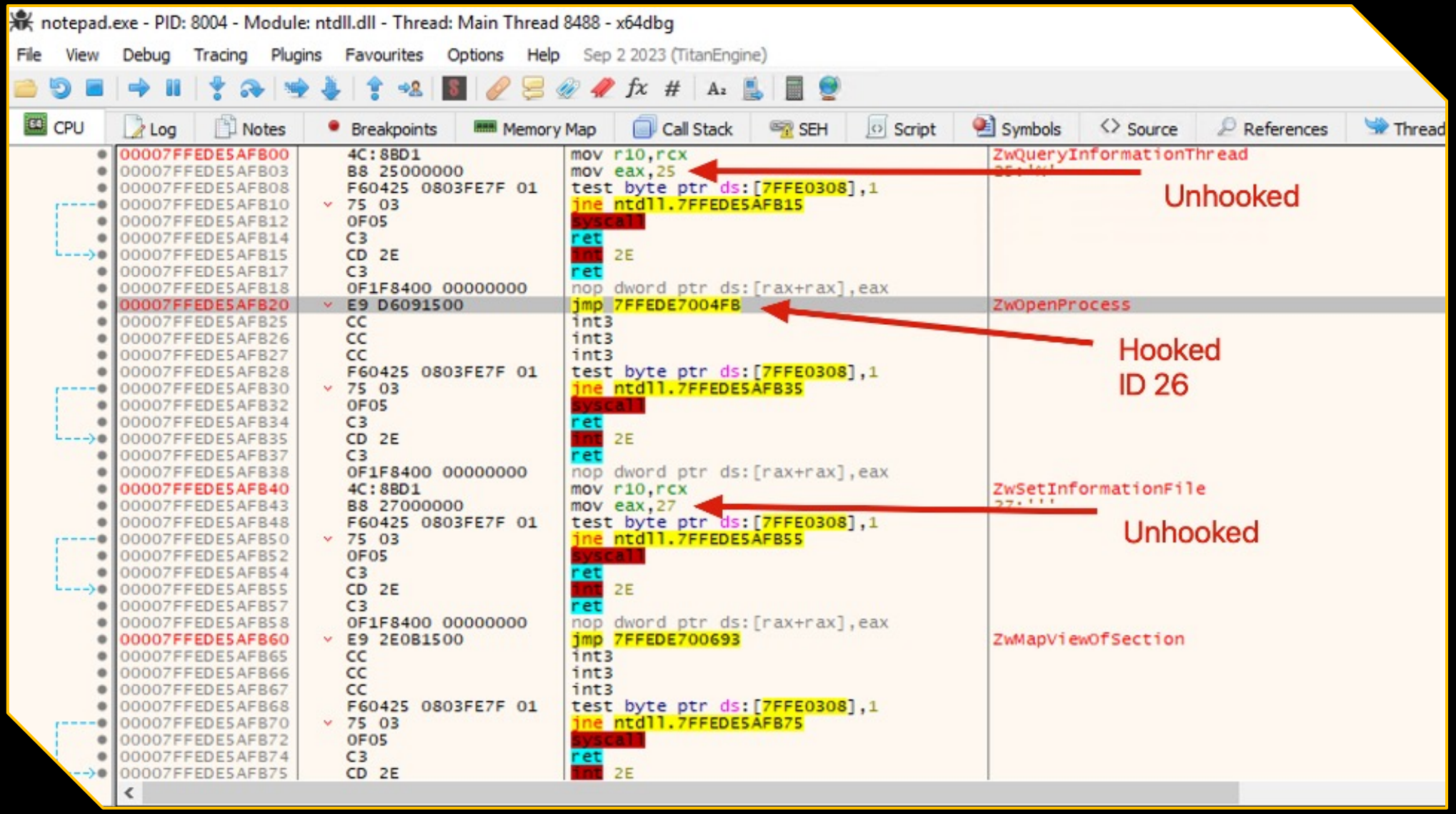


System Service Number - SSN



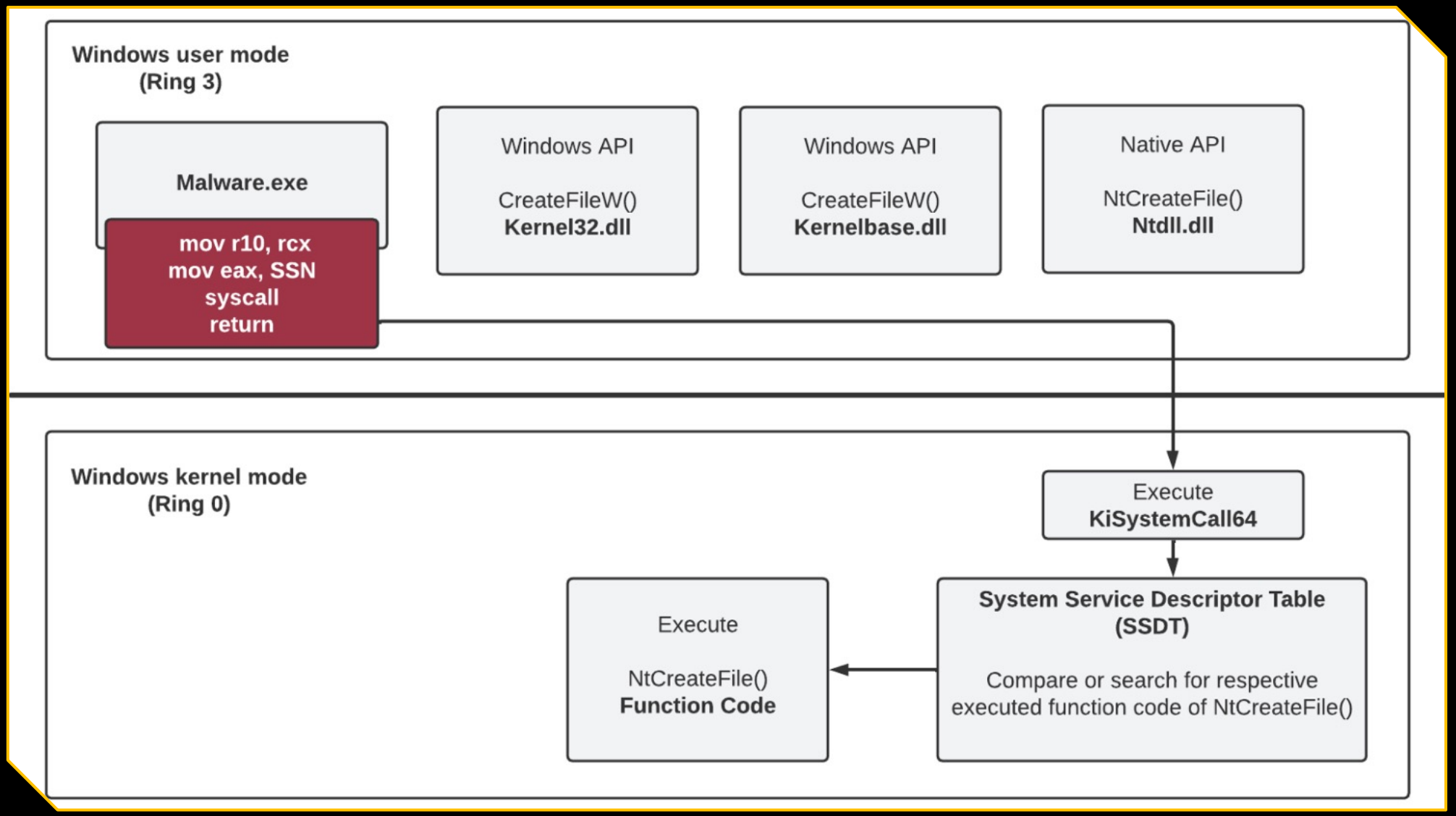
HACK & BEER// 2023 Curitiba

System Service Number – SSN (Hallo's Gate)



HACK & BEER 2023 Curitiba

Direct System Call



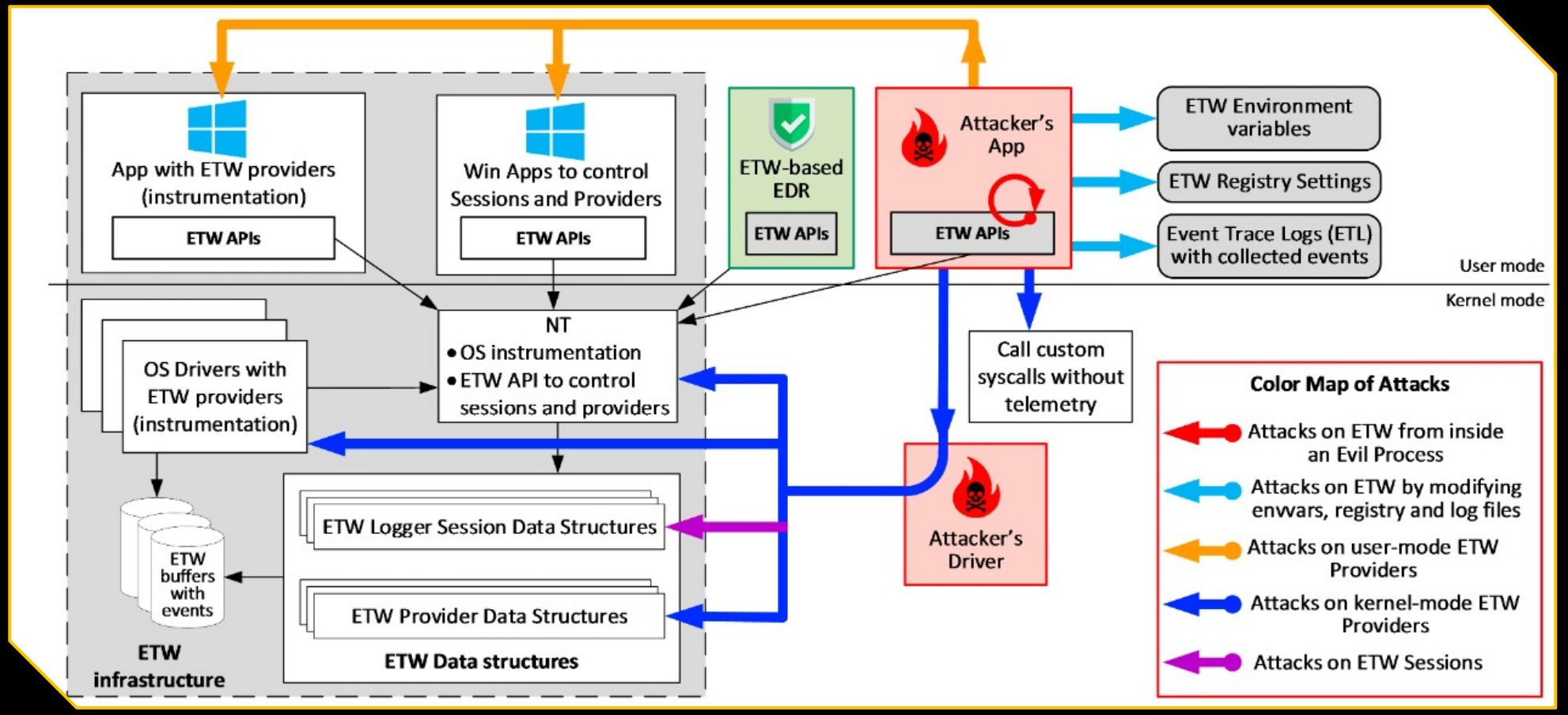
HACK & BEER//
2023 Curitiba

Sim!

Porém, nem todos!

ETW

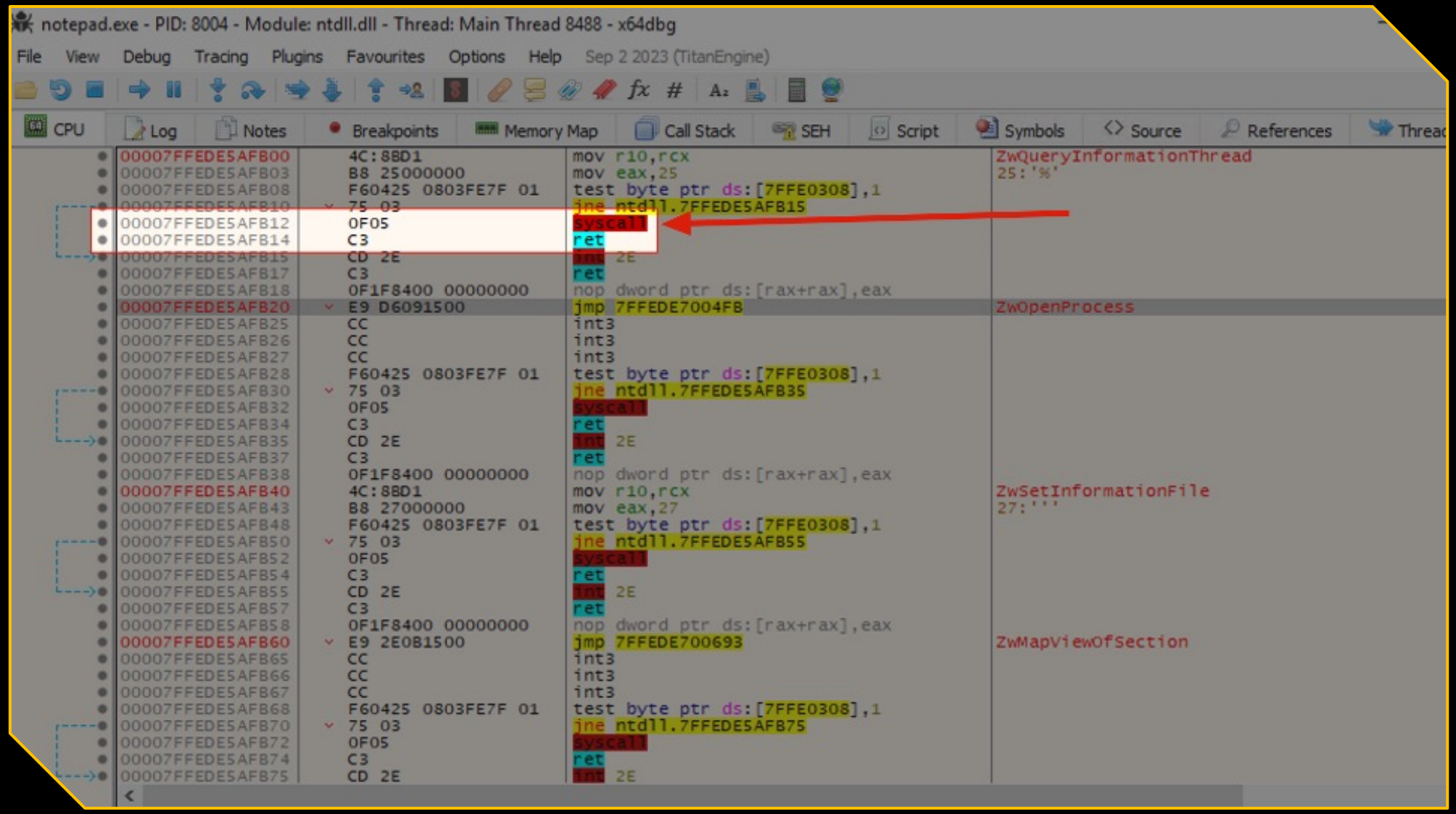
Event Tracing for Windows



HACK & BEER

2023 Curitiba

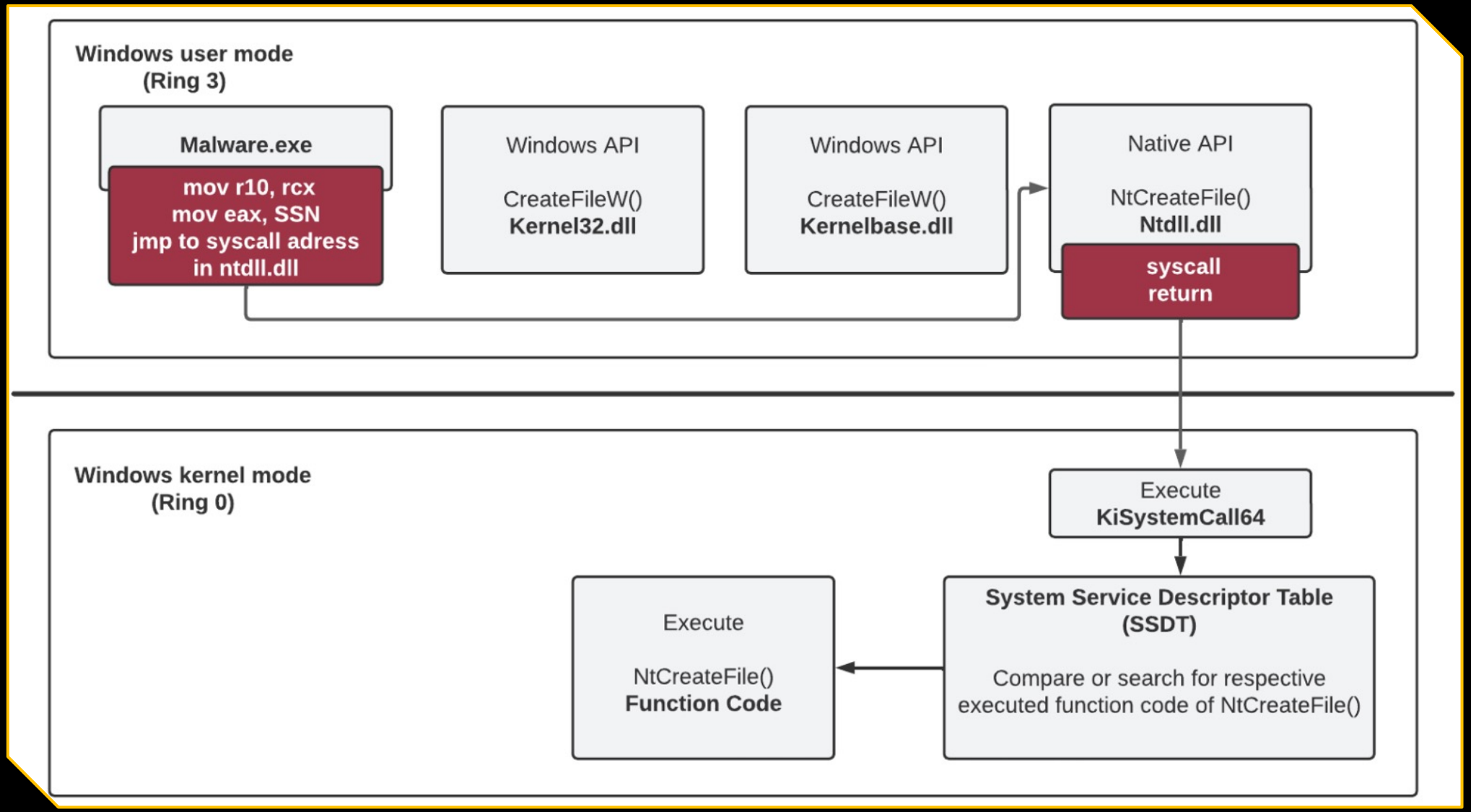
Indirect System Call



HACK & BEER

2023 Curitiba

Indirect System Call



Indirect System Call

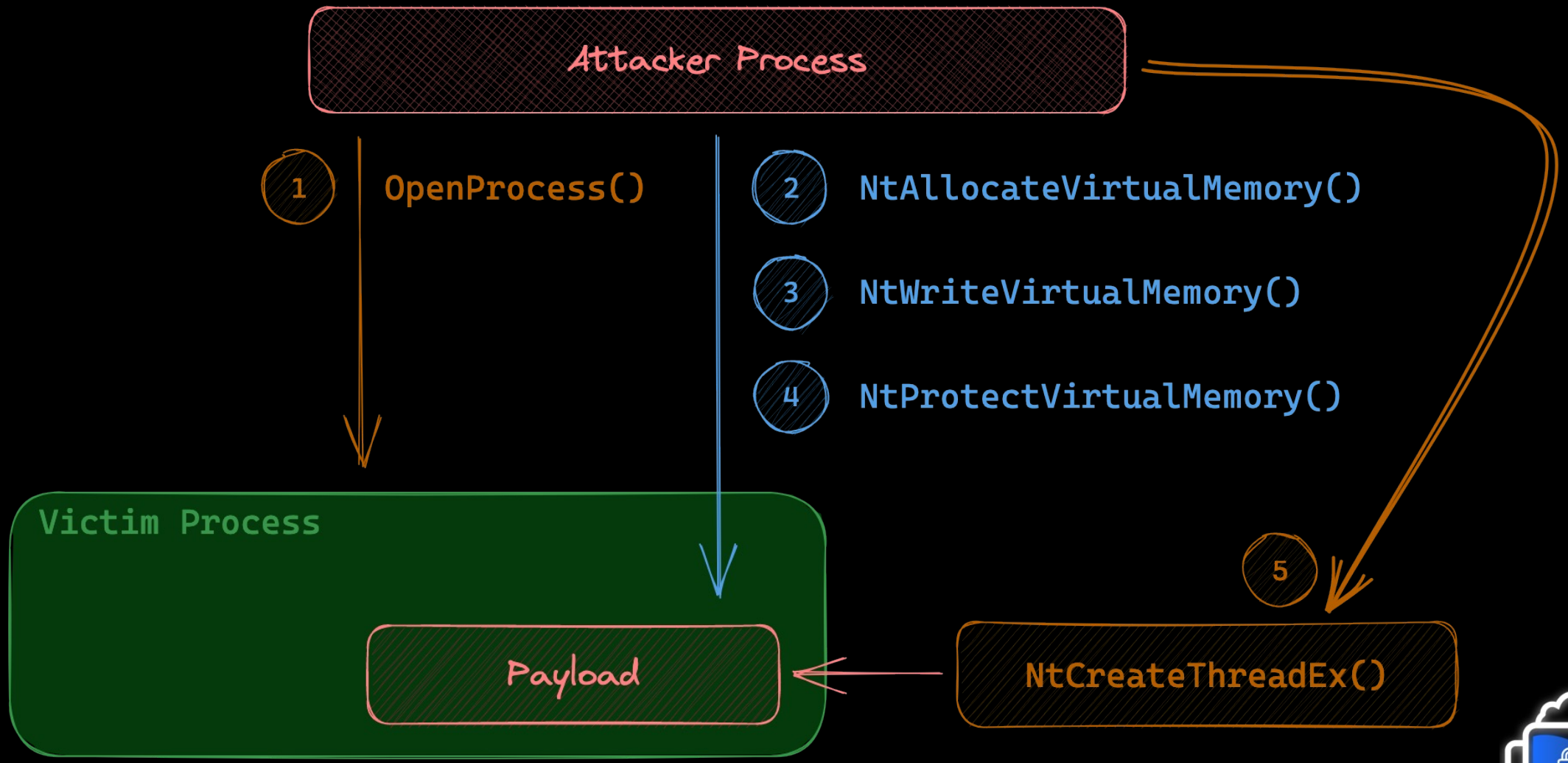
```
0:003> x ntdll!NtAllocateVirtualMemory
00007fff`f8a2d350 ntdll!NtAllocateVirtualMemory (NtAllocateVirtualMemory)
0:003> u 00007fff`f8a2d350
ntdll!NtAllocateVirtualMemory:
00007fff`f8a2d350 4c8bd1          mov     r10,rcx
00007fff`f8a2d353 b818000000      mov     eax,18h
00007fff`f8a2d358 f604250803fe7f01 test    byte ptr [SharedUserData+0x308 (00000000`7ffe0308)],1
00007fff`f8a2d360 7503            jne     ntdll!NtAllocateVirtualMemory+0x15 (00007fff`f8a2d365)
00007fff`f8a2d362 0f05            syscall
00007fff`f8a2d364 c3              ret
00007fff`f8a2d365 cd2e            int     2Eh
00007fff`f8a2d367 c3              ret
```

Can be hooked by EDR

Can't be hooked by EDR


O que você quer fazer agora cérebro?
O que fazemos somente no Hack & Beer Pink: Mostrar a PoC

Process Injection



HACK & BEER
2023 Curitiba

I'm just a child who has never grown up. I still keep asking these 'how' & 'why' questions. Occasionally, I find an answer.

Stephen Hawking

- Fontes utilizadas nesta apresentação
  - Pavel, Y at all. Windows Internals Part 1: 1. ed. Washington: Microsoft, 2017. Pg 47
  - Russinovich, M at all. Windows Internals: 5. ed. Washington: Microsoft Press, 2009. Pg 2
  - https://redops.at/en/blog/direct-syscalls-vs-indirect-syscalls
  - https://redops.at/en/blog/direct-syscalls-a-journey-from-high-to-low
  - https://www.naksyn.com/edr%20evasion/2022/09/01/operating-into-EDRs-blindspot.html
  - https://www.binarly.io/posts/Design_issues_of_modern_EDRs_bypassing_ETW-based_solutions/index.html
  - https://rioasmara.com/2020/09/06/basic-remote-thread-injection/

HACK & BEER //

2023 Curitiba