



HACK & BEER // 2023

Curitiba - 04/OUT/2023

Organizadores



Patrocinador



Bypassing AV/EDR using Windows In/Direct System Call

Helvio Junior (M4v3r1ck)

Pesquisador de segurança e Co-Fundador da Sec4US



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



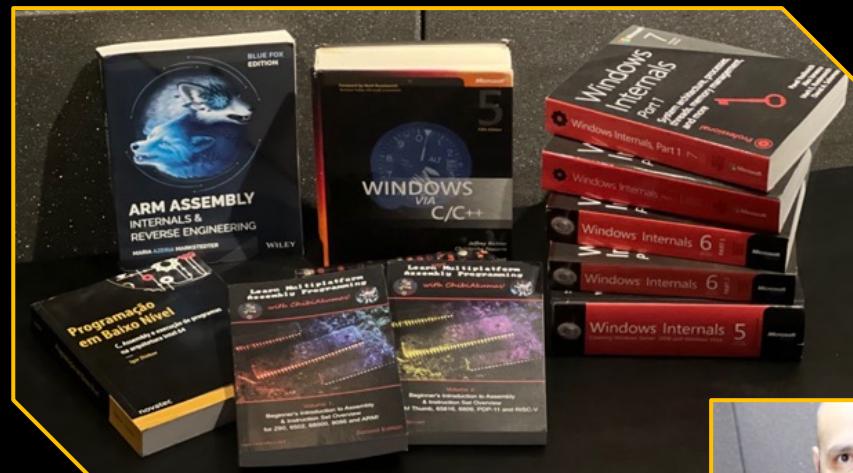
Whoami

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/>



Motivação

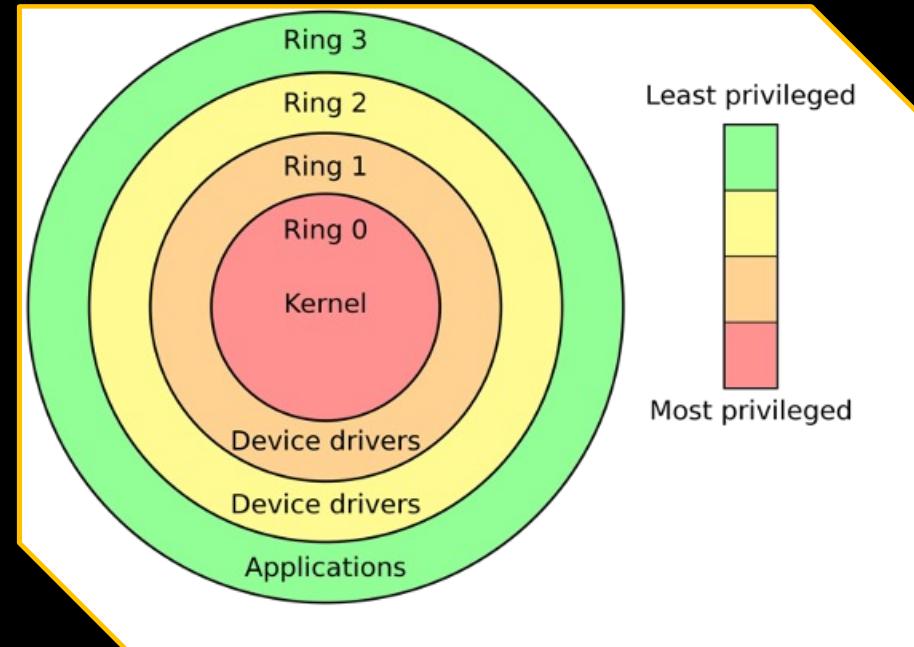
- Muitos acreditam, tenho a solução X, que é líder do Gartner, então estou 100% protegido.
- Não existe uma bala de prata
- Bypass/contorno das camadas de defesa
- FUD - Fully UnDetectable
- FUD é quando o seu código não é detectado por nenhuma camada/ferramenta de defesa
- Importante ser 100% FUD em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



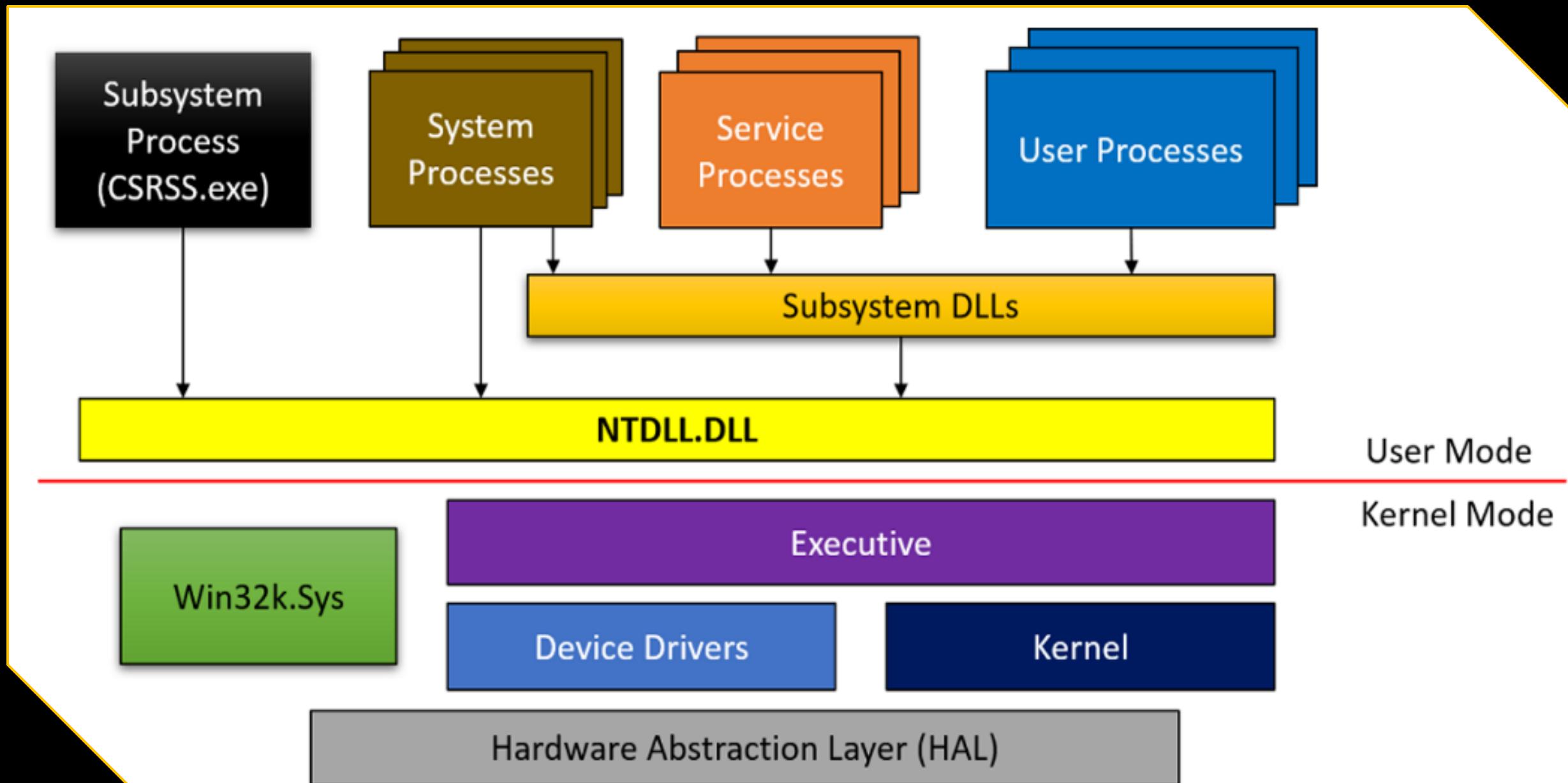
API

- 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 prática 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...).

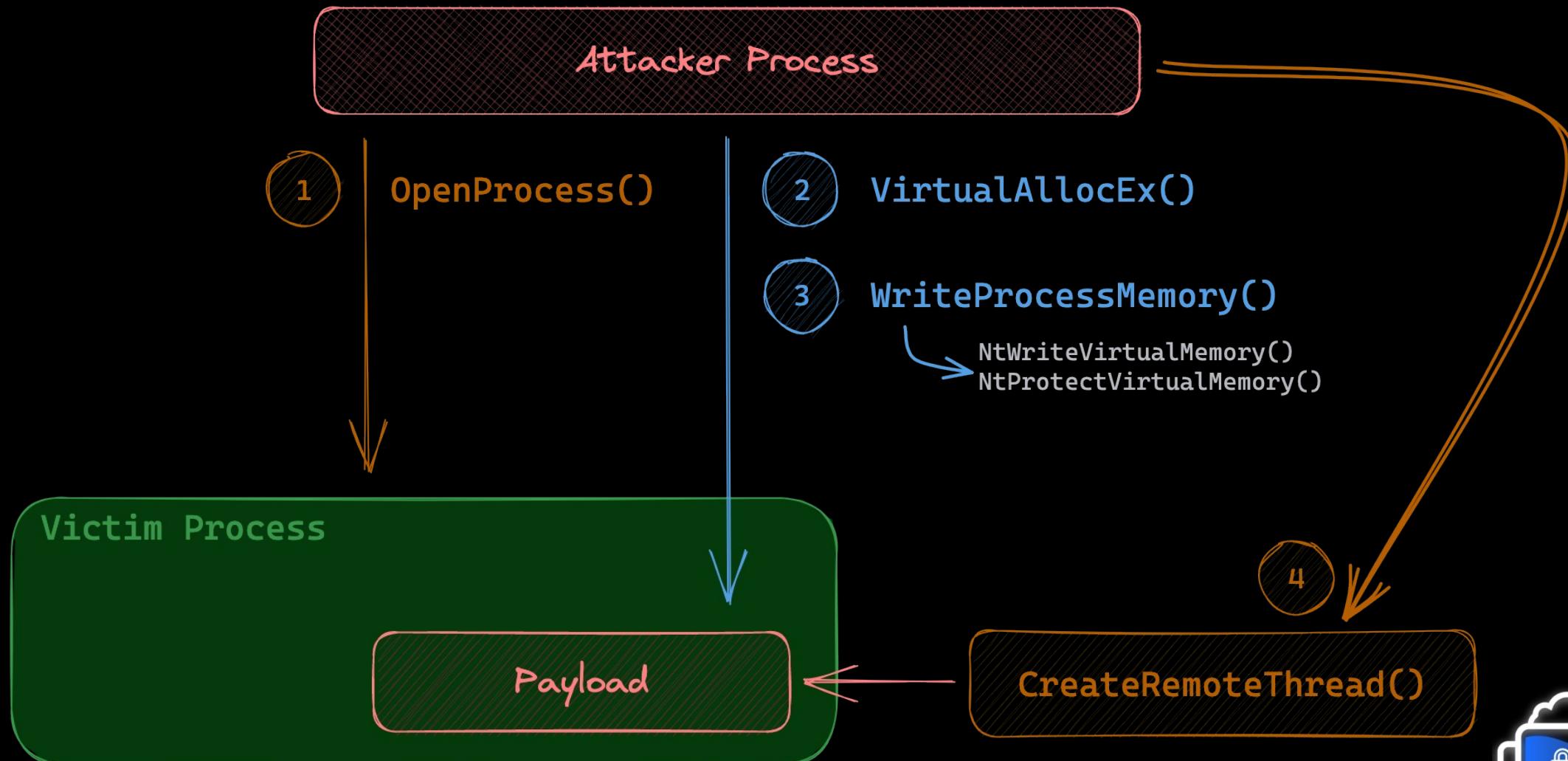
API

- 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

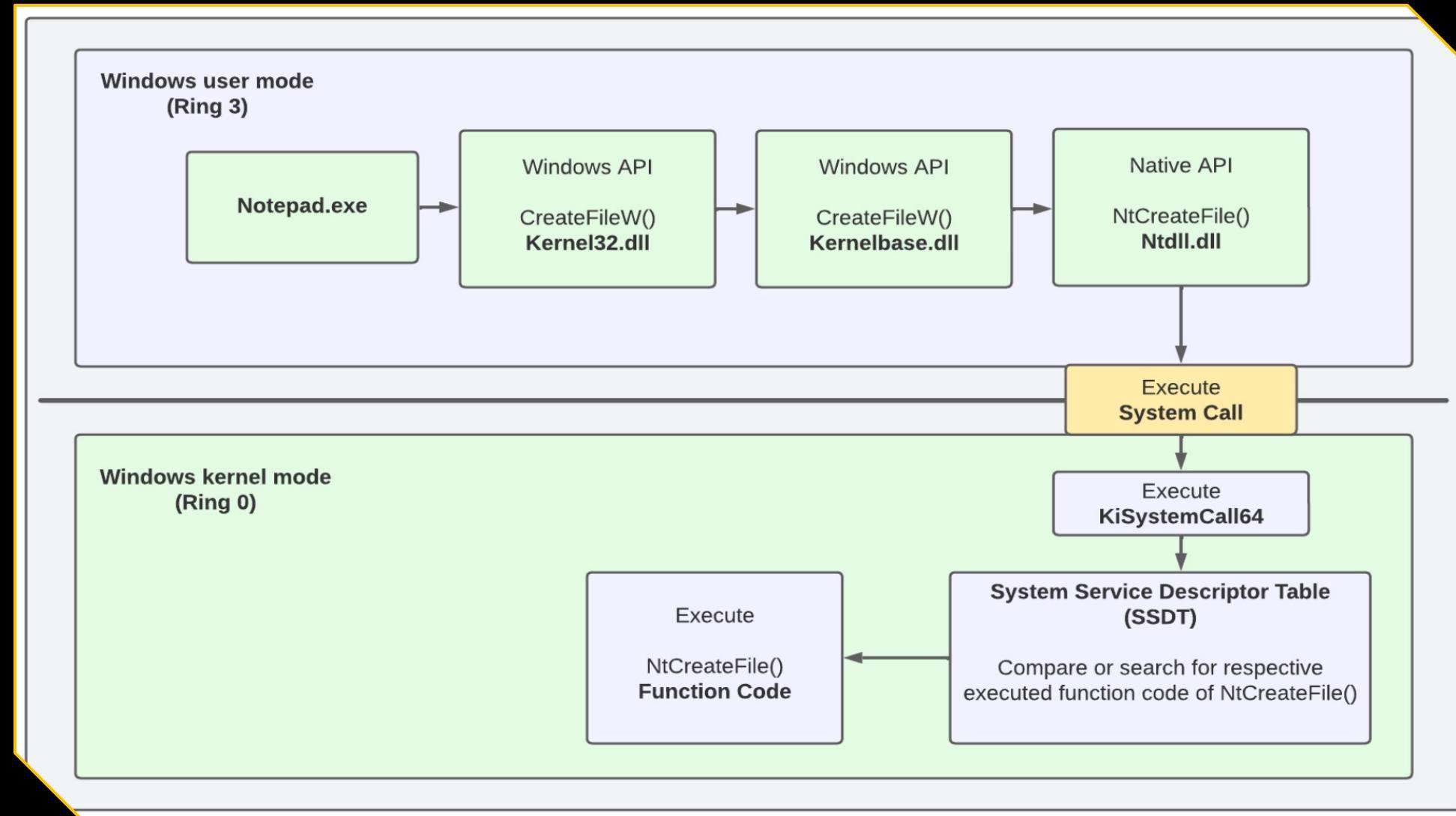
Windows APIs



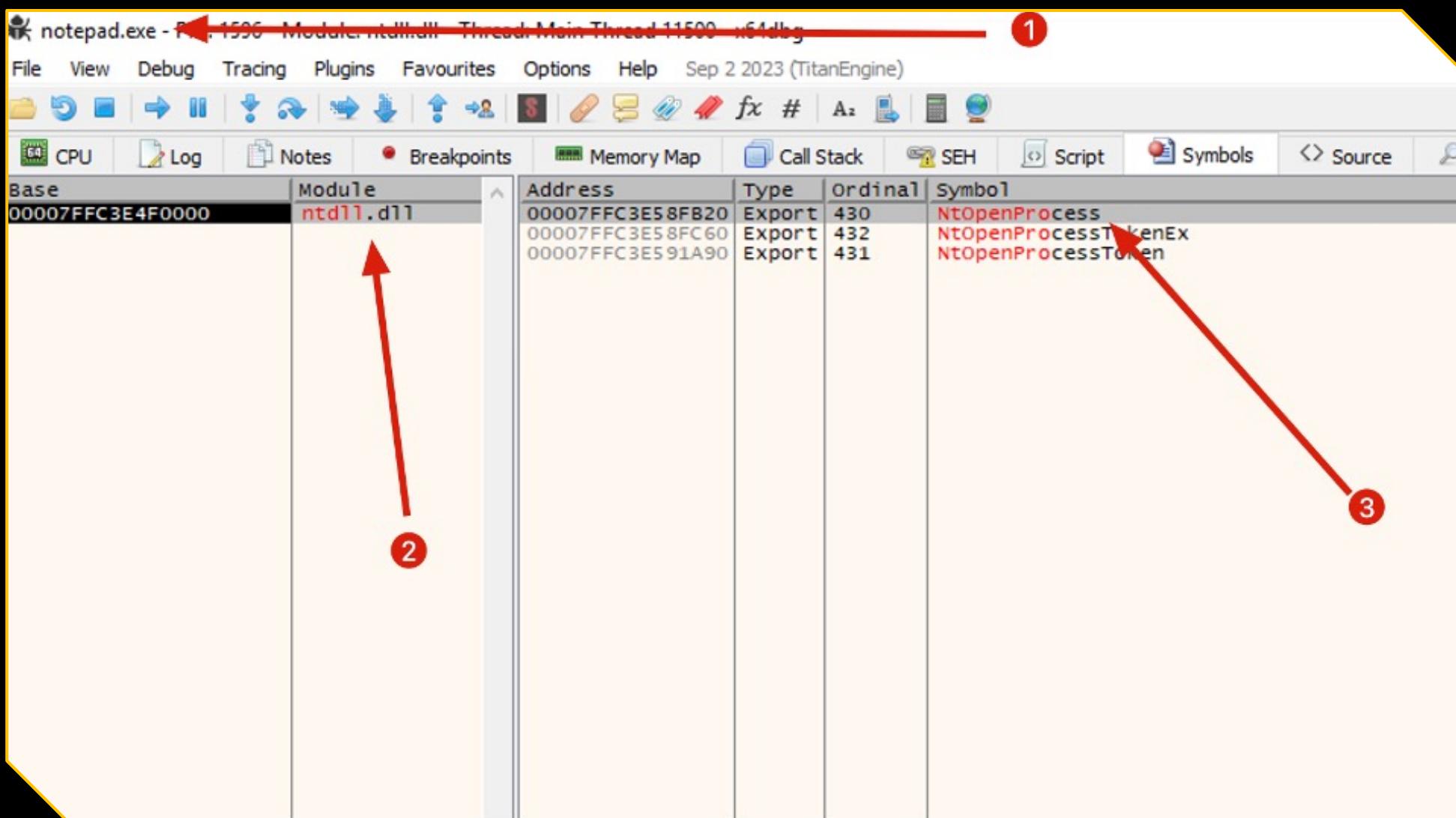
O ataque – Process Injection



Windows APIs



Unhooked API



Unhooked API

notepad.exe - PID: 1596 - Module: ntdll.dll - Thread: Main Thread 11500 - x64dbg

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

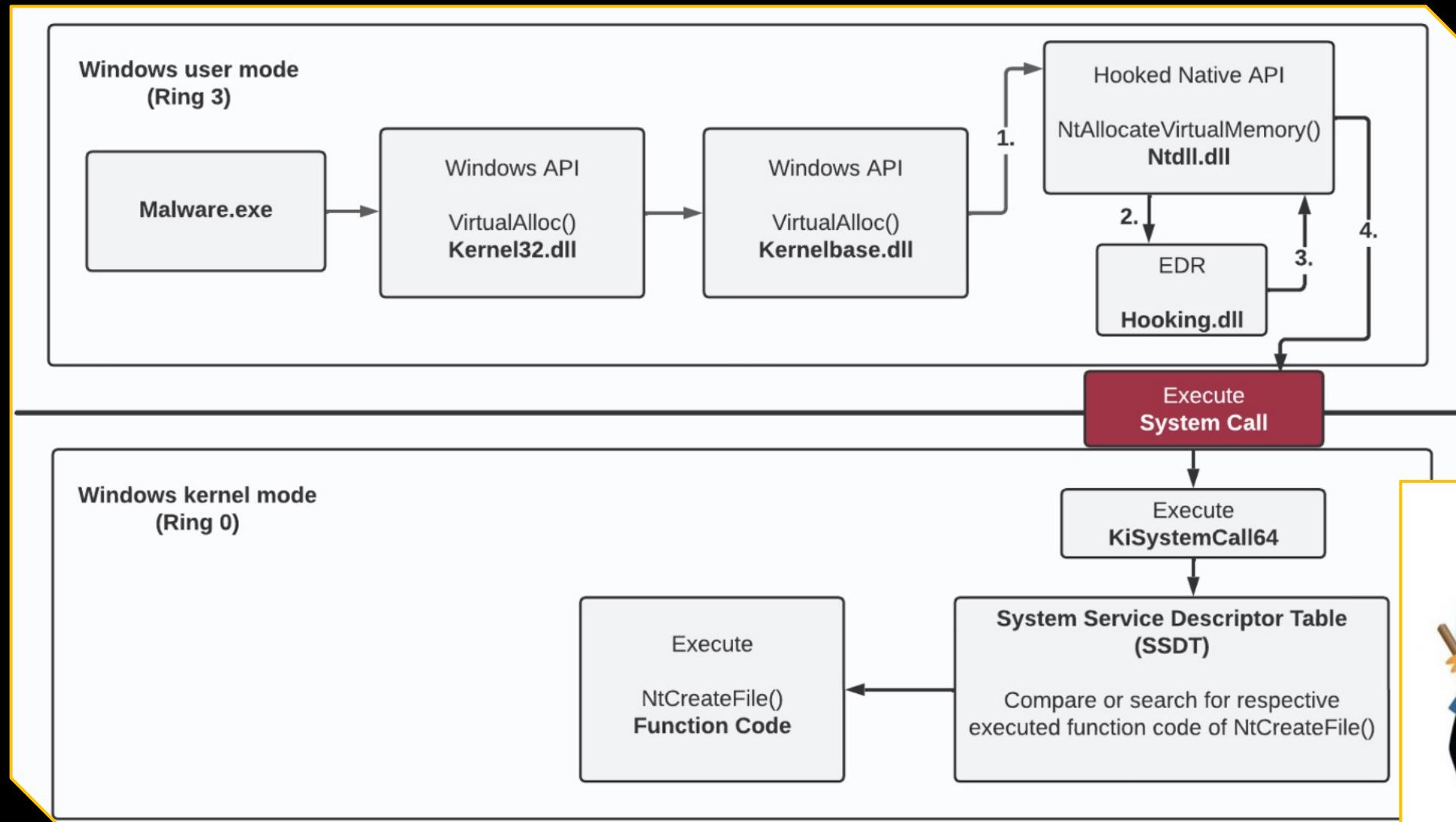
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols

```
mov r10,rcx  
mov eax,26  
test byte ptr ds:[1/FFC3E081],1  
jne ntdll.7FFC3E58FB35  
syscall  
ret  
int 2E  
ret  
nop dword ptr ds:[rax+rax],eax  
mov r10,rcx  
mov eax,27  
test byte ptr ds:[7FFE0308],1  
jne ntdll.7FFC3E58FB55  
syscall  
ret  
int 2E  
ret  
nop dword ptr ds:[rax+rax],eax  
mov r10,rcx  
mov eax,28  
test byte ptr ds:[7FFE0308],1  
jne ntdll.7FFC3E58FB75  
syscall  
ret  
int 2E  
ret  
nop dword ptr ds:[rax+rax],eax
```

ZwOpenProcess
26: '&'
ZwSetInformationFile
27: '''
ZwMapViewOfSection
28: '('

ID Syscall

Overview EDR

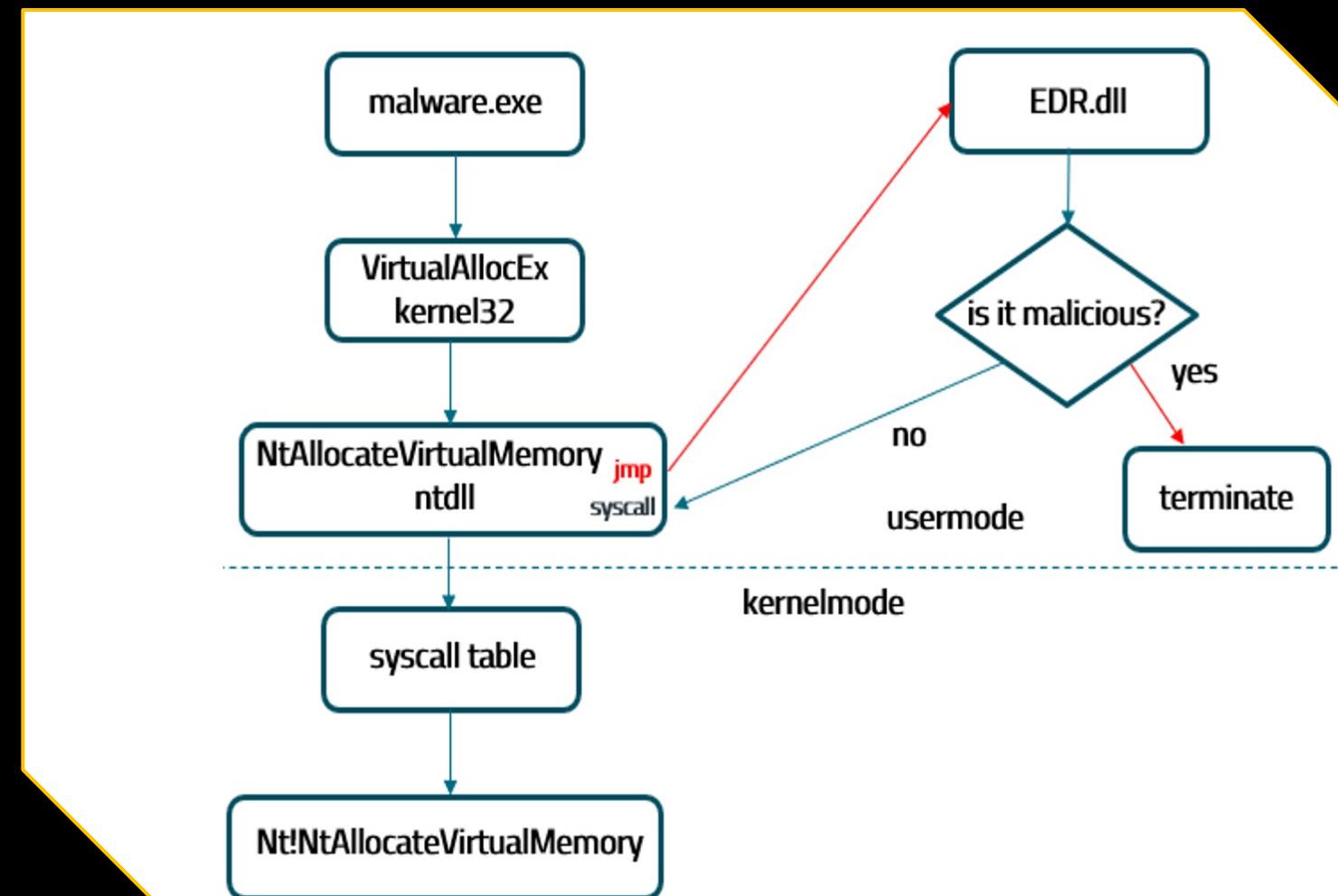


O QUE HÁ
GUARDADO
EMBAIXO
DO SEU
TAPETE



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

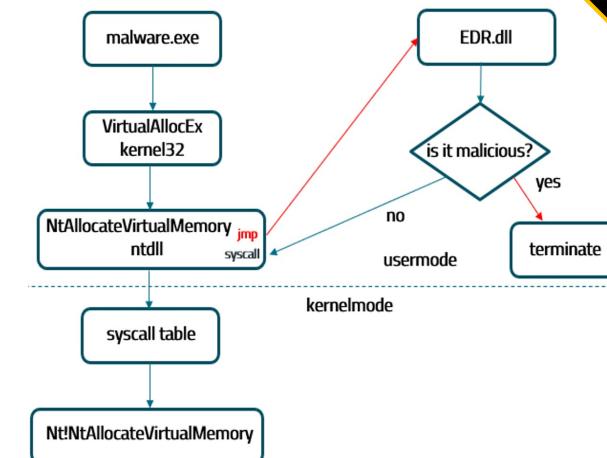
Processes Services Network Disk

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	0x7ffb1d50000	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	0x7ffb1eb0000	852 kB	BitDefender Hooking DLL
cfgmgr32.dll	0x7ffc3aa80000	296 kB	Configuration Manager DLL
clbcatq.dll	0x7ffc3beb0000	648 kB	COM+ Configuration Catalog
combase.dll	0x7ff624f00000	2.12 MB	Microsoft COM for Windows



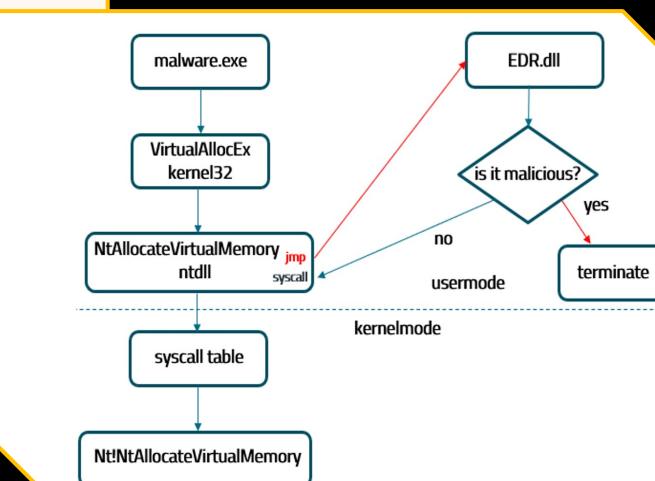
Hooked API

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

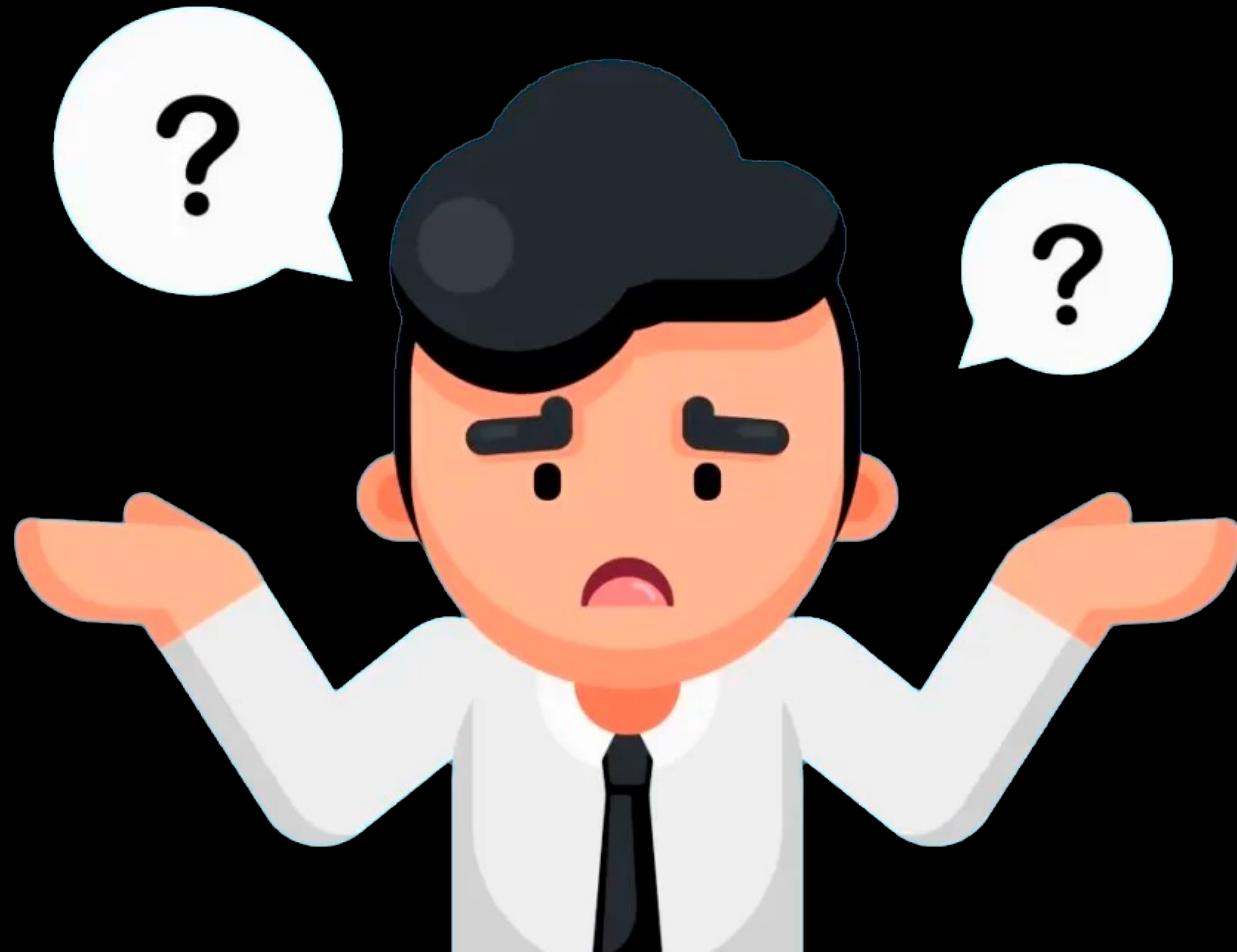
File View Debug Tracing Plugins Favourites Options Help Sep 2 2023 (TitanEngine)

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

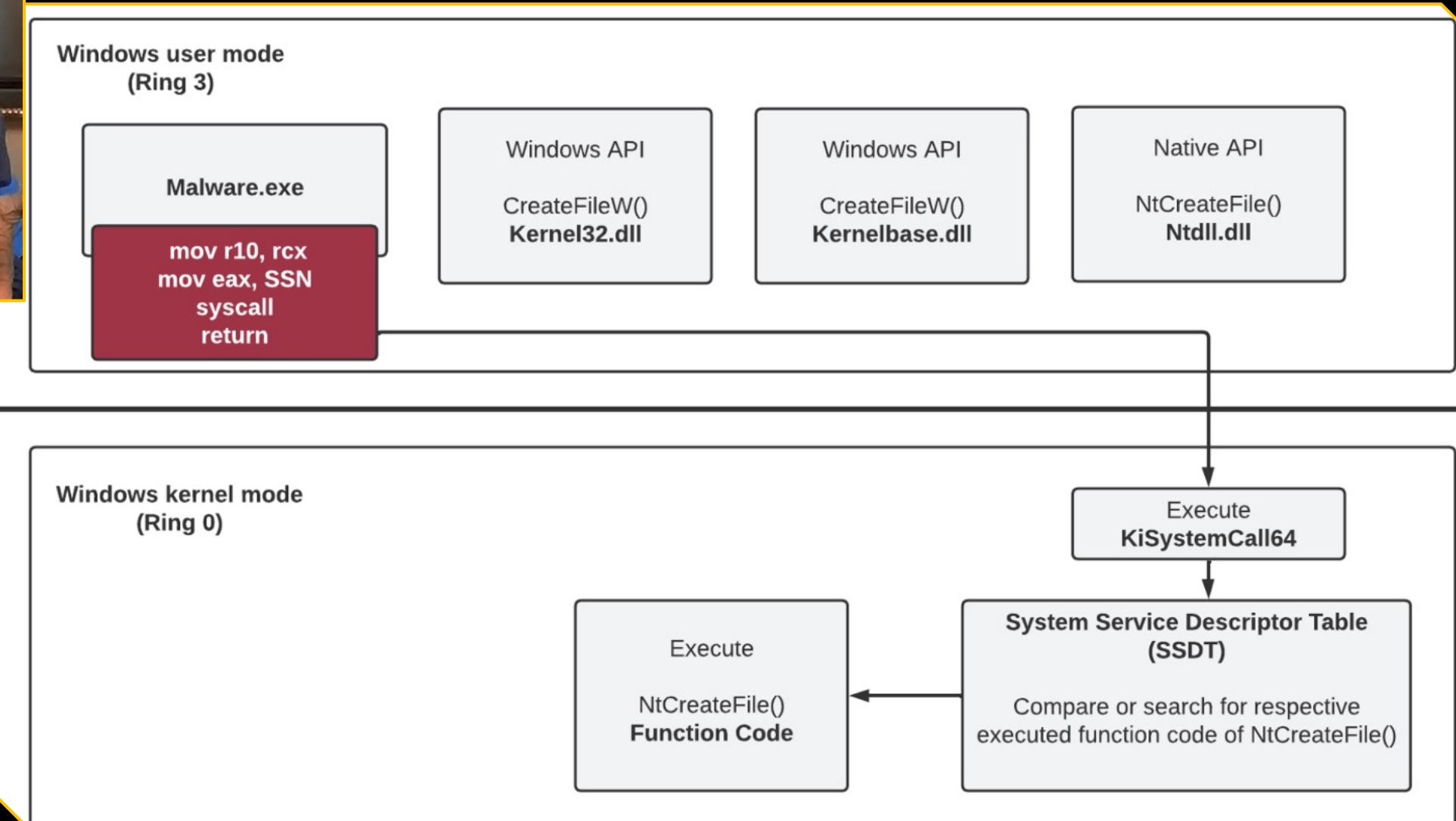
Address	Instruction	Description
00007FFEDE5AFB00	4C:88D1 B8 25000000 F60425 0803FE7F 01 v 75 03 OF05 C3 CD 2E C3 OF1F8400 00000000	ZwQueryInformationThread Unhooked
00007FFEDE5AFB20	E9 D6091500 CC CC CC F60425 0803FE7F 01 v 75 03 OF05 C3 CD 2E C3 OF1F8400 00000000	ZwOpenProcess Hooked ID 26
00007FFEDE5AFB40	4C:88D1 B8 27000000 F60425 0803FE7F 01 v 75 03 OF05 C3 CD 2E C3 OF1F8400 00000000	ZwSetInformationFile Unhooked
00007FFEDE5AFB60	E9 2E0B1500 CC CC CC F60425 0803FE7F 01 v 75 03 OF05 C3 CD 2E C3 OF1F8400 00000000	ZwMapViewOfSection



E agora?

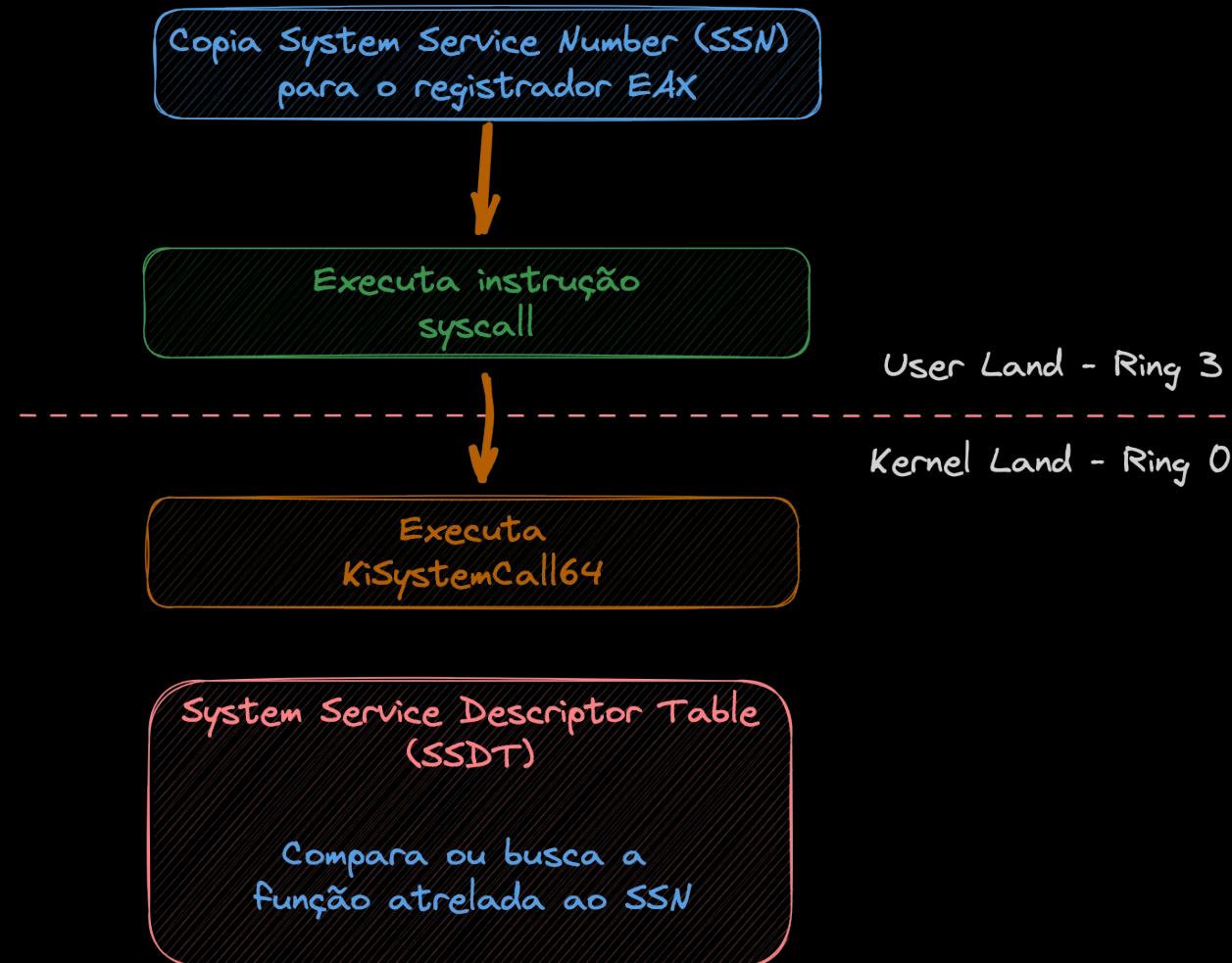


Direct System Call



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

The screenshot shows the CFF Explorer interface for the ntdll.dll file. A red arrow labeled 1 points to the title bar. Another red arrow labeled 2 points to the 'TimeDateStamp' entry in the table, which has a value of CA65C822. A third red arrow labeled 3 points to the 'Name' column header in the table below, which contains the string szAnsi.

Member	Offset	Size	Value
Characteristics	00149BB0	Dword	00000000
TimeDateStamp	00149BB4	Dword	CA65C822
MajorVersion	00149BB8	Word	0000
MinorVersion	00149BBA	Word	0000
Name	00149BBC	Dword	0015182A
Base	00149BC0	Dword	00000000

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
000000C7	0009F6A0	00BF	00152999	NtAcceptConnectPort
000000C8	0009F660	00C0	001529AD	NtAccessCheck
000000C9	0009FB80	00C1	001529BB	NtAccessCheckAndAuditAlarm
000000CA	000A02B0	00C2	001529D6	NtAccessCheckByType
000000CB	000A0180	00C3	001529EA	NtAccessCheckByTypeAndAuditAi...
000000CC	000A02D0	00C4	00152A0B	NtAccessCheckByTypeResultList
000000CD	000A02F0	00C5	00152A29	NtAccessCheckByTypeResultListAn...
000000CE	000A0310	00C6	00152A54	NtAccessCheckByTypeResultListAn...
000000CF	000A0330	00C7	00152A87	NtAcquireProcessActivityReference

Exportação ordenada pelo nome

The screenshot shows the Immunity Debugger interface with the module ntdll.dll selected. A red box highlights the export table. The table lists various exports with their addresses, types, ordinals, and symbols. The symbol 'NtAccessCheck' is highlighted.

Module	Address	Type	Ordinal	Symbol
ntdll.dll	00007FFC3E58F660	Export	200	NtAccessCheck
	00007FFC3E58F680	Export	657	NtWorkerFactoryWorkerReady
	00007FFC3E58F6A0	Export	199	NtAcceptConnectPort
	00007FFC3E58F6C0	Export	404	NtMapViewPhysicalPagesScatter
	00007FFC3E58F6E0	Export	653	NtWaitForSingleObject
	00007FFC3E58F700	Export	252	NtCallbackReturn
	00007FFC3E58F720	Export	520	NtReadFile
	00007FFC3E58F740	Export	334	NtDeviceIoControlFile
	00007FFC3E58F760	Export	658	NtWriteFile
	00007FFC3E58F780	Export	534	NtRemoveIoCompletion
	00007FFC3E58F7A0	Export	532	NtReleaseSemaphore
	00007FFC3E58F7C0	Export	542	NtReplyWaitReceivePort
	00007FFC3E58F7E0	Export	541	NtReplyPort
	00007FFC3E58F800	Export	588	NtSetInformationThread
	00007FFC3E58F820	Export	574	NtSetEvent
	00007FFC3E58F840	Export	260	NtClose
	00007FFC3E58F860	Export	492	NtQueryObject
	00007FFC3E58F880	Export	475	NtQueryInformationFile
	00007FFC3E58F8A0	Export	421	NtOpenKey
	00007FFC3E58F8C0	Export	346	NtEnumerateValueKey
	00007FFC3E58F8E0	Export	351	NtFindAtom
	00007FFC3E58F900	Export	463	NtQueryDefaultLocale
	00007FFC3E58F920	Export	488	NtQueryKey
	00007FFC3E58F940	Export	511	NtQueryValueKey
	00007FFC3E58F960	Export	222	NtAllocateVirtualMemory

Exportação ordenada pelo endereço de memória

System Service Number - SSN

notepad.exe - PID: 1596 - Module: ntdll.dll - Thread: Main Thread 11500 - x64dbg

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

CPU Log Notes Breakpoints Memory Map Cell Stack SEH Script Symbols Source References Threads

Address	OpCode	Assembly	Symbol
00007FFC3E58F660	4C:8BD1	mov r10,rcx	ZwAccessCheck
00007FFC3E58F663	B8 00000000	mov eax,0	
00007FFC3E58F668	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1 jne ntdll.7FFC3E58F675	
00007FFC3E58F670	v 75 03	ret	
00007FFC3E58F672	0F05	int 2E	
00007FFC3E58F674	C3	ret	
00007FFC3E58F675	CD 2E	int 2E	
00007FFC3E58F677	C3	ret	
00007FFC3E58F678	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFC3E58F680	4C:8BD1	mov r10,rcx	NtWorkerFactoryWorkerReady
00007FFC3E58F683	B8 01000000	mov eax,1	
00007FFC3E58F688	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1 jne ntdll.7FFC3E58F695	
00007FFC3E58F690	v 75 03	ret	
00007FFC3E58F692	0F05	int 2E	
00007FFC3E58F694	C3	ret	
00007FFC3E58F695	CD 2E	int 2E	
00007FFC3E58F697	C3	ret	
00007FFC3E58F698	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFC3E58F6A0	4C:8BD1	mov r10,rcx	ZwAcceptConnectPort
00007FFC3E58F6A3	B8 02000000	mov eax,2	
00007FFC3E58F6A8	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1 jne ntdll.7FFC3E58F6B5	
00007FFC3E58F6B0	v 75 03	ret	
00007FFC3E58F6B2	0F05	int 2E	
00007FFC3E58F6B4	C3	ret	
00007FFC3E58F6B5	CD 2E	int 2E	
00007FFC3E58F6B7	C3	ret	
00007FFC3E58F6B8	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFC3E58F6C0	4C:8BD1	mov r10,rcx	NtMapUserPhysicalPagesScatter
00007FFC3E58F6C3	B8 03000000	mov eax,3	
00007FFC3E58F6C8	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1 jne ntdll.7FFC3E58F6D5	
00007FFC3E58F6D0	v 75 03	ret	
00007FFC3E58F6D2	0F05	int 2E	
00007FFC3E58F6D4	C3	ret	
00007FFC3E58F6D5	CD 2E	int 2E	
00007FFC3E58F6D7	C3	ret	
00007FFC3E58F6D8	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFC3E58F6E0	4C:8BD1	mov r10,rcx	NtWaitForSingleObject
00007FFC3E58F6E3	B8 04000000	mov eax,4	

System Service Number – SSN (Hallo's Gate)

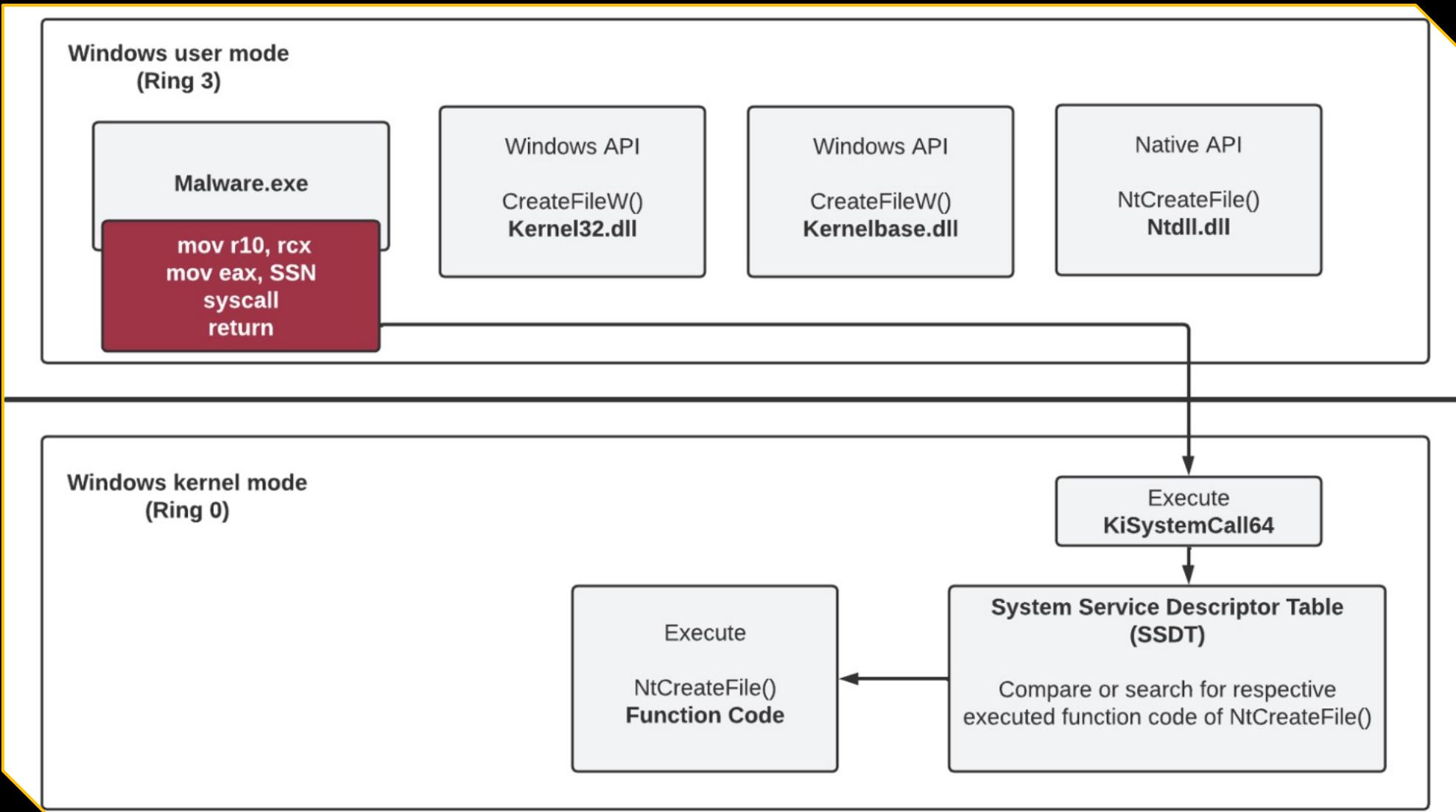
notepad.exe - PID: 8004 - Module: ntdll.dll - Thread: Main Thread 8488 - x64dbg

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 Thread

Address	OpCode	Assembly	Description
00007FFEDE5AFB00	4C:8BD1	mov r10,rcx	ZwQueryInformationThread
00007FFEDE5AFB03	B8 25000000	mov eax,25	Unhooked
00007FFEDE5AFB08	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB10	75 03	je ntdll.7FFEDE5AFB15	
00007FFEDE5AFB12	OF05	syscall	
00007FFEDE5AFB14	C3	ret	
00007FFEDE5AFB15	CD 2E	int 2E	
00007FFEDE5AFB17	C3	ret	
00007FFEDE5AFB18	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFEDE5AFB20	E9 D6091500	jmp 7FFEDE7004FB	ZwOpenProcess
00007FFEDE5AFB25	CC	int3	
00007FFEDE5AFB26	CC	int3	
00007FFEDE5AFB27	CC	int3	
00007FFEDE5AFB28	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB30	75 03	je ntdll.7FFEDE5AFB35	
00007FFEDE5AFB32	OF05	syscall	
00007FFEDE5AFB34	C3	ret	
00007FFEDE5AFB35	CD 2E	int 2E	
00007FFEDE5AFB37	C3	ret	
00007FFEDE5AFB38	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFEDE5AFB40	4C:8BD1	mov r10,rcx	ZwSetInformationFile
00007FFEDE5AFB43	B8 27000000	mov eax,27	Unhooked
00007FFEDE5AFB48	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB50	75 03	je ntdll.7FFEDE5AFB55	
00007FFEDE5AFB52	OF05	syscall	
00007FFEDE5AFB54	C3	ret	
00007FFEDE5AFB55	CD 2E	int 2E	
00007FFEDE5AFB57	C3	ret	
00007FFEDE5AFB58	OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFEDE5AFB60	E9 2E0B1500	jmp 7FFEDE700693	ZwMapViewOfSection
00007FFEDE5AFB65	CC	int3	
00007FFEDE5AFB66	CC	int3	
00007FFEDE5AFB67	CC	int3	
00007FFEDE5AFB68	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB70	75 03	je ntdll.7FFEDE5AFB75	
00007FFEDE5AFB72	OF05	syscall	
00007FFEDE5AFB74	C3	ret	
00007FFEDE5AFB75	CD 2E	int 2E	

Direct System Call



ESTÁ ME DIZENDO QUE COM 3 "FORS" E UM
CALL VOCÊ BYPASSOU OS
NEXTULTRATOPGENERATION'S EDRS?



makeameme.org

HACK &
BEER//
2023 Curitiba

Sim!

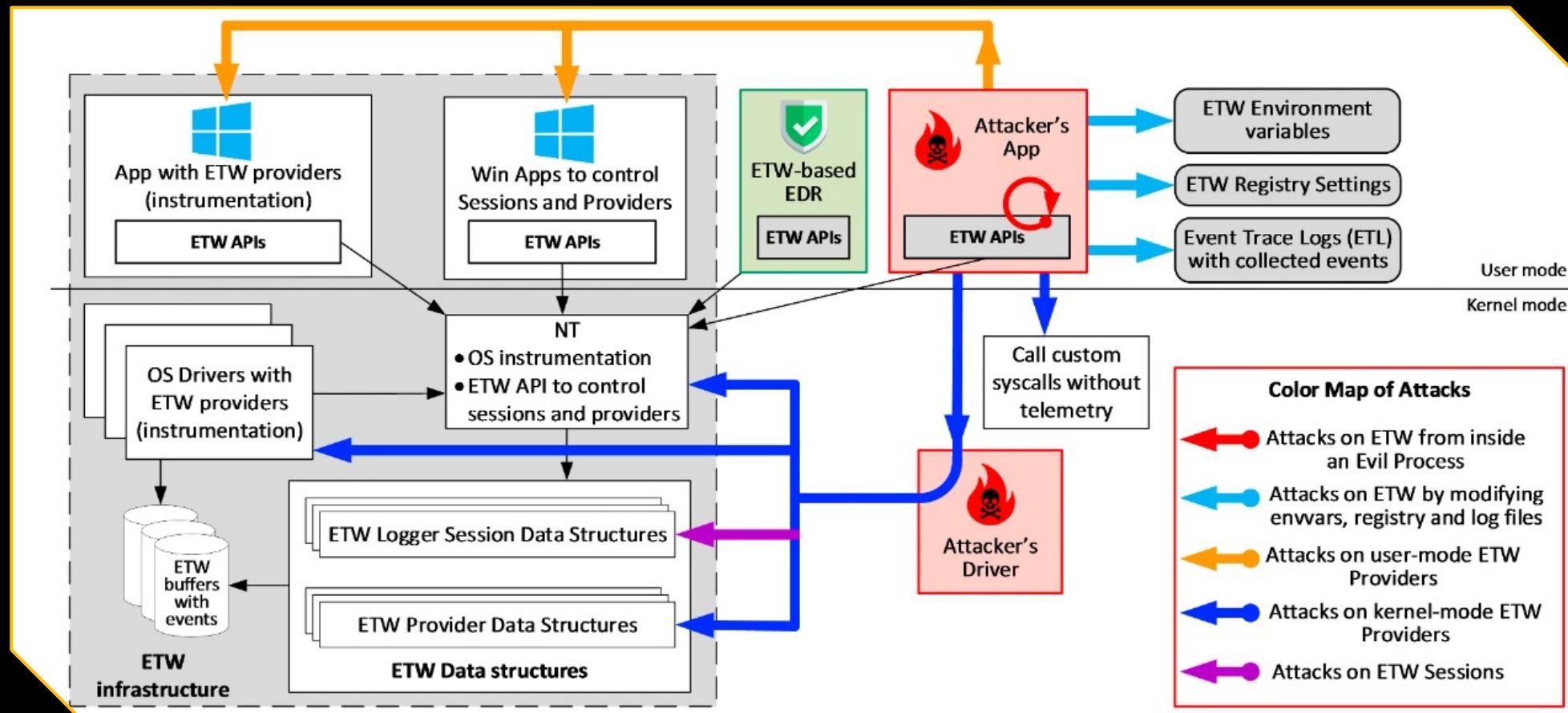


*Porém, nem
todos!*



ETW

Event Tracing for Windows



Indirect System Call

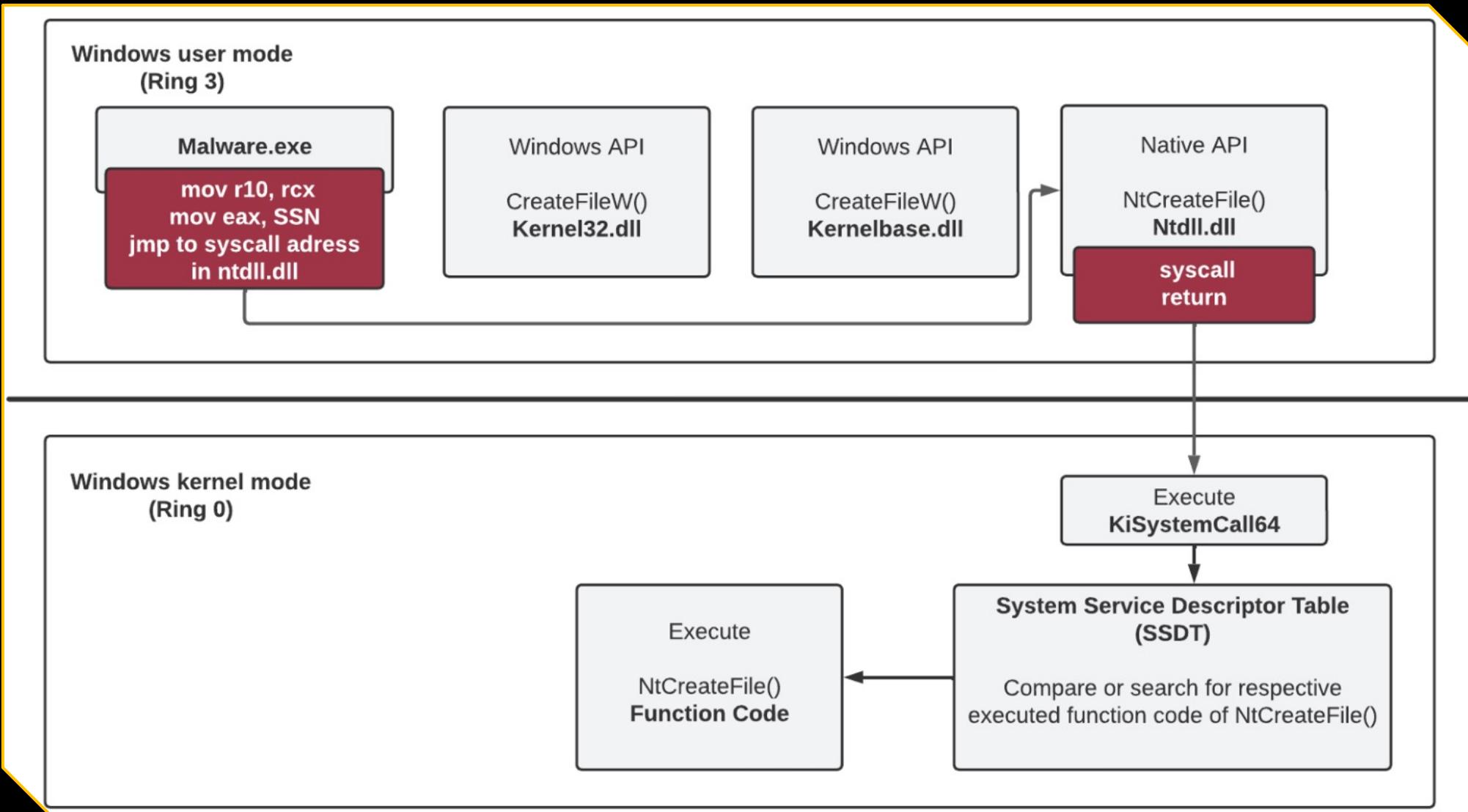
notepad.exe - PID: 8004 - Module: ntdll.dll - Thread: Main Thread 8488 - x64dbg

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 Threads

Address	OpCode	Assembly	Description
00007FFEDE5AFB00	4C:8BD1	mov r10,rcx	ZwQueryInformationThread
00007FFEDE5AFB03	B8 25000000	mov eax,25	
00007FFEDE5AFB08	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB10	75 03	jne ntdll.7FFEDE5AFB15	
00007FFEDE5AFB12	0F05	syscall	
00007FFEDE5AFB14	C3	ret	
00007FFEDE5AFB15	CD 2E	int 2E	
00007FFEDE5AFB17	C3	ret	
00007FFEDE5AFB18	0F1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFEDE5AFB20	E9 D6091500	jmp 7FFEDE7004FB	ZwOpenProcess
00007FFEDE5AFB25	CC	int3	
00007FFEDE5AFB26	CC	int3	
00007FFEDE5AFB27	CC	int3	
00007FFEDE5AFB28	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB30	75 03	jne ntdll.7FFEDE5AFB35	
00007FFEDE5AFB32	0F05	syscall	
00007FFEDE5AFB34	C3	ret	
00007FFEDE5AFB35	CD 2E	int 2E	
00007FFEDE5AFB37	C3	ret	
00007FFEDE5AFB38	0F1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFEDE5AFB40	4C:8BD1	mov r10,rcx	ZwSetInformationFile
00007FFEDE5AFB43	B8 27000000	mov eax,27	
00007FFEDE5AFB48	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB50	75 03	jne ntdll.7FFEDE5AFB55	
00007FFEDE5AFB52	0F05	syscall	
00007FFEDE5AFB54	C3	ret	
00007FFEDE5AFB55	CD 2E	int 2E	
00007FFEDE5AFB57	C3	ret	
00007FFEDE5AFB58	0F1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
00007FFEDE5AFB60	E9 2E0B1500	jmp 7FFEDE700693	ZwMapViewOfSection
00007FFEDE5AFB65	CC	int3	
00007FFEDE5AFB66	CC	int3	
00007FFEDE5AFB67	CC	int3	
00007FFEDE5AFB68	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FFEDE5AFB70	75 03	jne ntdll.7FFEDE5AFB75	
00007FFEDE5AFB72	0F05	syscall	
00007FFEDE5AFB74	C3	ret	
00007FFEDE5AFB75	CD 2E	int 2E	

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

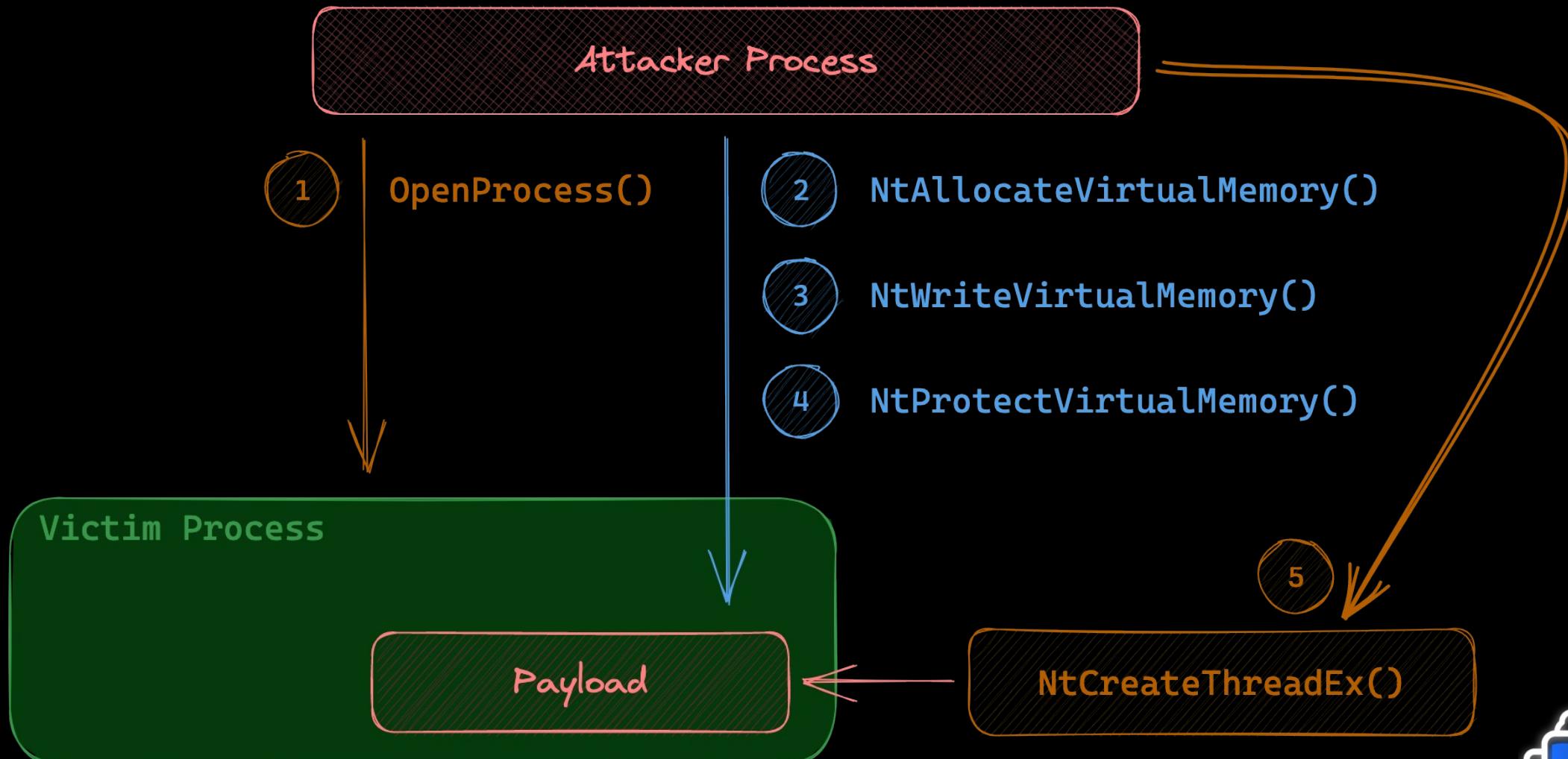
Can't be hooked by EDR



*O que você quer
fazer agora
cérebro?*

*O que fazemos
somente no
Hack & Beer Pink:
Mostrar a PoC*

Process Injection



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