

AV/EDR

Bypassing using
Windows In/Direct
System Call



Agenda

- ✓ Whoami (or not)
- ✓ 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)



- ✓ 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)

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
- ✓ Fully UnDetectable
 - ✓ Importante ser 100% FUD em relação ao seu alvo
- ✓ FUD é quando o seu código não é detectado por nenhuma camada/ferramenta de defesa

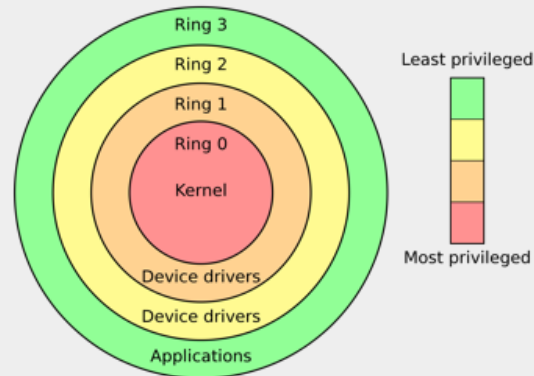
Motivação

- ✓ 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



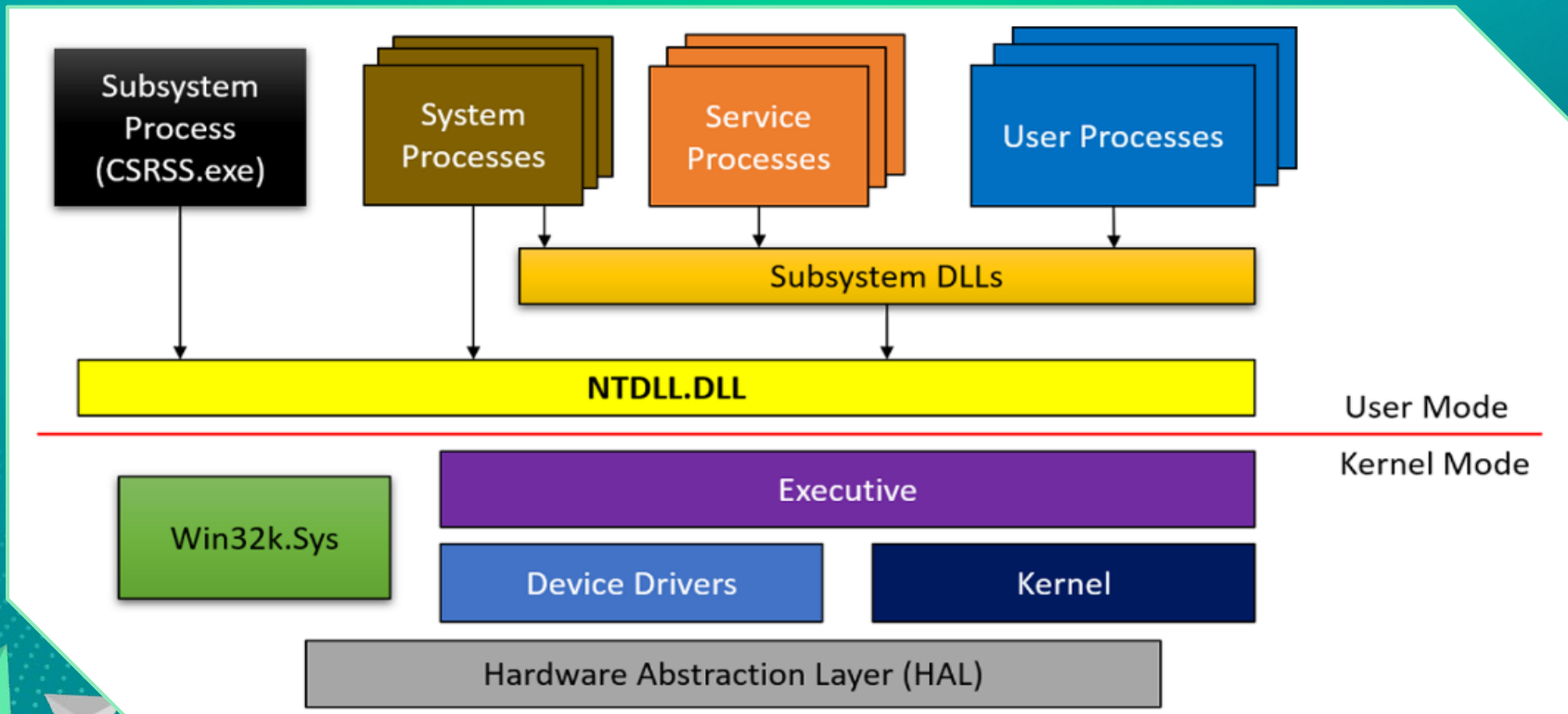
APIs

- ✓ API é um acrônimo para **A**pplication **P**rogramming **I**nterface (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...).

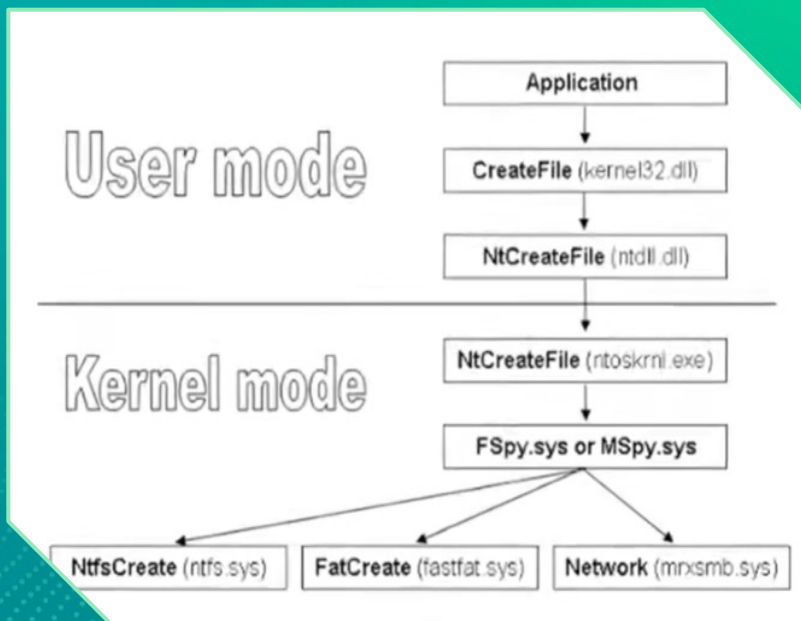
APIs

- ✓ 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

APIs



APIs

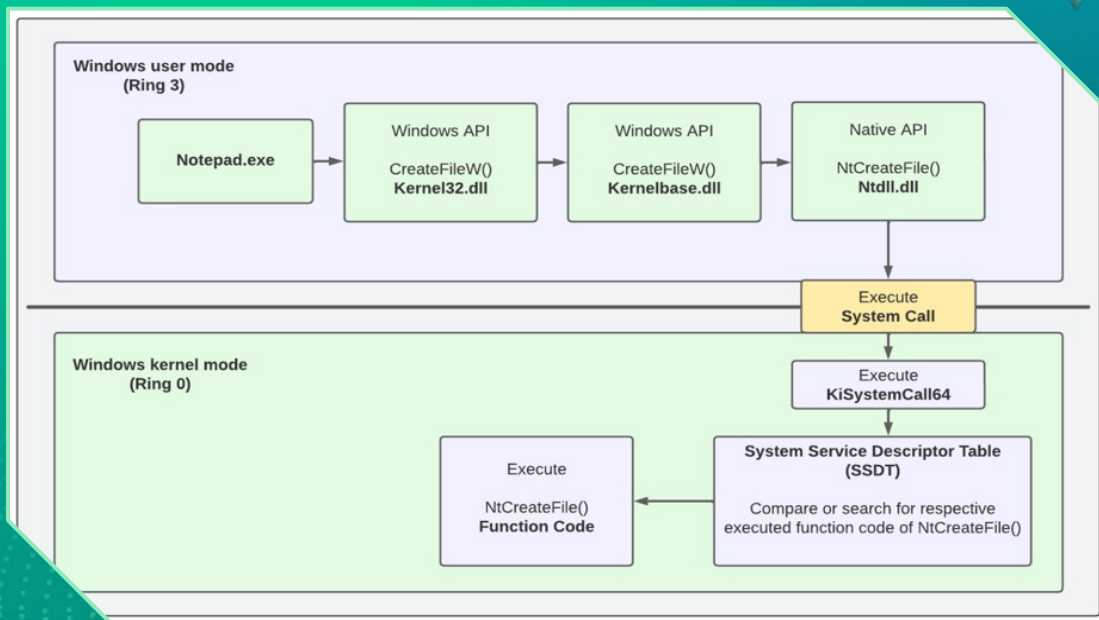


Sequência de chamadas
(criação de arquivo)

- ✓ CreateFile
- ✓ NtCreateFile (ntdll.dll)
- ✓ NtCreateFile (ntoskrnl.exe)
- ✓ ...

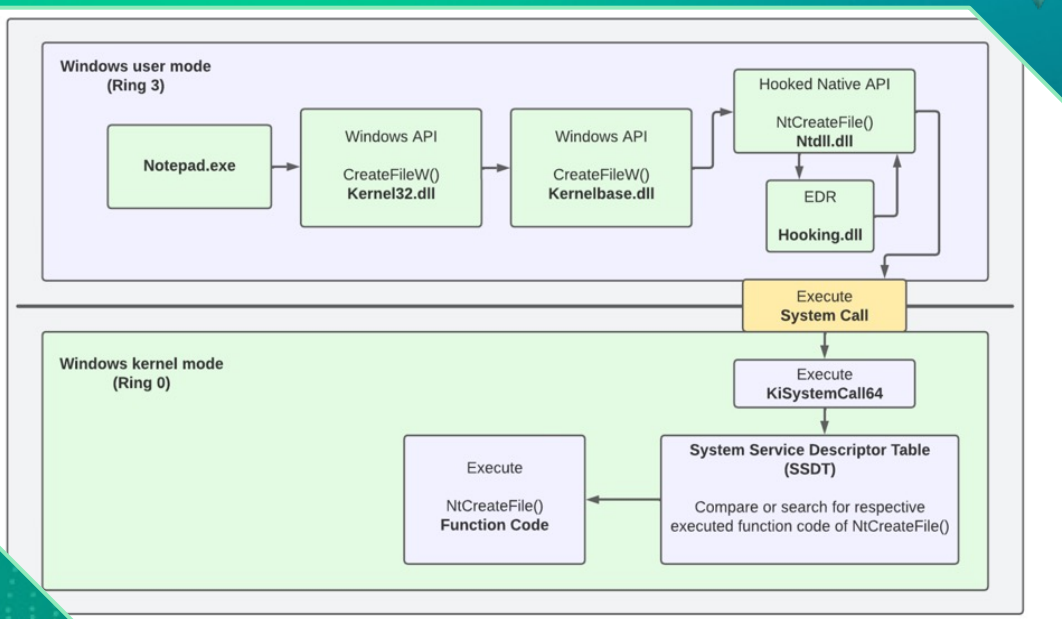
Ntdll.dll

- ✓ É a ponte entre o ring 3 e o ring 0
- ✓ Porém ...
 - ✓ (deixa para depois)



Overview EDR

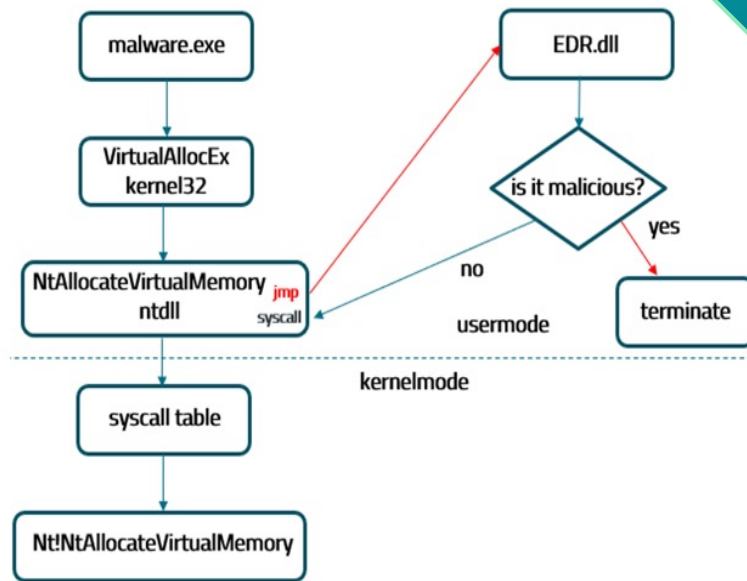
O QUE HA
GUARDADO
EMBAIXO
DO SEU
TAPETE



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



Unhooked API

notepad.exe - 1596 - Module: ntdll.dll - Thread: Main Thread 11500 - i64dbg

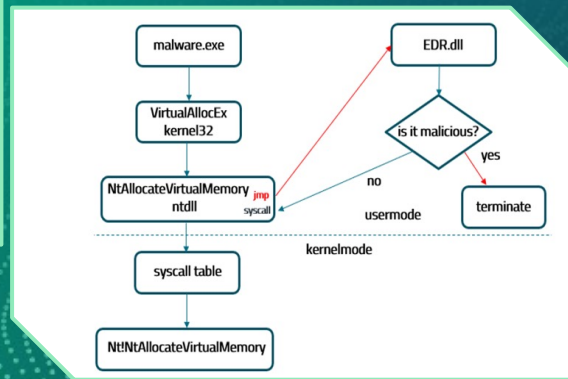
File View Debug Tracing Plugins Favourites Options Help Sep 2 2023 (TitanEngine)

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

Base	Module	Address	Type	Ordinal	Symbol
00007FFC3E4F0000	ntdll.dll	00007FFC3E58FB20	Export	430	NtOpenProcess
		00007FFC3E58FC60	Export	432	NtOpenProcessTokenEx
		00007FFC3E591A90	Export	431	NtOpenProcessToken

Diagram illustrating the unhooking process:

- 1. Target process (notepad.exe) is loaded.
- 2. Module (ntdll.dll) is identified.
- 3. Symbol (NtOpenProcess) is located.



Unhooked API

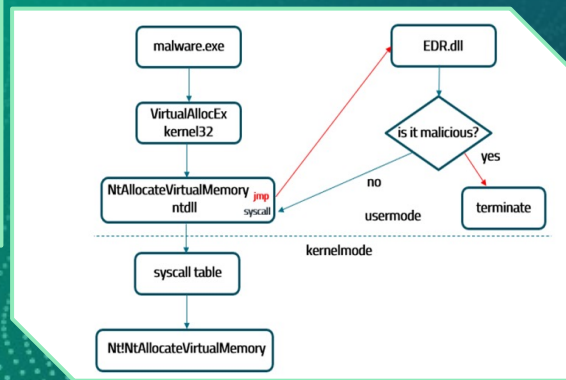
otepad.exe - PID: 1596 - Module: ntdll.dll - Thread: Main Thread 11500 - x64dbg

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

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols

<pre> :8BD1 mov r10,rcx 26000000 mov eax,26 0425 0803FE7F 01 test byte ptr ds:[7FFE0308],1 03 05 ine ntdll.7FFC3E58FB35 syscall ret 2E ine 2E ret ret 1F8400 00000000 nop dword ptr ds:[rax+rax],eax :8BD1 mov r10,rcx 27000000 mov eax,27 0425 0803FE7F 01 test byte ptr ds:[7FFE0308],1 03 05 ine ntdll.7FFC3E58FB55 syscall ret 2E ine 2E ret ret 1F8400 00000000 nop dword ptr ds:[rax+rax],eax :8BD1 mov r10,rcx 28000000 mov eax,28 0425 0803FE7F 01 test byte ptr ds:[7FFE0308],1 03 05 ine ntdll.7FFC3E58FB75 syscall ret 2E ine 2E ret ret 1F8400 00000000 nop dword ptr ds:[rax+rax],eax </pre>	<pre> ZwOpenProcess 26: '&' ZwSetInformationFile 27: '' ZwMapViewOfSection 28: '(' </pre>
---	---

ID Syscall (indicated by a red arrow pointing to the highlighted instruction)



Hooked API

Process Hacker [MSEDGEWIN10\IEUser]

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information notepad

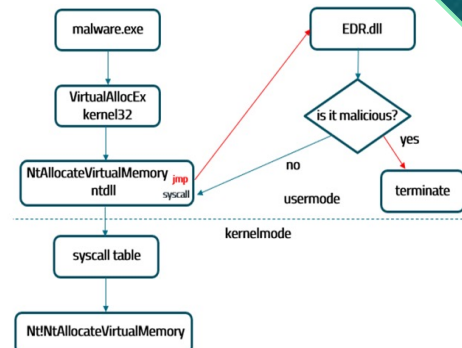
Processes Services Network Disk

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

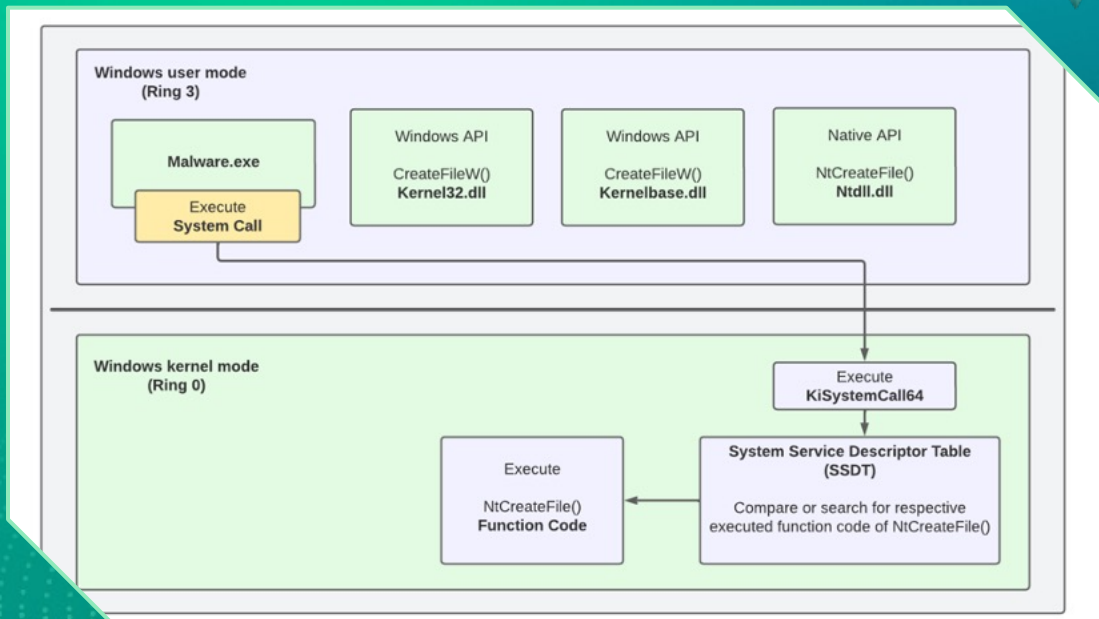
Name	Base address	Size	Description
notepad.exe	0x7ff610050000	268 kB	Notepad
advapi32.dll	0x7ffc3c900000	652 kB	Advanced Windows 32 Base API
atcuf64.dll	0x7ffb1d50000	1.35 MB	Bitdefender Active Threat Control Usermode Filter
bcrypt.dll	0x7ffc3a930000	152 kB	Windows Cryptographic Primitives Library
bcryptprimitives...	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	0x7ffc3bf00000	3.18 MB	Microsoft COM for Windows



E agora?



Direct System Call



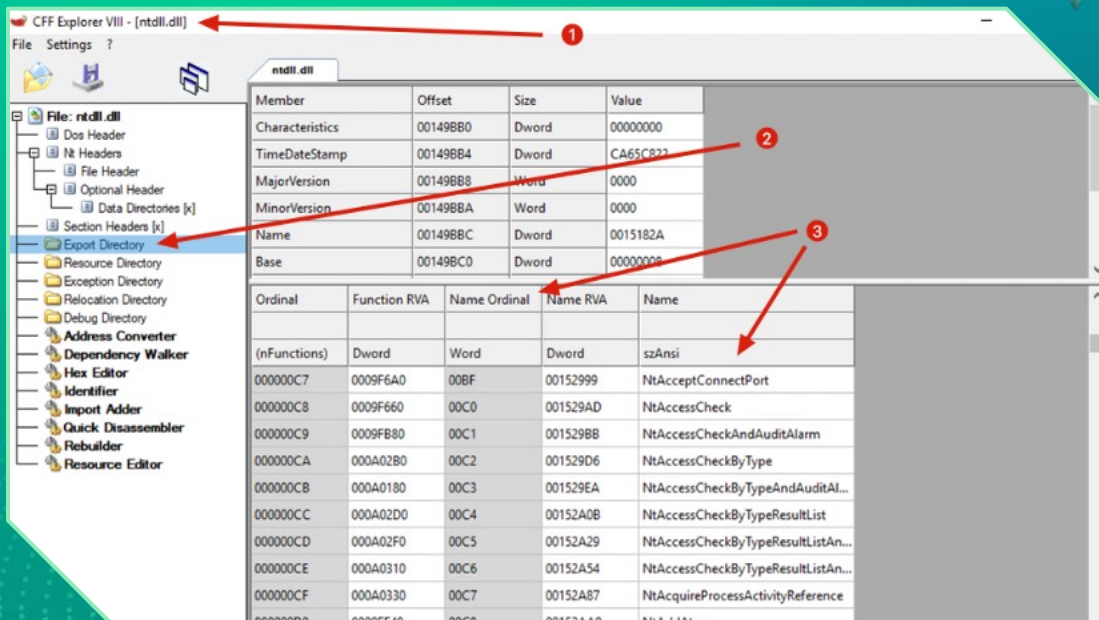
Direct System Call

- ✓ System Call depende de um **ID**entificador de cada função da Ntdll
- ✓ Este ID é randomizado pela Microsoft a cada Release/HotFix
- ✓ Mas o ID pode estar em algum lugar...

System call ID

Export Directory

- ✓ Tabela com a lista das APIs disponíveis, seus respectivos nomes e endereços



CFF Explorer VIII - [ntdll.dll]

File Settings ?

File: ntdll.dll

- File Header
- NT Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Export Directory**
- Resource Directory
- Exception Directory
- Relocation Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor

Member	Offset	Size	Value
Characteristics	00149BB0	Dword	00000000
TimeDateStamp	00149BB4	Dword	CA65C827
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	NtAccessCheckByTypeAndAuditAl...
000000CC	000A02D0	00C4	00152A0B	NtAccessCheckByTypeResultList
000000CD	000A02F0	00C5	00152A29	NtAccessCheckByTypeResultListAn...
000000CE	000A0310	00C6	00152A54	NtAccessCheckByTypeResultListAn...
000000CF	000A0330	00C7	00152A87	NtAcquireProcessActivityReference

System call ID

Exportação ordenada pelo nome

1596 - Module: ntdll.dll - Thread: Main Thread 11500 - x64dbg

Tracing Plugins Favourites Options Help Sep 2 2023 (TitanEngine)

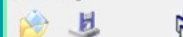
Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source

Module	Address	Type	Ordinal	Symbol
ntdll.dll	00007FFC3E58F660	Export	200	NtAccessCheck
	00007FFC3E58F680	Export	657	NtWorkerFactoryWorkerReady
	00007FFC3E58F6A0	Export	199	NtAcceptConnectPort
	00007FFC3E58F6C0	Export	404	NtMapUserPhysicalPagesScatter
	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	NtQueryValue
	00007FFC3E58F940	Export	511	NtQueryValueKey
	00007FFC3E58F960	Export	222	NtAllocateVirtualMemory

Ordenada pelo endereço

CFF Explorer VIII - [ntdll.dll]

File Settings ?



File: ntdll.dll

Dos Header

NT Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Export Directory

Resource Directory

Exception Directory

Relocation Directory

Debug Directory

Address Converter

Dependency Walker

Hex Editor

Identifier

Import Adder

Quick Disassembler

Rebuilder

Resource Editor

ntdll.dll

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	0015298B	NtAccessCheckAndAuditAlarm
000000CA	000A02B0	00C2	001529D6	NtAccessCheckByType
000000CB	000A0180	00C3	001529EA	NtAccessCheckByTypeAndAuditAl...
000000CC	000A02D0	00C4	00152A08	NtAccessCheckByTypeResultList
000000CD	000A02F0	00C5	00152A29	NtAccessCheckByTypeResultListAn...
000000CE	000A0310	00C6	00152A34	NtAccessCheckByTypeResultListAn...
000000CF	000A0330	00C7	00152A87	NtAcquireProcessActivityReference

System call ID

Export Directory

✓ Ordem em memória = ordem dos IDs

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 Call Stack SEH Script Symbols <> Source References Thre

Address	Disassembly	Comment
00007FFC3E58F660	mov r10,rcx	
00007FFC3E58F663	mov eax,0	
00007FFC3E58F668	test byte ptr ds:[7FFE0308],1	ZwAccessCheck
00007FFC3E58F670	jne ntdll.7FFC3E58F675	
00007FFC3E58F672	syscall	
00007FFC3E58F674	ret	
00007FFC3E58F675	ret 2E	
00007FFC3E58F677	ret	
00007FFC3E58F678	ret	
00007FFC3E58F680	mov r10,rcx	
00007FFC3E58F683	mov eax,1	NtworkerFactoryWorkerReady
00007FFC3E58F688	test byte ptr ds:[7FFE0308],1	
00007FFC3E58F690	jne ntdll.7FFC3E58F695	
00007FFC3E58F692	syscall	
00007FFC3E58F694	ret	
00007FFC3E58F695	ret 2E	
00007FFC3E58F697	ret	
00007FFC3E58F698	ret	
00007FFC3E58F6A0	mov r10,rcx	
00007FFC3E58F6A3	mov eax,2	ZwAcceptConnectPort
00007FFC3E58F6A8	test byte ptr ds:[7FFE0308],1	
00007FFC3E58F6B0	jne ntdll.7FFC3E58F6B5	
00007FFC3E58F6B2	syscall	
00007FFC3E58F6B4	ret	
00007FFC3E58F6B5	ret 2E	
00007FFC3E58F6B7	ret	
00007FFC3E58F6B8	ret	
00007FFC3E58F6C0	mov r10,rcx	
00007FFC3E58F6C3	mov eax,3	NtMapuserPhysicalPagesScatter
00007FFC3E58F6C8	test byte ptr ds:[7FFE0308],1	
00007FFC3E58F6D0	jne ntdll.7FFC3E58F6D5	
00007FFC3E58F6D2	syscall	
00007FFC3E58F6D4	ret	
00007FFC3E58F6D5	ret 2E	
00007FFC3E58F6D7	ret	
00007FFC3E58F6D8	ret	
00007FFC3E58F6E0	mov r10,rcx	
00007FFC3E58F6E3	mov eax,4	NtwaitForSingleobject

System call ID

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

Address	Disassembly	Comment
00007FFEDE5AFB00	4C:8BD1	mov r10,rcx
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 7FFEDE7004F8
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
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
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

Unhooked

Hooked ID 26

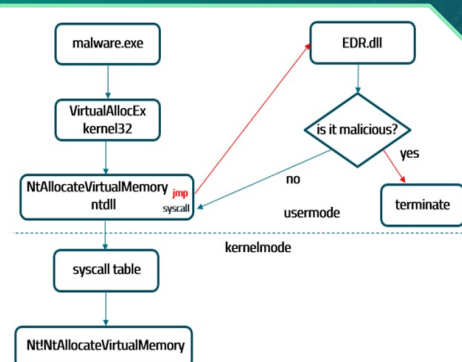
Unhooked

ZwQueryInformationThread

ZwOpenProcess

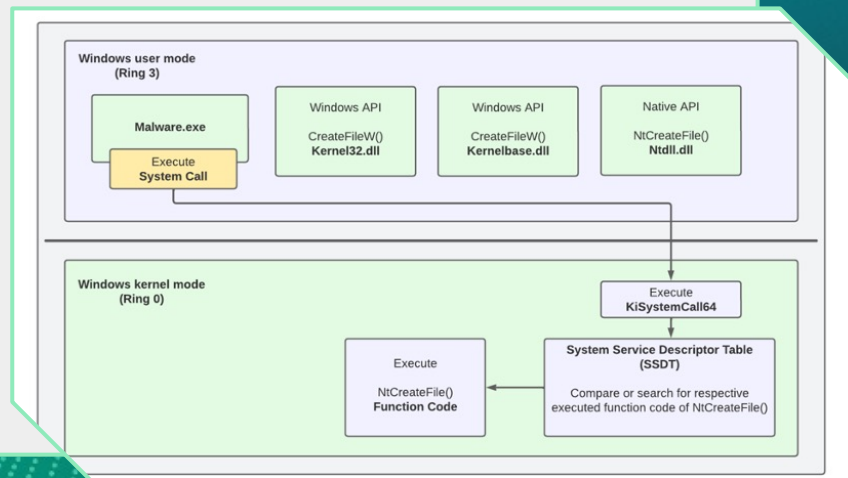
ZwSetInformationFile

ZwMapViewOfSection



Direct System Call

- ✓ System Call depende de um **ID**entificador de cada função da Ntdll
- ✓ Este ID é randomizado pela Microsoft a cada Release/HotFix
- ✓ Ficou mais fácil:
 - ✓ Lista as funções da Ntdll
 - ✓ Ordena pelo endereço da API
 - ✓ Obtém o ID de system call desejado
 - ✓ Realiza a chamada da função



Espera aí!

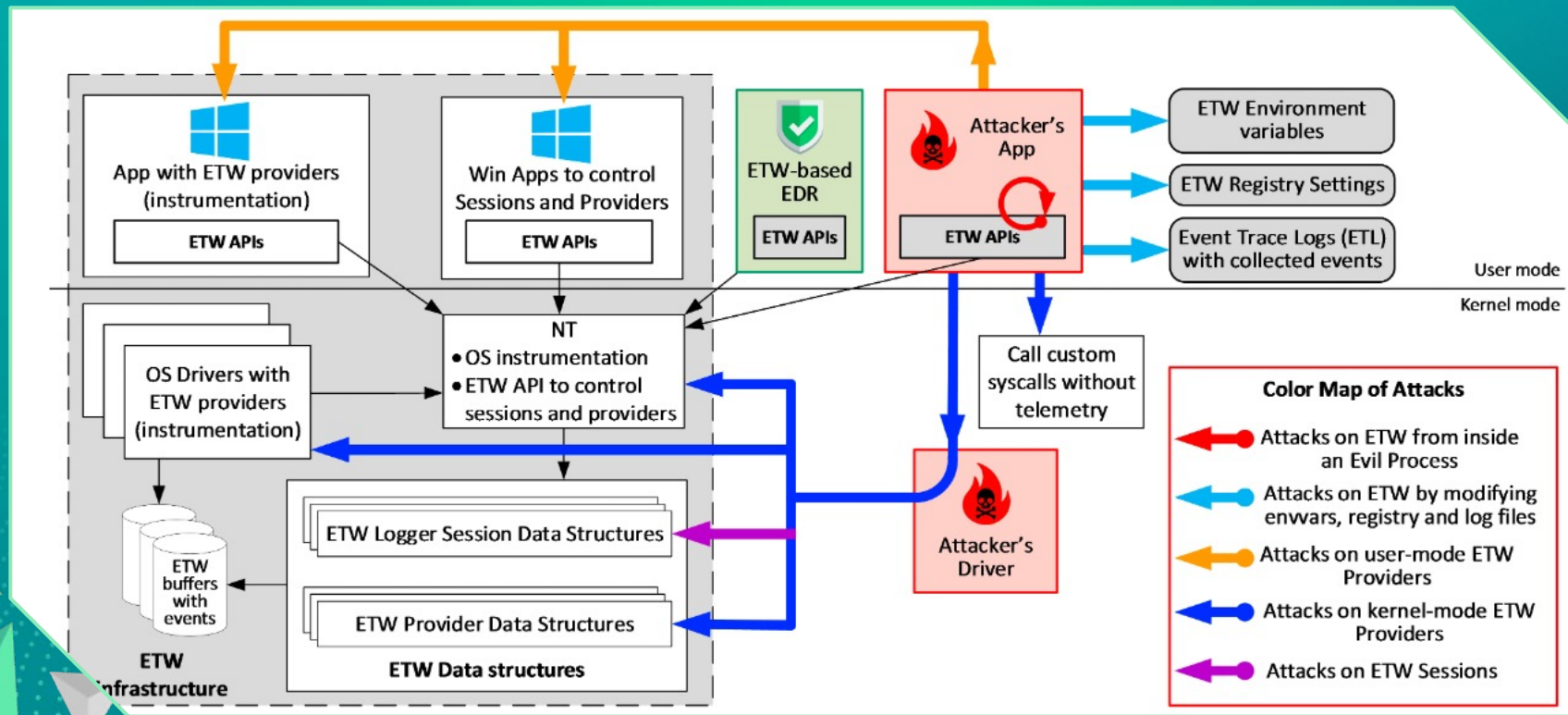


Sim e não!

- ✓ Sim, com essa técnica é possível contornar diversos fabricantes de AV/EDR
- ✓ Porém nem todos!
- ✓ Calma ae, estamos só começando...

ETW

Event Tracing for Windows



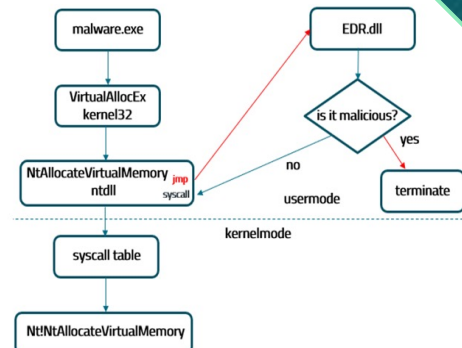
Indirect Syscall

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

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

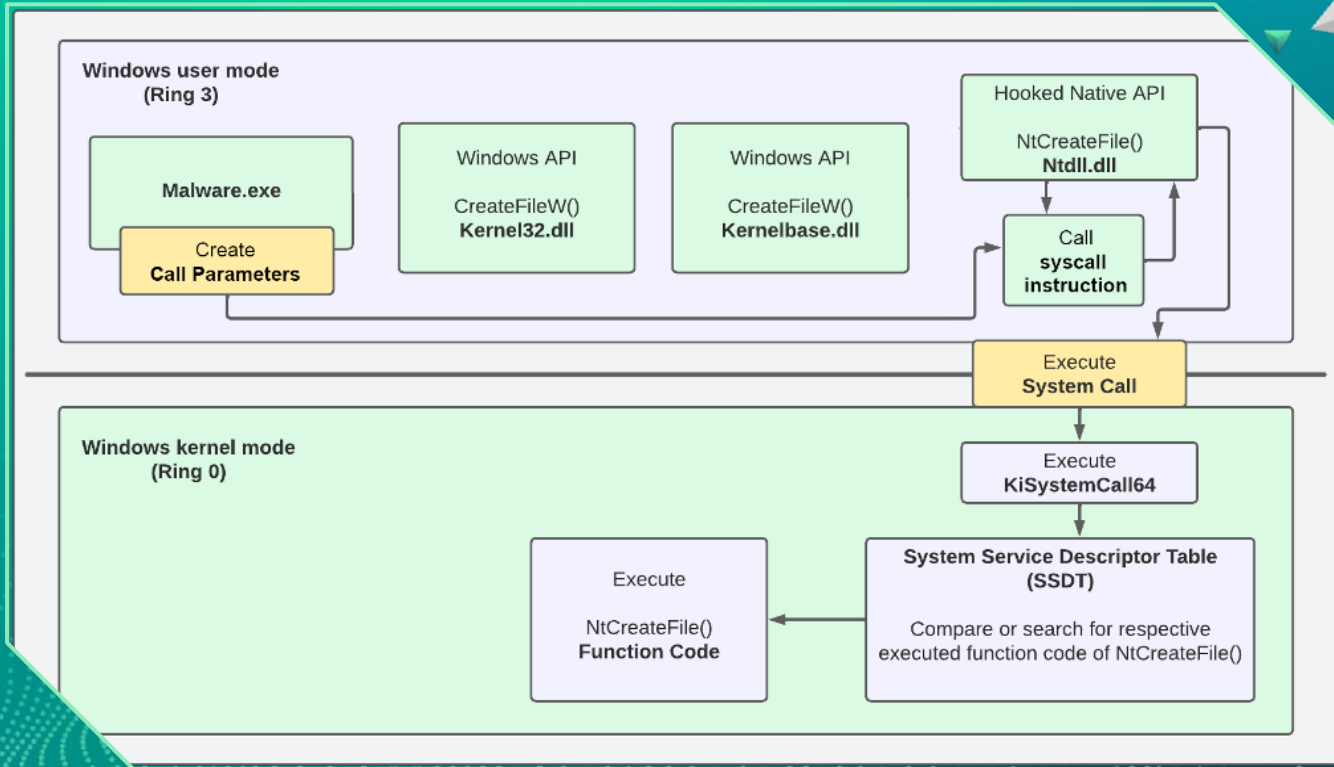
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols <> Source References Thre...

00007FFEDE5AFB00	4C:8BD1	mov r10,rcx	ZwQueryInformationThread
00007FFEDE5AFB03	B8 25000000	mov eax,25	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 7FFEDE7004F8	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	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 Syscall

- ✓ Monta os parâmetros de chamada
- ✓ Não chama a instrução Syscall diretamente
- ✓ Realiza um JMP para um endereço onde há a instrução Syscall



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



✓ Nada apresentado é novo, ou seja, não sou o autor

- ✓ PPT e referências estão em meu GitHub
- ✓ <https://github.com/helviojunior/Presentations>



✓ 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-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



Helvio Junior

Helvio.junior@sec4us.com.br

(41) 9.9855.9300

in /helviojunior

