Unveiling the underground world of ANTI-CHEATS

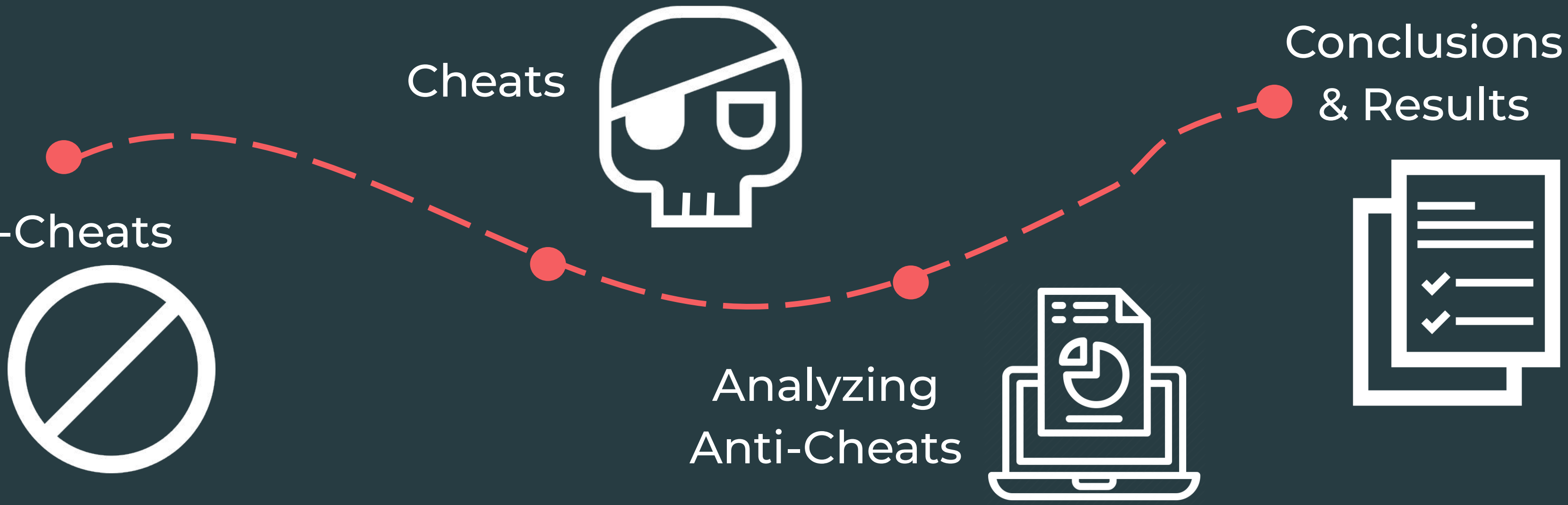
Joel Noguera

Security Consultant at Immunity Inc

@niemand_sec - niemand.com.ar

REcon
MONTREAL
2019

What are we going to talk about?



Anti-Cheats

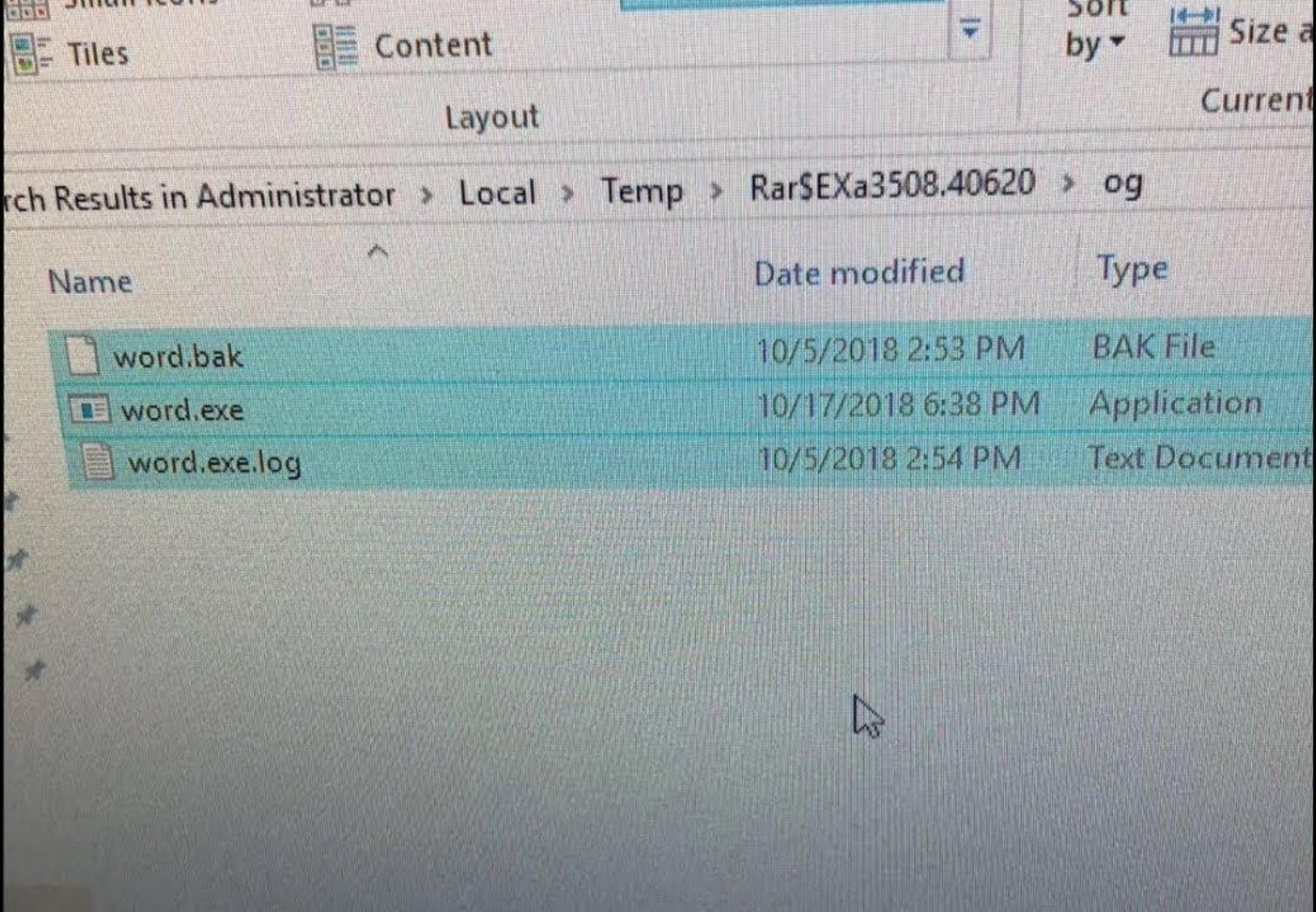
Cheats

Analyzing Anti-Cheats

Conclusions & Results

FIRST RULE OF THE GAMING CLUB, YOU DON'T CHEAT

~~(or get caught doing it)~~



rch Results in Administrator › Local › Temp › Rar$EXa3508.40620 › og

Name	Date modified	Type
word.bak	10/5/2018 2:53 PM	BAK File
word.exe	10/17/2018 6:38 PM	Application
word.exe.log	10/5/2018 2:54 PM	Text Document

Anti *Cheats*

Anti-Cheats

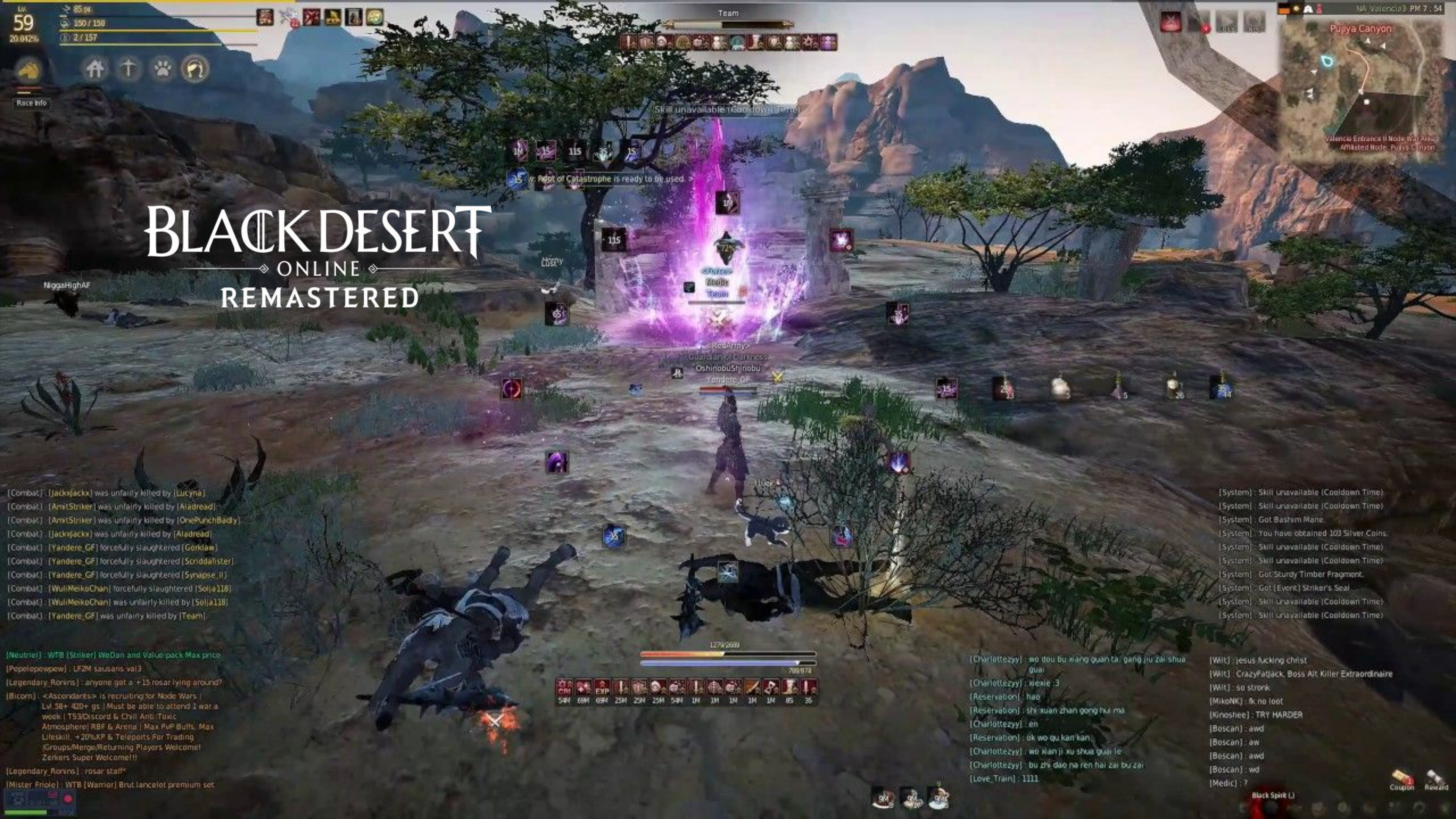
LIVEGUARD
ANTI-CHEAT SYSTEM
sXe I
nProtect GameGuard
SPARTAN ANTICHEAT
FACEIT
AC
ANTI-CHEAT
PUNKBUSTER
ONLINE COUNTERMEASURES
CAL ANTI-CHEAT SYSTEM
AUTOEYE
Hackshield
VAC
S

Let’s see some numbers...

336.500.000

Monthly Active Users

EAC	XC3	BE	VAC
275.000.000	500.000	30.000.000	31.000.000



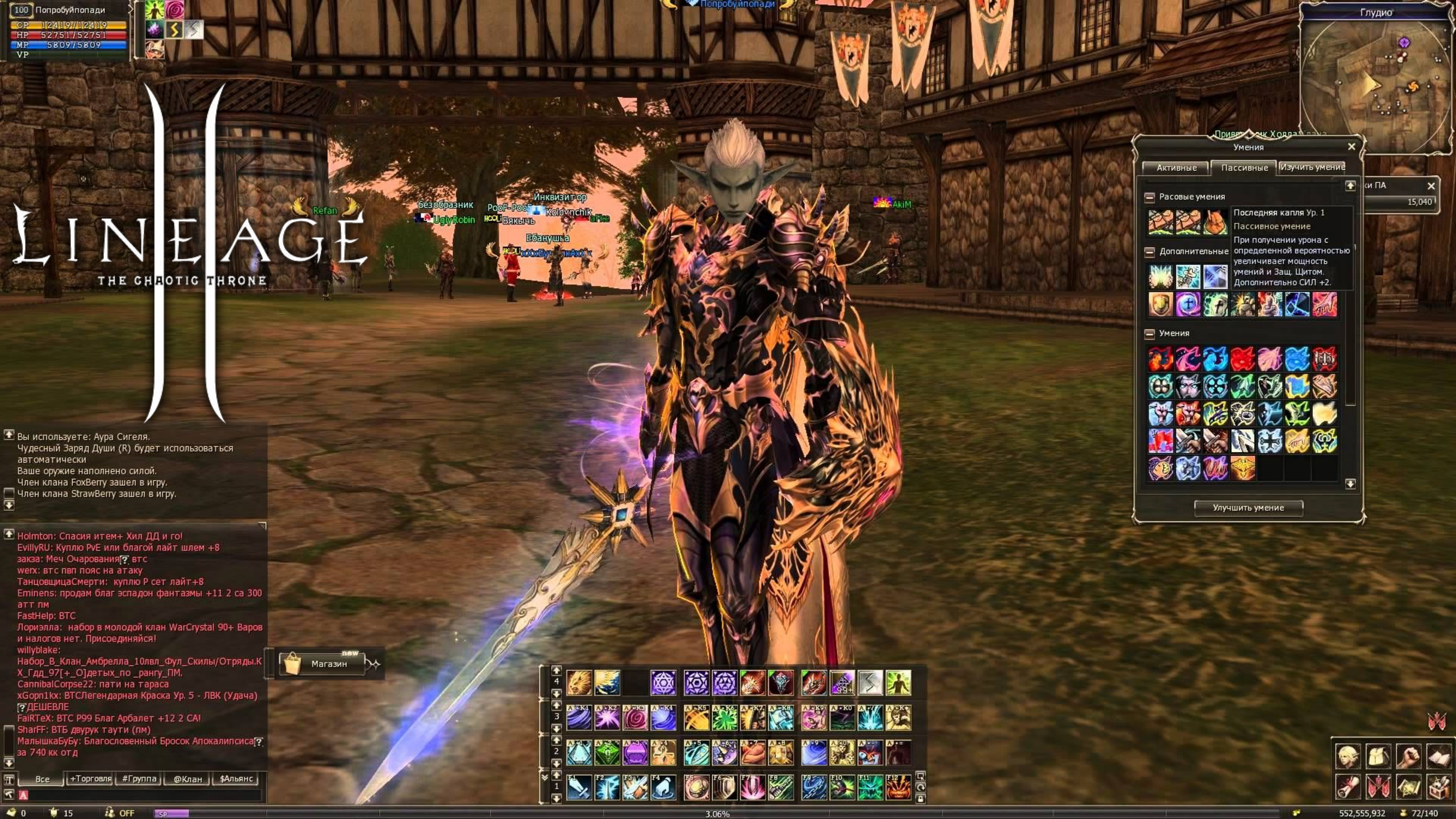
```
[Combat] : [Jackxjackx] was unfairly killed by [Lucyna].
[Combat] : [AmitStriker] was unfairly killed by [Aladread].
[Combat] : [AmitStriker] was unfairly killed by [OnePunchBadly].
[Combat] : [Jackxjackx] was unfairly killed by [Aladread].
[Combat] : [Yandere_GF] forcefully slaughtered [Gorklaw].
[Combat] : [Yandere_GF] forcefully slaughtered [Scriddafister].
[Combat] : [Yandere_GF] forcefully slaughtered [Synapse_II].
[Combat] : [WuliMeikoChan] forcefully slaughtered [Solja118].
[Combat] : [WuliMeikoChan] was unfairly killed by [Solja118].
[Combat] : [Yandere_GF] was unfairly killed by [Team].
```

```
[Neutriel] : WTB [Striker] WeDan and Value pack Max price
[Pepelepewpew] : LF2M sausans val3
[Legendary_Ronins] : anyone got a +15 rosar lying around?
[Bicorn] : <Ascendants> is recruiting for Node Wars |
           Lvl 58+ 420+ gs | Must be able to attend 1 war a
           week | TS3/Discord & Chill Anti-Toxic
           Atmosphere| RBF & Arena | Max PvP Buffs, Max
           Lifeskill, +20%XP & Teleports For Trading
           |Groups/Merge/Returning Players Welcome!
           Zerkers Super Welcome!!!
[Legendary_Ronins] : rosar staff*
[Mister Friole] : WTB [Warrior] Brut lancelot premium set
```

```
[System] : Skill unavailable (Cooldown Time)
[System] : Skill unavailable (Cooldown Time)
[System] : Got Bashim Mane.
[System] : You have obtained 103 Silver Coins.
[System] : Skill unavailable (Cooldown Time)
[System] : Skill unavailable (Cooldown Time)
[System] : Got Sturdy Timber Fragment.
[System] : Got [Event] Striker's Seal
[System] : Skill unavailable (Cooldown Time)
[System] : Skill unavailable (Cooldown Time)
```

```
[Charlottezyy] : wo dou bu xiang guan ta, gang jiu zai shua
                 guai
[Charlottezyy] : xiexie :3
[Reservation] : hao
[Reservation] : shi xuan zhan gong hui ma
[Charlottezyy] : en
[Reservation] : ok wo qu kan kan
[Charlottezyy] : wo xian ji xu shua guai le
[Charlottezyy] : bu zhi dao na ren hai zai bu zai
[Love_Train] : 1111
```

```
[Wilt] : jesus fucking christ
[Wilt] : CrazyFatJack, Boss Alt Killer Extraordinaire
[Wilt] : so stronk
[MikoNK] : fk no loot
[Kinoshee] : TRY HARDER
[Boscan] : awd
[Boscan] : aw
[Boscan] : awd
[Boscan] : wd
[Medic] : ?
```



Последняя капля Ур. 1

Пассивное умение

При получении урона с определенной вероятностью увеличивает мощность умений и Защ. Щитом. Дополнительно СИЛ +2.

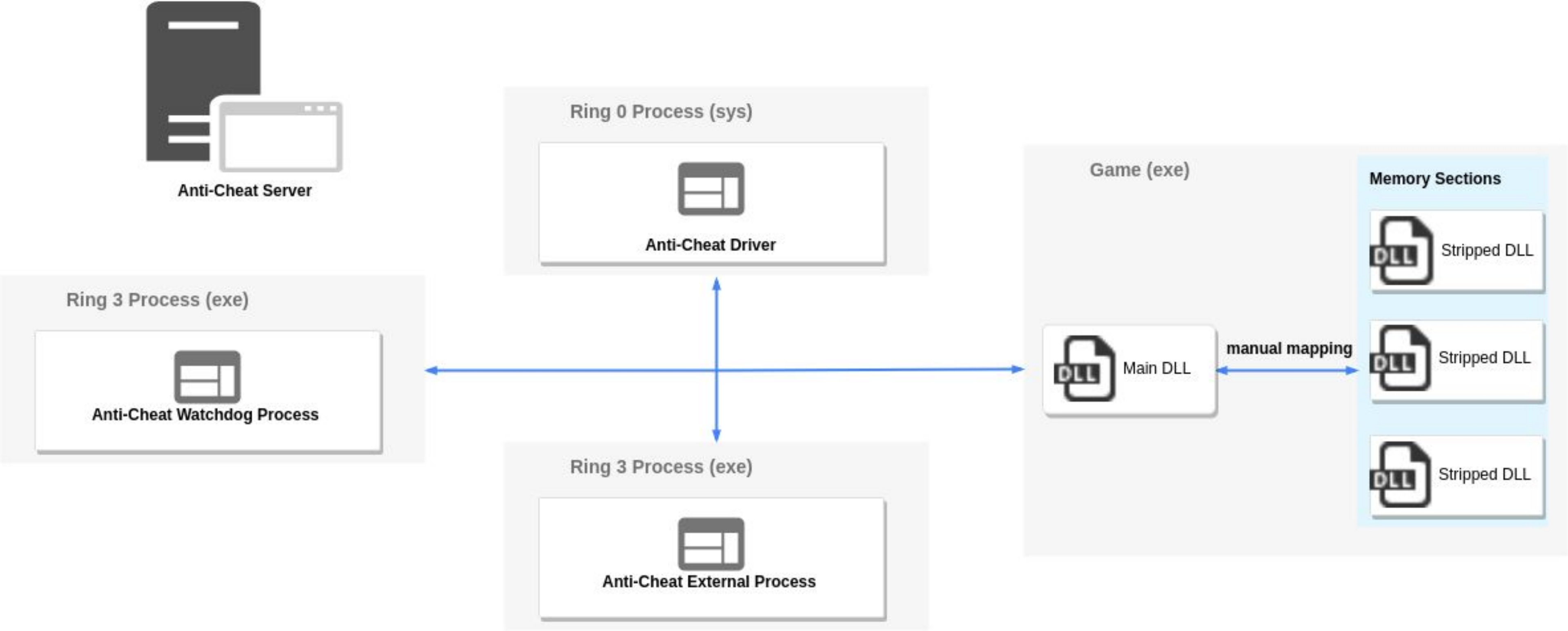
Вы используете: Аура Сигеля.
Чудесный Заряд Души (R) будет использоваться автоматически
Ваше оружие наполнено силой.
Член клана FoxBerry зашел в игру.
Член клана StrawBerry зашел в игру.

Holmton: Спасия итем+ Хил ДД и го!
EvillyRU: Куплю PvE или благой лайт шлем +8
заказа: Меч Очарования[?] втс
werx: втс пвп пояс на атаку
ТанцовщицаСмерти: куплю Р сет лайт+8
Eminens: продам благ эспадон фантазмы +11 2 са 300 атт пм
FastHelp: ВТС
Лориэлла: набор в молодой клан WarCrystal 90+ Варов и налогов нет. Присоединяйся!
willyblake: Набор_В_Клан_Амбрелла_10лвл_Фул_Скилы/Отряды.КХ_Гдд_97[+_О]детых_по _рангу_ПМ.
CannibalCorpse22: пати на тараса
xGopn1kx: ВТСЛегендарная Краска Ур. 5 - ЛВК (Удача)[?]ДЕШЕВЛЕ
FaiRTeX: ВТС Р99 Благ Арбалет +12 2 СА!
SharFF: ВТБ двурук таути (пм)
МалышкаБуБу: Благословенный Бросок Апокалипсиса[?] за 740 кк отд

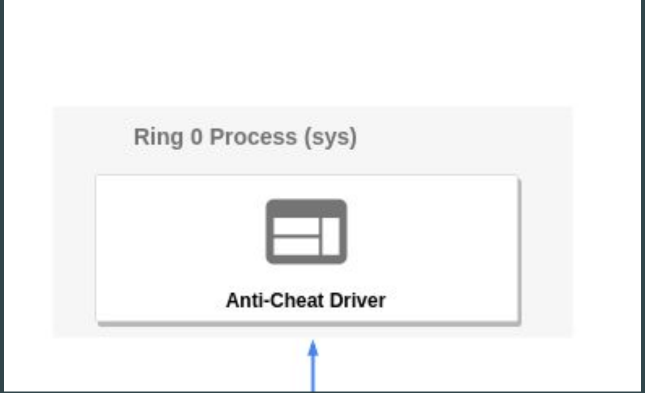
APEX
LEGENDS
Respawn
ENTERTAINMENT
EA

PLAYERUNKNOWN'S
BATTLEGROUNDS

Anti-Cheat Components



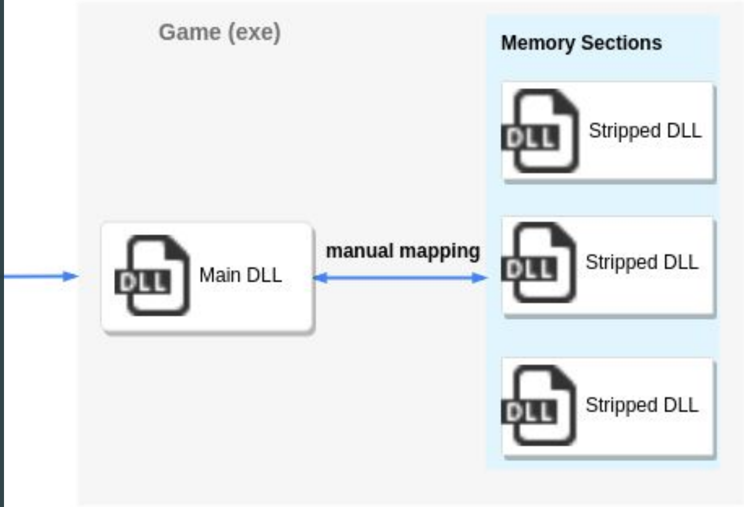
Kernel Driver



- Handle stripping/Access Control
- Register kernel callbacks
- Rejection of Kernel/User mode debugging
- Analysis of privileged process (lsass and csrss)
- Block blacklisted/unsigned drivers
- Monitoring of kernel function calls

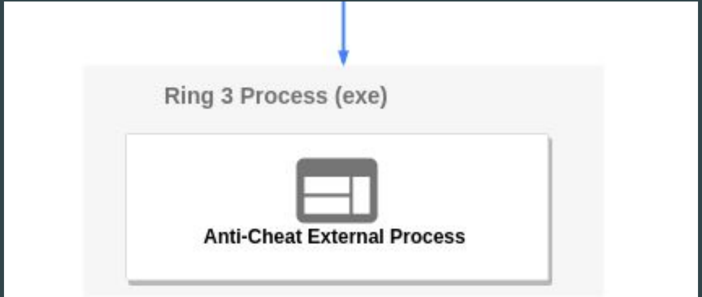
DLL inside Games

- Control of access flags to different sections
- Identification of hooks
- Thread Hijacking
- DLL Injection
- Function signatures
- VEH/SEH modification
- Game resources modification
- Detection of virtual environment



External Ring 3 Process

- Process/File Controls
- Blacklisted programs detection
- Manage logic from Driver
- Control of game client and DLL hashes
- Multi-client detection
- Program integrity controls



Cheats

LOL
UNITED AIRLINES
WRONG CHEAT CODE
memecenter.com
MemeCenter

Internal (DLL) vs External (Process)

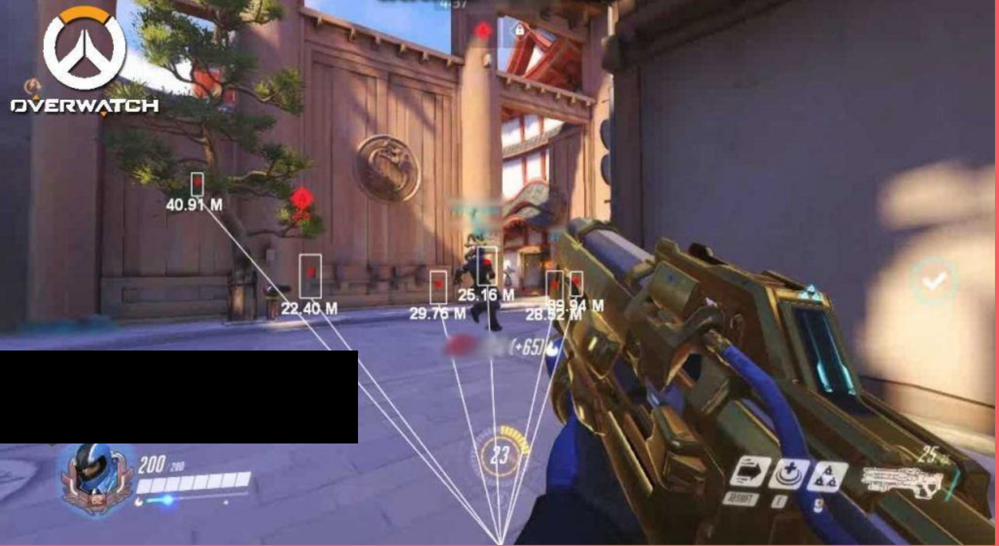
	Pros	Cons
External	[•] Quick for small patches [•] Easy to master [•] Can be closed in certain cases	[•] Slow [•] Easy to detect [•] Limited potential [•] Requires a Handle
Internal	[•] Great performance [•] Direct access to memory [•] Hard to detect if you are good enough	[•] Hard to master [•] Easier to detect if you mess it up

ELIMINATED BY
RESPAWN IN
3
ATTACK
KILL CAM
PRESS H TO CHANGE HERO

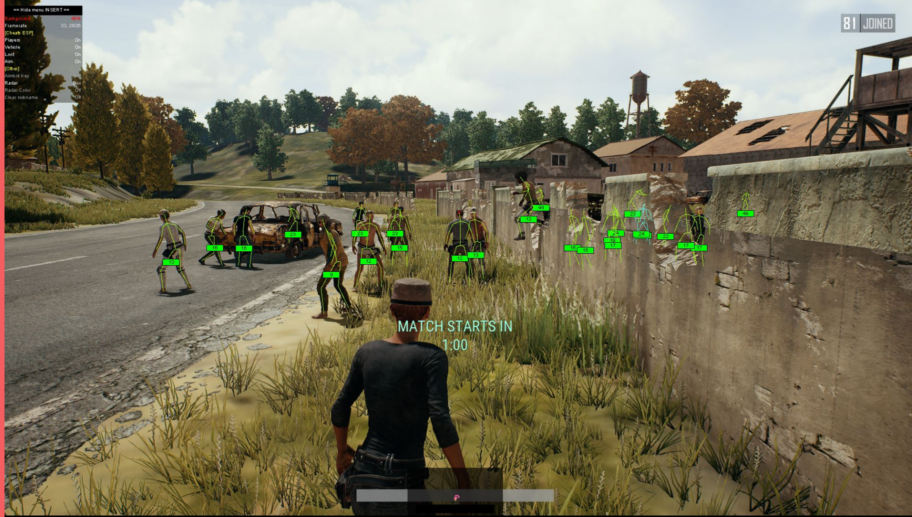
ORB OF HARMONY GAINED FROM AREOMIX
35%

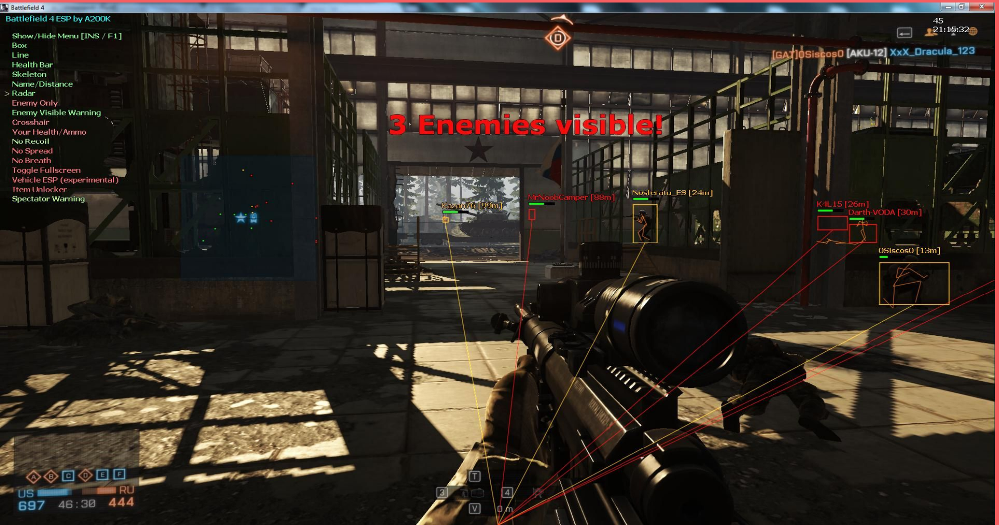
$34463
100
92
30

Aimbots



[redacted]

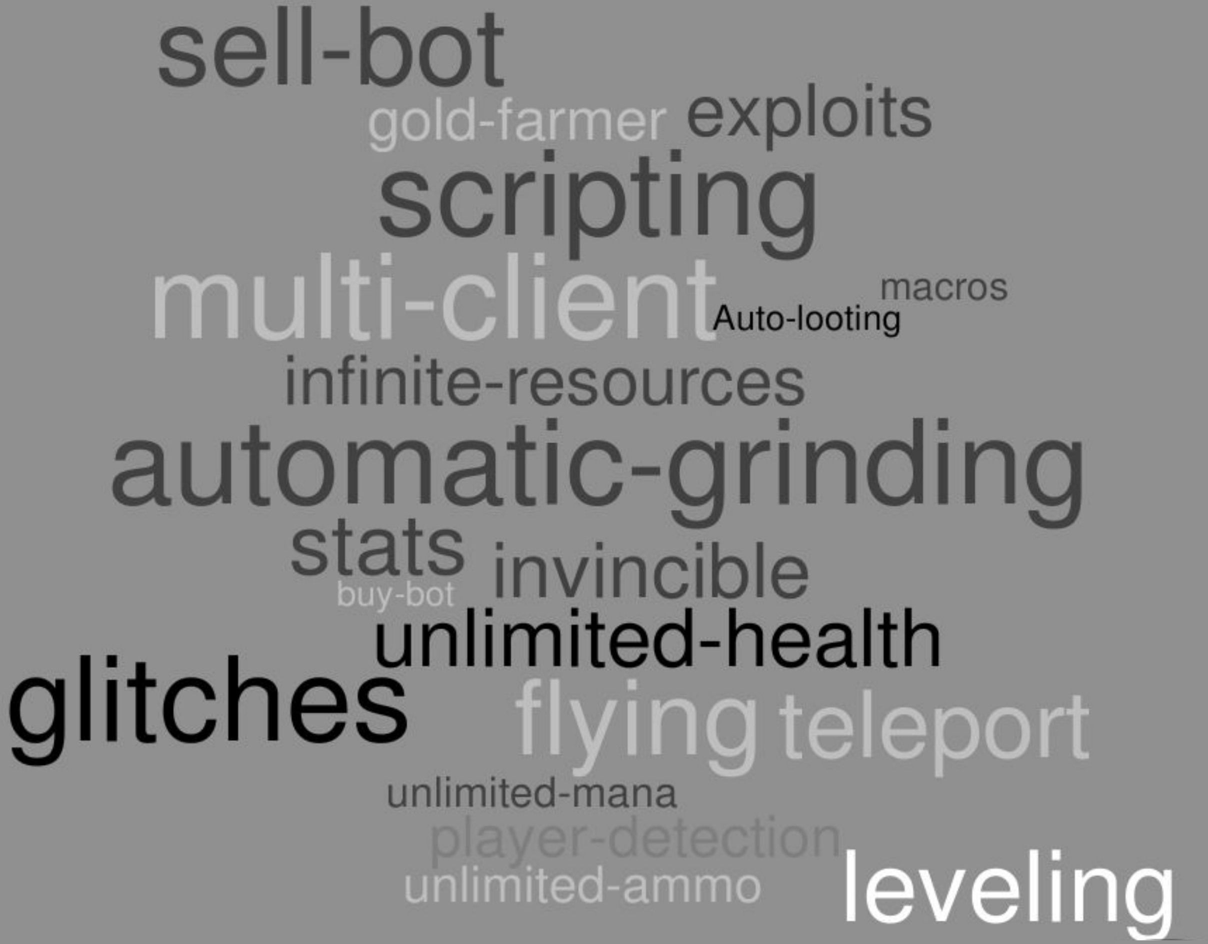




Wallhack/ESP

Pro players getting caught? Why not

Automatization
Utility



Motivation!

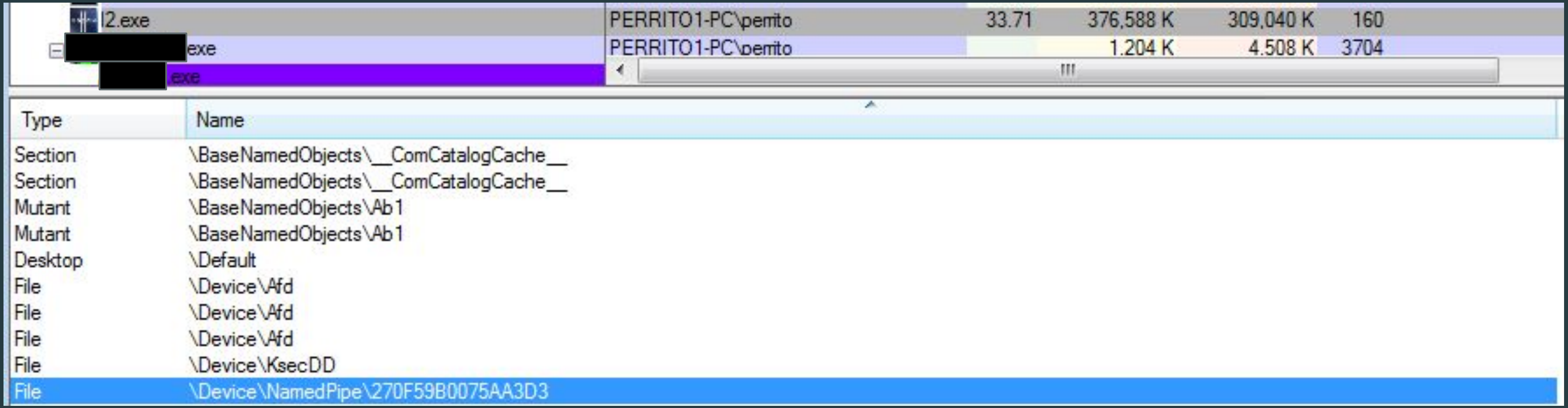
Let me tell you a story...

We decided to reverse a cheat for Lineage 2

Characteristics: Made in Russia, good bypasses for AC, Lineage 2

Extra Gold Coins for:

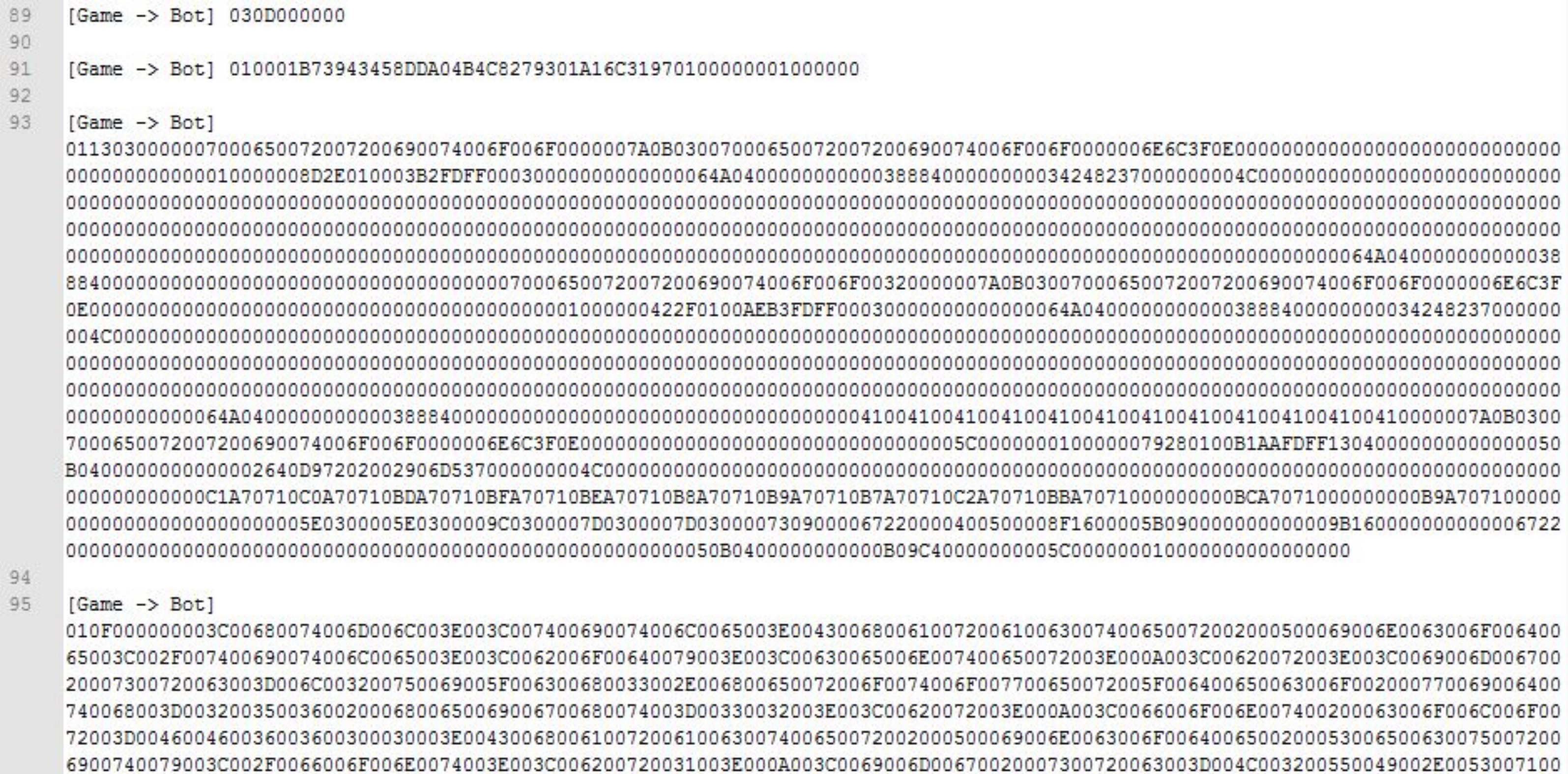
- Emiliano Del Peon (@Dolphin01684386)
- Lautaro Fain (@LautaroFain)



```
l2.exe                 PERRITO1-PC\perrito     33.71   376,588 K   309,040 K    160
[redacted]exe          PERRITO1-PC\perrito              1,204 K     4,508 K   3704
[redacted]exe
```

Type	Name
Section	\BaseNamedObjects__ComCatalogCache__
Section	\BaseNamedObjects__ComCatalogCache__
Mutant	\BaseNamedObjects\Ab1
Mutant	\BaseNamedObjects\Ab1
Desktop	\Default
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\KsecDD
File	\Device\NamedPipe\270F59B0075AA3D3

Let me tell you a story

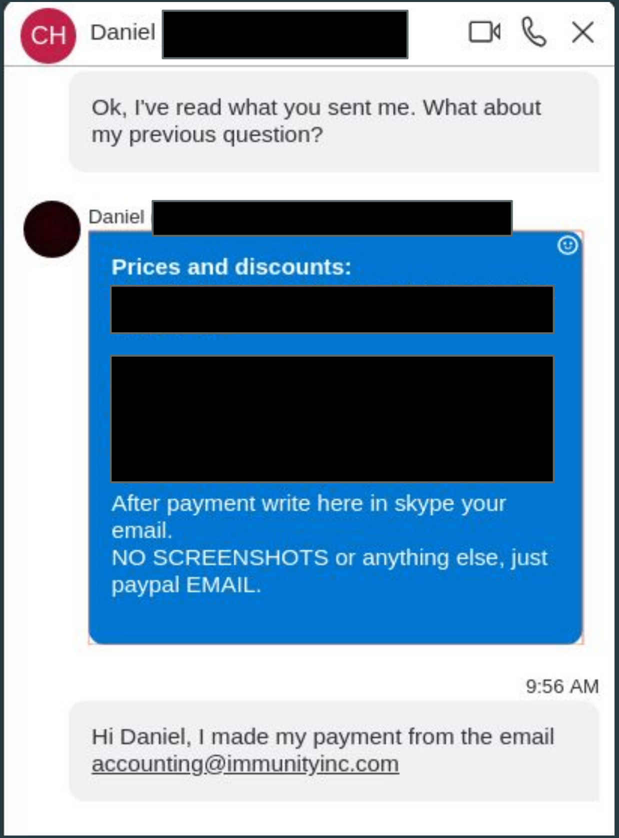


```
[Game -> Bot] 030D000000

[Game -> Bot] 010001B73943458DDA04B4C8279301A16C31970100000001000000

[Game -> Bot]
0113030000007000650072007200690074006F006F0000007A0B03007000650072007200690074006F006F0000006E6C3F0E0000000000000000000000000000
000000000000010000008D2E010003B2FDFF00030000000000000064A04000000000003888400000000034248237000000004C00000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000064A040000000000038
884000000000000000000000000000000000000070006500720072006900740 06F006F00320000007A0B03007000650072007200690074006F006F0000006E6C3F
0E0000000000000000000000000000000000000000010000000422F0100AEB3FDFF000300000000000000064A0400000000000388840000000003424823700000000
004C0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000064A040000000000038884000000000000000000000000000000000000004100410041004100410041004100410041004100410000007A0B0300
7000650072007200690074006F006F0000006E6C3F0E000000000000000000000000000000005C0000000100000079280100B1AAFDFF13040000000000000050
B04000000000002640D97202002906D53700000000004C0000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000C1A70710C0A70710BDA70710BFA70710BEA70710B8A70710B9A70710B7A70710C2A70710BBA7071000000000BCA7071000000000B9A707100000
000000000000000000005E0300005E0300009C0300007D0300007D030000730900006722000040050000 8F1600005B090000000000009B160000000000006722
0000000000000000000000000000000000000000000000000000000050B04000000000000B09C4000000000005C000000010000000000000000000

[Game -> Bot]
010F000000003C00680074006D006C003E003C007400690074006C0065003E004300680061007200610063007400650072002000500069006E0063006F006400
65003C002F007400690074006C0065003E003C0062006F00640079003E003C00630065006E007400650072003E000A003C00620072003E003C0069006D006700
20007300720063003D006C0032007500690005F00630068003300 2E0068006500720 06F0074006F0077006500720 05F00640065006300 6F002000770069006400
740068003D003200350036002000680065006900670068007400 3D00330032003E003C00620072003E000A003C0066006F006E007400200063006F006C006F00
72003D0046004600360036003000300 03E004300680061007200610063007400650072002000500069006E0063006F00640065002000530065006300750072 00
6900740079003C002F0066006F006E0074003E003C00620072003100 3E000A003C0069006D00670020007300720063003D004C003200550049002E0053007100
```

Let me tell you a story

Old version is detected by ACs

The new version moved to a stealthier approach: **FileMapping**



CH Daniel [redacted]

Ok, I've read what you sent me. What about my previous question?

Daniel [redacted]

Prices and discounts:

[redacted]

[redacted]

After payment write here in skype your email.
NO SCREENSHOTS or anything else, just paypal EMAIL.

9:56 AM

Hi Daniel, I made my payment from the email accounting@immunityinc.com

Parallel Market

Parallel Market

Cheat Prices:
U$S 1 to U$S25
Some up to U$S500

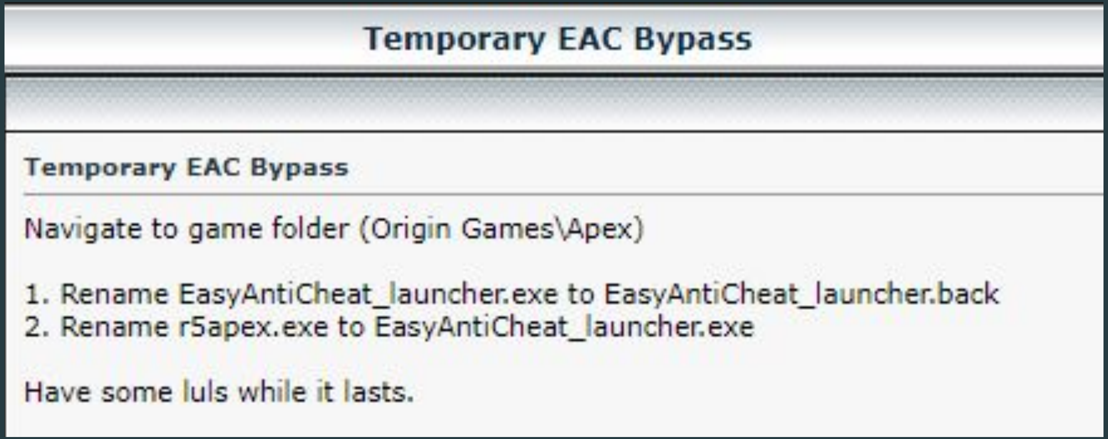
Ex: 2500 paid members
U$S 10 * 2500 = U$S25000
(150000 memberships)

U$S 1,25 M
PER YEAR
(Wait... what?)

Are they fighting back?

Apex claims:

- More than 770k players banned
- Over 300K account creations blocked
- Over than 4k cheat sellers accounts (spammers) banned in 20 days



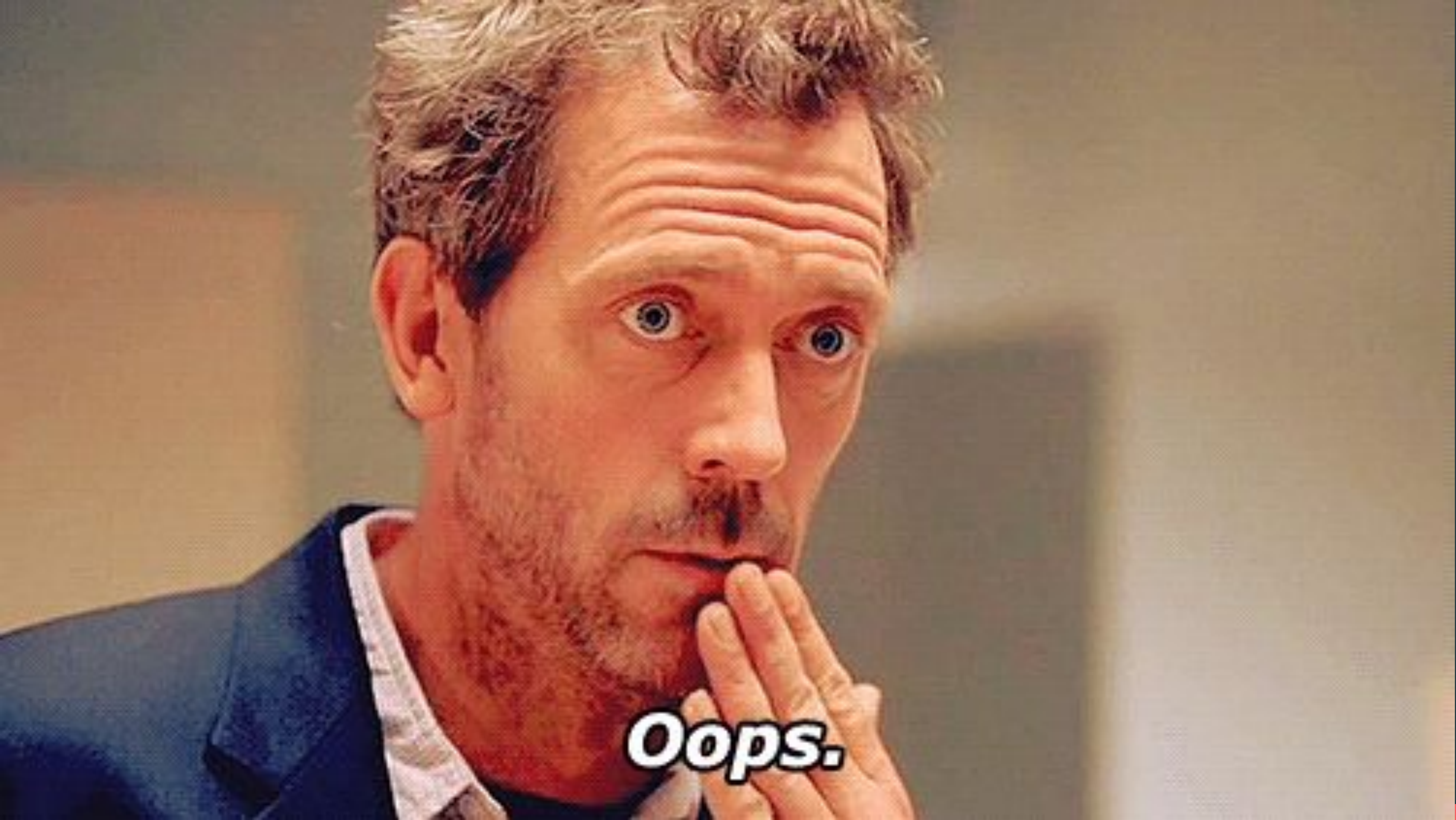
Temporary EAC Bypass

Temporary EAC Bypass

Navigate to game folder (Origin Games\Apex)

1. Rename EasyAntiCheat_launcher.exe to EasyAntiCheat_launcher.back
2. Rename r5apex.exe to EasyAntiCheat_launcher.exe

Have some luls while it lasts.


Oops.

Analyzing Anti-Cheats

Methodology

Goal:

- Read/Write/Alloc Memory (Internal & External)
- Run Code inside Game’s Process
- Be as **stealthy** as possible

Hijacking Techniques

AC usually control/block/reject new HANDLEs to the game process:

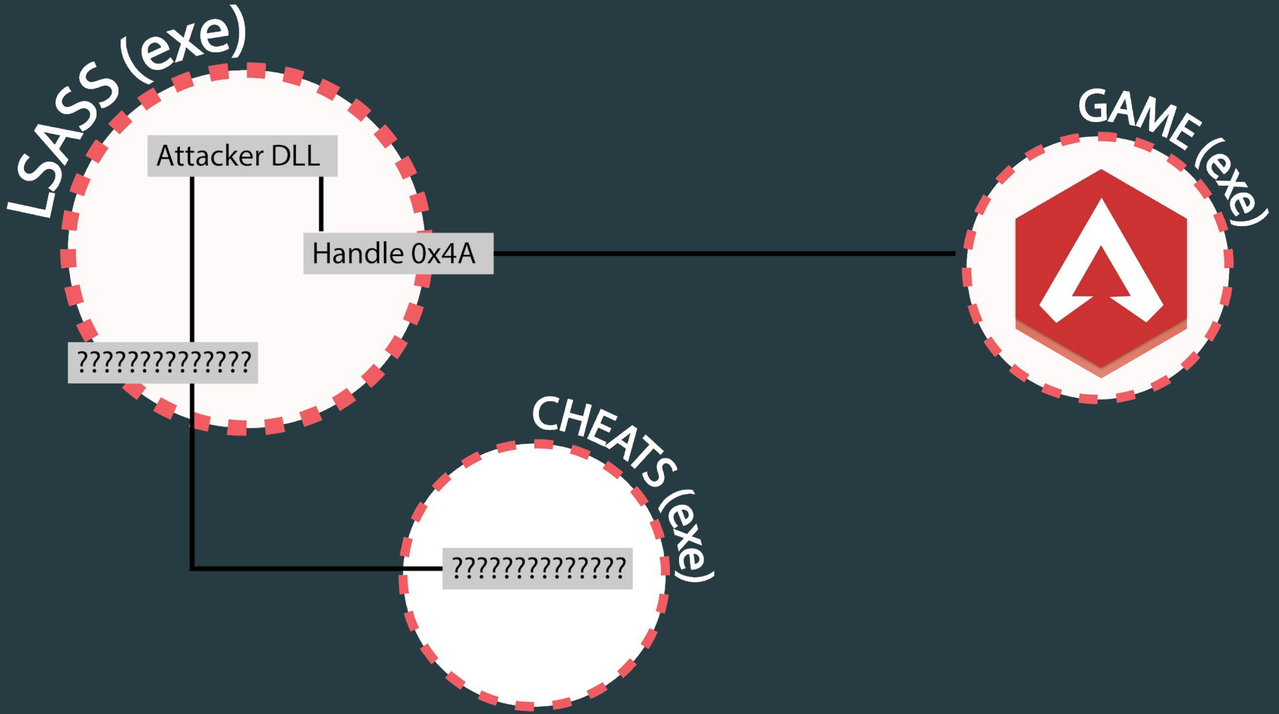
- Driver that protects game and AC processes

Some process need to be whitelisted: **lsass**, **csrss**, **AC**

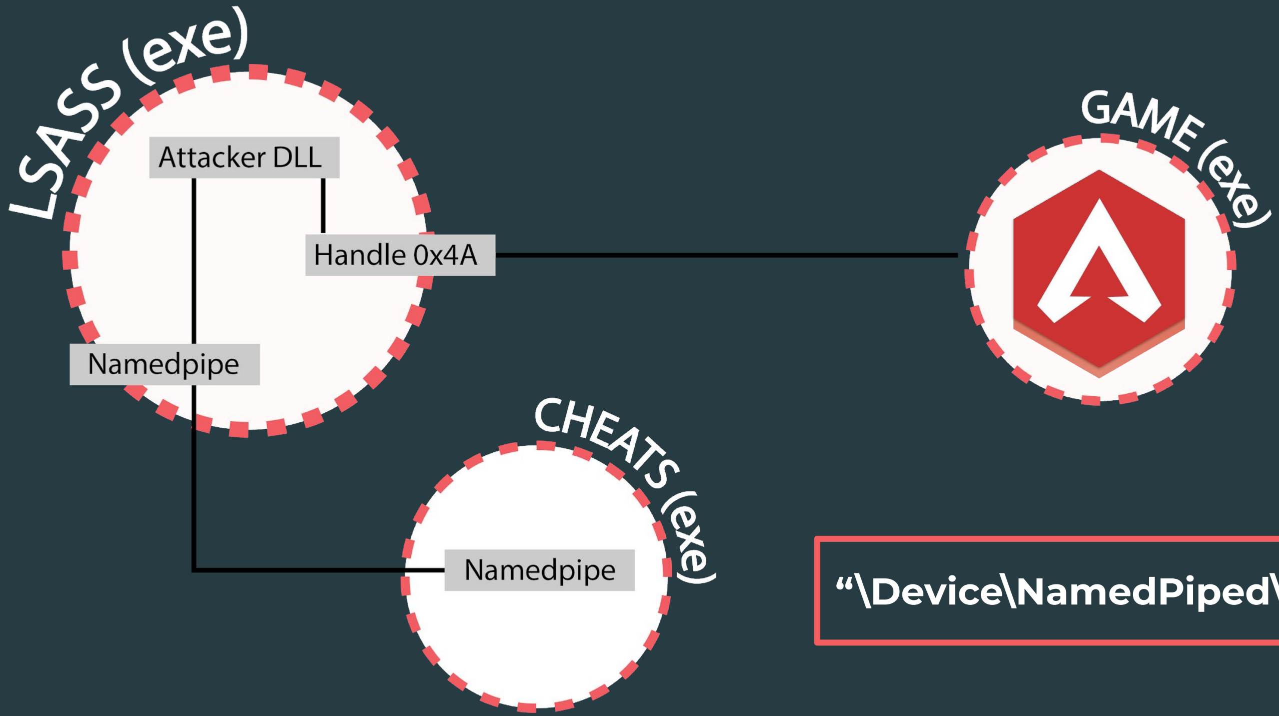
Hijacking techniques come to our rescue:

- Handle Hijacking
- Stealth Handle Hijacking
- Hooking

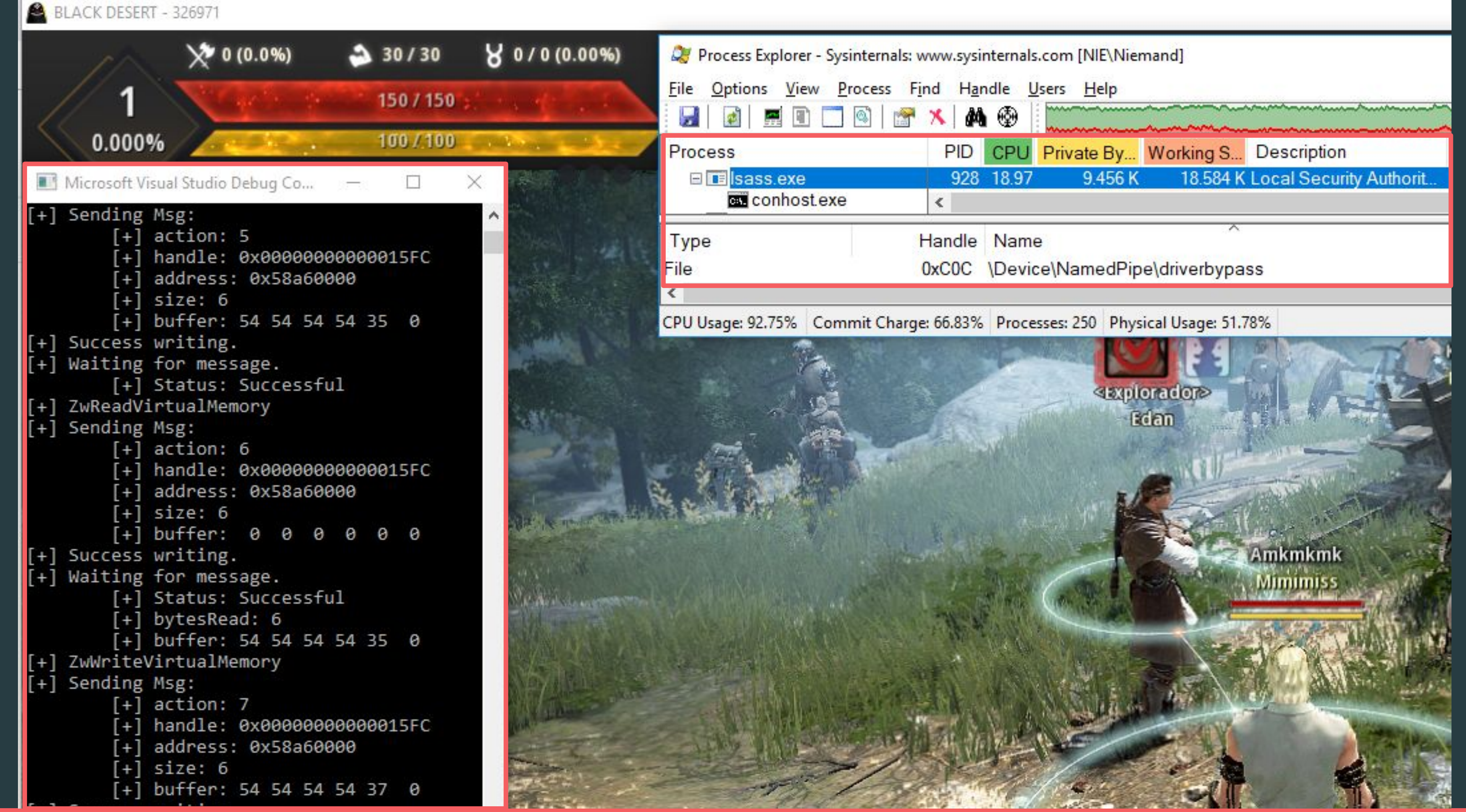
Hijacking Techniques



Hijacking Techniques - NamedPipe



“\Device\NamedPiped\270F59B0075AA3D3”



Microsoft Visual Studio Debug Co...

```
[+] Sending Msg:
        [+] action: 5
        [+] handle: 0x00000000000015FC
        [+] address: 0x58a60000
        [+] size: 6
        [+] buffer: 54 54 54 54 35  0
[+] Success writing.
[+] Waiting for message.
        [+] Status: Successful
[+] ZwReadVirtualMemory
[+] Sending Msg:
        [+] action: 6
        [+] handle: 0x00000000000015FC
        [+] address: 0x58a60000
        [+] size: 6
        [+] buffer:  0  0  0  0  0  0
[+] Success writing.
[+] Waiting for message.
        [+] Status: Successful
        [+] bytesRead: 6
        [+] buffer: 54 54 54 54 35  0
[+] ZwWriteVirtualMemory
[+] Sending Msg:
        [+] action: 7
        [+] handle: 0x00000000000015FC
        [+] address: 0x58a60000
        [+] size: 6
        [+] buffer: 54 54 54 54 37  0
```

Process Explorer - Sysinternals: www.sysinternals.com [NIE\Niemand]

Process	PID	CPU	Private By...	Working S...	Description
lsass.exe	928	18.97	9.456 K	18.584 K	Local Security Authorit...
conhost.exe					

Type	Handle	Name
File	0xC0C	\Device\NamedPipe\driverbypass

CPU Usage: 92.75% Commit Charge: 66.83% Processes: 250 Physical Usage: 51.78%

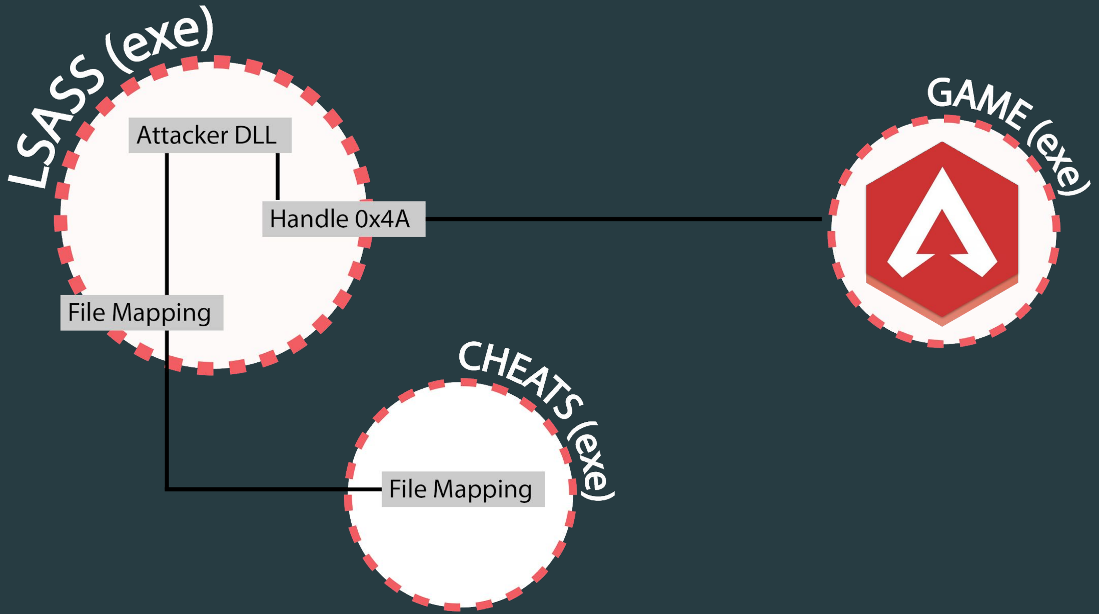
Hijacking Techniques - NamedPipe

Disadvantages

- Suspicious new HANDLEs
- Hooks to user-mode WIN API
- Thread with suspicious context
- Downgrade of HANDLE privileges

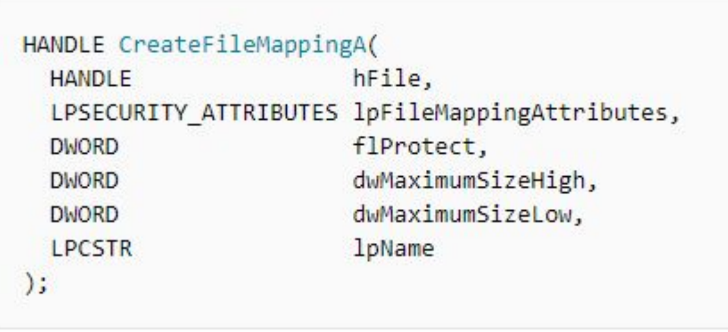
Hijacking Techniques - FileMapping

Imagine a world where our shared memory **does not leave an open HANDLE** and we can cover better our tracks.

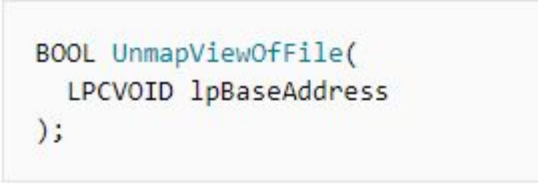


Hijacking Techniques - FileMapping

“**File mapping** object does not close until all references to it are released”



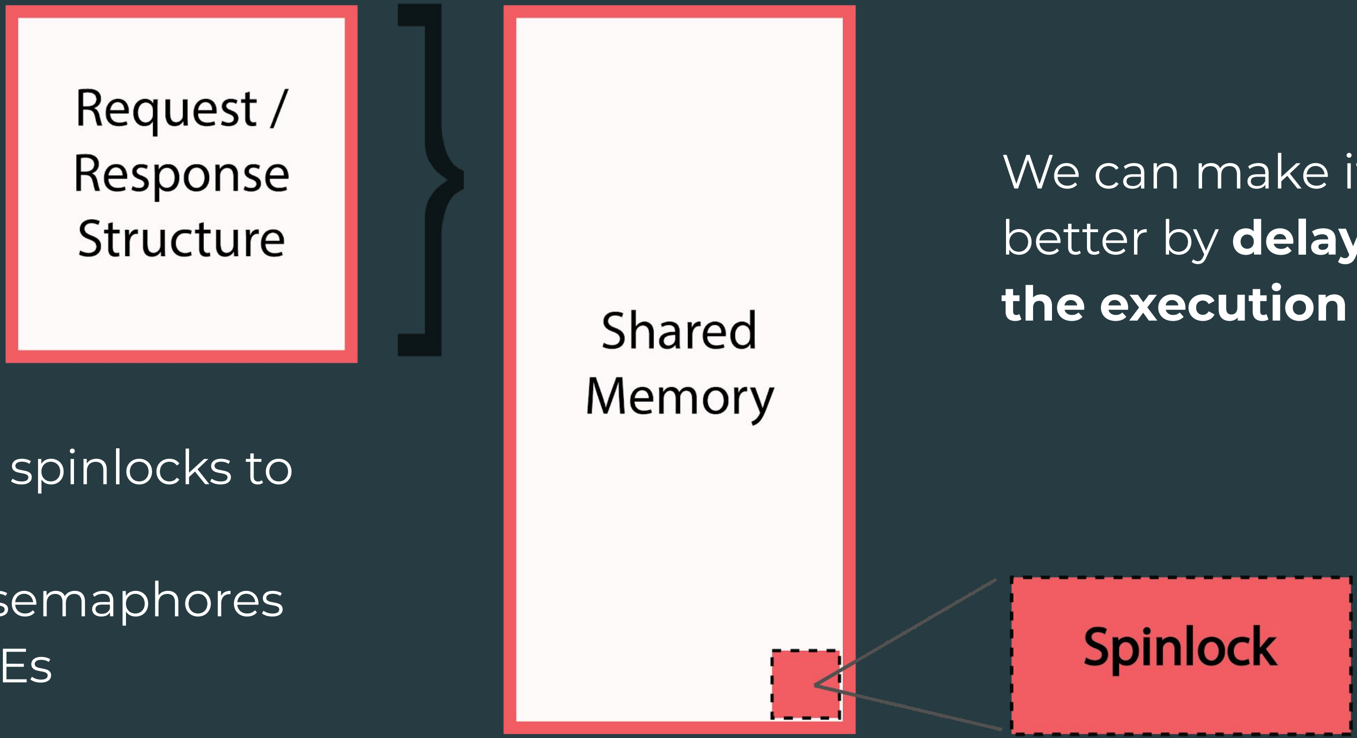
```
HANDLE CreateFileMappingA(
  HANDLE                hFile,
  LPSECURITY_ATTRIBUTES lpFileMappingAttributes,
  DWORD                 flProtect,
  DWORD                 dwMaximumSizeHigh,
  DWORD                 dwMaximumSizeLow,
  LPCSTR                lpName
);
```



```
BOOL UnmapViewOfFile(
  LPCVOID lpBaseAddress
);
```

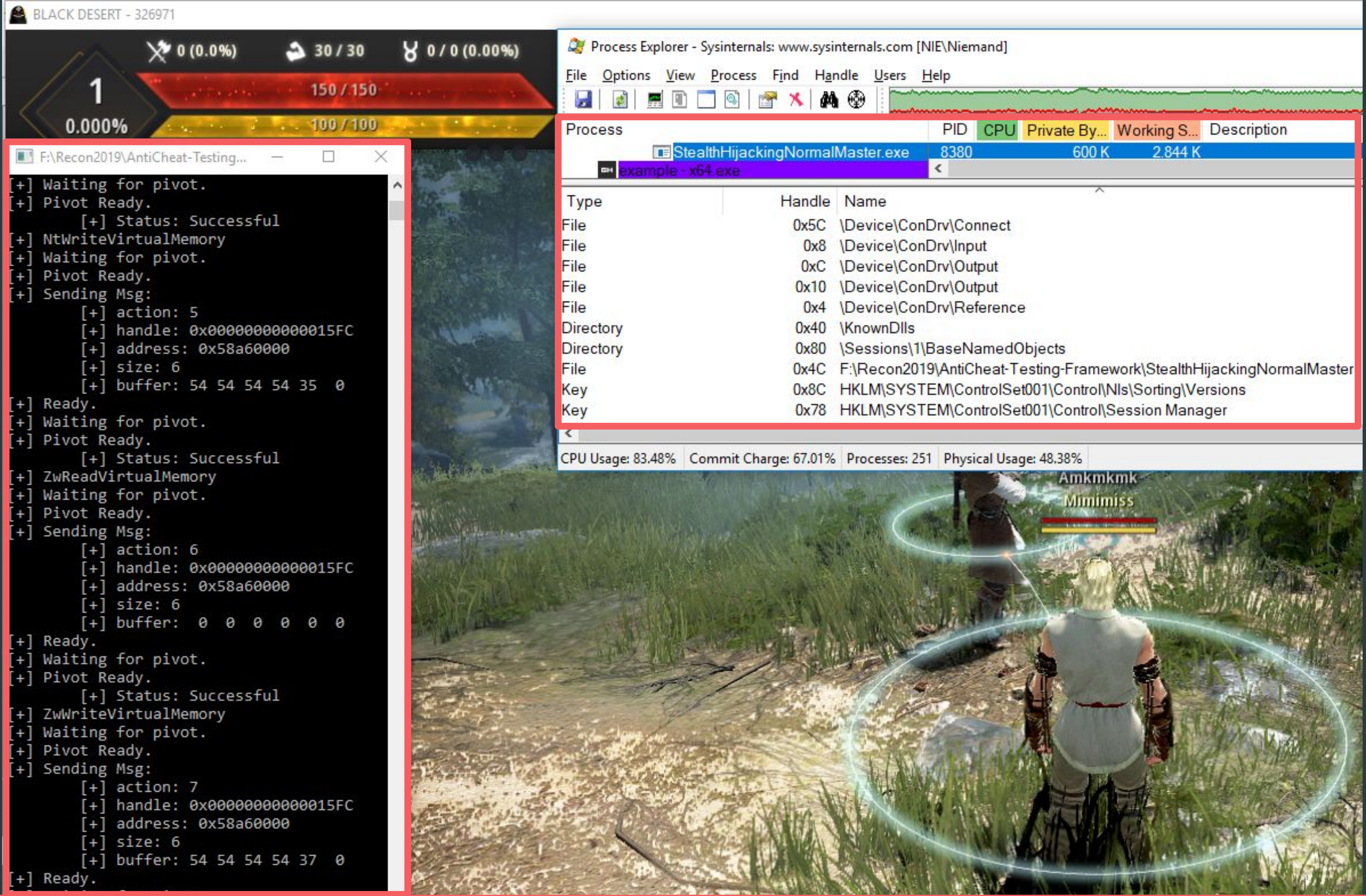
We can call **CloseHandle** without calling to **UnmapViewOfFile**.

Hijacking Techniques - FileMapping



We can make it even better by **delaying the execution**

Manual spinlocks to avoid mutex/semaphores HANDLEs



```
[+] Waiting for pivot.
[+] Pivot Ready.
        [+] Status: Successful
[+] NtWriteVirtualMemory
[+] Waiting for pivot.
[+] Pivot Ready.
[+] Sending Msg:
        [+] action: 5
        [+] handle: 0x00000000000015FC
        [+] address: 0x58a60000
        [+] size: 6
        [+] buffer: 54 54 54 54 35  0
[+] Ready.
[+] Waiting for pivot.
[+] Pivot Ready.
        [+] Status: Successful
[+] ZwReadVirtualMemory
[+] Waiting for pivot.
[+] Pivot Ready.
[+] Sending Msg:
        [+] action: 6
        [+] handle: 0x00000000000015FC
        [+] address: 0x58a60000
        [+] size: 6
        [+] buffer:  0  0  0  0  0  0
[+] Ready.
[+] Waiting for pivot.
[+] Pivot Ready.
        [+] Status: Successful
[+] ZwWriteVirtualMemory
[+] Waiting for pivot.
[+] Pivot Ready.
[+] Sending Msg:
        [+] action: 7
        [+] handle: 0x00000000000015FC
        [+] address: 0x58a60000
        [+] size: 6
        [+] buffer: 54 54 54 54 37  0
[+] Ready.
```

Process	PID	CPU	Private By...	Working S...	Description
StealthHijackingNormalMaster.exe	8380		600 K	2.844 K	
example - x64.exe					

Type	Handle	Name
File	0x5C	\Device\ConDrv\Connect
File	0x8	\Device\ConDrv\Input
File	0xC	\Device\ConDrv\Output
File	0x10	\Device\ConDrv\Output
File	0x4	\Device\ConDrv\Reference
Directory	0x40	\KnownDlls
Directory	0x80	\Sessions\1\BaseNamedObjects
File	0x4C	F:\Recon2019\AntiCheat-Testing-Framework\StealthHijackingNormalMaster
Key	0x8C	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	0x78	HKLM\SYSTEM\ControlSet001\Control\Session Manager

CPU Usage: 83.48% | Commit Charge: 67.01% | Processes: 251 | Physical Usage: 48.38%

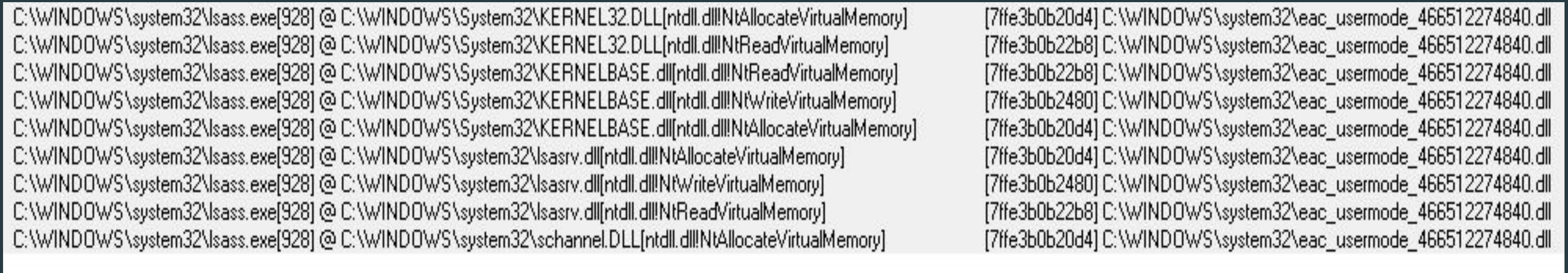
Hijacking Techniques - FileMapping

Disadvantages

- Suspicious new HANDLEs
- Hooks to user-mode WIN API
- Thread with suspicious context
- Downgrade of HANDLE privileges

Hijacking Techniques - Bypass Hooks

EAC also hook functions on **lsass.exe**:

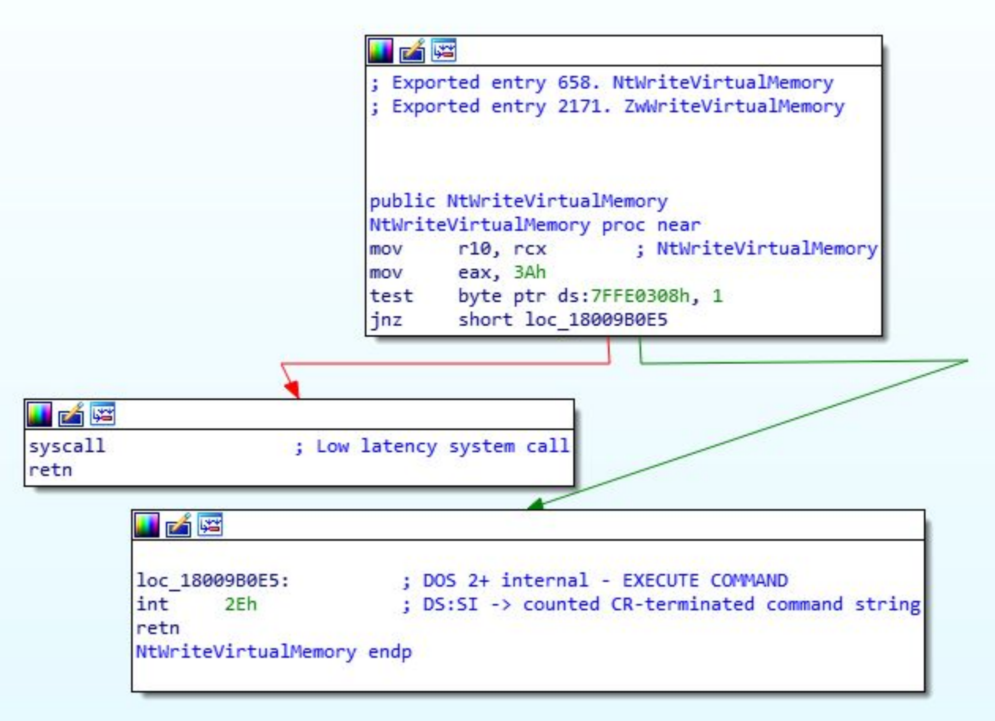


```
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNEL32.DLL[ntdll.dll!NtAllocateVirtualMemory]       [7ffe3b0b20d4] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNEL32.DLL[ntdll.dll!NtReadVirtualMemory]           [7ffe3b0b22b8] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNELBASE.dll[ntdll.dll!NtReadVirtualMemory]         [7ffe3b0b22b8] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNELBASE.dll[ntdll.dll!NtWriteVirtualMemory]        [7ffe3b0b2480] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNELBASE.dll[ntdll.dll!NtAllocateVirtualMemory]     [7ffe3b0b20d4] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lsasrv.dll[ntdll.dll!NtAllocateVirtualMemory]         [7ffe3b0b20d4] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lsasrv.dll[ntdll.dll!NtWriteVirtualMemory]            [7ffe3b0b2480] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lsasrv.dll[ntdll.dll!NtReadVirtualMemory]             [7ffe3b0b22b8] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\schannel.DLL[ntdll.dll!NtAllocateVirtualMemory]       [7ffe3b0b20d4] C:\WINDOWS\system32\eac_usermode_46651227484 0.dll
```

Why?

- Validate/Control/Track each action done against the game

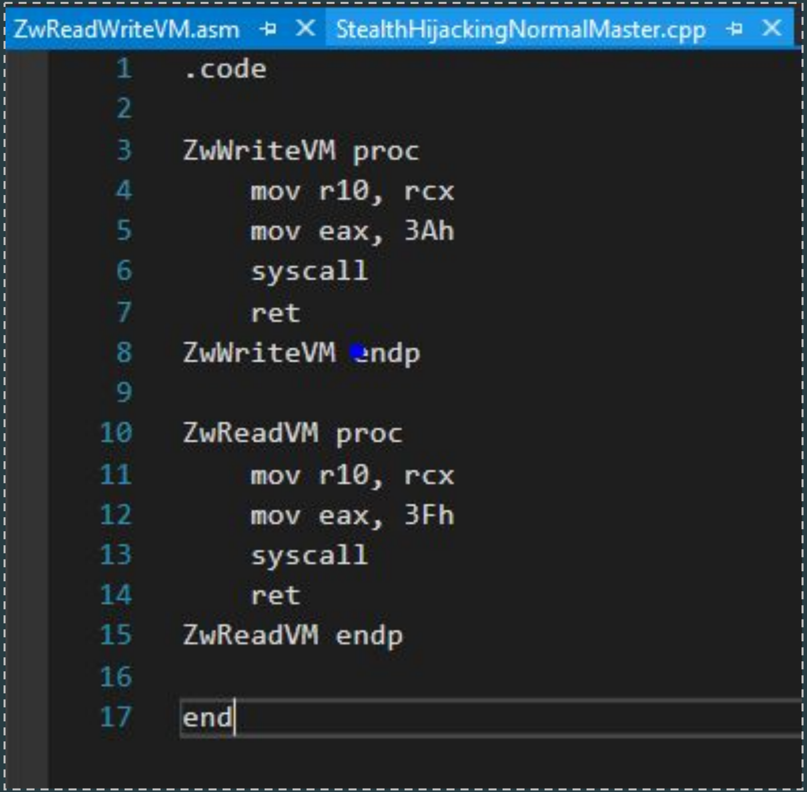
Hijacking Techniques - Bypass Hooks



```
; Exported entry 658. NtWriteVirtualMemory
; Exported entry 2171. ZwWriteVirtualMemory



public NtWriteVirtualMemory
NtWriteVirtualMemory proc near
mov     r10, rcx        ; NtWriteVirtualMemory
mov     eax, 3Ah
test    byte ptr ds:7FFE0308h, 1
jnz     short loc_18009B0E5
```

```
syscall                 ; Low latency system call
retn
```

```

loc_18009B0E5:          ; DOS 2+ internal - EXECUTE COMMAND
int     2Eh             ; DS:SI -> counted CR-terminated command string
retn
NtWriteVirtualMemory endp
```



```
.code

ZwWriteVM proc
    mov r10, rcx
    mov eax, 3Ah
    syscall
    ret
ZwWriteVM endp

ZwReadVM proc
    mov r10, rcx
    mov eax, 3Fh
    syscall
    ret
ZwReadVM endp

end
```

Hijacking Techniques - Bypass Hooks

Disadvantages

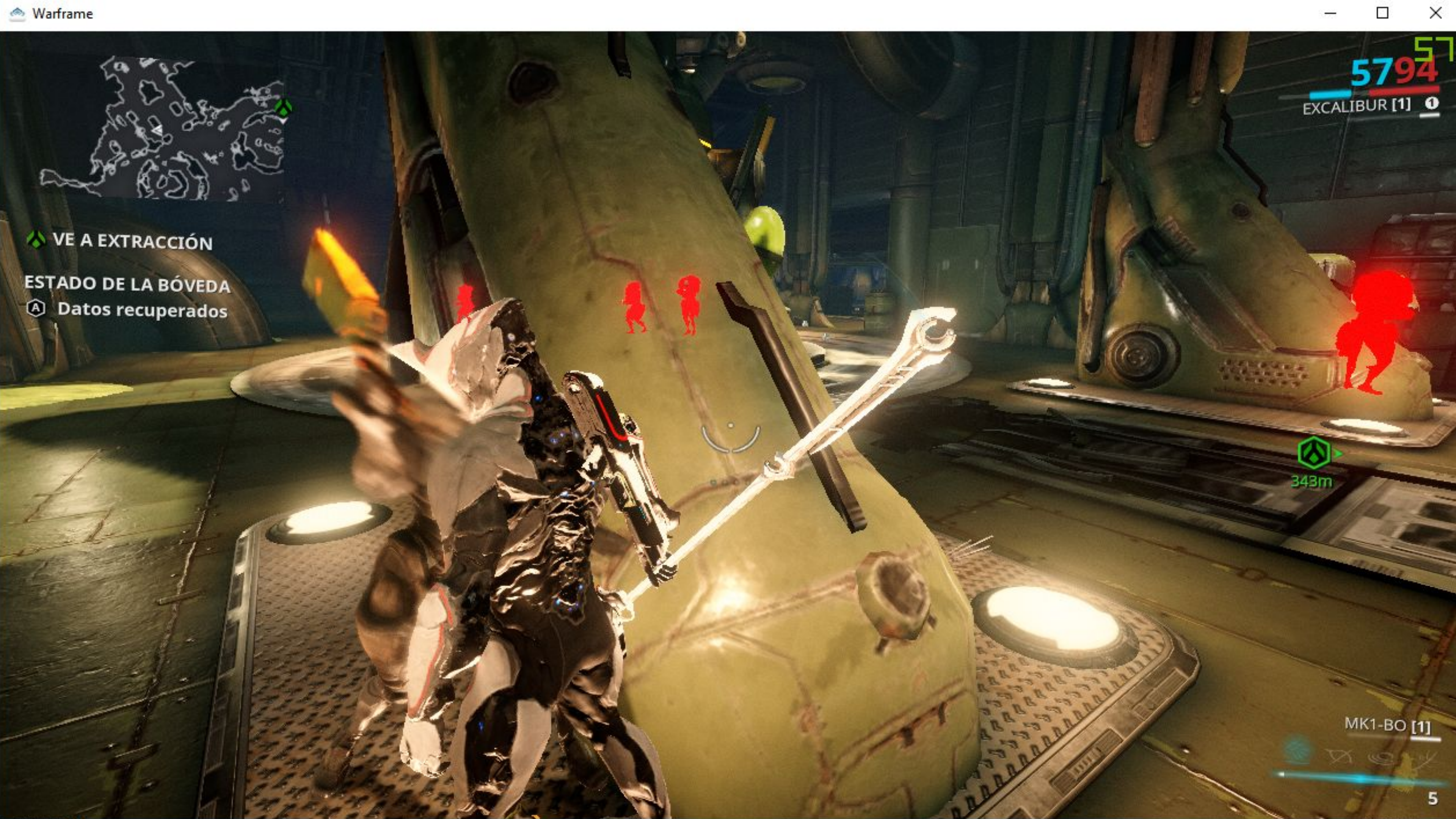
Suspicious new HANDLEs

Hooks to user-mode WIN API

Thread with suspicious context

Downgrade of HANDLE privileges

Hooking



VE A EXTRACCIÓN

ESTADO DE LA BÓVEDA

Ⓐ Datos recuperados

Hooking

Cheats usually **hook** functions from Graphic Engines:

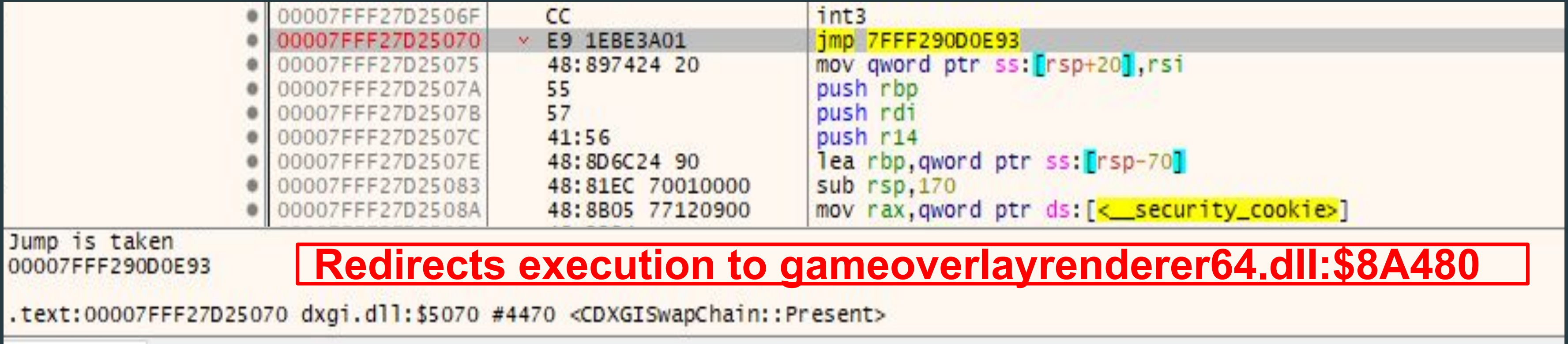
- IAT hooking, JMPs on Prolog functions, etc

But AC usually control this.

Inside their own game is easy, but what about trusted external libraries?

- Steam Overlay
- Open Broadcaster Software (OBS)

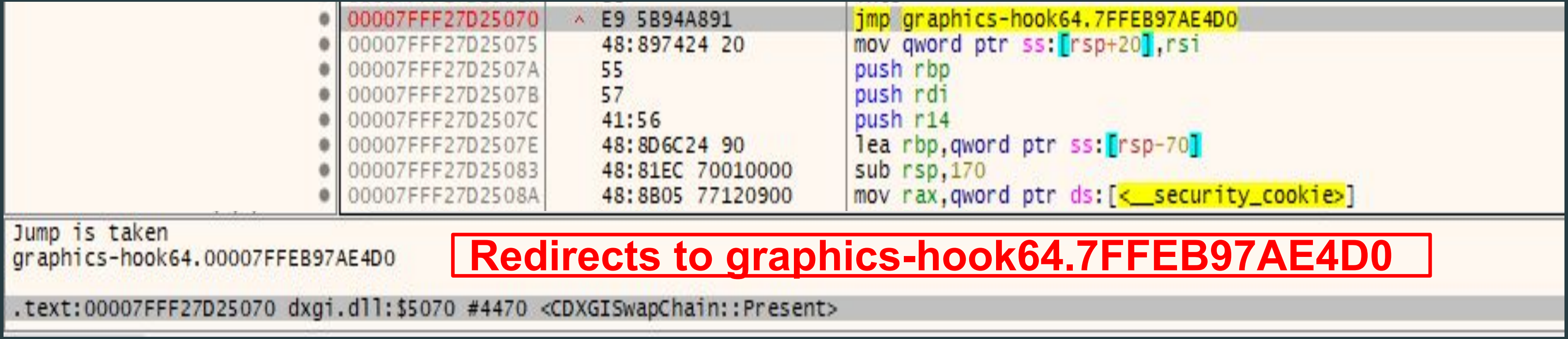
Steam Overlay



```
00007FFF27D2506F    CC                 int3
00007FFF27D25070  v E9 1EBE3A01        jmp 7FFF290D0E93
00007FFF27D25075    48:897424 20       mov qword ptr ss:[rsp+20],rsi
00007FFF27D2507A    55                 push rbp
00007FFF27D2507B    57                 push rdi
00007FFF27D2507C    41:56              push r14
00007FFF27D2507E    48:8D6C24 90       lea rbp,qword ptr ss:[rsp-70]
00007FFF27D25083    48:81EC 70010000   sub rsp,170
00007FFF27D2508A    48:8B05 77120900   mov rax,qword ptr ds:[<__security_cookie>]

Jump is taken
00007FFF290D0E93

.text:00007FFF27D25070 dxgi.dll:$5070 #4470 <CDXGISwapChain::Present>
```

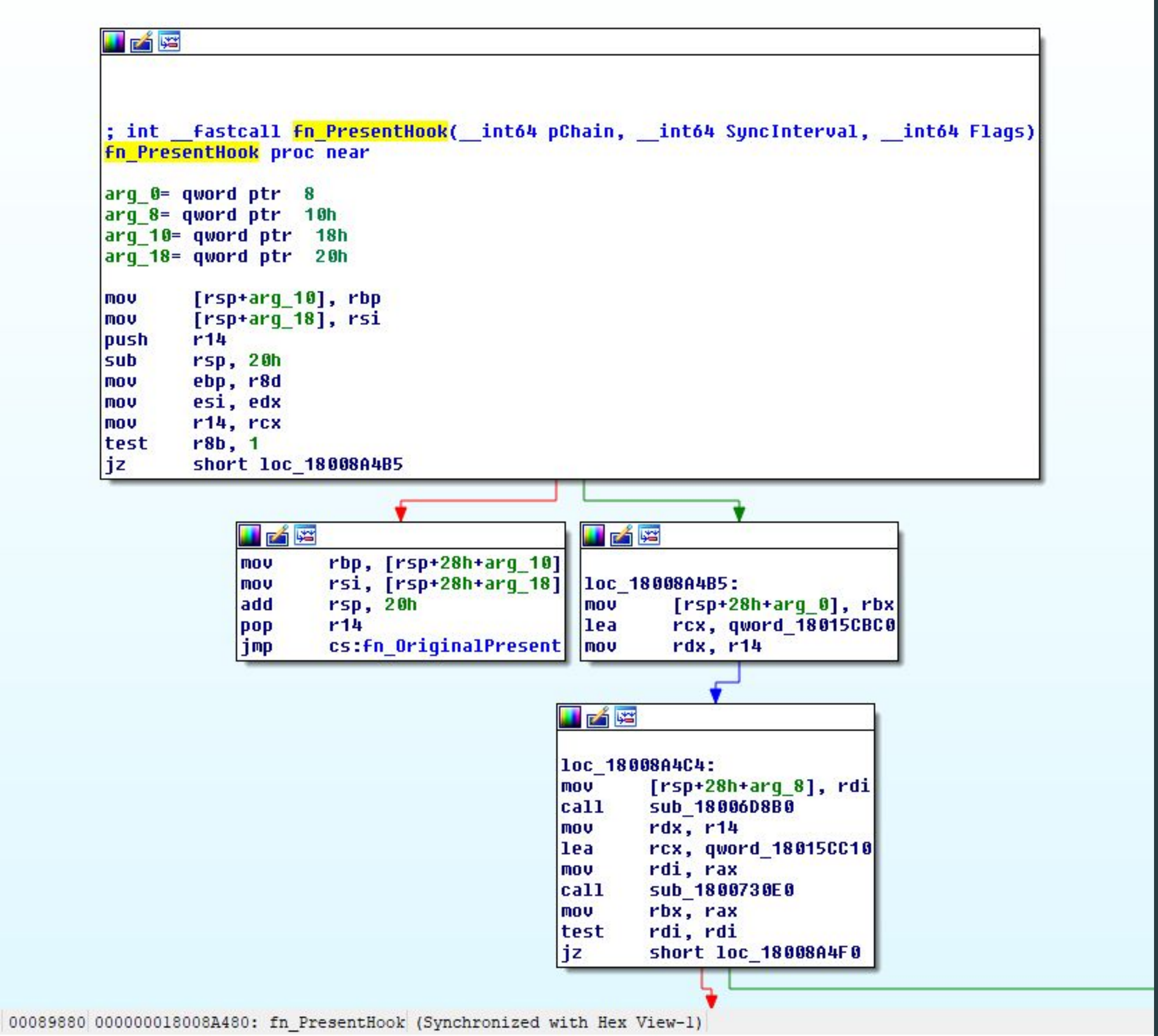
Redirects execution to gameoverlayrenderer64.dll:$8A480

Open Broadcaster Software



```
00007FFF27D25070  ^ E9 5B94A891        jmp graphics-hook64.7FFEB97AE4D0
00007FFF27D25075    48:897424 20       mov qword ptr ss:[rsp+20],rsi
00007FFF27D2507A    55                 push rbp
00007FFF27D2507B    57                 push rdi
00007FFF27D2507C    41:56              push r14
00007FFF27D2507E    48:8D6C24 90       lea rbp,qword ptr ss:[rsp-70]
00007FFF27D25083    48:81EC 70010000   sub rsp,170
00007FFF27D2508A    48:8B05 77120900   mov rax,qword ptr ds:[<__security_cookie>]

Jump is taken
graphics-hook64.00007FFEB97AE4D0

.text:00007FFF27D25070 dxgi.dll:$5070 #4470 <CDXGISwapChain::Present>
```

Redirects to graphics-hook64.7FFEB97AE4D0



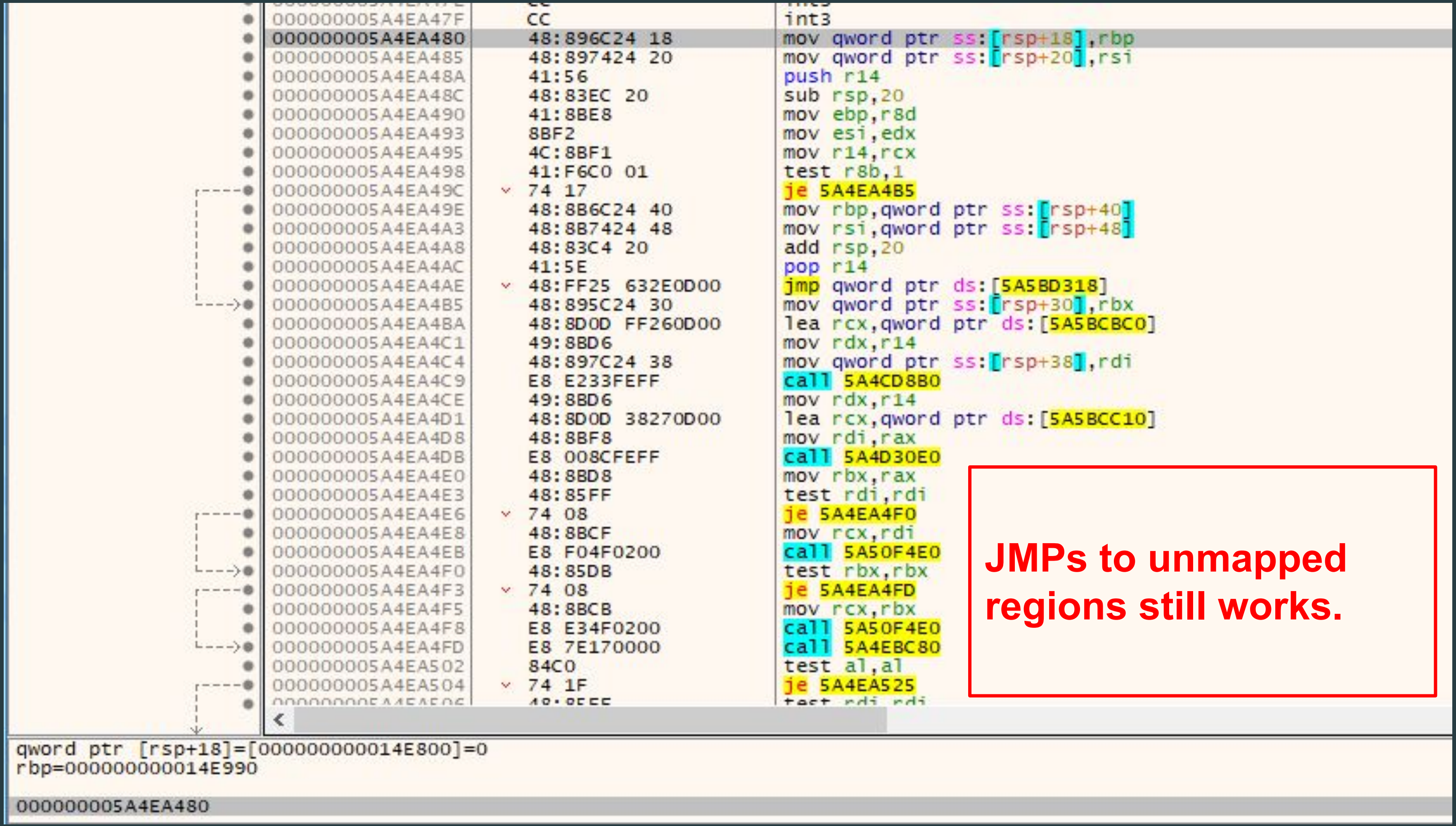
```
; int __fastcall fn_PresentHook(__int64 pChain, __int64 SyncInterval, __int64 Flags)
fn_PresentHook proc near

arg_0= qword ptr  8
arg_8= qword ptr  10h
arg_10= qword ptr  18h
arg_18= qword ptr  20h

mov     [rsp+arg_10], rbp
mov     [rsp+arg_18], rsi
push    r14
sub     rsp, 20h
mov     ebp, r8d
mov     esi, edx
mov     r14, rcx
test    r8b, 1
jz      short loc_18008A4B5
```

```
mov     rbp, [rsp+28h+arg_10]
mov     rsi, [rsp+28h+arg_18]
add     rsp, 20h
pop     r14
jmp     cs:fn_OriginalPresent
```

```
loc_18008A4B5:
mov     [rsp+28h+arg_0], rbx
lea     rcx, qword_18015CBC0
mov     rdx, r14
```

```
loc_18008A4C4:
mov     [rsp+28h+arg_8], rdi
call    sub_18006D8B0
mov     rdx, r14
lea     rcx, qword_18015CC10
mov     rdi, rax
call    sub_1800730E0
mov     rbx, rax
test    rdi, rdi
jz      short loc_18008A4F0
```

```
00089880 000000018008A480: fn_PresentHook (Synchronized with Hex View-1)
```



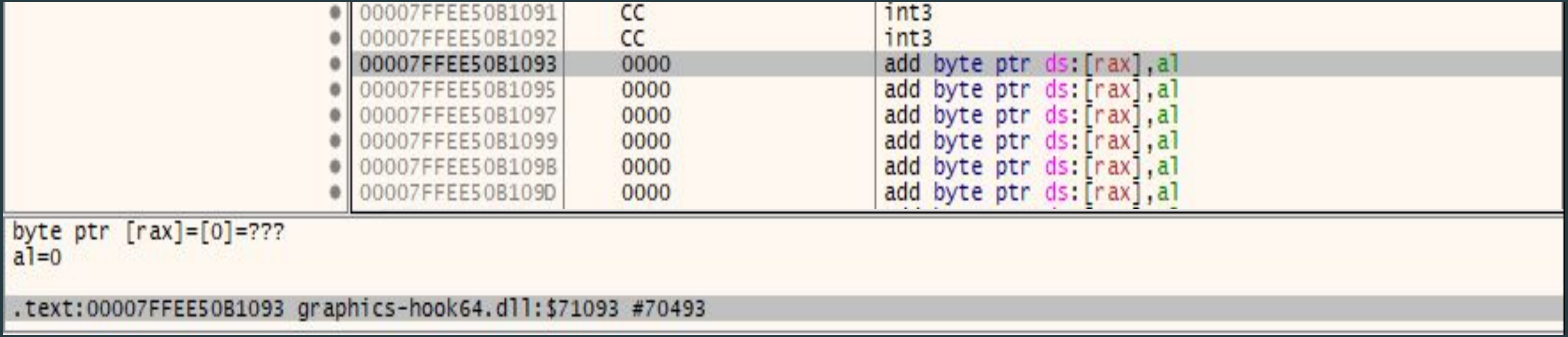
```
000000005A4EA47F   CC                 int3
000000005A4EA480   48:896C24 18       mov qword ptr ss:[rsp+18],rbp
000000005A4EA485   48:897424 20       mov qword ptr ss:[rsp+20],rsi
000000005A4EA48A   41:56              push r14
000000005A4EA48C   48:83EC 20         sub rsp,20
000000005A4EA490   41:8BE8            mov ebp,r8d
000000005A4EA493   8BF2               mov esi,edx
000000005A4EA495   4C:8BF1            mov r14,rcx
000000005A4EA498   41:F6C0 01         test r8b,1
000000005A4EA49C   74 17              je 5A4EA4B5
000000005A4EA49E   48:8B6C24 40       mov rbp,qword ptr ss:[rsp+40]
000000005A4EA4A3   48:8B7424 48       mov rsi,qword ptr ss:[rsp+48]
000000005A4EA4A8   48:83C4 20         add rsp,20
000000005A4EA4AC   41:5E              pop r14
000000005A4EA4AE   48:FF25 632E0D00   jmp qword ptr ds:[5A5BD318]
000000005A4EA4B5   48:895C24 30       mov qword ptr ss:[rsp+30],rbx
000000005A4EA4BA   48:8D0D FF260D00   lea rcx,qword ptr ds:[5A5BCBC0]
000000005A4EA4C1   49:8BD6            mov rdx,r14
000000005A4EA4C4   48:897C24 38       mov qword ptr ss:[rsp+38],rdi
000000005A4EA4C9   E8 E233FEFF        call 5A4CD8B0
000000005A4EA4CE   49:8BD6            mov rdx,r14
000000005A4EA4D1   48:8D0D 38270D00   lea rcx,qword ptr ds:[5A5BCC10]
000000005A4EA4D8   48:8BF8            mov rdi,rax
000000005A4EA4DB   E8 008CFEFF        call 5A4D30E0
000000005A4EA4E0   48:8BD8            mov rbx,rax
000000005A4EA4E3   48:85FF            test rdi,rdi
000000005A4EA4E6   74 08              je 5A4EA4F0
000000005A4EA4E8   48:8BCF            mov rcx,rdi
000000005A4EA4EB   E8 F04F0200        call 5A50F4E0
000000005A4EA4F0   48:85DB            test rbx,rbx
000000005A4EA4F3   74 08              je 5A4EA4FD
000000005A4EA4F5   48:8BCB            mov rcx,rbx
000000005A4EA4F8   E8 E34F0200        call 5A50F4E0
000000005A4EA4FD   E8 7E170000        call 5A4EBC80
000000005A4EA502   84C0               test al,al
000000005A4EA504   74 1F              je 5A4EA525
```

```
qword ptr [rsp+18]=[000000000014E800]=0
rbp=000000000014E990
```

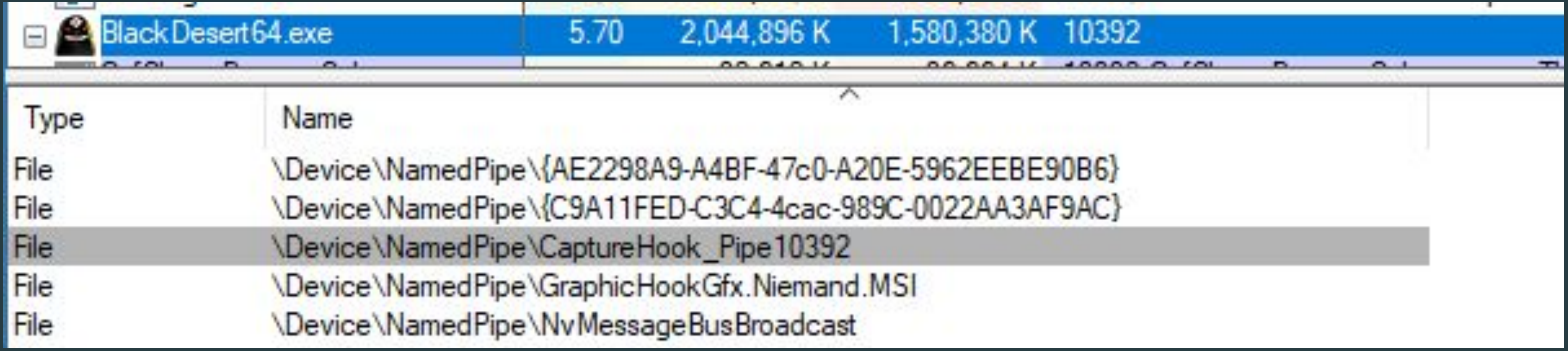
```
000000005A4EA480
```

JMPs to unmapped regions still works.

Hooking - Code Caves and NamedPipes?



```
00007FFEE50B1091    CC      int3
00007FFEE50B1092    CC      int3
00007FFEE50B1093    0000    add byte ptr ds:[rax],al
00007FFEE50B1095    0000    add byte ptr ds:[rax],al
00007FFEE50B1097    0000    add byte ptr ds:[rax],al
00007FFEE50B1099    0000    add byte ptr ds:[rax],al
00007FFEE50B109B    0000    add byte ptr ds:[rax],al
00007FFEE50B109D    0000    add byte ptr ds:[rax],al

byte ptr [rax]=[0]=???
al=0

.text:00007FFEE50B1093 graphics-hook64.dll:$71093 #70493
```



```
BlackDesert64.exe    5.70    2,044,896 K    1,580,380 K    10392

Type    Name
File    \Device\NamedPipe\{AE2298A9-A4BF-47c0-A20E-5962EEBE90B6}
File    \Device\NamedPipe\{C9A11FED-C3C4-4cac-989C-0022AA3AF9AC}
File    \Device\NamedPipe\CaptureHook_Pipe10392
File    \Device\NamedPipe\GraphicHookGfx.Niemand.MSI
File    \Device\NamedPipe\NvMessageBusBroadcast
```

Refresher- Bypass Hooks

Disadvantages

Suspicious new HANDLEs

Hooks to user-mode WIN API

Thread with suspicious context

Downgrade of HANDLE privileges

Moving to kernel...Drivers

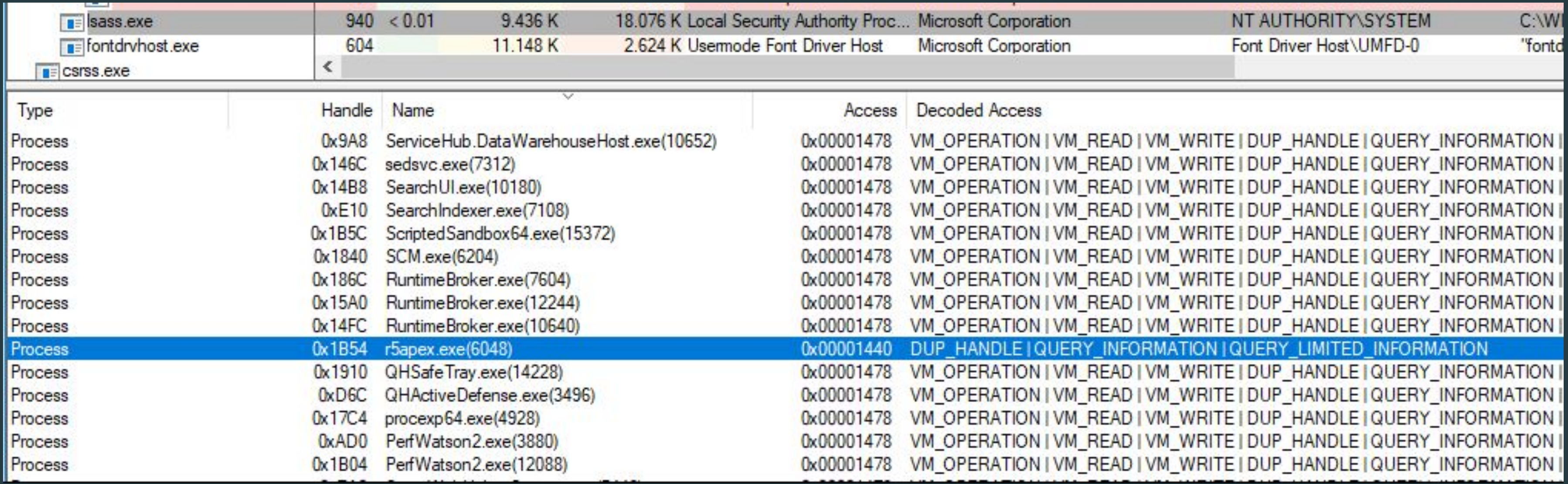
Drivers

Cheat developers also develop their own to fight inside the kernel.

Loading a Driver:

- Test Mode
- Sign your own Driver ($$$$$$$$)
- Abuse of another driver

EAC downgrading the HANDLE



```
    lsass.exe          940  < 0.01   9.436 K   18.076 K Local Security Authority Proc...  Microsoft Corporation   NT AUTHORITY\SYSTEM        C:\WI
    fontdrvhost.exe    604          11.148 K    2.624 K Usermode Font Driver Host         Microsoft Corporation   Font Driver Host\UMFD-0    "fontd
  csrss.exe
```

Type	Handle	Name	Access	Decoded Access
Process	0x9A8	ServiceHub.DataWarehouseHost.exe(10652)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x146C	sedsvc.exe(7312)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x14B8	SearchUI.exe(10180)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0xE10	SearchIndexer.exe(7108)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x1B5C	ScriptedSandbox64.exe(15372)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x1840	SCM.exe(6204)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x186C	RuntimeBroker.exe(7604)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x15A0	RuntimeBroker.exe(12244)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x14FC	RuntimeBroker.exe(10640)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x1B54	r5apex.exe(6048)	0x00001440	DUP_HANDLE | QUERY_INFORMATION | QUERY_LIMITED_INFORMATION
Process	0x1910	QHSafeTray.exe(14228)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0xD6C	QHActiveDefense.exe(3496)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x17C4	procexp64.exe(4928)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0xAD0	PerfWatson2.exe(3880)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |
Process	0x1B04	PerfWatson2.exe(12088)	0x00001478	VM_OPERATION | VM_READ | VM_WRITE | DUP_HANDLE | QUERY_INFORMATION |

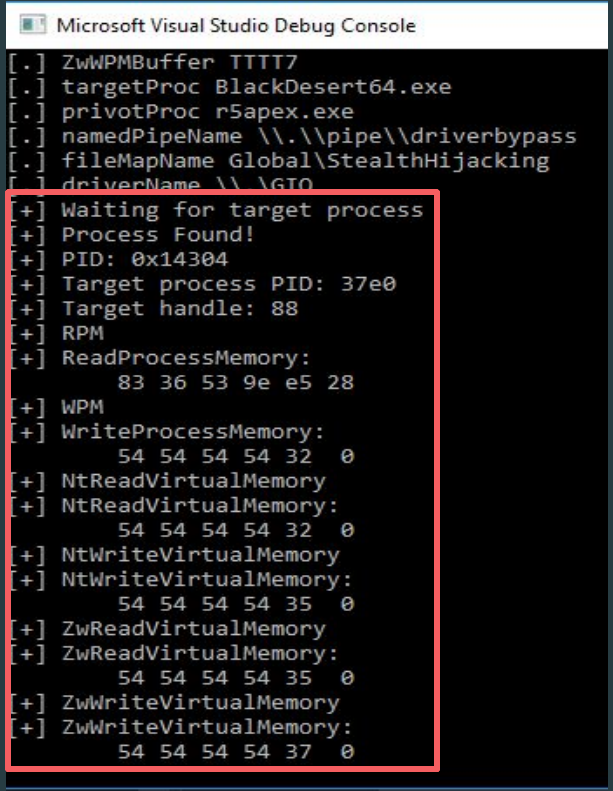
We need to find a different approach.

Driver - Synapse (CVE-2017-9769)

- IOCTL gives us access to ZwOpenProcess

- If AC control the access at kernel level it won’t work :(

- We need a better approach



```
[.] ZwWPMBuffer TTTT7
[.] targetProc BlackDesert64.exe
[.] privotProc r5apex.exe
[.] namedPipeName \\.\\pipe\\driverbypass
[.] fileMapName Global\StealthHijacking
[.] driverName \\.\GIO
[+] Waiting for target process
[+] Process Found!
[+] PID: 0x14304
[+] Target process PID: 37e0
[+] Target handle: 88
[+] RPM
[+] ReadProcessMemory:
        83 36 53 9e e5 28
[+] WPM
[+] WriteProcessMemory:
        54 54 54 54 32  0
[+] NtReadVirtualMemory
[+] NtReadVirtualMemory:
        54 54 54 54 32  0
[+] NtWriteVirtualMemory
[+] NtWriteVirtualMemory:
        54 54 54 54 35  0
[+] ZwReadVirtualMemory
[+] ZwReadVirtualMemory:
        54 54 54 54 35  0
[+] ZwWriteVirtualMemory
[+] ZwWriteVirtualMemory:
        54 54 54 54 37  0
```

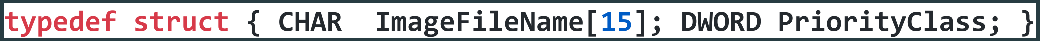
Driver - GIGABYTE Drivers

- CVE-2018-19320 (ring0 memcpy with VA)
- CVE-2018-19321 (read/write arbitrary physical memory)

- Non-privileged user processes are able to get a HANDLE and issue IOCTL codes
- **How could we use this?**

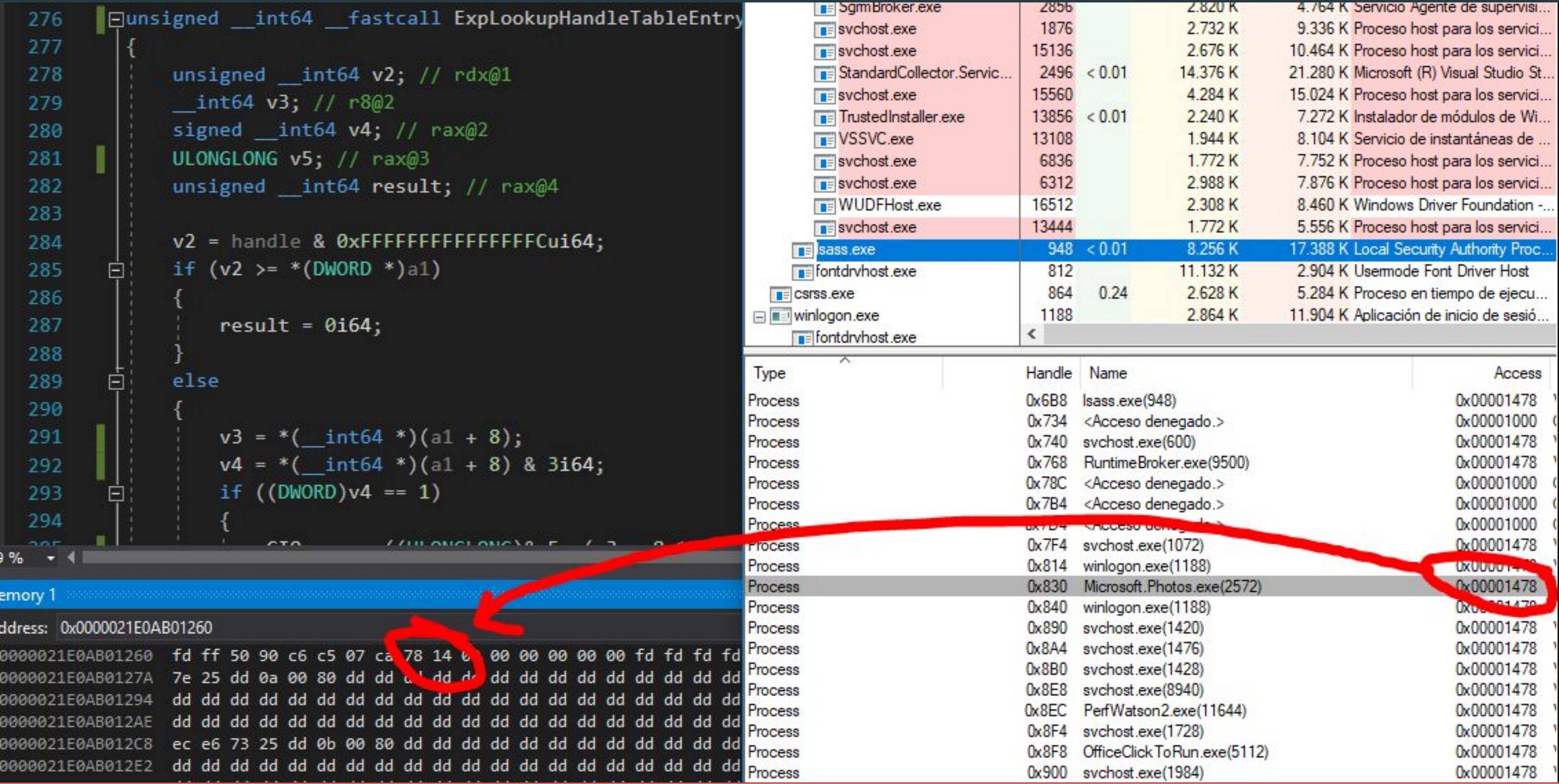
Driver - DKOM

1) Load the vulnerable Driver and get a HANDLE (open DACL)
2) Search for EPROCESS Struct in kernel



```
typedef struct { CHAR  ImageFileName[15]; DWORD PriorityClass; }
```

3) Obtain the ObjectTable (HANDLE_TABLE)
4) Use ExpLookupHandleTableEntry(HandleTable, Handle)
5) Retrieve HANDLE
6) Modify GrantedAccess
7) Overwrite kernel memory
8) Profit

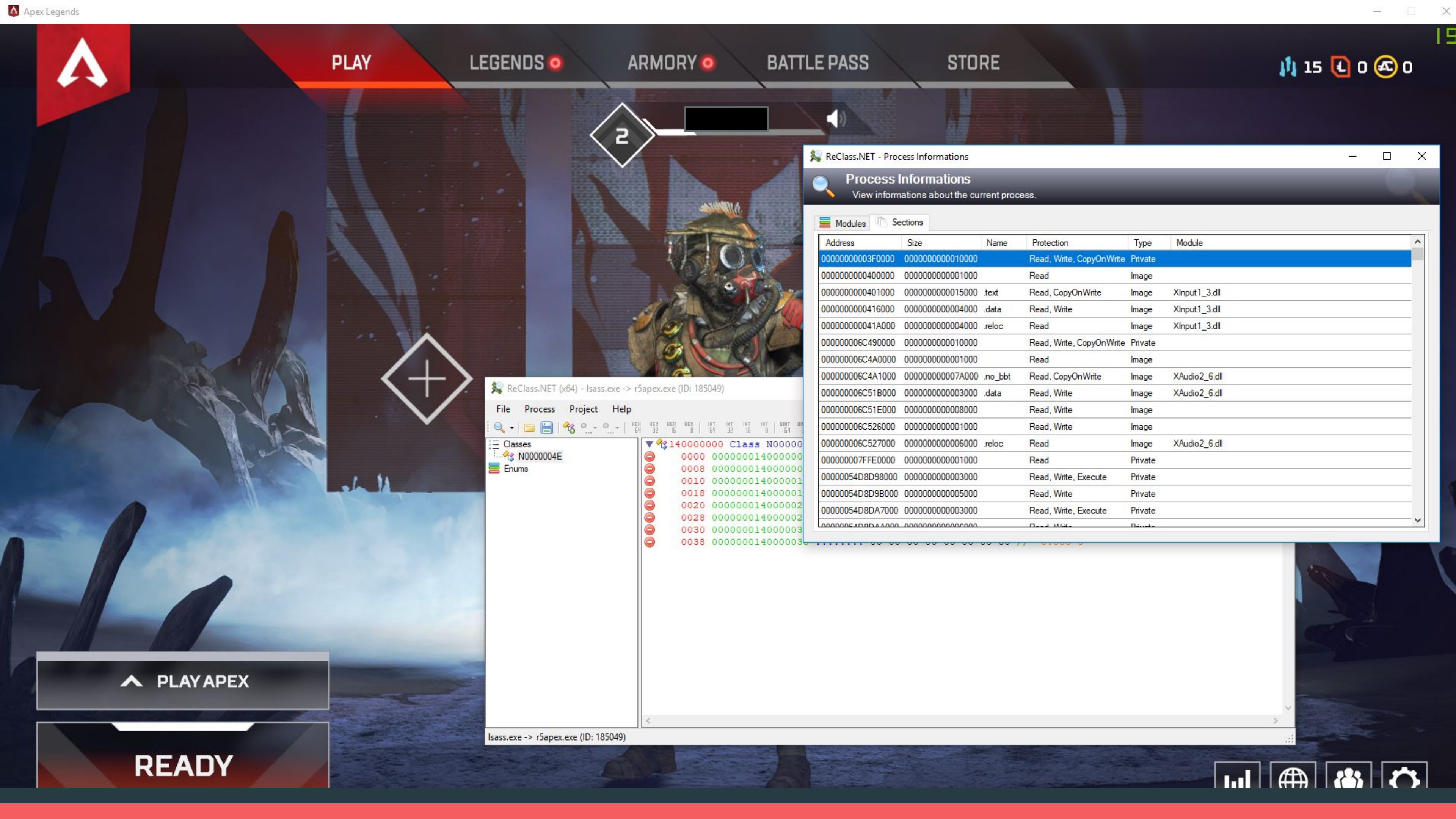


```
unsigned __int64 __fastcall ExpLookupHandleTableEntry
{
    unsigned __int64 v2; // rdx@1
    __int64 v3; // r8@2
    signed __int64 v4; // rax@2
    ULONGLONG v5; // rax@3
    unsigned __int64 result; // rax@4

    v2 = handle & 0xFFFFFFFFFFFFFFFCui64;
    if (v2 >= *(DWORD *)a1)
    {
        result = 0i64;
    }
    else
    {
        v3 = *(__int64 *)(a1 + 8);
        v4 = *(__int64 *)(a1 + 8) & 3i64;
        if ((DWORD)v4 == 1)
        {
```

```
ddress: 0x0000021E0AB01260
0000021E0AB01260  fd ff 50 90 c6 c5 07 ca 78 14 00 00 00 00 00 00 fd fd fd fd
0000021E0AB0127A  7e 25 dd 0a 00 80 dd dd dd dd dd dd dd dd dd dd dd dd dd dd
0000021E0AB01294  dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
0000021E0AB012AE  dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
0000021E0AB012C8  ec e6 73 25 dd 0b 00 80 dd dd dd dd dd dd dd dd dd dd dd dd
0000021E0AB012E2  dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
```

SgmBroker.exe	2856		2.820 K	4.764 K	Servicio Agente de supervisi...
svchost.exe	1876		2.732 K	9.336 K	Proceso host para los servici...
svchost.exe	15136		2.676 K	10.464 K	Proceso host para los servici...
StandardCollector.Servic...	2496	< 0.01	14.376 K	21.280 K	Microsoft (R) Visual Studio St...
svchost.exe	15560		4.284 K	15.024 K	Proceso host para los servici...
TrustedInstaller.exe	13856	< 0.01	2.240 K	7.272 K	Instalador de módulos de Wi...
VSSVC.exe	13108		1.944 K	8.104 K	Servicio de instantáneas de ...
svchost.exe	6836		1.772 K	7.752 K	Proceso host para los servici...
svchost.exe	6312		2.988 K	7.876 K	Proceso host para los servici...
WUDFHost.exe	16512		2.308 K	8.460 K	Windows Driver Foundation -...
svchost.exe	13444		1.772 K	5.556 K	Proceso host para los servici...
lsass.exe	948	< 0.01	8.256 K	17.388 K	Local Security Authority Proc...
fontdrvhost.exe	812		11.132 K	2.904 K	Usermode Font Driver Host
csrss.exe	864	0.24	2.628 K	5.284 K	Proceso en tiempo de ejecu...
winlogon.exe	1188		2.864 K	11.904 K	Aplicación de inicio de sesió...
fontdrvhost.exe					

Type	Handle	Name	Access
Process	0x6B8	lsass.exe(948)	0x00001478
Process	0x734	<Acceso denegado.>	0x00001000
Process	0x740	svchost.exe(600)	0x00001478
Process	0x768	RuntimeBroker.exe(9500)	0x00001478
Process	0x78C	<Acceso denegado.>	0x00001000
Process	0x7B4	<Acceso denegado.>	0x00001000
Process	0x7D4	<Acceso denegado.>	0x00001000
Process	0x7F4	svchost.exe(1072)	0x00001478
Process	0x814	winlogon.exe(1188)	0x00001478
Process	0x830	Microsoft.Photos.exe(2572)	0x00001478
Process	0x840	winlogon.exe(1188)	0x00001478
Process	0x890	svchost.exe(1420)	0x00001478
Process	0x8A4	svchost.exe(1476)	0x00001478
Process	0x8B0	svchost.exe(1428)	0x00001478
Process	0x8E8	svchost.exe(8940)	0x00001478
Process	0x8EC	PerfWatson2.exe(11644)	0x00001478
Process	0x8F4	svchost.exe(1728)	0x00001478
Process	0x8F8	OfficeClickToRun.exe(5112)	0x00001478
Process	0x900	svchost.exe(1984)	0x00001478



ReClass.NET - Process Informations

Process Informations

View informations about the current process.

Address	Size	Name	Protection	Type	Module
00000000003F0000	0000000000010000		Read, Write, CopyOnWrite	Private	
0000000000400000	0000000000001000		Read	Image	
0000000000401000	0000000000015000	.text	Read, CopyOnWrite	Image	XInput1_3.dll
0000000000416000	0000000000004000	.data	Read, Write	Image	XInput1_3.dll
000000000041A000	0000000000004000	.reloc	Read	Image	XInput1_3.dll
000000006C490000	0000000000010000		Read, Write, CopyOnWrite	Private	
000000006C4A0000	0000000000001000		Read	Image	
000000006C4A1000	000000000007A000	.no_bbt	Read, CopyOnWrite	Image	XAudio2_6.dll
000000006C51B000	0000000000003000	.data	Read, Write	Image	XAudio2_6.dll
000000006C51E000	0000000000008000		Read, Write	Image	
000000006C526000	0000000000001000		Read, Write	Image	
000000006C527000	0000000000006000	.reloc	Read	Image	XAudio2_6.dll
000000007FFE0000	0000000000001000		Read	Private	
00000054D8D98000	0000000000003000		Read, Write, Execute	Private	
00000054D8D9B000	0000000000005000		Read, Write	Private	
00000054D8DA7000	0000000000003000		Read, Write, Execute	Private	

ReClass.NET (x64) - lsass.exe -> r5apex.exe (ID: 185049)

```
140000000 Class N00000
    0000 000000014000000
    0008 000000014000000
    0010 000000014000001
    0018 000000014000001
    0020 000000014000002
    0028 000000014000002
    0030 000000014000003
    0038 000000014000003
```

lsass.exe -> r5apex.exe (ID: 185049)

Refresher- Bypass Hooks

Disadvantages

- Suspicious new HANDLEs
- Hooks to user-mode WIN API
- Thread with suspicious context
- Downgrade of HANDLE privileges

Conclusions

- Fight at kernel level
- It could be trivial
- Blacklisting all drivers is impossible
- Compatibility with Windows and 3rd applications is a problem

Conclusions

AntiCheat-Testing-Framework

- CheatHelper & DriverHelper
- DriverDisabler
- HandleHijackingDLL and HandleHijackingMaster
- StealthHijackingDLL and StealthHijackingMaster
- WinApi Hooking Bypass (Direct call to syscalls)
- Lua Hooking (with pattern scanning)
- Synapse Driver exploit (Razer)
- Handle Elevation (Gigabyte Driver)

Github:niemand-sec/AntiCheat-Testing-Framework

THANK YOU!

More information at niemand.com.ar