

# *Unveiling the underground world of*

# ANTI-CHEATS

---



**Joel Noguera**

Security Consultant at Immunity Inc

@niemand\_sec

# What are we going to talk about?






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

~~(or get caught doing it)~~



Search 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



Let's see some numbers...

336.500.000

Monthly Active Users

**EAC**

275.000.000

**XC3**

500.000

**BE**

30.000.000

**VAC**

31.000.000





# BLACK DESERT

## ONLINE

# REMASTERED



[Combat] [Jackpaxx] was unfairly killed by [Lucyna]  
[Combat] [ArniStriker] was unfairly killed by [Aladread]  
[Combat] [ArniStriker] was unfairly killed by [OnePunchBady]  
[Combat] [Jackpaxx] was unfairly killed by [Aladread]  
[Combat] [Yandere\_GF] forcefully slaughtered [Gorklax]  
[Combat] [Yandere\_GF] forcefully slaughtered [Sciddalister]  
[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].

[Neutral] : WTB [Striker] WeDan and Value pack Max price.  
[Pepelepewpew] : LF2M sauzants.val3  
[Legendary\_Rorix] : anyone got a +15 rosar lying around?  
[Bicorn] : <Ascondantes> is recruiting for Node Wars :  
Lv. 58+ 40d+ gs | Must be able to attend 1 war a week | T53Discord & Chill Anti-Toxic Atmosphere| RBF & Arena | Max PvP Bufts, Max Lifeskill, +20%XP & Teleports For Trading  
Group/Merge/Returning Players Welcome! Zerkars Super Welcome!  
[Legendary\_Rorix] : rosar stall!  
[Mister Prince] : WTB [Warrior] Brut lancelet premium set

1279/6699

789/974

|    |     |     |     |     |     |     |     |       |     |     |     |     |
|----|-----|-----|-----|-----|-----|-----|-----|-------|-----|-----|-----|-----|
| 54 | 691 | 694 | 231 | 231 | 231 | 541 | 14  | 14    | 14  | 14  | 85  | 35  |
| HP | MP  | EXP | DEF | STR | AGI | INT | LUK | SKILL | WIS | CHA | RES | RES |

[Charlottezzy] : wo dou bu xiang quan ta gang jiu zai shua guai  
[Charlottezzy] : wexie 3  
[Reservation] : heq  
[Reservation] : shi xuan zhan gong hui ma  
[Charlottezzy] : en  
[Reservation] : ok wo qu kan kan  
[Charlottezzy] : wo xian ji xu shua guai le  
[Charlottezzy] : bu zhi dao na ren hai zai bu zai  
[Love Train] : 1111

[System] : Skill Unavailable (Cooldown Time)  
[System] : Skill Unavailable (Cooldown Time)  
[System] : Got Bash'rim 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)

[WIK] : Jesus Acking Christ  
[WIK] : CrazyFatJack, Boss Aik Killer Extraordinaire  
[WIK] : so stromk  
[MikoNK] : ik no loot  
[Kinoshee] : TRY HARDER  
[Boscan] : awd  
[Boscan] : aw  
[Boscan] : awd  
[Boscan] : wd  
[Medic] : ?

Black Spirit (.)



100 Попробуй попади  
Ор 1221109/1221109  
Нр 527511/527511  
Мр 58097/58097  
Vp



# LINEAGE

THE CHAOTIC THRONE



### Умения

Активные Пассивные Изучить умения

**Расовые умения**

- Последняя капля Ур. 1  
Пассивное умение  
При получении урона с определенной вероятностью увеличивает мощность умений и Защ. Щитом. Дополнительно СИЛ +2.

**Дополнительные**

**Умения**

Улучшить умение



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.

Holmtom: Спасия итем+ Хил ДД и гол  
EvillyRU: Куплю PvE или благой лайт шлем +8 зака: Меч Очарования?  
wex: втс ппв пояс на атаку  
ТанцовщицаСмерти: куплю Р сет лайт+8  
Eminens: продам благ аспадон фантазмы +11 2 са 300 атт пм  
FastHelp: ВТС  
Лоризелла: набор в молодой клан WarCrystal 90+ Варов и валков нет. Присоединяйся!  
willyblake:  
Набор в Клан Амбрелла 10млв Фул Скилы/Отряды.К  
Х\_Глд\_97(+\_Одетых\_по\_рангу\_ПМ,  
SannibalCorpse22: пати на тараса  
xGorn1kx: ВТСЛегендарная Краска Ур. 5 - ЛВК (Удача)  
?ДЕШЕВЛЕ  
FairTeX: ВТС P99 Благ Арбалет +12 2 СА!  
ShaFF: ВТБ двурк таугти (пм)  
МалышкаБуБу: Благословенный Бросок Алокалipsis[? за 740 кк отд

# APEX

— LEGENDS™ —

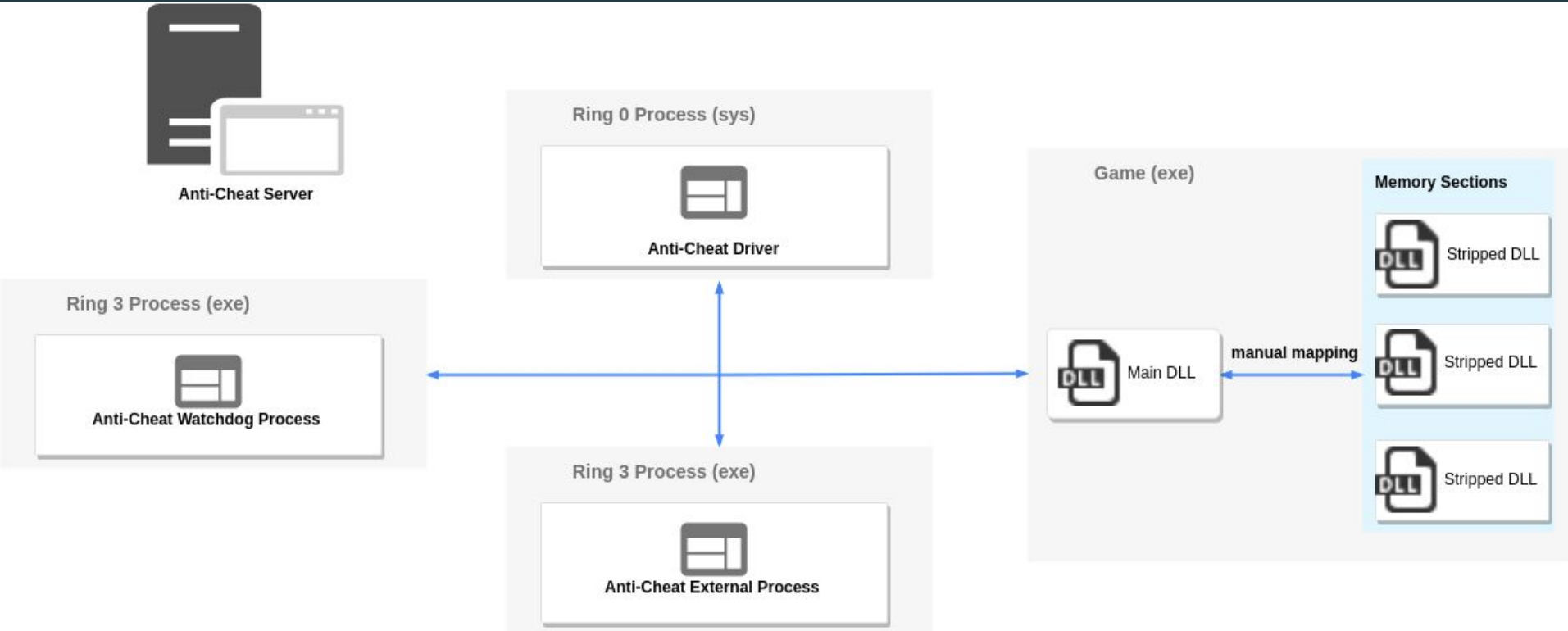




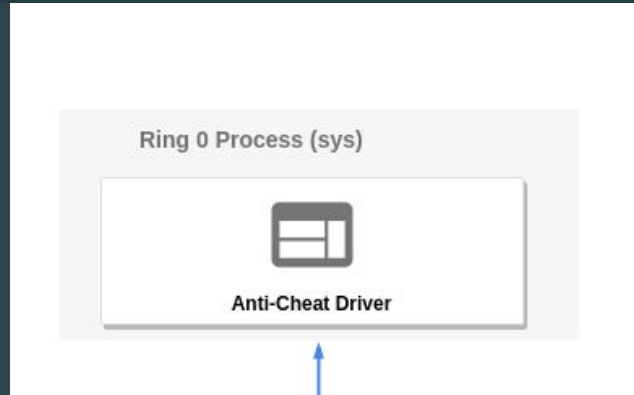
PLAYERUNKNOWN'S  
**BATTLEGROUNDS**



# Anti-Cheat Components



# Kernel Driver



[-] Handle stripping/Access Control

[-] Register kernel callbacks

[-] Rejection of Kernel/User mode debugging

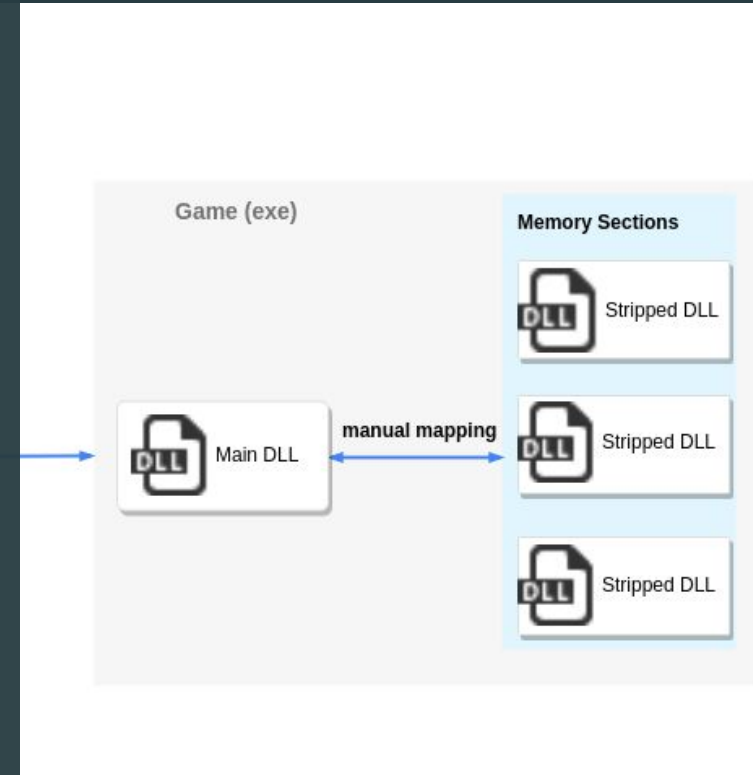
[-] Analysis of privileged process (lsass and csrss)

[-] 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

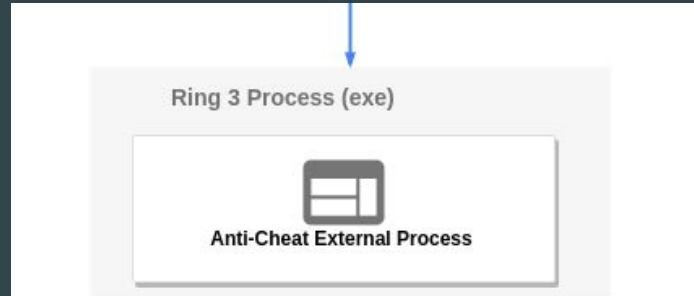
[•] Blacklisted programs  
detection

[•] Manage logic from Driver

[•] Control of game client and  
DLL hashes

[•] Multi-client detection

[•] Program integrity controls





# Cheats



# Internal (DLL) vs External (Process)

|          | Pros  | Cons  |
|----------|---|---|
| External | <ul style="list-style-type: none"><li>[•] Quick for small patches</li><li>[•] Easy to master</li><li>[•] Can be closed in certain cases</li></ul>           | <ul style="list-style-type: none"><li>[•] Slow</li><li>[•] Easy to detect</li><li>[•] Limited potential</li><li>[•] Requires a Handle (usually)</li></ul> |
| Internal | <ul style="list-style-type: none"><li>[•] Great performance</li><li>[•] Direct access to memory</li><li>[•] Hard to detect if you are good enough</li></ul> | <ul style="list-style-type: none"><li>[•] Hard to master</li><li>[•] Easier to detect if you mess it up</li></ul>   |



Wallhack/ESP



Aimbots

# Pro players getting caught? Why not



# Parallel Market

# Parallel Market

Cheat Prices:  
U\$\$ 1 to U\$\$25  
Some up to U\$\$500



Ex: 2500 paid members  
U\$\$ 10 \* 2500 = U\$\$25000  
(150000 memberships)

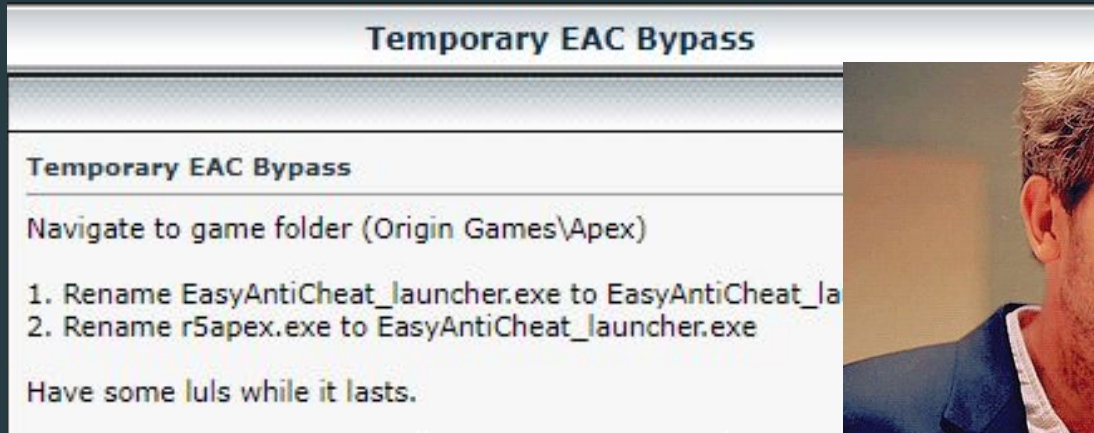
U\$\$ 1,25 M  
PER YEAR  
(Wait... what?)



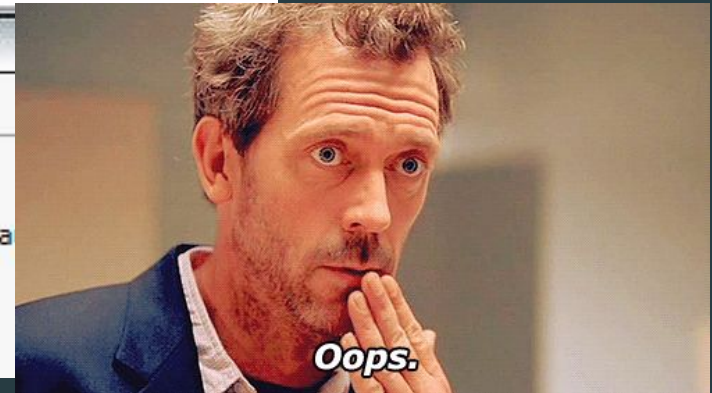
# Are they fighting back?

Apex claims:

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



<https://unknowncheats.me/>



# 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**

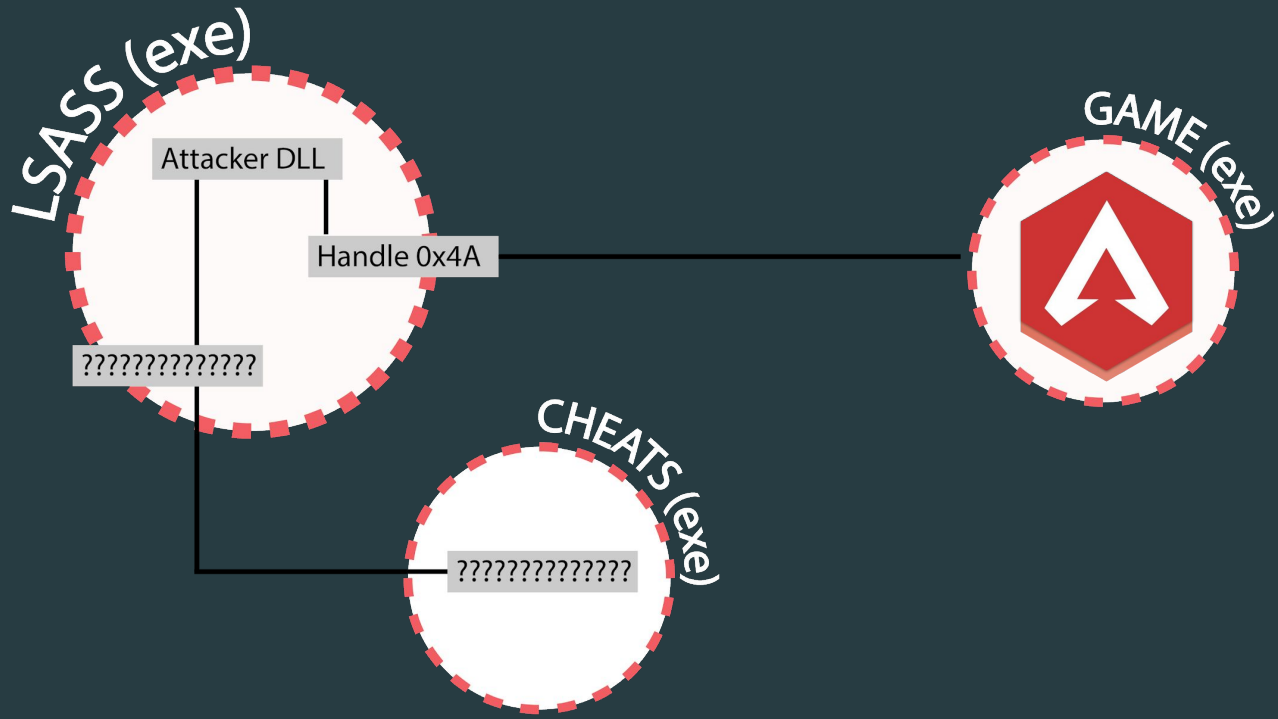
Hijacking techniques come to our rescue:

- [•] Handle Hijacking

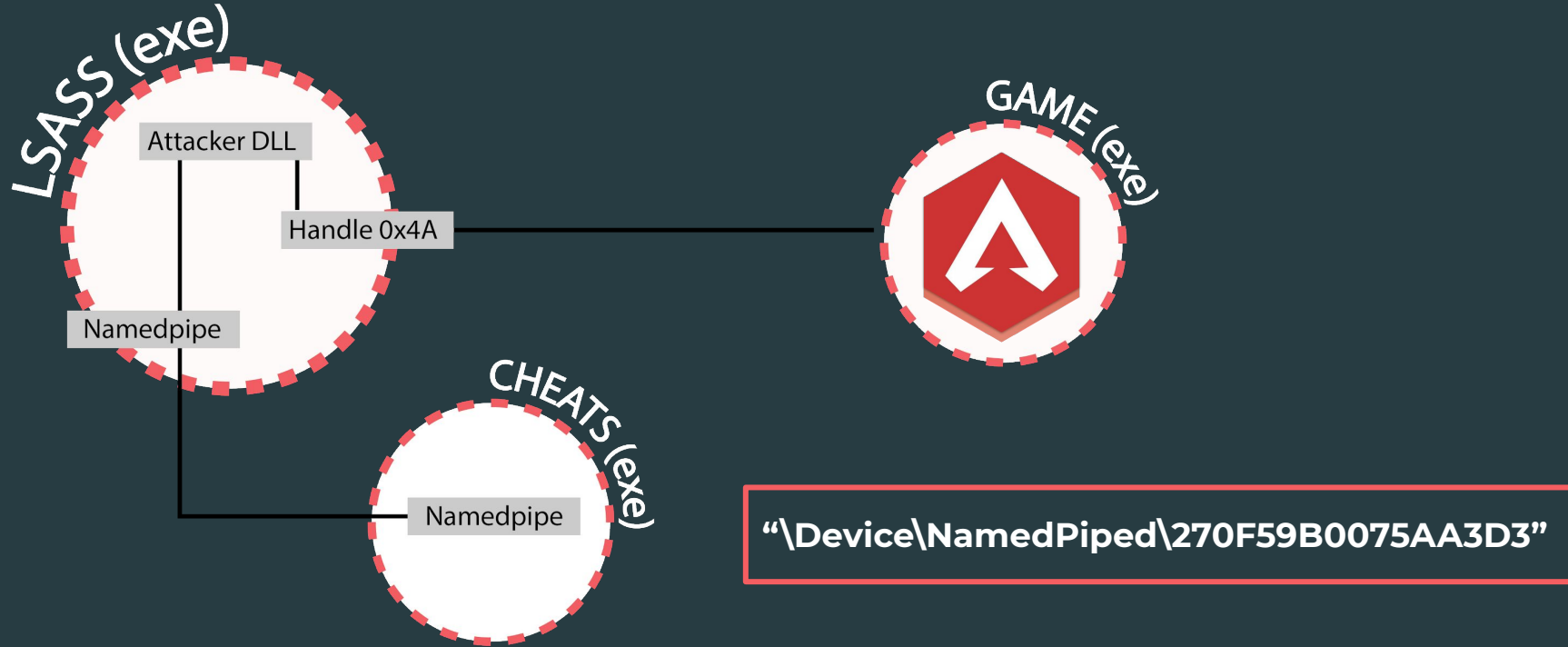
- [•] Stealth Handle Hijacking

- [•] Hooking

# Hijacking Techniques



# Hijacking Techniques - NamedPipe



0 (0.0%) 30 / 30 0 / 0 (0.00%)

1  
0.000%  
150 / 150  
100 / 100

```

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
  
```

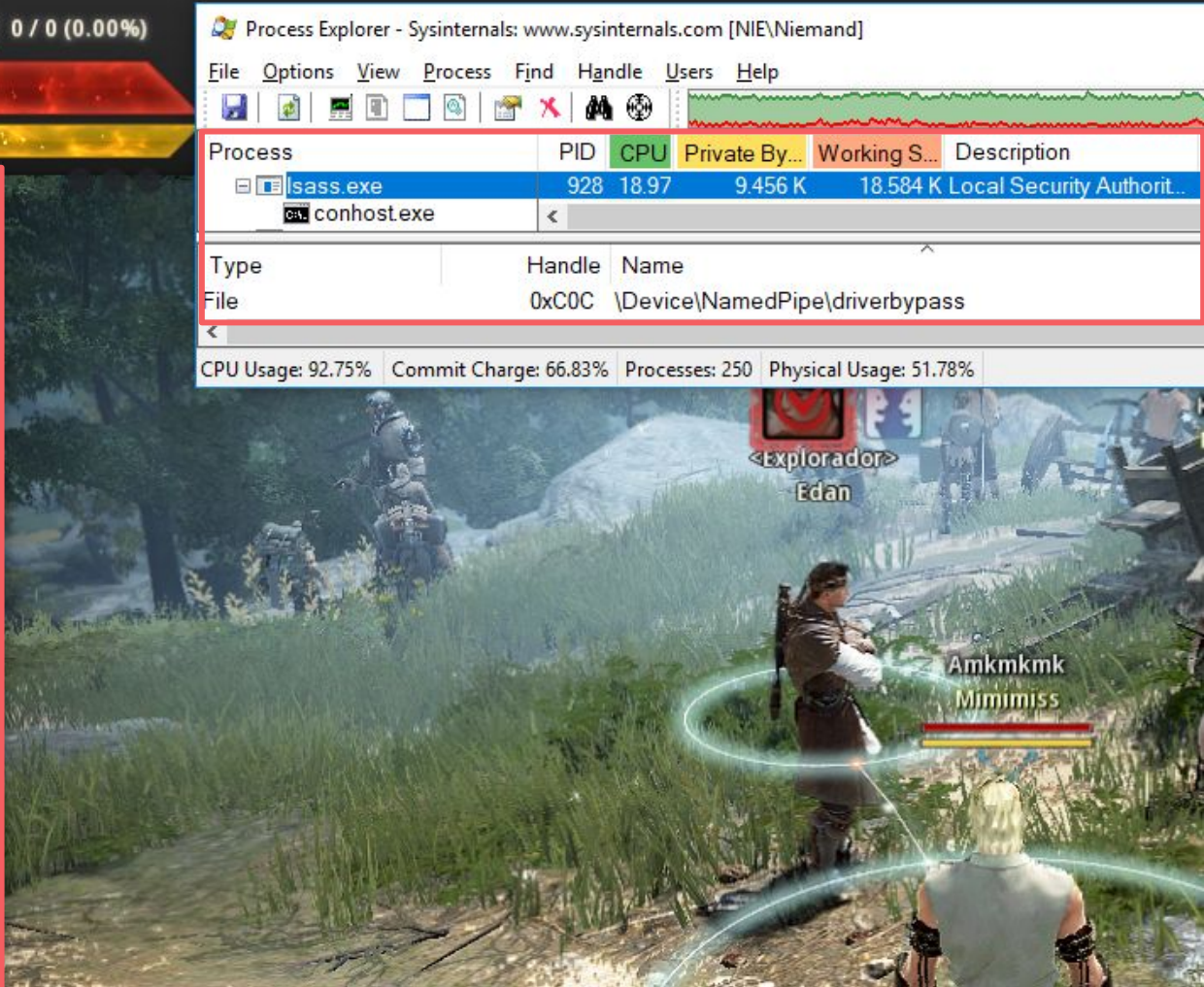
Process Explorer - Sysinternals: www.sysinternals.com [NIE\Niemand]

File Options View Process Find Handle Users Help

| 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

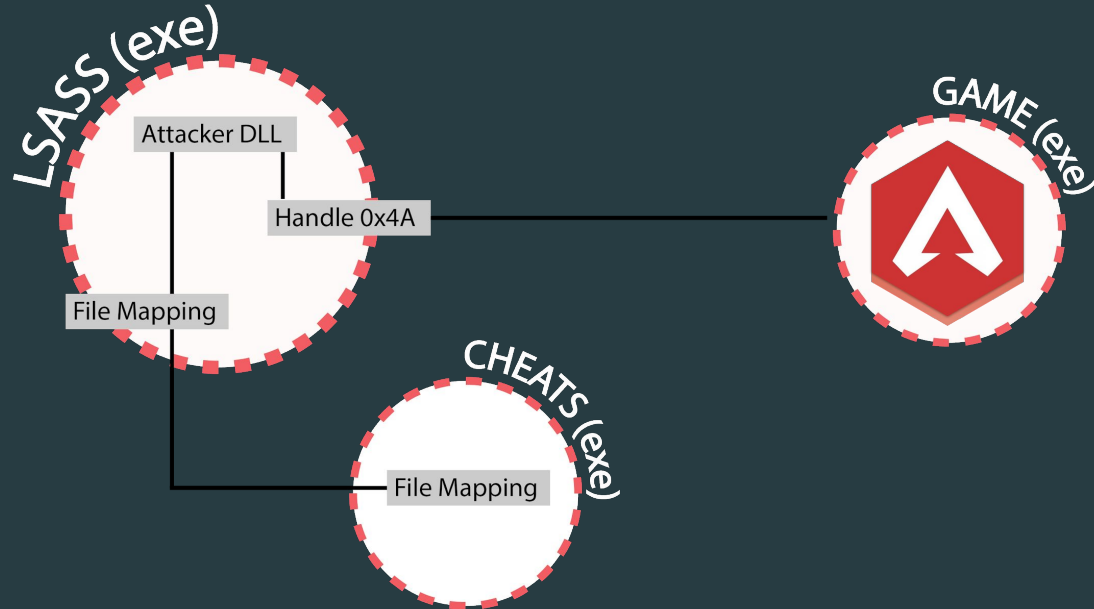
Hooks to  
user-mode  
WIN API

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”

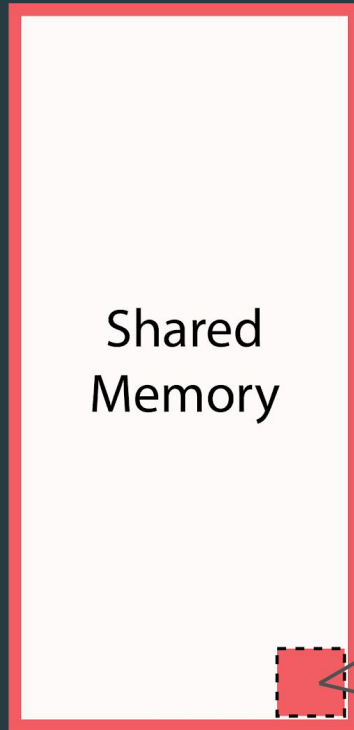
```
HANDLE CreateFileMappingA(  
    HANDLE          hFile,  
    LPSECURITY_ATTRIBUTES lpFileMappingAttributes,  
    DWORD          flProtect,  
    DWORD          dwMaximumSizeHigh,  
    DWORD          dwMaximumSizeLow,  
    LPCSTR         lpName  
);
```

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

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

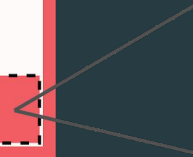


# Hijacking Techniques - FileMapping



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

Manual spinlocks to avoid mutex/semaphores HANDLES



0 (0.0%) 30 / 30 0 / 0 (0.00%)

1

0.000%

150 / 150

100 / 100

F:\Recon2019\AntiCheat-Testing...

```
[+] Waiting for pivot.
[+] Pivot Ready.
    [+] Status: Successful
[+] NtWriteVirtualMemory
[+] Waiting for pivot.
[+] Pivot Ready.
[+] Sending Msg:
    [+] action: 5
    [+] handle: 0x0000000000015FC
    [+] 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: 0x0000000000015FC
    [+] 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: 0x0000000000015FC
    [+] address: 0x58a60000
    [+] size: 6
    [+] buffer: 54 54 54 54 37 0
[+] Ready.
```

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

File Options View Process Find Handle Users Help

| 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   | \Sessions1\BaseNamedObjects                                 |
| File      | 0x4C   | F:\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

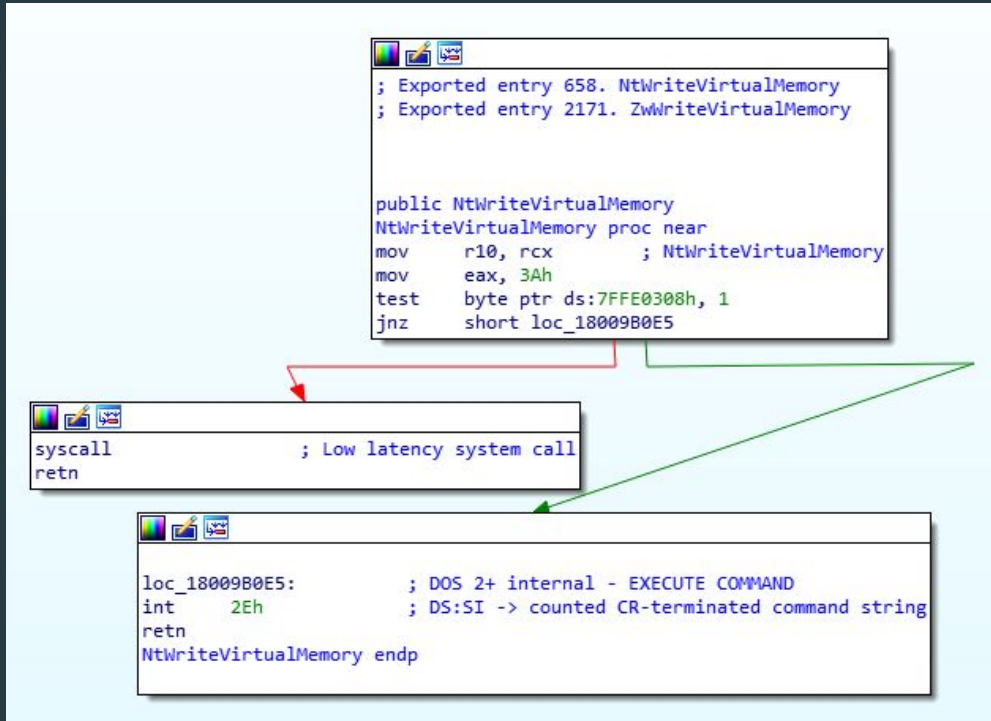
EAC also hook functions on **lsass.exe**:

```
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNEL32.DLL[ntdll.dll!NtAllocateVirtualMemory] [7fe3b0b20d4] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNEL32.DLL[ntdll.dll!NtReadVirtualMemory] [7fe3b0b22b8] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNELBASE.dll[ntdll.dll!NtReadVirtualMemory] [7fe3b0b22b8] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNELBASE.dll[ntdll.dll!NtWriteVirtualMemory] [7fe3b0b2480] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\System32\KERNELBASE.dll[ntdll.dll!NtAllocateVirtualMemory] [7fe3b0b20d4] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lsasrv.dll[ntdll.dll!NtAllocateVirtualMemory] [7fe3b0b20d4] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lsasrv.dll[ntdll.dll!NtWriteVirtualMemory] [7fe3b0b2480] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lsasrv.dll[ntdll.dll!NtReadVirtualMemory] [7fe3b0b22b8] C:\WINDOWS\system32\eac_usermode_466512274840.dll
C:\WINDOWS\system32\lsass.exe[928] @ C:\WINDOWS\system32\lschannel.DLL[ntdll.dll!NtAllocateVirtualMemory] [7fe3b0b20d4] C:\WINDOWS\system32\eac_usermode_466512274840.dll
```

Why?

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

# Hijacking Techniques - Bypass Hooks



```
ZwReadWriteVM.asm  X StealthHijackingNormalMaster.cpp  X
1  .code
2
3  ZwWriteVM proc
4      mov r10, rcx
5      mov eax, 3Ah
6      syscall
7      ret
8  ZwWriteVM endp
9
10 ZwReadVM proc
11     mov r10, rcx
12     mov eax, 3Fh
13     syscall
14     ret
15 ZwReadVM endp
16
17 end
```

# Hijacking Techniques - Bypass Hooks

## Disadvantages

Suspicious  
new  
HANDLEs

Hooks to  
user-mode  
WIN API

Thread with  
suspicious  
context

Downgrade  
of HANDLE  
privileges

# Hooking



# Hooking

**Hooking** Graphic Engines:

[•] IAT hooking

[•] JMPs on Prolog functions

What about 3rd party libraries?

[•] Steam Overlay

[•] Open Broadcaster Software





# Steam Overlay

|   |                  |                  |  |
|---|------------------|------------------|--|
| ● | 00007FFF27D2506F | CC               | int3                                       |
| ● | 00007FFF27D25070 | ▼ 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

**Redirects execution to gameoverlayrenderer64.dll:\$8A480**

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

# 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

**Redirects to graphics-hook64.7FFEB97AE4D0**

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

# 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 |
| ● | 00007FFEE50B1098 | 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

| 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

## GIGABYTE Driver

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

# EAC downgrading the HANDLE

| 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 |

# Driver - DKOM

1) Search for EPROCESS Struct in kernel

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

2) Obtain the ObjectTable (HANDLE\_TABLE)

3) Use ExpLookupHandleTableEntry(HandleTable, Handle)

4) Retrieve HANDLE

5) Modify GrantedAccess

6) Overwrite kernel memory

7) Profit



PLAY

LEGENDS

ARMORY

BATTLE PASS

STORE

15 0 0

2



ReClass.NET (x64) - Isass.exe -&gt; r5apex.exe (ID: 185049)

File Process Project Help

| Classes   | Enums           |
|-----------|-----------------|
| N0000004E |                 |
| 140000000 | Class N0000000  |
| 0000      | 000000014000000 |
| 0008      | 000000014000000 |
| 0010      | 000000014000001 |
| 0018      | 000000014000001 |
| 0020      | 000000014000002 |
| 0028      | 000000014000002 |
| 0030      | 000000014000003 |
| 0038      | 000000014000003 |

| Address          | Size             | Name    | Protection               | Type    | Module        |
|------------------|------------------|---------|--------------------------|---------|---------------|
| 0000000003F0000  | 0000000000010000 |         | Read, Write, CopyOnWrite | Private |               |
| 000000000400000  | 0000000000001000 |         | Read                     | Image   |               |
| 000000000401000  | 0000000000015000 | .text   | Read, CopyOnWrite        | Image   | XInput1_3.dll |
| 000000000416000  | 0000000000004000 | .data   | Read, Write              | Image   | XInput1_3.dll |
| 00000000041A000  | 0000000000004000 | .reloc  | Read                     | Image   | XInput1_3.dll |
| 000000006C49000  | 0000000000010000 |         | Read, Write, CopyOnWrite | Private |               |
| 000000006C4A000  | 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 |               |
| 00000054D8D98000 | 0000000000005000 |         | Read, Write              | Private |               |
| 00000054D8DA7000 | 0000000000003000 |         | Read, Write, Execute     | Private |               |
| 00000054D8DA7000 | 0000000000003000 |         | Read, Write              | Private |               |

Isass.exe -&gt; r5apex.exe (ID: 185049)

ReClass.NET - Process Informations

## Process Informations

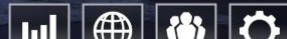
View informations about the current process.

Modules Sections

| Address          | Size             | Name    | Protection               | Type    | Module        |
|------------------|------------------|---------|--------------------------|---------|---------------|
| 0000000003F0000  | 0000000000010000 |         | Read, Write, CopyOnWrite | Private |               |
| 000000000400000  | 0000000000001000 |         | Read                     | Image   |               |
| 000000000401000  | 0000000000015000 | .text   | Read, CopyOnWrite        | Image   | XInput1_3.dll |
| 000000000416000  | 0000000000004000 | .data   | Read, Write              | Image   | XInput1_3.dll |
| 00000000041A000  | 0000000000004000 | .reloc  | Read                     | Image   | XInput1_3.dll |
| 000000006C49000  | 0000000000010000 |         | Read, Write, CopyOnWrite | Private |               |
| 000000006C4A000  | 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 |               |
| 00000054D8D98000 | 0000000000005000 |         | Read, Write              | Private |               |
| 00000054D8DA7000 | 0000000000003000 |         | Read, Write, Execute     | Private |               |
| 00000054D8DA7000 | 0000000000003000 |         | Read, Write              | Private |               |

PLAY APEX

READY





# Refresher- Bypass Hooks

## Disadvantages

Suspicious  
new  
HANDLEs

Hooks to  
user-mode  
WIN API

Thread with  
suspicious  
context

Downgrade  
of HANDLE  
privileges

One Last  
**Attempt**

# Driver - Just do it from kernel!

- 1) Leak handle pointers using NtQuerySystemInformation  
`SystemExtendedHandleInformation (0x40)` as `SYSTEM_INFORMATION_CLASS`
- 2) Locate valid KPROCESS pointer  
`_KPROCESS.Header == 0x00B60003`
- 3) Traverse linked list -> `_EPROCESS.ActiveProcessLinks`
- 4) Obtain DirectoryBaseTable -> `_EPROCESS.PEB.DirectoryBaseTable`
- 5) Obtain target Base Address -> `_EPROCESS.SectionBaseAddress`
- 6) Dereference Ring3 virtual addresses
- 7) Directly modify/read memory

**DEMO**

What about the  
tools?

Classes

- N0000004E
- Enums

```

1EC13CF0000 Class N0000004E [1088] //
0000 000001EC13CF0000 ..... 00 00 00 00 00 00 00 // 0.000 0
0008 000001EC13CF0008 P9.H... 50 39 F1 48 F4 E4 00 01 // 494026.500 72309331884849488 0x100E4F448F13950
0010 000001EC13CF0010 ..... EE FF EE FF 01 00 00 // ##### 8588820462 0x1FFEEFFEE
0018 000001EC13CF0018 ..... 20 01 CF 13 EC 01 00 00 // 0.000 2113456242976 0x1EC13CF0120
0020 000001EC13CF0020 ..... 20 01 CF 13 EC 01 00 00 // 0.000 2113456242976 0x1EC13CF0120
0028 000001EC13CF0028 ..... 00 00 CF 13 EC 01 00 00 // 0.000 2113456242688 0x1EC13CF0000
0030 000001EC13CF0030 ..... 00 00 CF 13 EC 01 00 00 // 0.000 2113456242688 0x1EC13CF0000
0038 000001EC13CF0038 ..... 10 00 00 00 00 00 00 // 0.000 16 0x10
0040 000001EC13CF0040 ..... 20 07 CF 13 EC 01 00 00 // 0.000 2113456244512 0x1EC13CF0720
0048 000001EC13CF0048 ..... 00 00 D0 13 EC 01 00 00 // 0.000 2113456308224 0x1EC13D00000
0050 000001EC13CF0050 ..... 0F 00 00 00 01 00 00 // 0.000 4294967311 0x10000000F
0058 000001EC13CF0058 ..... 00 00 00 00 00 00 00 // 0.000 0
  
```

### ReClass.NET - Process Informations

#### Process Informations

View informations about the current process.

Modules Sections

| Module               | Address          | Size             | Path  |
|----------------------|------------------|------------------|---|
| ntdll.dll            | 00007FFCBCE50000 | 00000000001D1000 | C:\Windows\SYSTEM32\ntdll.dll   |
| KERNEL32.DLL         | 00007FFCBB600000 | 00000000000AB000 | C:\Windows\System32\KERNEL32.DLL  |
| KERNELBASE.dll       | 00007FFCB93E0000 | 000000000021D000 | C:\Windows\System32\KERNELBASE.dll  |
| apphelp.dll          | 00007FFCB7940000 | 000000000007A000 | C:\Windows\system32\apphelp.dll   |
| combase.dll          | 00007FFCBB330000 | 00000000002C7000 | C:\Windows\System32\combase.dll   |
| ucrtbase.dll         | 00007FFCB9F80000 | 00000000000F5000 | C:\Windows\System32\ucrtbase.dll  |
| RPCRT4.dll           | 00007FFCBA3E0000 | 0000000000121000 | C:\Windows\System32\RPCRT4.dll  |
| bcryptPrimitives.dll | 00007FFCB9600000 | 000000000006A000 | C:\Windows\System32\bcryptPrimitives.dll                                      |
| vccorlib140_app.DLL  | 00007FFC96D20000 | 0000000000058000 | C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.27323.0_x64__8we... |

# Black Hat Sound Bytes

- [•] Fight at kernel level vs Trivial Bypasses
- [•] Blacklisting all drivers is impossible
- [•] Compatibility with Windows and 3rd applications is a problem

# Open Source Projects

## ReClass Plugin - Driver Reader



niemand-sec/ReClass.NET-DriverReader

## AntiCheat-Testing-Framework



niemand-sec/AntiCheat-Testing-Framework

- [•] CheatHelper & DriverHelper
- [•] DriverDisabler & Synapse Driver exploit (Razer)
- [•] HandleHijackingDLL and HandleHijackingMaster
  - [•] NamePipes and FileMapping
- [•] WinApi Hooking Bypass & Lua Hooking
- [•] Handle Elevation and External Driver



# THANK YOU!



@niemand\_sec



[niemand-sec/AntiCheat-Testing-Framework](#)



[niemand-sec/ReClass.NET-DriverReader](#)