大吉大利 今晚吃雞

論FPS遊戲外掛的愛與恨

Kenny @ chroot.org

About me

- Team T5 Senior Researcher
- Chroot Member / HackStuff Member
- Hitcon 2013 speaker
- Hitcon 2017 training

緣起

- 有趣，又極富挑戰性
- 遊戲外掛是我的初衷
- 不建議破壞
  別人遊戲體驗
- 開掛當神仙?

Agenda

01 PUBG 遊戲介紹

02 遊戲外掛原理與實作

03 修改 Unreal Engine 虛幻遊戲引擎

04 分析反外掛系統與 Intel 虛擬化技術

01 PUBG 遊戲介紹

PUBG (絕地求生)，暱稱吃雞

PUBG是一款以 一局100人的大逃殺生存射擊遊戲，在推出後爆紅大受歡迎，2017全盛時期有300萬人同時線上競賽。

吃雞是冠軍的標誌

吃雞的典故


PLAY 100 CREDITS
5 Quick Hit Jackpots
PAY LINES
20
LINE BET
1
WIN PAID
0
1¢
CREDIT
0
TOTAL BET
20


WINNER! WINNER!
CHICKEN DINNER!

外掛為何抓不完?

技術面:

FPS遊戲，本機運算佔大多數(伺服器負荷量)，所以可透過本機修改來影響伺服器上的資料。

- 改人物座標 => 飛天遁地
- 改人物骨骼 => 魯夫橡膠人
- 改敵人座標 => 吸星大法

外掛為何抓不完?

利益面:

一個帳號要台幣800左右,
但被封鎖的外掛帳號已超過百萬...

猜一個月外掛多少錢??

利益夠大，殺頭生意有人做，被鎖包賠帳號服務

外掛為何抓不完?

開設神仙專區:

- 開掛被發現,強制送到此處永不得翻身.
- 測試誰的掛仙力爆表.

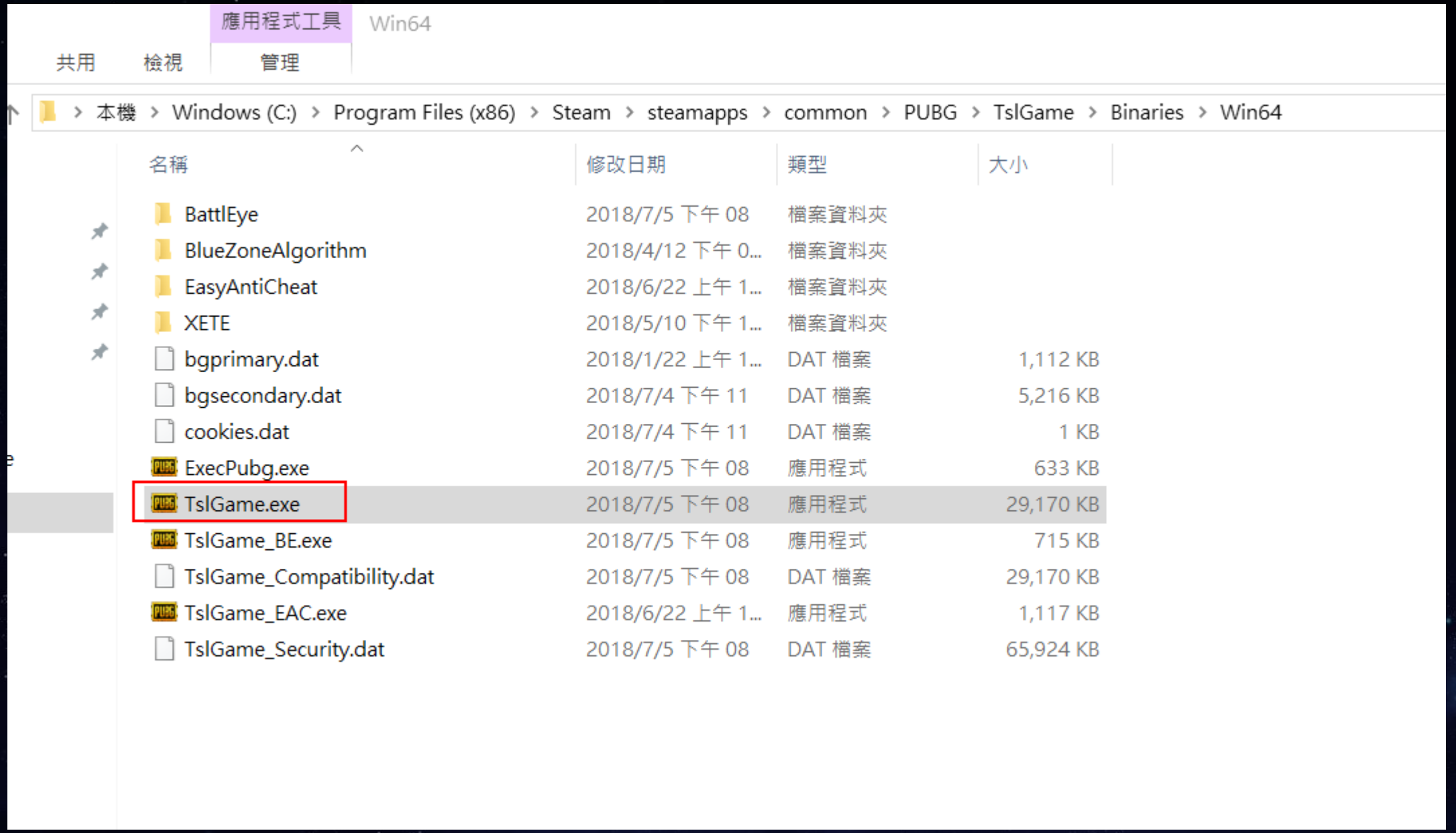
02 遊戲外掛原理與實作

萬事起頭難 – 通用的分析方法

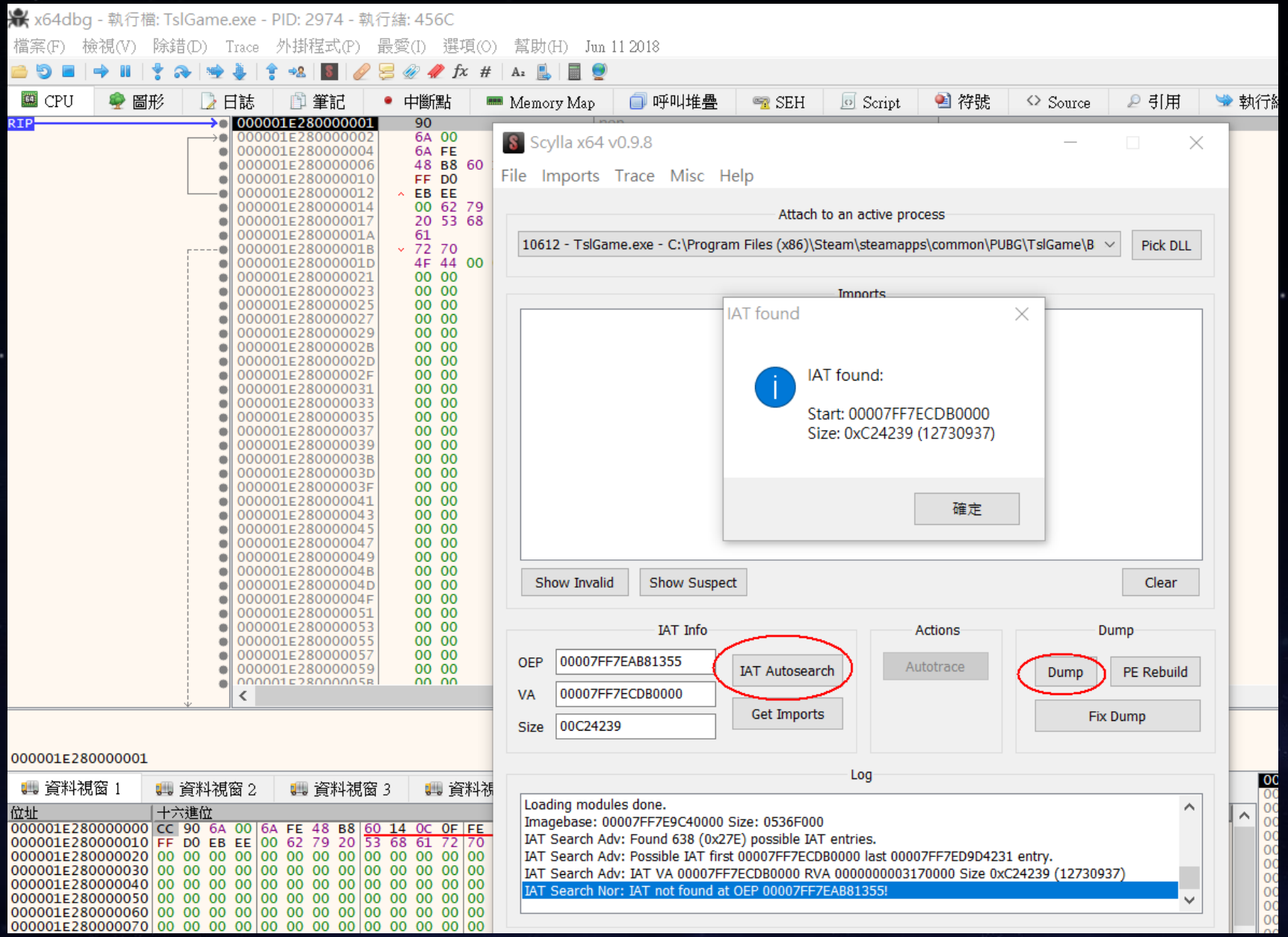
靜態分析 - Dump Memory + IDA分析

- 遊戲主程式加殼?
- 遊戲反作弊保護?

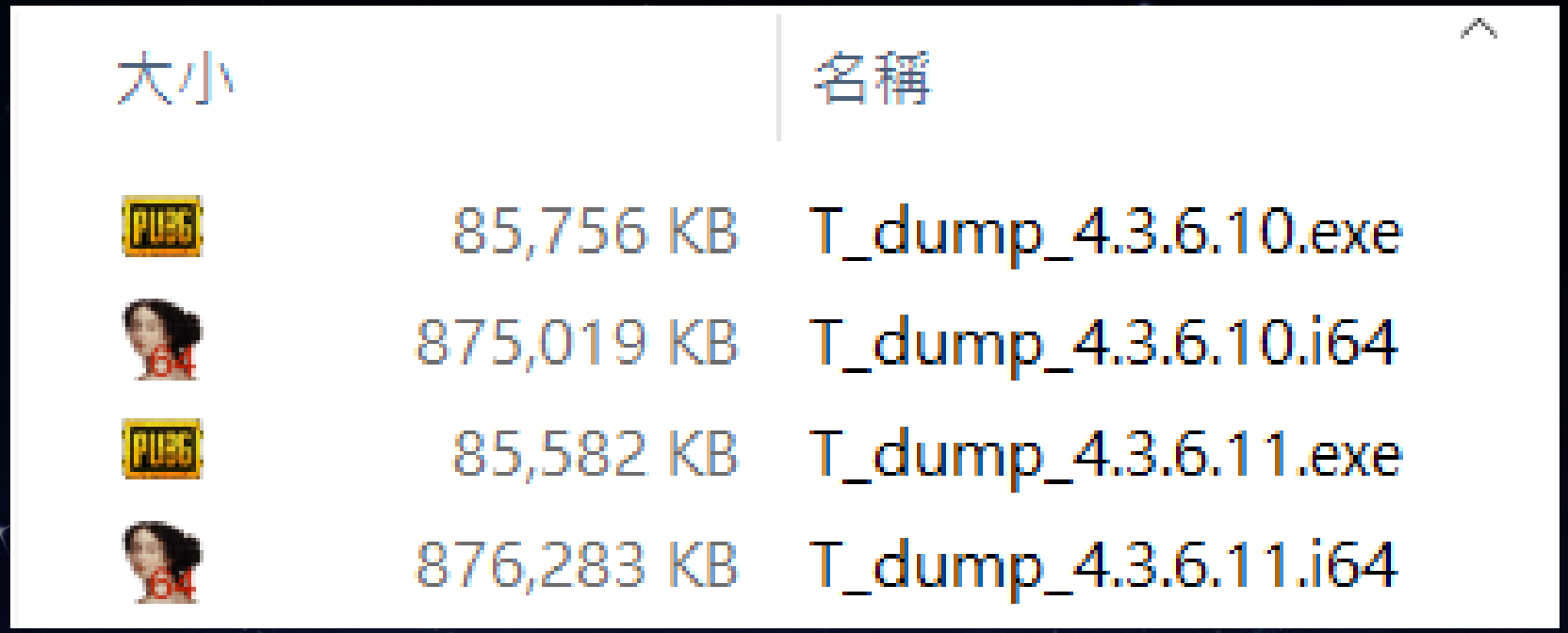
直接開啟法(不透過Steam)



X64Dbg + Scylla 插件



X64Dbg + Scylla 插件



快快樂樂的IDA時間?

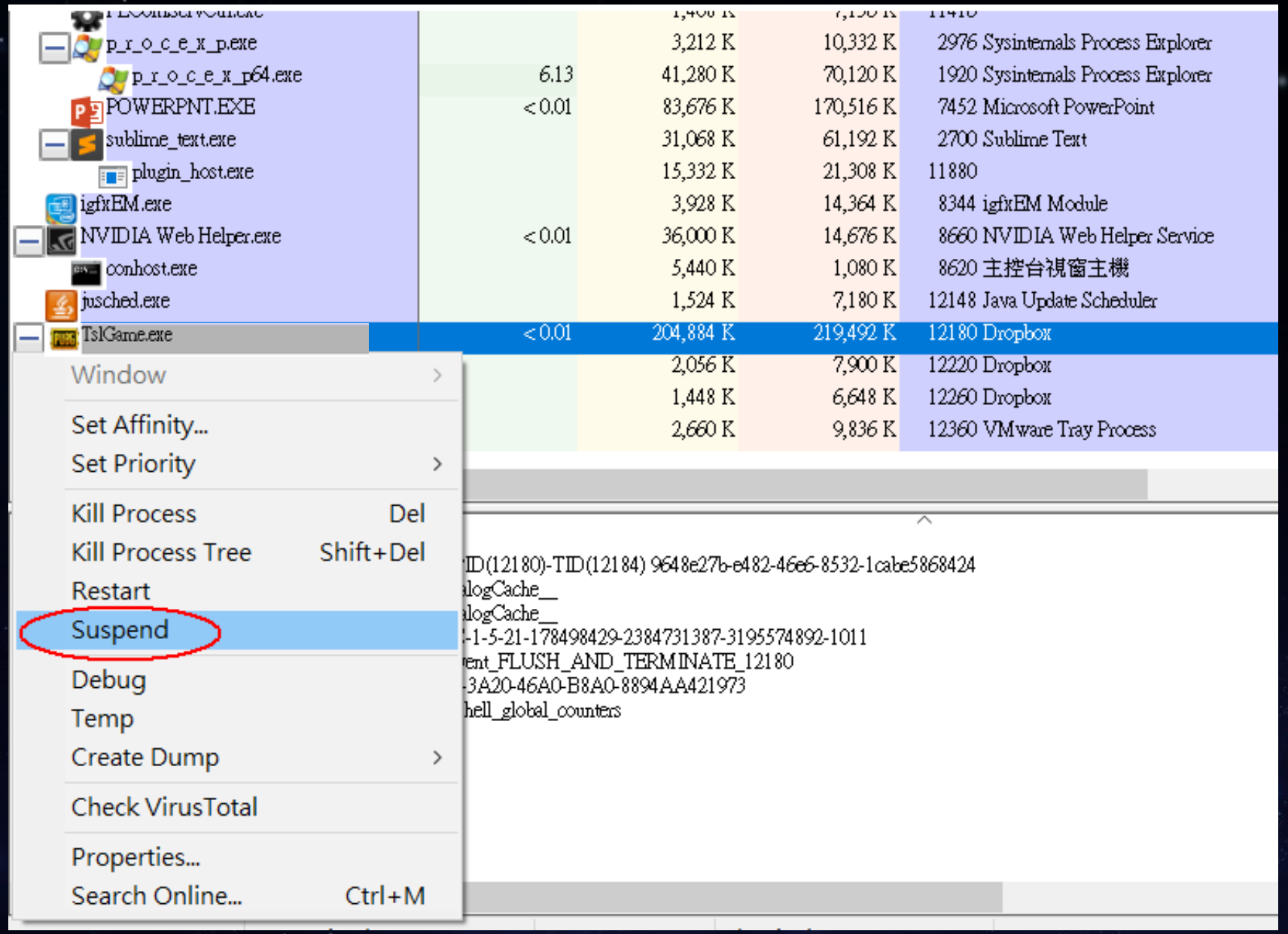
萬事起頭難 – 通用的分析方法

動態分析 – 不會被偵測的外掛開發環境

- Q: 想輕鬆的讀取遊戲記憶體?
- Q: 遊戲反作弊保護?

Process Suspend 大法

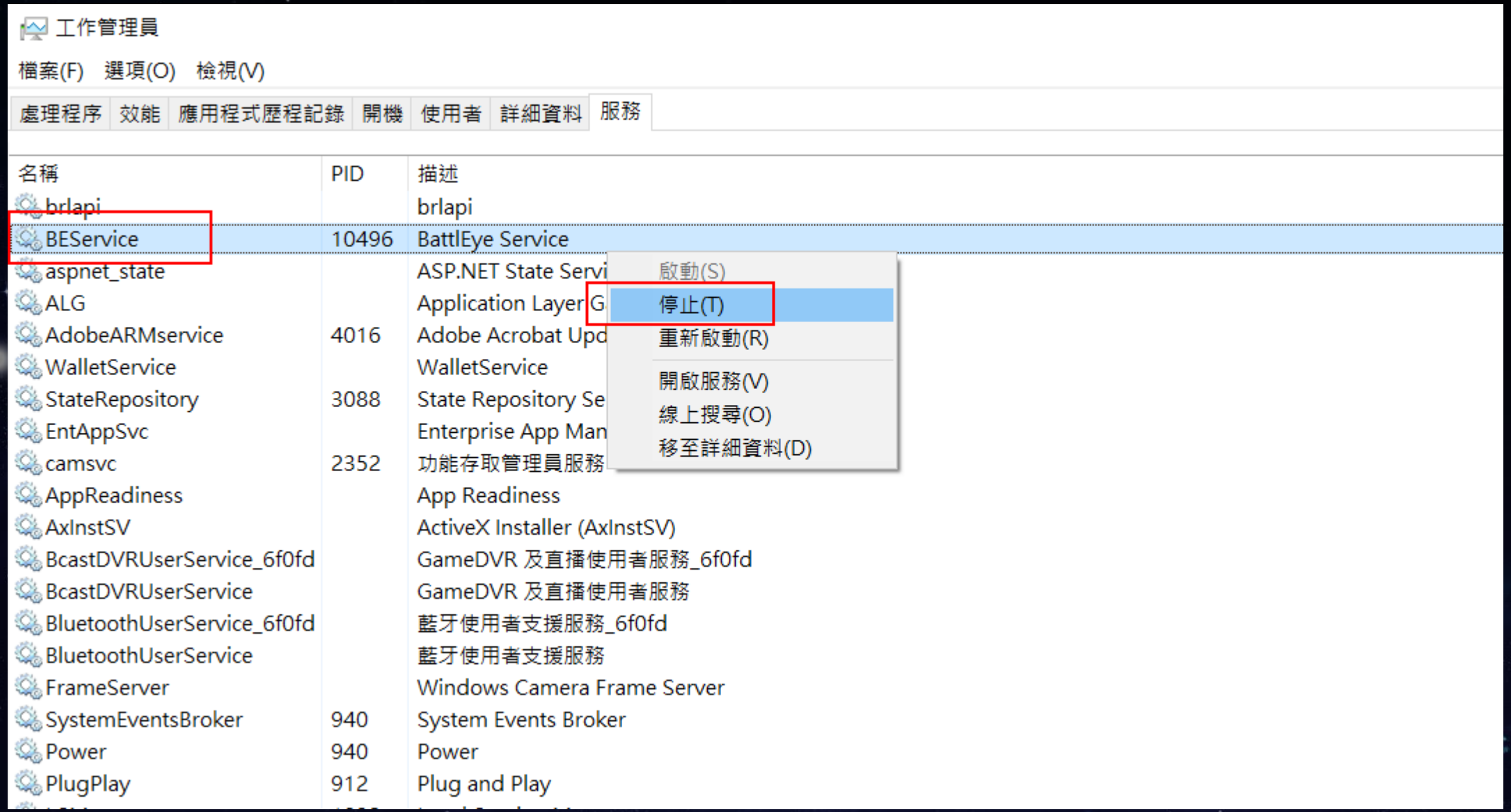
Process Suspend 大法



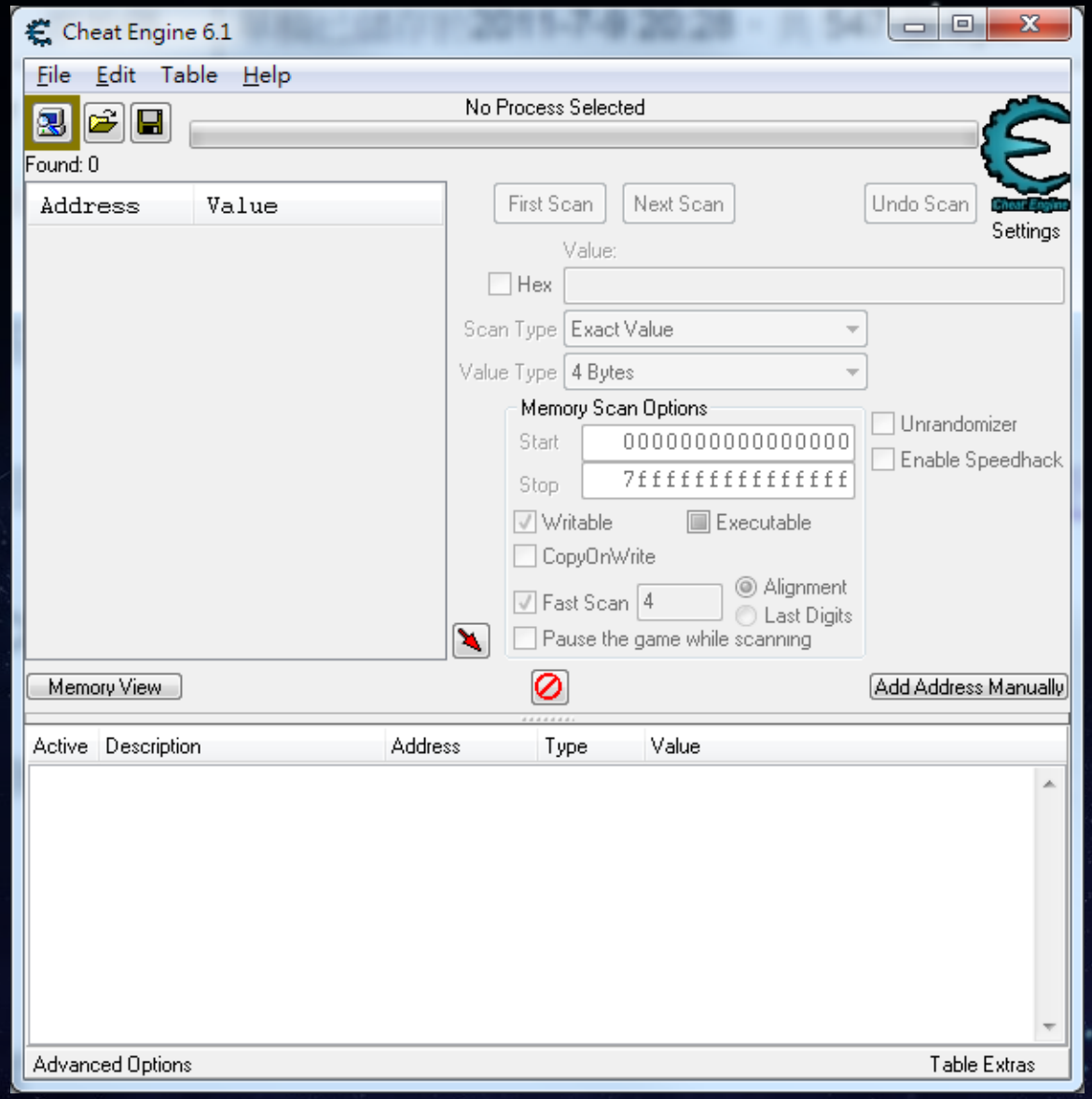
Process Suspend 大法

p_r_o_c_e_x_p.exe		3,352 K	10,356 K	2976 Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	0.67
p_r_o_c_e_x_p64.exe	6.61	41,008 K	68,884 K	1920 Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	0.67
Steam.exe	1.20	57,276 K	83,252 K	8692 Steam Client Bootstrapper	Valve Corporation	0.64
steamwebhelper.exe	0.01	15,260 K	37,492 K	2064 Steam Client WebHelper	Valve Corporation	0.65
steamwebhelper.exe		11,580 K	19,492 K	9368 Steam Client WebHelper	Valve Corporation	0.65
steamwebhelper.exe		21,768 K	37,356 K	11540 Steam Client WebHelper	Valve Corporation	0.65
steamwebhelper.exe		14,932 K	24,220 K	11364 Steam Client WebHelper	Valve Corporation	0.65
TslGame_BE.exe		5,492 K	31,340 K	5220 BattlEye Launcher	BattlEye Innovations	0.68
GameOverlayUI.exe	0.20	29,056 K	26,540 K	2244 gameoverlayui.exe	Valve Corporation	0.68
igfxEM.exe		4,052 K	14,452 K	8344 igfxEM Module	Intel Corporation	0.64
NVIDIA Web Helper.exe	< 0.01	38,276 K	20,000 K	8660 NVIDIA Web Helper Service	Node.js	0.67
conhost.exe		5,468 K	740 K	8620 主控台視窗主機	Microsoft Corporation	0.64
jusched.exe		1,736 K	7,248 K	12148 Java Update Scheduler	Oracle Corporation	0.68
Dropbox.exe	< 0.01	138,980 K	147,484 K	12180 Dropbox	Dropbox, Inc.	0.64
Dropbox.exe		2,132 K	7,828 K	12220 Dropbox	Dropbox, Inc.	0.64
Dropbox.exe		1,524 K	6,624 K	12260 Dropbox	Dropbox, Inc.	0.64
vmware-tray.exe		2,736 K	9,828 K	12360 VMware Tray Process	VMware, Inc.	0.66
TslGame.exe	Suspended	668,472 K	561,540 K	11856 TslGame	Bluehole GinnoGames, Inc.	0.68

Process Suspend 大法



Process Suspend 大法



萬事起頭難 – Kernel Driver 開發?

- 沒錢買驅動簽章..QQ
- 開啟 Windows 測試模式
  - 遊戲保護不給玩遊戲...

濫用數位簽章程式

01 找出有數位簽章，並有弱點可濫用的程式

02 載入有弱點的驅動程式進 Kernel

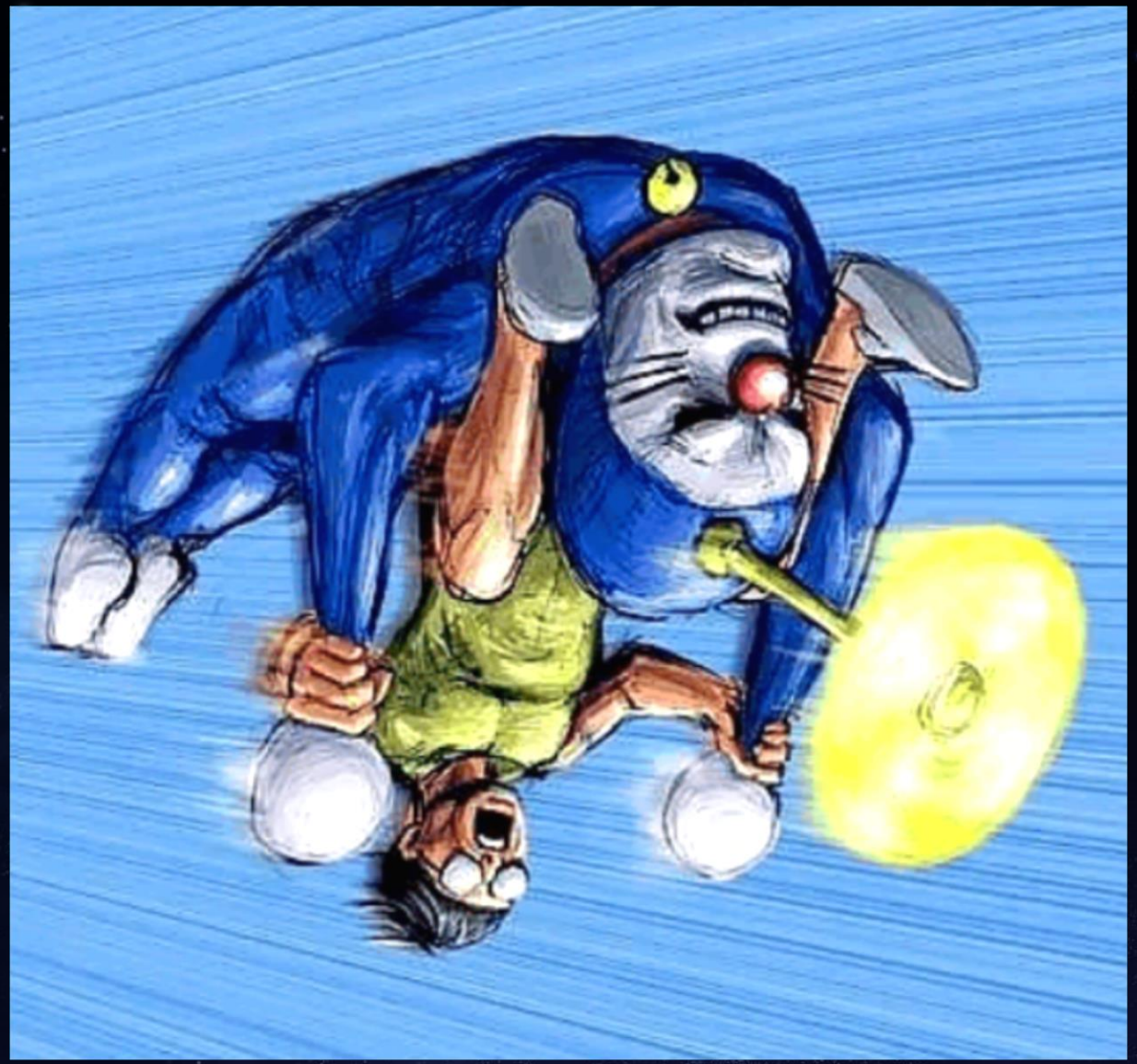
03 修改 Kernel Windows 簽章檢查

(CI.DLL!g_CiEnabled)

(CI.DLL!g_**CiOptions**)

04 載入未簽署的驅動，Hacking for fun.

坐時光機 回去2013年 =>Hitcon Talk 講過

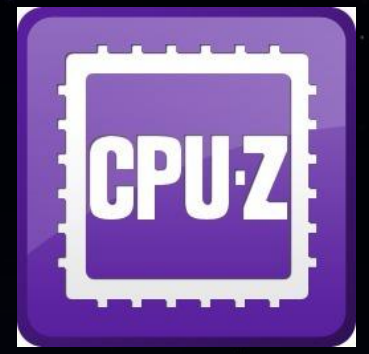


坐時光機 回來2018年 => 依然好用

Exploit Driver

CAPCOM®

很好用的 Rootkit Driver



CPU 偵測軟體 CVE 2017-15303

VirtualBox 知名虛擬機軟體

GitHub

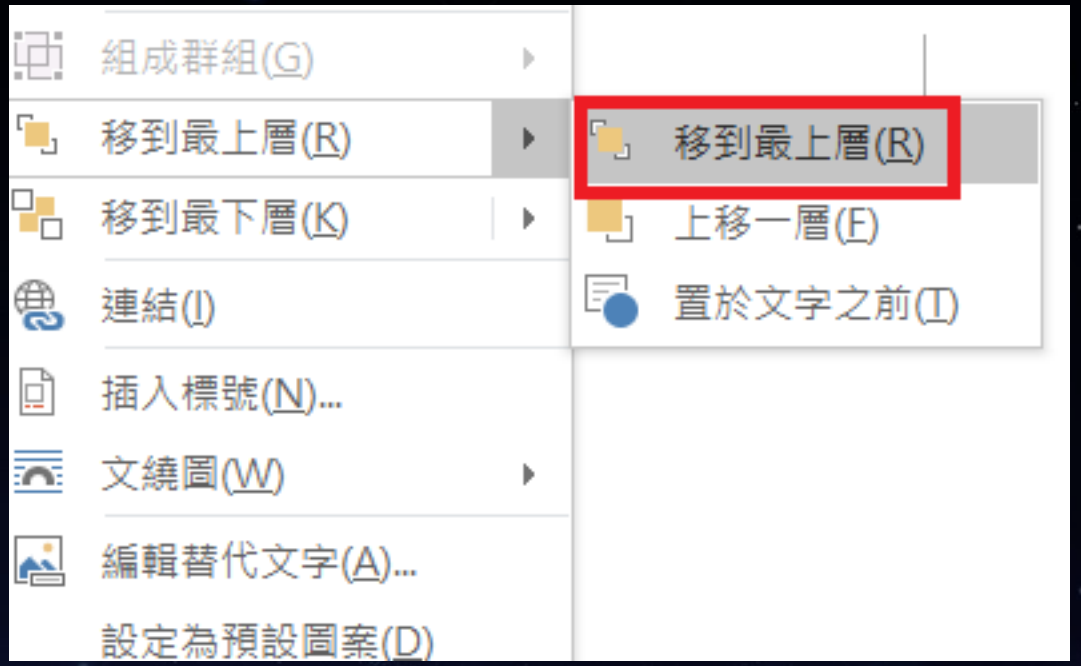
全世界最大的男性交友平台


WITH GREAT POWER COMES
GREAT RESPONSIBILITY

遊戲透視原理

DirectX（Direct eXtension，縮寫：DX）是由微軟公司建立的一系列專為多媒體以及遊戲開發的應用程式介面。DirectX被廣泛用於Microsoft Windows、Microsoft Xbox電子遊戲開發。

遊戲透視原理 – Internel Hack



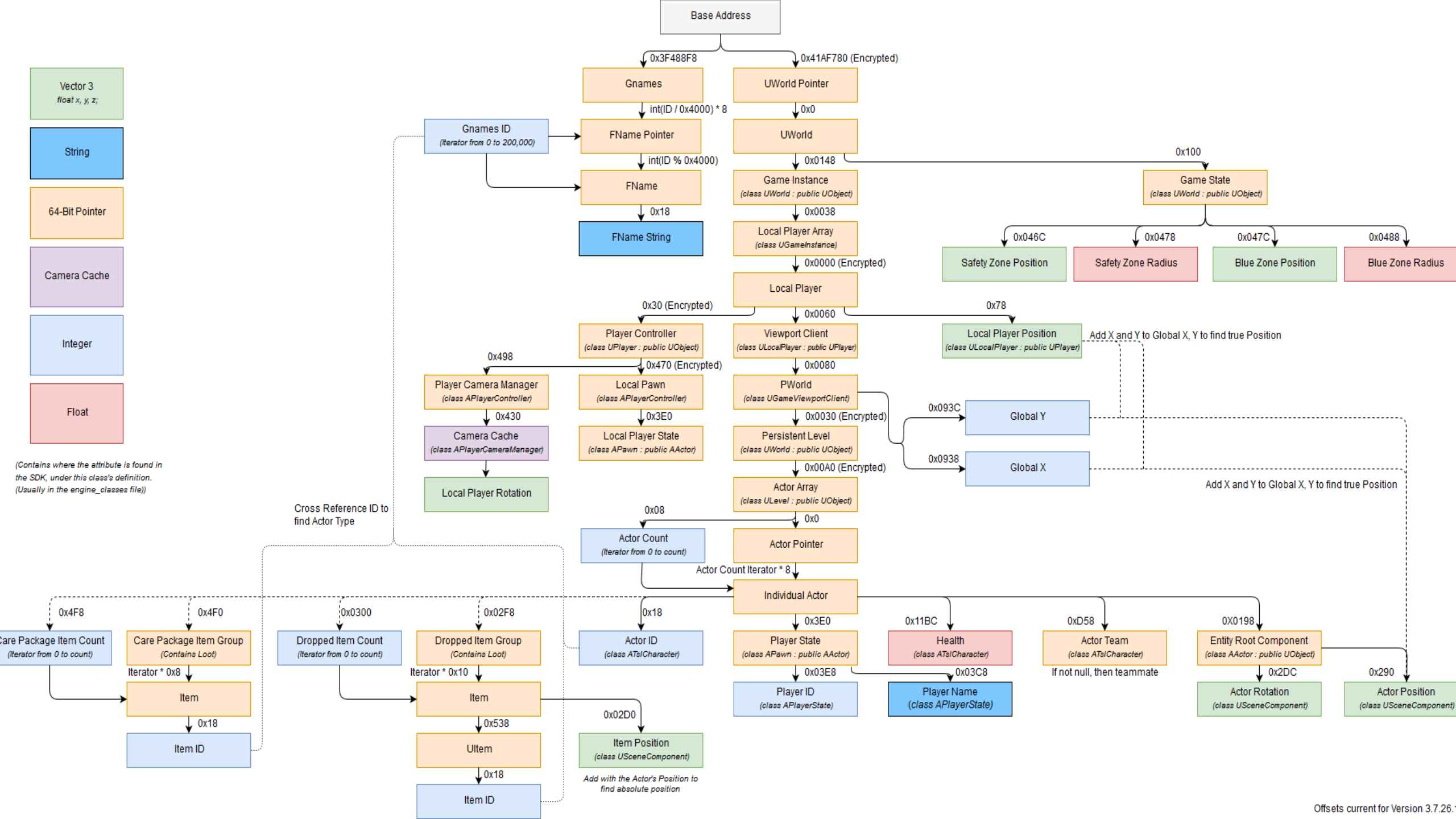
- 將外掛 dll 注入遊戲 Process
- Hook DirectX 函數 [需遊戲支援]
  - DrawIndexedPrimitive
    - 繪製人物模型時
      調整顯示順序(Z軸)
    - SetRenderState(D3DRS_ZENABLE, FALSE);
    - 不是所有人都用過DirectX，但你一定用過Word

神奇的傳送門:https://github.com/iCollin/pubg-internal

遊戲透視原理 – Externel Hack

- 獨立的 Process [不須注入遊戲]
- 建立透明視窗覆蓋在遊戲之上
  - 可劫持現有的 process
    - Ex: 記事本 / Nvidia Experience
- 記憶體讀取遊戲資訊
  - 人物座標 / 物品座標 …
- 將遊戲資訊透過 DirectX 函數繪製在透明視窗上

神奇的傳送門: https://github.com/codectile/crappy-esp


Vector 3
float x, y, z;
String
64-Bit Pointer
Camera Cache
Integer
Float
(Contains where the attribute is found in the SDK, under this class's definition. (Usually in the engine_classes file))
Base Address
0x3F488F8
0x41AF780 (Encrypted)
Gnames
UWorld Pointer
int(ID / 0x4000) * 8
0x0
Gnames ID
(Iterator from 0 to 200,000)
FName Pointer
UWorld
int(ID % 0x4000)
0x0148
0x100
FName
Game Instance
(class UWorld : public UObject)
Game State
(class UWorld : public UObject)
0x18
0x0038
FName String
Local Player Array
(class UGameInstance)
0x046C
0x0478
0x047C
0x0488
Safety Zone Position
Safety Zone Radius
Blue Zone Position
Blue Zone Radius
0x0000 (Encrypted)
Local Player
0x30 (Encrypted)
0x0060
0x78
Player Controller
(class UPlayer : public UObject)
Viewport Client
(class ULocalPlayer : public UPlayer)
Local Player Position
(class ULocalPlayer : public UPlayer)
Add X and Y to Global X, Y to find true Position
0x498
0x470 (Encrypted)
0x0080
Player Camera Manager
(class APlayerController)
Local Pawn
(class APlayerController)
PWorld
(class UGameViewportClient)
0x093C
Global Y
0x430
0x3E0
0x0030 (Encrypted)
Camera Cache
(class APlayerCameraManager)
Local Player State
(class APawn : public AActor)
Persistent Level
(class UWorld : public UObject)
0x0938
Global X
Local Player Rotation
0x00A0 (Encrypted)
Add X and Y to Global X, Y to find true Position
Actor Array
(class ULevel : public UObject)
Cross Reference ID to find Actor Type
0x08
0x0
Actor Count
(Iterator from 0 to count)
Actor Pointer
Actor Count Iterator * 8
Individual Actor
0x4F8
0x4F0
0x0300
0x02F8
0x18
0x3E0
0x11BC
0xD58
0X0198
Care Package Item Count
(Iterator from 0 to count)
Care Package Item Group
(Contains Loot)
Dropped Item Count
(Iterator from 0 to count)
Dropped Item Group
(Contains Loot)
Actor ID
(class ATslCharacter)
Player State
(class APawn : public AActor)
Health
(class ATslCharacter)
Actor Team
(class ATslCharacter)
Entity Root Component
(class AActor : public UObject)
Iterator * 0x8
Iterator * 0x10
If not null, then teammate
0x03E8
0x03C8
0x2DC
0x290
Item
Item
Player ID
(class APlayerState)
Player Name
(class APlayerState)
Actor Rotation
(class USceneComponent)
Actor Position
(class USceneComponent)
0x18
0x02D0
0x538
Item ID
Item Position
(class USceneComponent)
UItem
Add with the Actor's Position to find absolute position
0x18
Item ID
Offsets current for Version 3.7.26.1

How to Find Offset?

伸手黨

Unknown Cheats - 遊戲外掛論壇

https://www.unknowncheats.me/forum/playerunknown-s-battlegrounds/214976-pubg-structs-offsets.html


人生最厲害
就是這個
BUT!

Pubg - 六小時 patch 一次

```
LODWORD(v0) = sub_7FF7EBF64920();
v1 = v0;
if ( !v0
  || ((LODWORD(v2) = sub_7FF7EC1075F0(),
       v3 = __ROR8__(*(_QWORD *)(v1 + 8) ^ 0xFC000EBF4B6617FAui64, 1),
       v4 = v2 + 232,
       v5 = *(_DWORD *)(v2 + 240),
       (signed int)v5 > *(_DWORD *)((v3 ^ (v3 << 32) ^ 0xAD04D45AF02DE46Aui64) + 0xF0))
   || *(_QWORD *)(*(_QWORD *)((v3 ^ (v3 << 32) ^ 0xAD04D45AF02DE46Aui64) + 0xE8) + 8 * v5) != v4 ? (v6 = 0) : (v6 = 1),
      !v6) )
{
  v1 = 0i64;
LABEL_13:
  LOBYTE(v14) = 0;
  goto LABEL_14;
}
v7 = __ROL4__(*(_DWORD *)(v1 + 16) ^ 0x5D293031, 1);
v8 = v7 ^ (v7 << 16) ^ 0xB2BA0EBA;
if ( (signed int)v8 >= (signed int)qword_7FF7EFEC6F08 )
{
  v13 = 0i64;
}
else
{
  v9 = __ROL4__(862785416, 16);
  v10 = __ROL4__(v9 + 479996964, 16);
  LODWORD(v23) = v10 ^ 0x1C9C2C24;
  v11 = __ROR4__(1109147713, 8);
  v12 = __ROR4__(v11 + 463674276, 8);
  HIDWORD(v23) = v12 ^ 0xE45CE45C;
  v13 = v23 + 24i64 * (signed int)v8;
}
if ( (*(_DWORD *)(v13 + 8) >> 29) & 1 )
  goto LABEL_13;
LOBYTE(v14) = 1;
```


天下武功，无坚不破，唯快不破


eapon
No Weapon
No Weapon
No Weapon
MATCH STARTS IN
5

Old-school

遊戲透視原理 – 濫用遊戲功能

遊戲透視原理 – 濫用遊戲功能

Patch Code 強制進入觀察者模式

IDA View-A | Pseudocode-A | Occurrences of binary: 33 FF 4C 89 74 24 40 0F 29 74 24 30 | Hex View-1 | Structures | Enums

```
19  unsigned __int64 v17; // [sp+20h] [bp-38h]@12
20  int v18; // [sp+28h] [bp-30h]@12
21  char v19; // [sp+68h] [bp+10h]@12
22
23  v1 = a1;
24  sub_7FF7ED90B140();
25  if ( (unsigned __int8)sub_7FF7ED8F78C0(v1) || (result = sub_7FF7ED8F7BC0(v1), (_BYTE)result) )
26  {
27    v3 = 0i64;
28    if ( !*(_QWORD *)(v1 + 0xC58) )
29    {
30      LODWORD(v4) = sub_7FF7ECEEB5E0(v1 + 0xC40);
31      v5 = v4;
32      if ( !v4
33        || ((LODWORD(v6) = sub_7FF7ECBDAB10(),
34             v7 = __ROR8__(*(_QWORD *)(v5 + 8) ^ 0xFC000EBF4B6617FAui64, 1),
35             v8 = v6 + 232,
36             v9 = *(_DWORD *)(v6 + 240),
37             (signed int)v9 > *(_DWORD *)((v7 ^ (v7 << 32) ^ 0xAD04D45AF02DE46Aui64) + 0xF0))
38         || *(_QWORD *)(*(_QWORD *)((v7 ^ (v7 << 32) ^ 0xAD04D45AF02DE46Aui64) + 0xE8) + 8 * v9) != v8 ? (v10 = 0) : (v10 = 1),
39            !v10) )
40      {
41        v5 = 0i64;
42      }
43      *(_QWORD *)(v1 + 3160) = v5;
44    }
45    *(_BYTE *)(v1 + 3120) ^= (*(_BYTE *)(v1 + 3120) ^ ~*(_BYTE *)(v1 + 3120)) & 1;
46    v11 = sub_7FF7EBFF00B0(&v19, (__int64)L"IsShowXRay", 1u);
47    sub_7FF7EDDB00D0(v1, *(_QWORD *)(v1 + 3160), *v11);
48    sub_7FF7ED907870(v1, *(_BYTE *)(v1 + 3120) & 1);
49    sub_7FF7ED8E78E0(v1, &v17);
50    v14 = v17;
51    result = v18;
52    v15 = (_QWORD *)v17;
53    v16 = (unsigned __int64)(8i64 * v18 + 7) >> 3;
54    if ( v17 > v17 + 8i64 * v18 )
55      v16 = 0i64;
56    if ( v16 )
57    {
58      do
59      {
60        result = sub_7FF7EDA310C0(*v15, *(_BYTE *)(v1 + 3120) & 1);
61        ++v3;
62        ++v15;
```

https://www.unknowncheats.me/forum/playerunknown-s-battlegrounds/283879-spectator-xrays.html

遊戲透視原理 – 濫用遊戲功能

Internel Hack

檢測點:注入遊戲 / Func Hook

Externel Hack

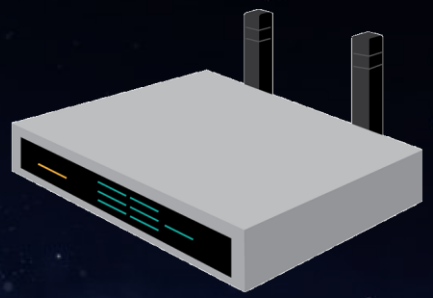
檢測點:透明視窗覆蓋遊戲

濫用遊戲功能

檢測點: Patch Code

100 % Bypass ???

遊戲透視原理 – 封包透視法



玩家端開啟遊戲

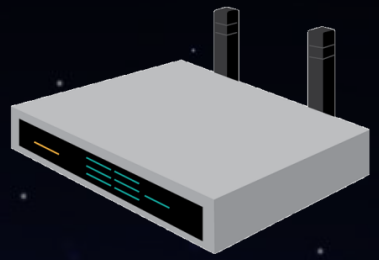
封包經過路由器

PUBG伺服器接收
遊戲封包

遊戲透視原理 – 封包透視法

玩家端開啟遊戲，
連線導向Sniffer機

Sniffer機
解析封包讓遊戲外掛
顯示，並轉送封包至
路由器



封包經過路由器

PUBG伺服器接收
遊戲封包

遊戲透視原理 – 封包透視法

解析封包讓遊戲外掛顯示

- 遊戲封包一直到 2018/03 都沒有加密...

Kotlin版本： https://github.com/Jerry1211/RadarProject
nodejs版本: https://github.com/txchen/scichicken

Demo 封包外掛

射擊無後座力 – 原理

射擊無後座力 – 原理

Demo – 射擊後座力

射擊無後座力 – Windows API 實作

GetAsyncKeyState => 監測滑鼠左鍵是否按下
mouse_event => 控制滑鼠移動

```
DWORD recoilTable[MAX_INDEX_WEAPON][MAX_INDEX_RECOIL] =
{
    { 24,24,24,24,24,24,24,24,24,24,24,28... }, //AKM
    { 20,21,22,21,22,22,23,22,23,23,24,24,... }, //SCAR-L
    { 25,25,25,29,33,33,32,33,32,32,30,30,...}, //M16A4
};

mouse_event( MOUSE_MOVE , (滑鼠移動事件)
             0, (X座標，忽略)
             recoilTable[iWeaponIndex][iCount] , (Y座標，關鍵)
             0,
             3);
```

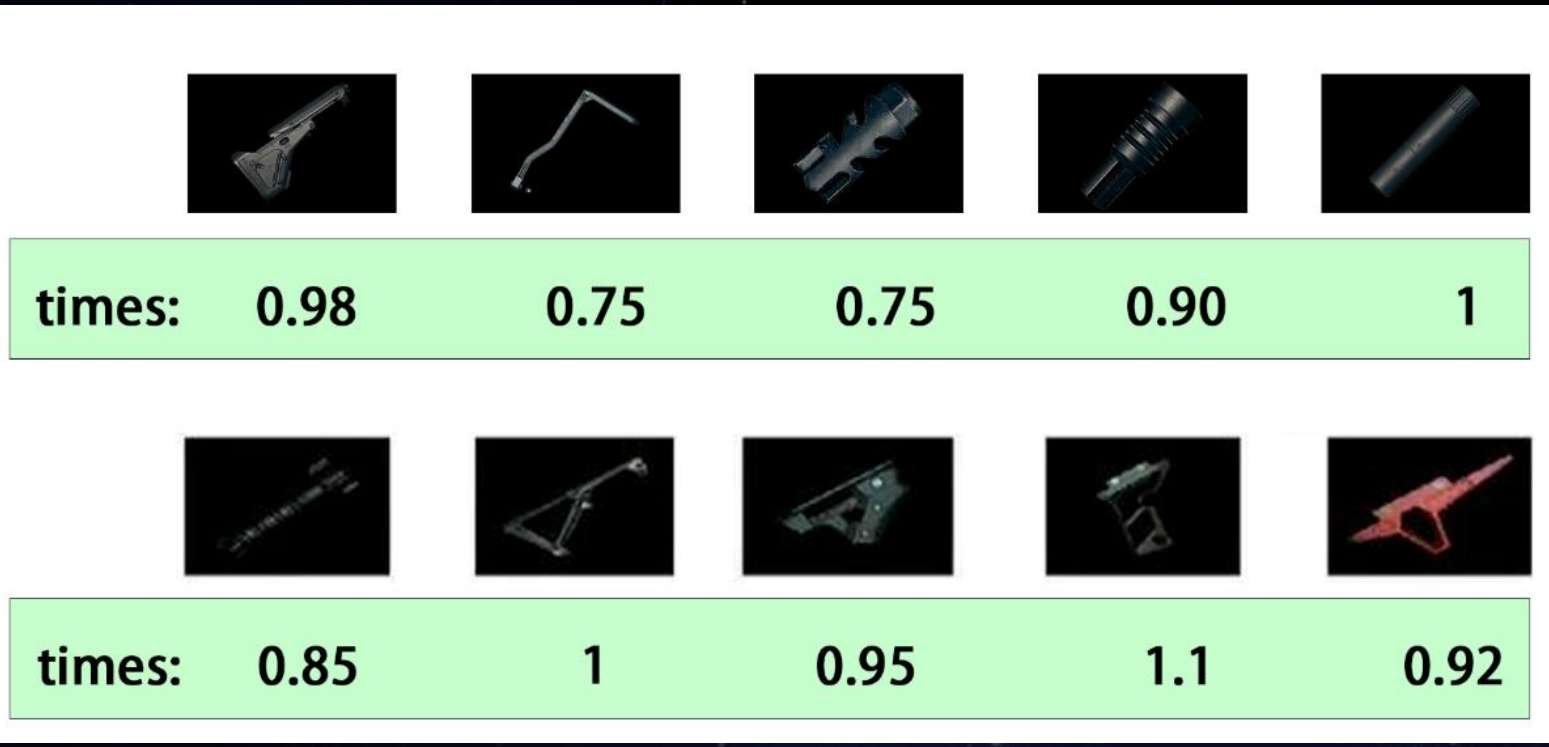
https://github.com/zhutoulala/NoRecoil

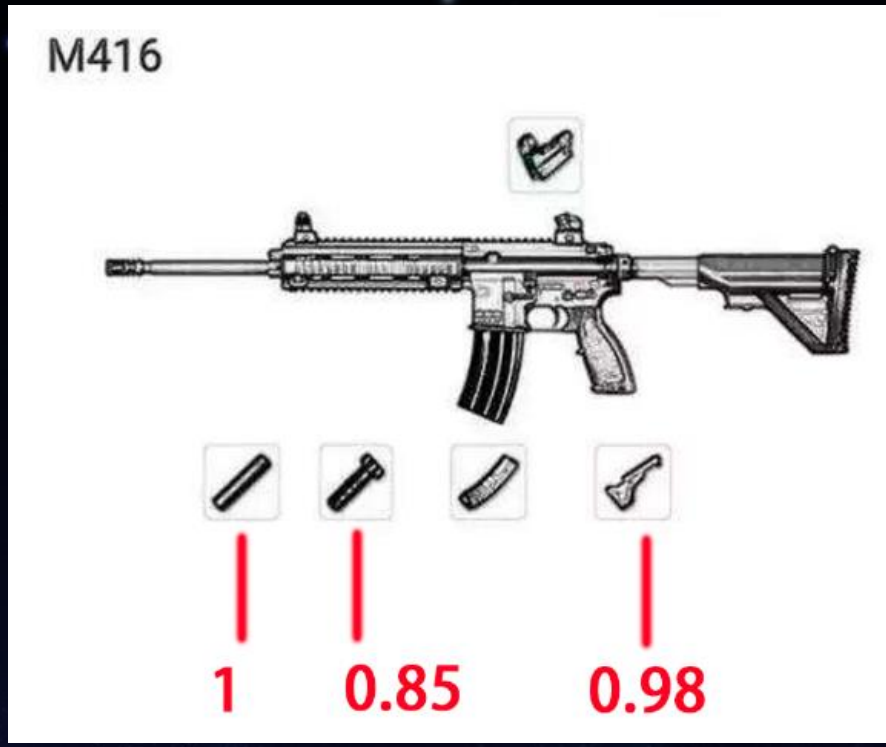
射擊無後座力 – 巨集滑鼠

射擊無後座力 – 巨集滑鼠


Command Editor
Keystroke
Multi Key
Text Block
Mouse Function
Media
Hotkeys
Shortcut
Function
Ventrilo
Multi Key
Name:
Double Click
Keystrokes
Left Button Down
Left Button Up
Left Button Down
Left Button Up
Record delays between events
Display command name on the GamePanel display
Start Recording
Repeat Options
None
Delay (milliseconds):
25
OK
Cancel

射擊無後座力 – 巨集滑鼠





https://github.com/minglich/logitech-pubg

射擊無後座力 – 巨集滑鼠

種類	武器	腰射	機瞄	基礎鏡	二倍鏡	三倍鏡	四倍鏡	六倍鏡	八倍鏡	倍鏡掃射
步槍	AKM	✓	✓	✓	✓	✓	✓	✓	不能裝	✓
	M416	✓	✓	✓	✓	✓	✓	✓	不能裝	✓
	SCAR-L	✓	✓	✓	✓	✓	✓	✓	不能裝	✓
	QBZ95	✓	✓	✓	✓	✓	✓	✓	不能裝	✓
	M16A4	✓	✓	✓	✓	✓	✓	✓	不能裝	X
機槍	DP28	✓	✓	✓	✓	✓	✓	✓	不能裝	✓

射擊無後座力

Demo – 巨集滑鼠影片

射擊無後座力 – 完美效果?

射擊無後座力 – 完美效果?

COMING SOON!

彈道一個點!

射撃自動瞄準

射擊自動瞄準 – 原理

- 結合透視獲得的敵人資料，(Internal / External)
- 3D 座標轉換成 2D (Screen Data)，WorldToScreen()
- 透過滑鼠移動+點擊的API (mouse_event), 移過去目標射擊
- 缺點:要一直配合遊戲更新
  - 有沒有更好的辦法?

射擊自動瞄準 – 抓圖大法

AutoHotkey Will Help You.

開放原始碼的自動化軟體工具，它讓使用者能夠快捷或自動執行重複性任務。

射擊自動瞄準 – 抓圖大法

關鍵 API: PixelSearch

抓取頭盔顏色:

level 1: 0x30474E (shiny) 0x4A5257 (not shiny)
level 2: 0xB3ACA8 (sand colour) 0x4E4F51/0x5A5A5A
level 3: 0x404348

優點:不需隨著遊戲更新，做出來可用很久

[還看過某外掛宣稱用 AI 動態掃描演算法判斷，好 AI 不用嗎?]

https://goo.gl/CPgZAW

抓圖大法 – 缺點

圖沒抓好會射錯目標

手一滑就爆掉隊友的頭

拿自瞄實戰的話...

拿自瞄實戰的話...

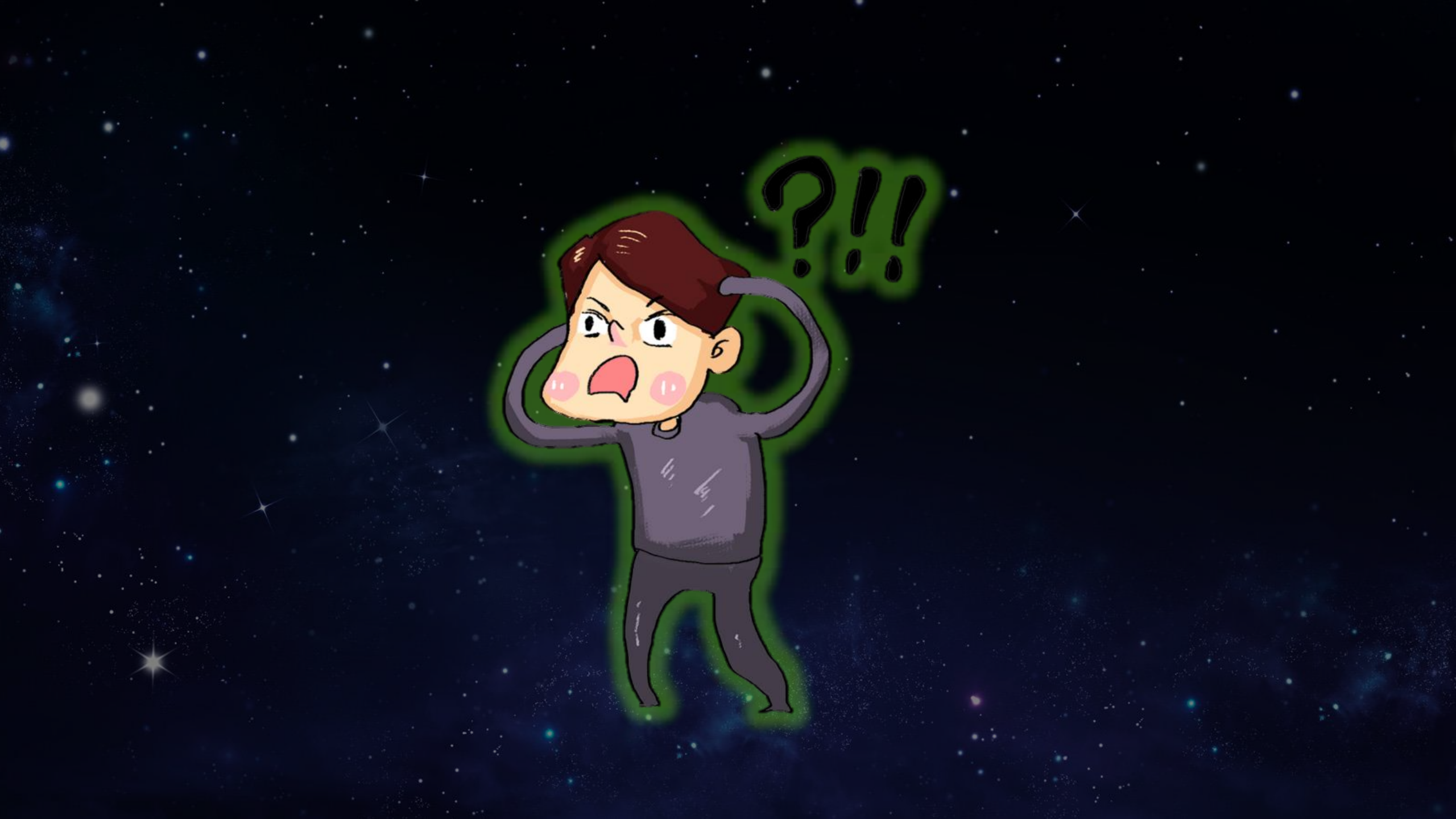
03 修改 Unreal 虛幻遊戲引擎


GOD
MODE

Unreal Engine 虛幻遊戲引擎介紹

虛幻引擎（英語：Unreal Engine）是一款由Epic Games開發的遊戲引擎，多用於開發第一人稱射擊遊戲。

UE1: 1996年，21年前
UE2: 2001年，17年前
UE3: 2006年，12年前
UE4: 2012年，5年前



你聽過黑吃黑嗎?

《绝地求生》7月13日更新《群11288820》全网最稳封号包赔，【刺激战场】【逆水寒】 版主推荐

0713亲测绝地蓝猫插件 激光无后 地板除草 人物上色 全功能 免费使用 新人帖 ... 2 3 4

《绝地求生》追神插件 >QQ群：478451653< 价格公道，进群送测卡 版主推荐

【贪玩盒子】致力于绝地求生高端 插件 百分百不封号 Q群：6805776 新人帖

7月10日▉武将插件▉透视自瞄▉追踪午后▉封号退款▉免费使用中▉唯一Q群：672012086

真牛推荐【免费 无后座 小彩人 除草】百分之百可以用,完全免费,盗号死全家,长期更...

绝地求生。震撼新闻震撼新闻！全网最稳绝地科技【雷神】回归啦！进来看看

網路上亂搜 PUBG 的現成外掛

強大@歪瓜

子弹类

- ○ 主播无后 [微抖一个点 真实质感 演员必备]
- ○ 变态无后 [零抖一个点 指哪打哪 超人必备]

人物上色类

- ○ 七彩黄人 [全身涂上金光粉 提供视野 增强命中率]
- ○ 小蓝人 [全身涂上高亮蓝色 提供视野 增强命中率]
- ○ 小粉人 [全身涂上高亮粉色 提供视野 增强命中率]

灵魂类

- ○ 攻击站立 [对面趴着或蹲着被击中后会站立2秒]

除草类

- ○ 普通除草 [全地图除草 只留草根 伏地魔终结者]
- ○ 马赛克除草 [全地图变成马赛克 视野清晰 专治各种不服]

控制天气类

- ○ 阴天天气 [天气会变成阴天，更好的视角发现敌人]
- ○ 雨天天气 [天气会变成雨天，更好的视角发现敌人]

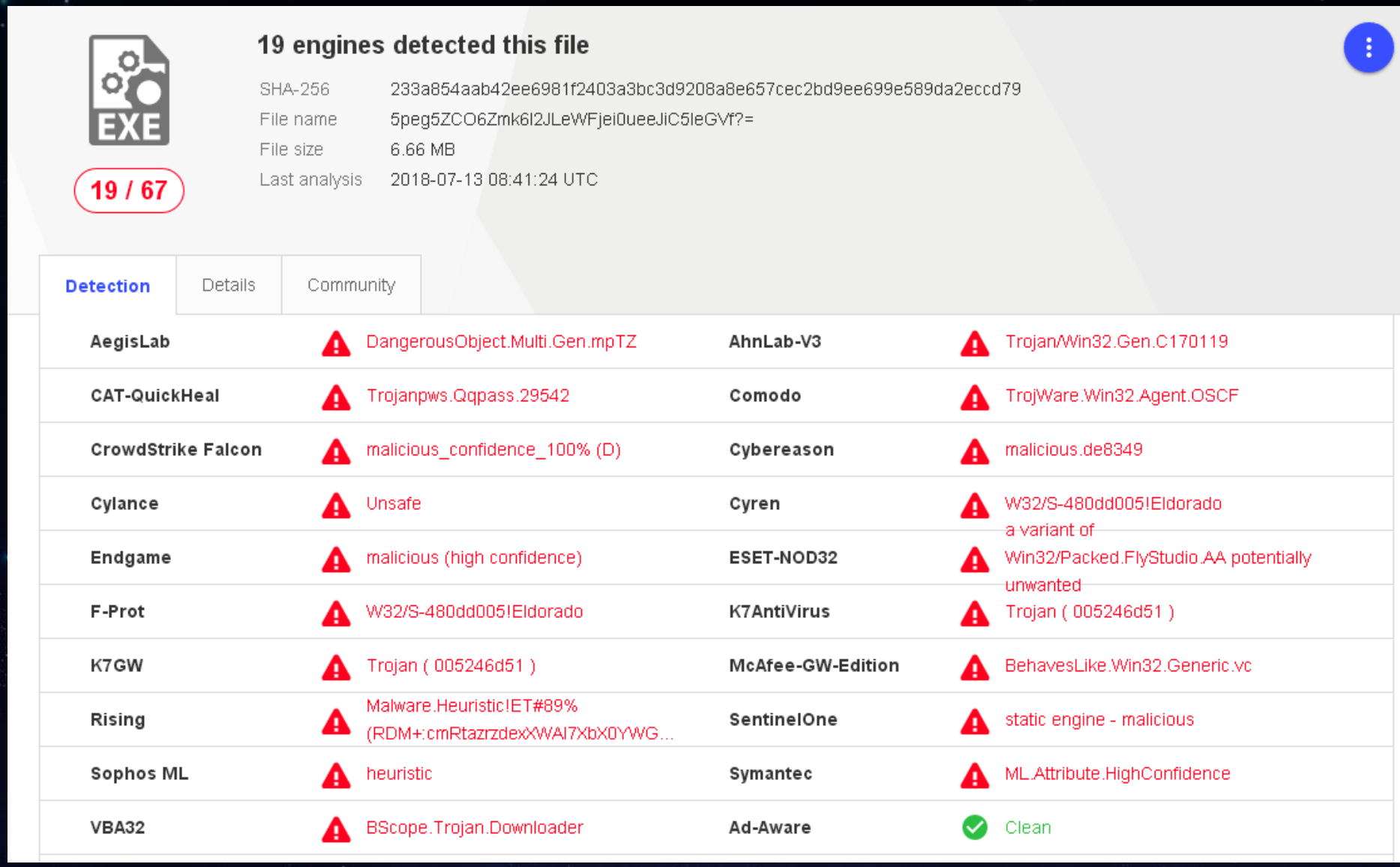
其他功能

- ☐ 屏蔽灌木 [全地图去除 灌木 杂物 专治伏地魔]
- ☐ 屏蔽烟闪 [无视游戏中的 烟雾 闪光 作死干就完了]
- ☐ 声音优化 [去除无用的声音 增加脚步 枪声 车声]
- ☐ 枪械换肤 [主流枪械换肤色 增加美观度]
- ☐ 去除厕所 [去除地图所有厕所，你可以躲里面阴人]
- ☐ 盒子上色 [给盒子加上颜色，高亮绿色，更容易发现]
- ☐ 去除窗框 [全地图去除 窗框 视野更好 跳窗户方便]

高危功能

- ☐ 屏蔽墙体 [去除老地图一楼墙体，子弹可以穿墙]
- ☐ 屏蔽树木 [全地图清除 树木 阴壁终结者 子弹能穿树]
- ☐ 屏蔽石头 [全地图清除 石头 阴壁终结者 子弹能穿石头]
- ☐ 开船蹲地 [人物可穿门 船开到岸上即可遁地]
- ☐ 穿集装箱 [可以穿集装箱 废车 门等物品]

免費的最貴



19 engines detected this file

SHA-256 233a854aab42ee6981f2403a3bc3d9208a8e657cec2bd9ee699e589da2eccd79
File name 5peg5ZCO6Zmk6I2JLeWFjei0ueeJiC5leGVf?=
File size 6.66 MB
Last analysis 2018-07-13 08:41:24 UTC

19 / 67

Detection | Details | Community

AegisLab	DangerousObject.Multi.Gen.mpTZ	AhnLab-V3	Trojan/Win32.Gen.C170119
CAT-QuickHeal	Trojanpws.Qqpass.29542	Comodo	TrojWare.Win32.Agent.OSCF
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.de8349
Cylance	Unsafe	Cyren	W32/S-480dd005!Eldorado
Endgame	malicious (high confidence)	ESET-NOD32	a variant of Win32/Packed.FlyStudio.AA potentially unwanted
F-Prot	W32/S-480dd005!Eldorado	K7AntiVirus	Trojan (005246d51)
K7GW	Trojan (005246d51)	McAfee-GW-Edition	BehavesLike.Win32.Generic.vc
Rising	Malware.Heuristic!ET#89% (RDM+:cmRtazrzdexXWAI7XbX0YWG...	SentinelOne	static engine - malicious
Sophos ML	heuristic	Symantec	ML.Attribute.HighConfidence
VBA32	BScope.Trojan.Downloader	Ad-Aware	Clean

修改 Unreal Engine 虚幻遊戲引擎

修改 Unreal Engine 虚幻遊戲引擎

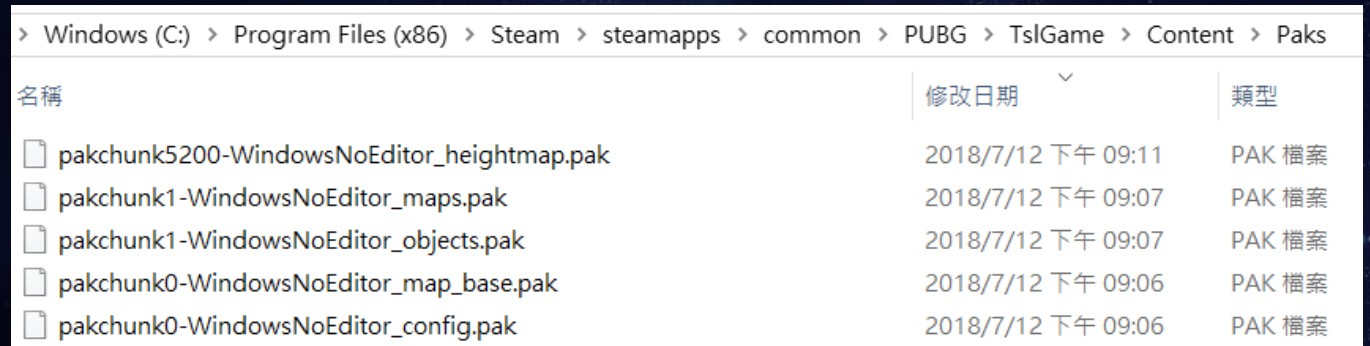
pe	String
	& UnrealPak.exe TslGame-WindowsNoEditor_ui1.pak -create=pak.txt -encrypt -encryptindex -aes=45DD15D6DD2DA50AEB71CE7A5284CF8EA498B2EC3D52B7E336F3EA
	TslGame
	TslGame-WindowsNoEditor_ui1.pak
	TslGame-WindowsNoEditor_ui1.pak\"
	TslGame-WindowsNoEditor_zxb.pak
	TslGame.exe
	TslGame_BE.exe
	[Common]\r\nVersion=2\r\nCount=1\r\n[0]\r\nPath=D:\\steam\\steamapps\\common\\PUBG\\TslGame\\Content\\Paks\\TslGame-WindowsNoEditor_ui1.pak\r\nType=0\
	\"TslGame*\" \"../../../TslGame/*\" \"-compress
	\\PUBG\\TslGame\\Content\\Paks
	\\TslGame-WindowsNoEditor_etc.pak
	\\TslGame-WindowsNoEditor_ui1.pak
	\\TslGame-WindowsNoEditor_ui1.pak\" \"
	\\TslGame-WindowsNoEditor_zxb.pak
	\\TslGame\\Binaries\\Win64
	\\TslGame\\Binaries\\Win64\\TslGame_BE.exe
	\\TslGame\\Content\\Paks
	\\TslGame\\Content\\Paks\\TslGame-WindowsNoEditor_etc.pak

修改 Unreal Engine 虚幻遊戲引擎

```
.text:027CF371                                          ; sub_407555+9F1↑o ...
.text:027CF37A aTslgameTslgame db '"TslGame\*" "../../../TslGame/*" "-compress"',0
.text:027CF37A                                          ; DATA XREF: sub_407555+945↑o
.text:027CF3A7 aUe4TxtEncryptE db '\Ue4.txt" "-encrypt" "-encryptindex" "-aes=45DD15D6DD2DA50AEB71CE'
.text:027CF3A7                                          ; DATA XREF: sub_407555+AAD↑o
.text:027CF3A7                 db '7A5284CF8EA498B2EC3D52B7E336F3EA0071CE44B3"',0
.text:027CF414 aTslgameWindows_1 db 'TslGame-WindowsNoEditor_ui1.pak" "-create=',0
```

修改 Unreal Engine 虛幻遊戲引擎 – 結論

- 外掛功能是透過修改 PUBG 的 PAK (資源檔案) 實作
- UnrealPak.exe 是 Unreal Engine的官方 Cmd 工具
  - 可以解開 / 打包 PAK
- PAK 透過 AES 演算法加/解密
  - Key
    - 45DD15D6DD2DA50AEB71CE7A5284CF8EA498B2EC3D52B7E336F3EA0071CE44B3
- 打包好的 PAK，放進遊戲Paks 目錄，遊戲就會自動載入
  - C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks



修改 Unreal Engine 虚幻遊戲引擎

- News
- Projects
  - UE Viewer
  - ActorX Importer
  - Zlib
  - Quake 2
- About me
- Downloads
- Donate
- Search
- Forum
- Links

UE Viewer

UE Viewer

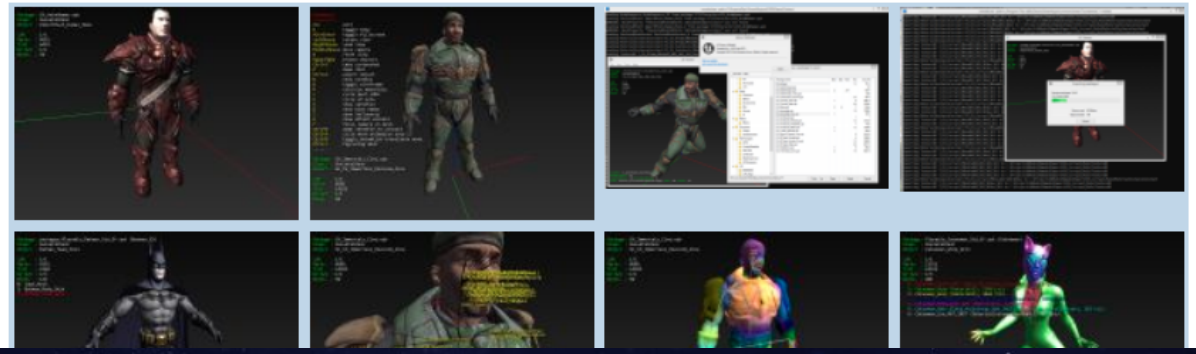
Last update: 21.06.

Download	Donate	FAQ	Screenshots	Discussion	Compatibility Table	Video Tutorial

Unreal Engine Resource Viewer also known as Umodel or Unreal Model Viewer is program for viewing and extracti resources from various games made with Unreal Engine.

Feature Highlights

- Loading packages from more than 300 games based on all Unreal engine generations
- Visualization of skeletal meshes with animations
- Visualization of internal skeletal mesh information like skeleton hierarchy and binding vertices to the skeleto bones
- Visualizarion of vertex meshes
- Visualization of static meshes
- Viewing supported material types and their internal structure
- Export of skeletal, vertex and static meshes and animations into formats supported by 3d modeling software by Unreal engine
- Export textures into tga or dds format
- Export sounds, ScaleForm and FaceFX



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Character]

File View Navigate SkeletalMesh Tools Help

Package : Avatar_Female/Face/Meshes/F_Face_01.uasset
Class : SkeletalMesh
Object : F_Face_01

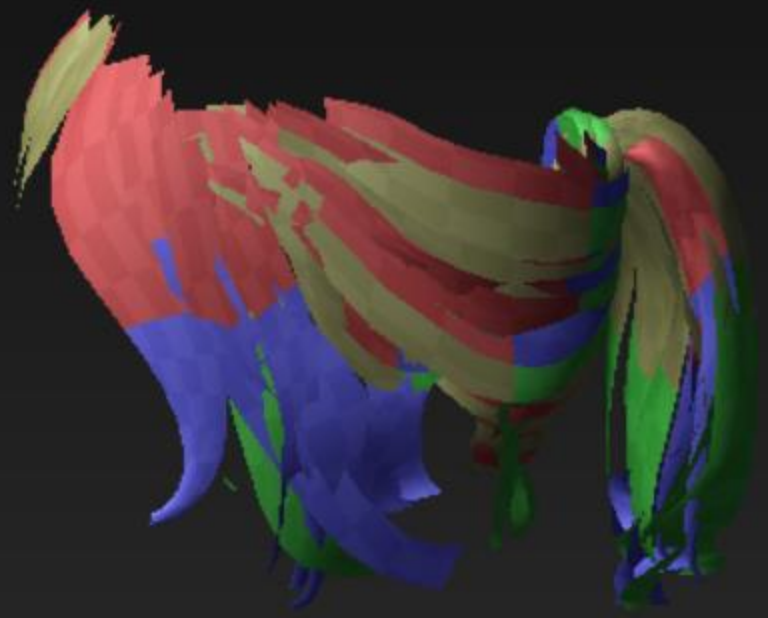
LOD : 1/3
Verts : 4976
Tris : 8144
UV Set : 1/3
Bones : 192

UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Character]

File View Navigate SkeletalMesh Tools Help

Package : Avatar_Female/Hair/Meshes/F_Hair_02_Zombie_Cut.uasset
Class : SkeletalMesh
Object : F_Hair_02_Zombie_Cut

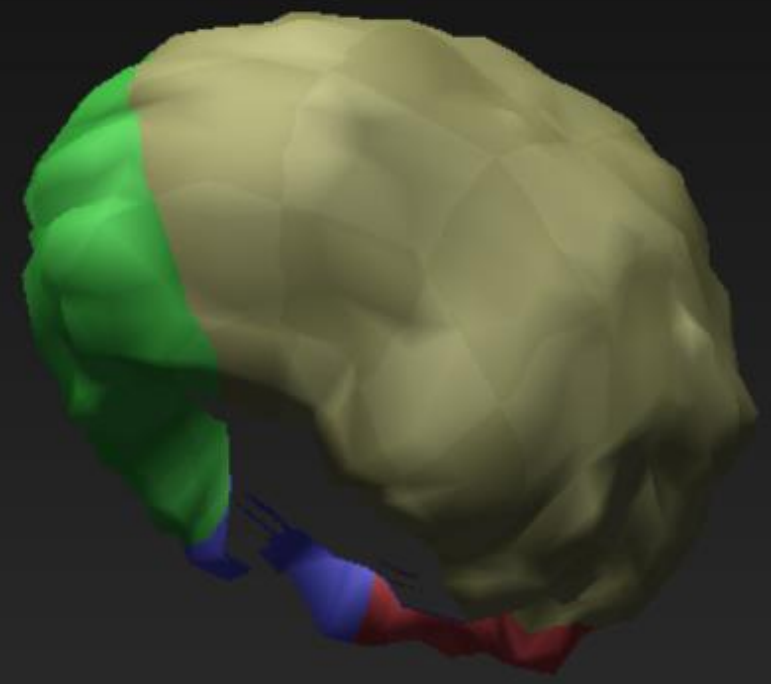
LOD : 1/3
Verts : 3566
Tris : 3912
UV Set : 1/2
Bones : 192



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-\x\x\pak\Character]

File View Navigate SkeletalMesh Tools Help

```
Package : Avatar_Female/Hair/Meshes/F_Hair_03.uasset
Class   : SkeletalMesh
Object  : F_Hair_03

LOD     : 1/3
Verts   : 3042
Tris    : 5972
UV Set  : 1/1
Bones   : 192
```

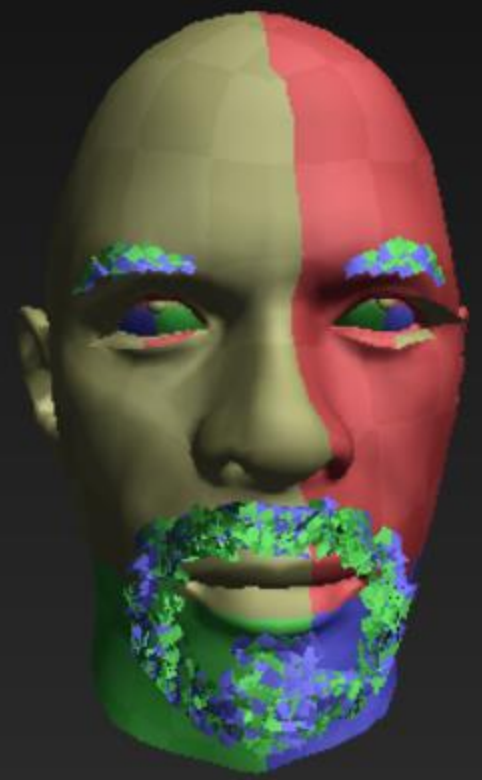


UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Character]

File View Navigate SkeletalMesh Tools Help

Package : Avatar_Male/Face/Meshes/M_Face_06.uasset
Class : SkeletalMesh
Object : M_Face_06

LOD : 1/3
Verts : 15966
Tris : 12973
UV Set : 1/3
Bones : 192



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-\x\x\pak\Character]

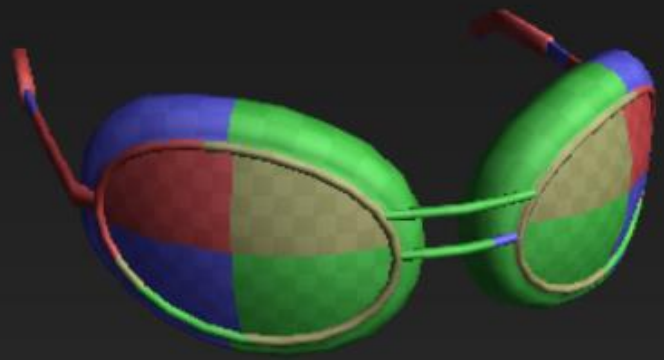
File View Navigate SkeletalMesh Tools Help

```
Package : Female/Eyes/Meshes/F_Eyes_K_01.uasset
Class   : SkeletalMesh
Object  : F_Eyes_K_01

LOD     : 1/1
Verts   : 1070
Tris    : 1508
UV Set  : 1/1
Bones   : 192
```

UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-\x\x\pak\Character]

File View Navigate SkeletalMesh Tools Help

```
Package : Female/Eyes/Meshes/F_Eyes_K_01.uasset
Class   : SkeletalMesh
Object  : F_Eyes_K_01

LOD     : 1/1
Verts   : 1070
Tris    : 1508
UV Set  : 1/1
Bones   : 192
```



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Character]

File View Navigate SkeletalMesh Tools Help

Package : Female/Back/Meshes/F_Back_A_01.uasset
Class : SkeletalMesh
Object : F_Back_A_01

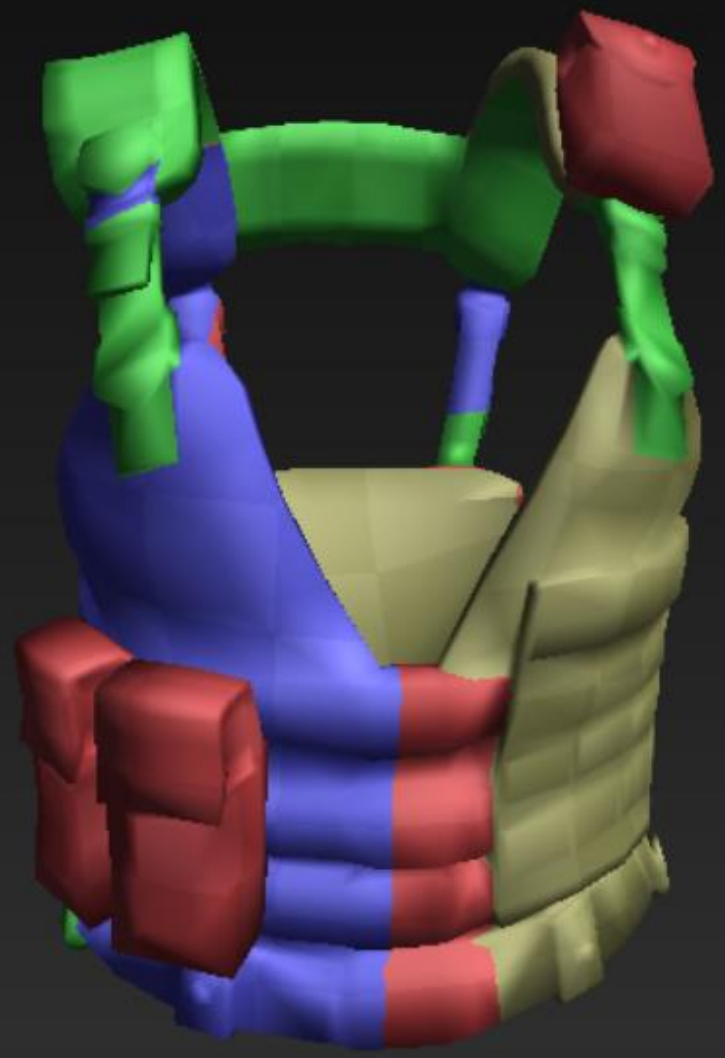
LOD : 1/3
Verts : 2108
Tris : 3098
UV Set : 1/1
Bones : 192

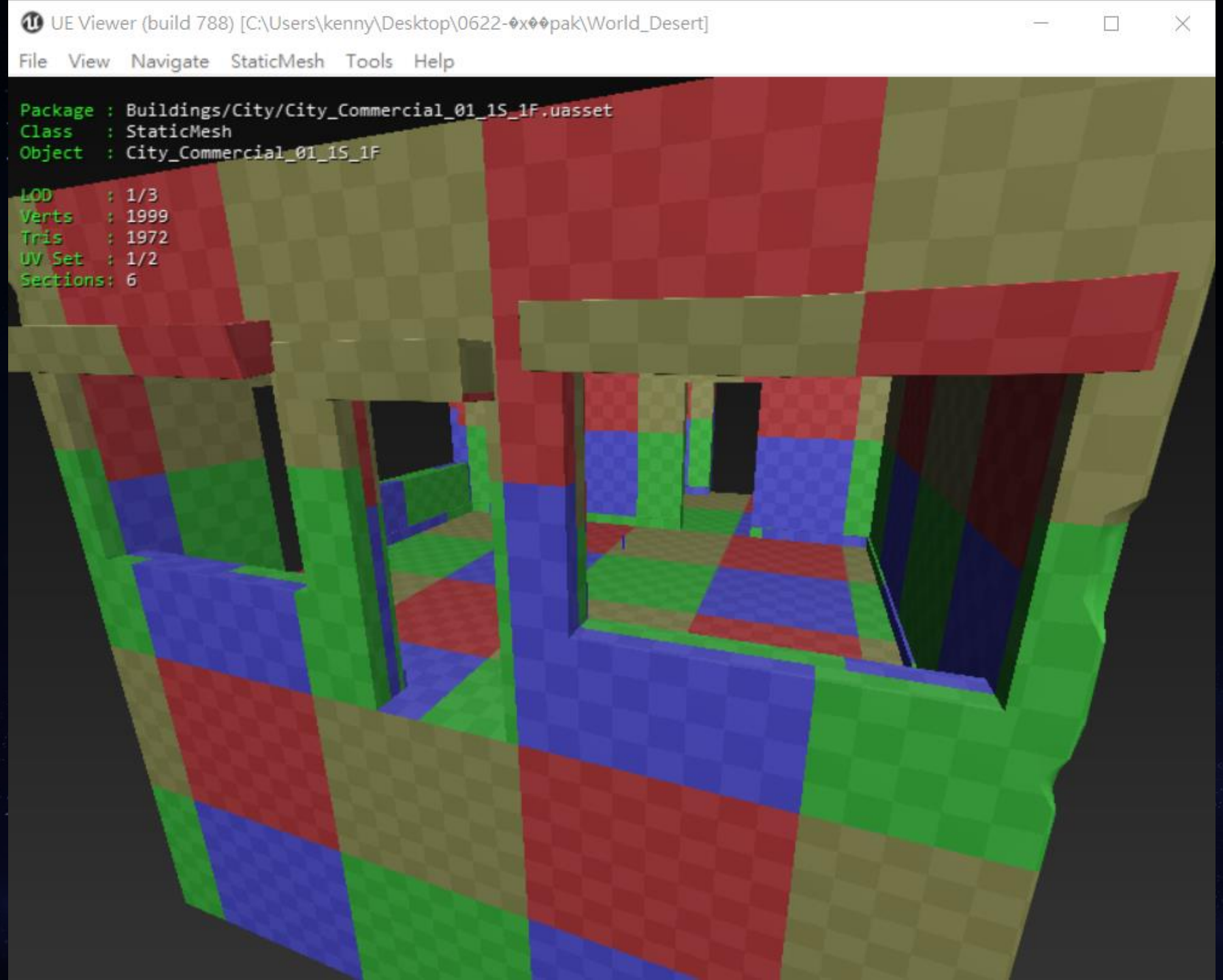
UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Character]

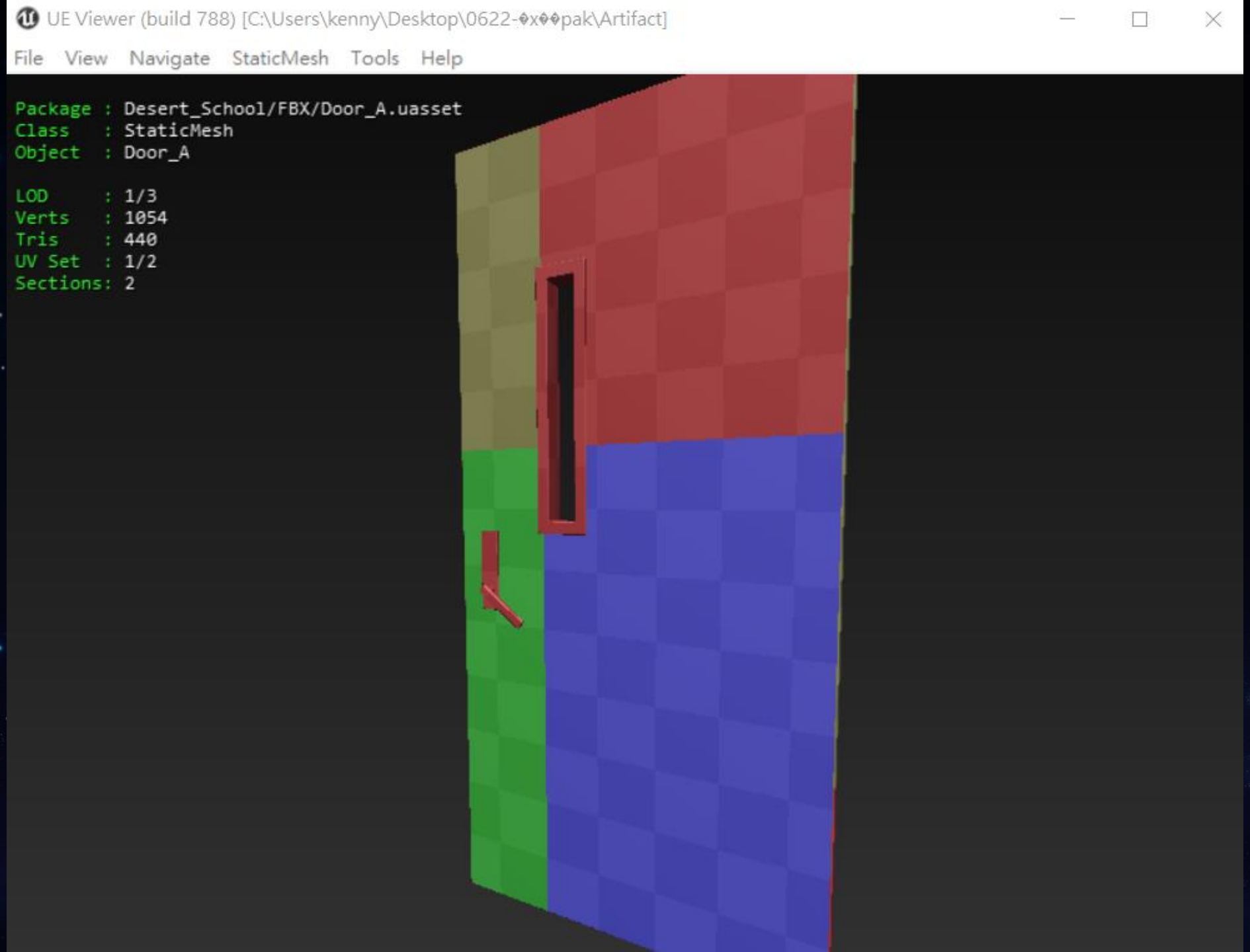
File View Navigate SkeletalMesh Tools Help

Package : Female/Armor/Meshes/F_Armor_E_01.uasset
Class : SkeletalMesh
Object : F_Armor_E_01

LOD : 1/3
Verts : 2525
Tris : 3954
UV Set : 1/1
Bones : 192

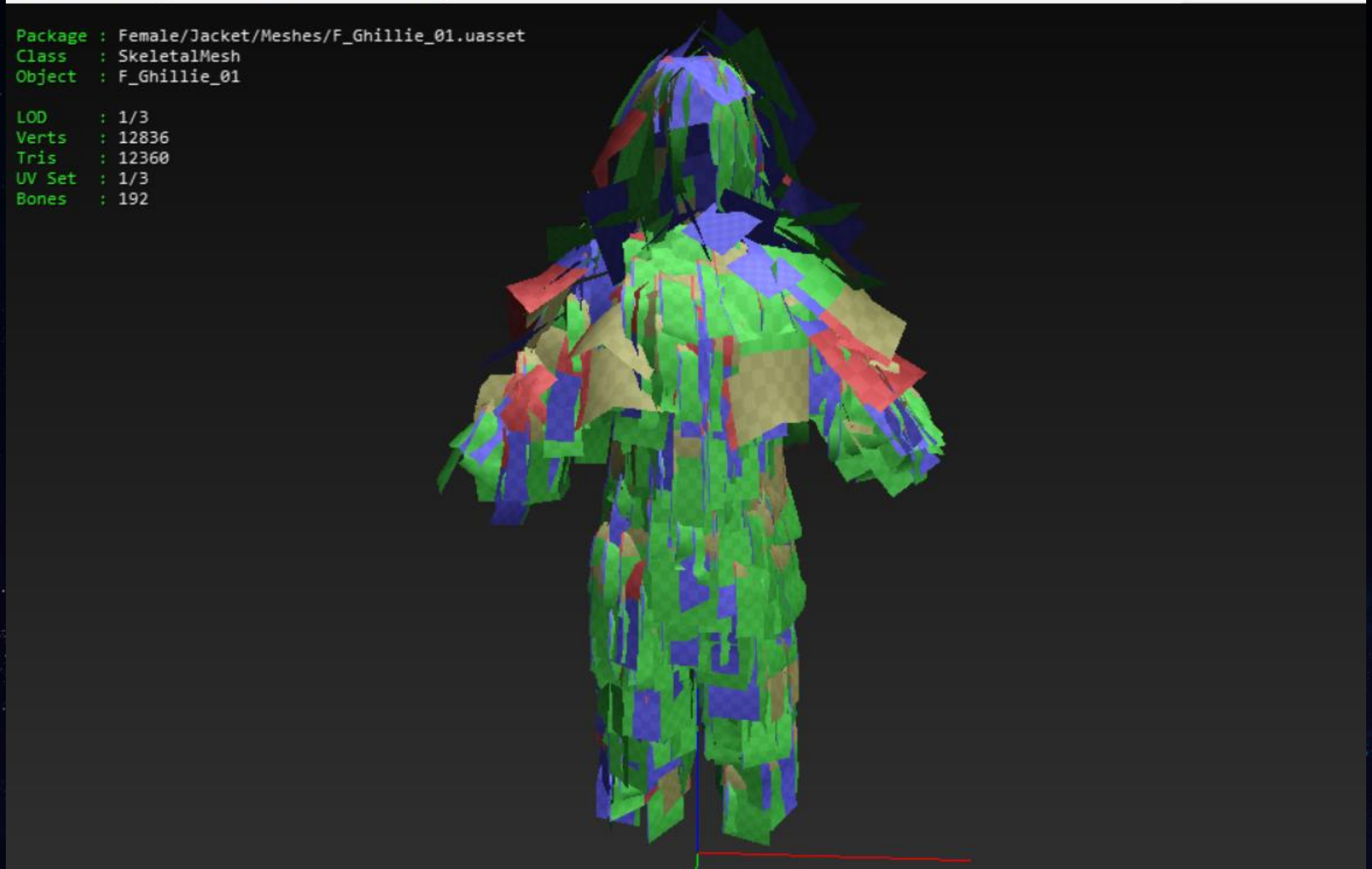



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\World_Desert]
File View Navigate StaticMesh Tools Help
Package : Buildings/City/City_Commercial_01_1S_1F.uasset
Class : StaticMesh
Object : City_Commercial_01_1S_1F
LOD : 1/3
Verts : 1999
Tris : 1972
UV Set : 1/2
Sections: 6


UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Artifact]
File View Navigate StaticMesh Tools Help
Package : Desert_School/FBX/Door_A.uasset
Class : StaticMesh
Object : Door_A
LOD : 1/3
Verts : 1054
Tris : 440
UV Set : 1/2
Sections: 2

UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-0x00pak\Character]

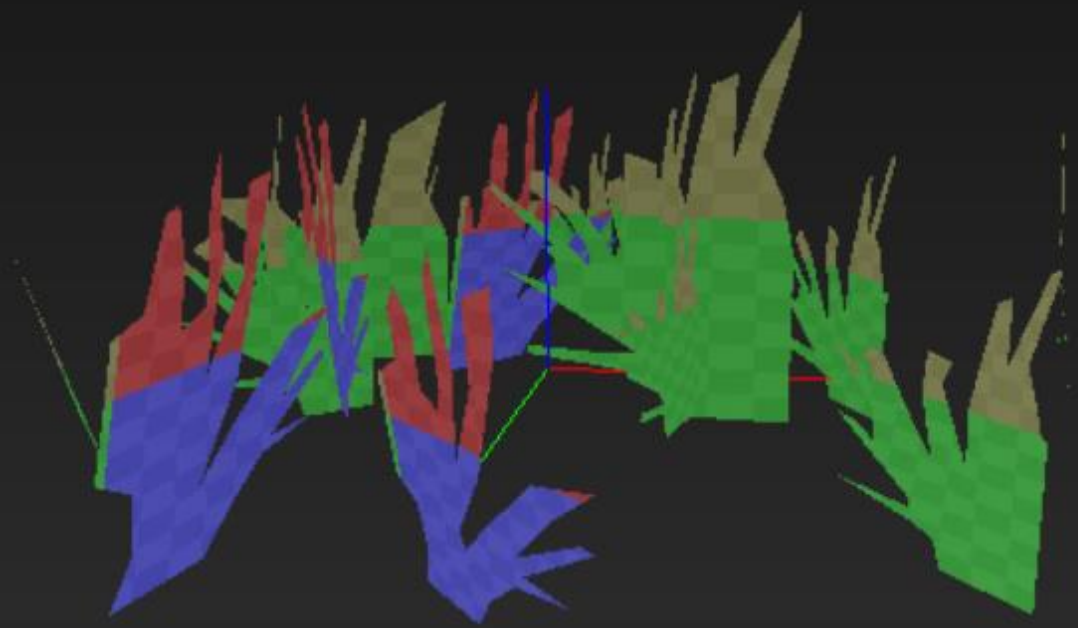
File View Navigate SkeletalMesh Tools Help



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-\x\pak\World_Desert]

File View Navigate StaticMesh Tools Help

```
Package : Vegetation/Grass/tsl_Grass_01_desert.uasset
Class   : StaticMesh
Object  : tsl_Grass_01_desert

LOD     : 1/3
Verts   : 858
Tris    : 803
UV Set  : 1/3
Sections: 1
```



UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Buildings]

File View Navigate StaticMesh Tools Help

Package : Artifacts/Desert/HLOD/HLOD_City_Center_Square_01.uasset
Class : StaticMesh
Object : HLOD_City_Center_Square_01

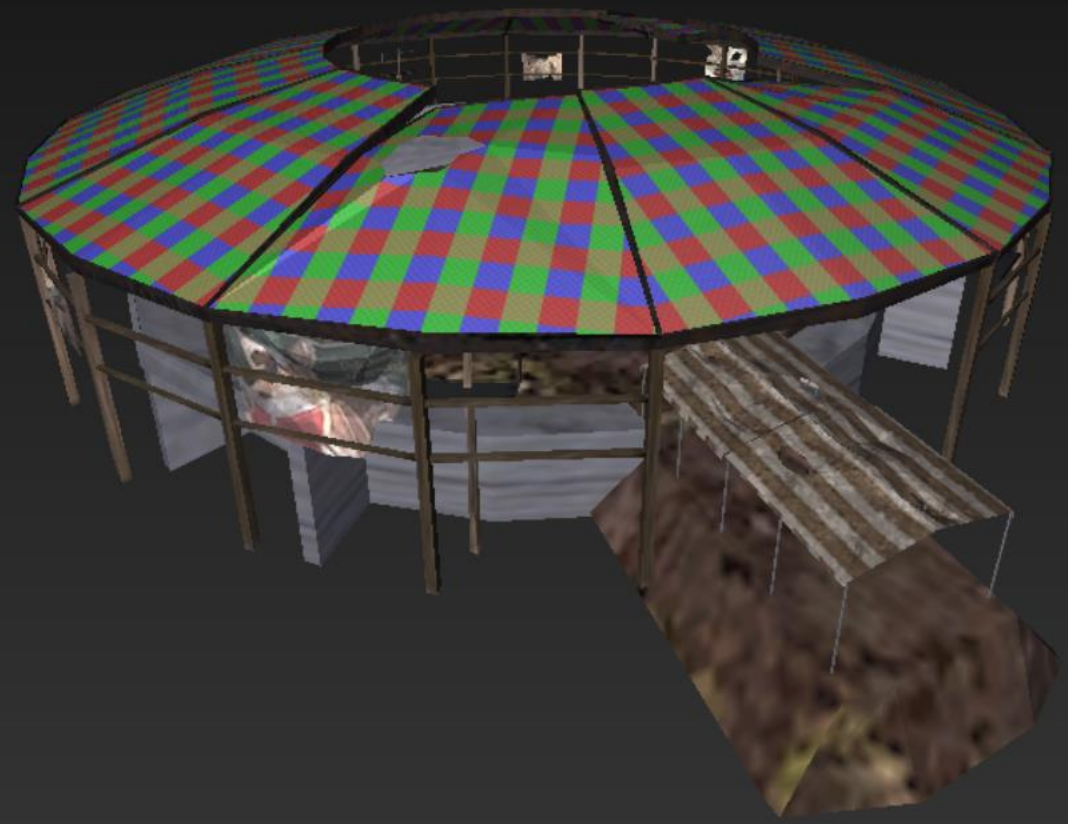
LOD : 1/1
Verts : 106434
Tris : 43223
UV Set : 1/2
Sections: 2

UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Buildings]

File View Navigate StaticMesh Tools Help

Package : Artifacts/Desert/HLOD/HLOD_Arena_a.uasset
Class : StaticMesh
Object : HLOD_Arena_a

LOD : 1/1
Verts : 7494
Tris : 2818
UV Set : 1/2
Sections: 2

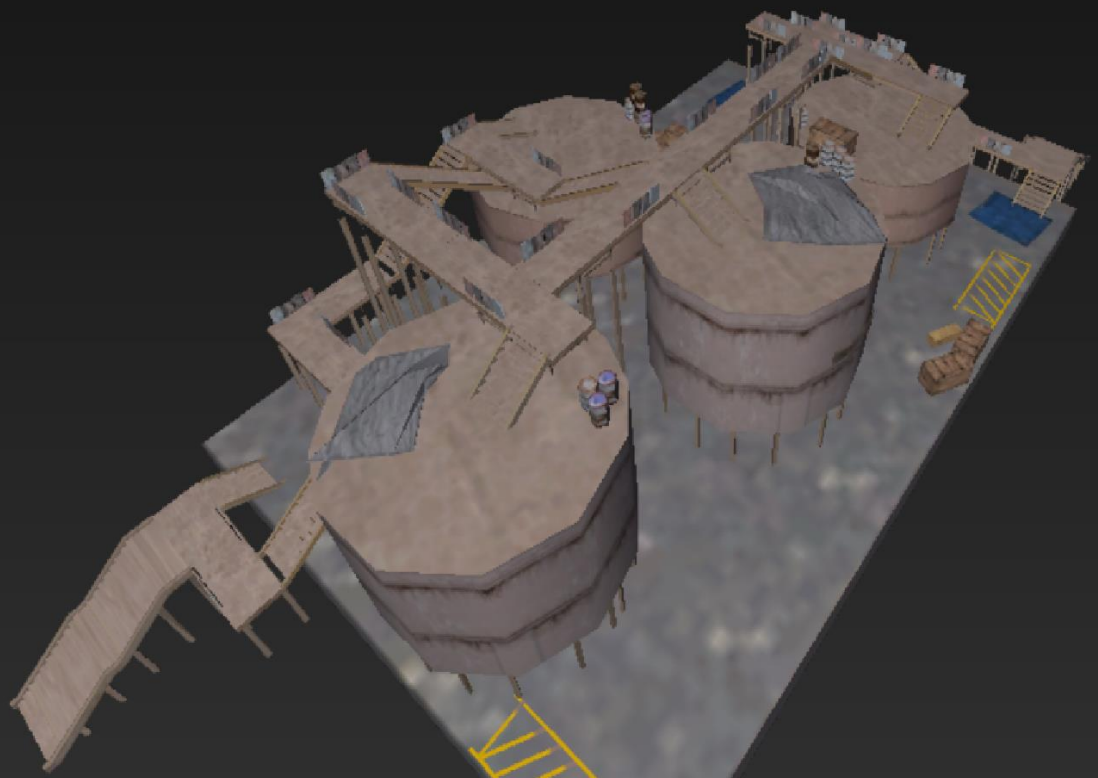


UE Viewer (build 788) [C:\Users\kenny\Desktop\0622-x\pak\Buildings]

File View Navigate StaticMesh Tools Help

Package : Artifacts/Desert/HLOD/HLOD_Village_Silver_Mine_Tanks_a.uasset
Class : StaticMesh
Object : HLOD_Village_Silver_Mine_Tanks_a

LOD : 1/1
Verts : 11461
Tris : 5286
UV Set : 1/2
Sections: 1



修改 Unreal Engine 虛幻遊戲引擎 – Unpack PAK

PAK 解出來會是成對的兩個檔案(package)

- *.uasset => 描述 package (info / file_path)
- *.uexp => Resource File

修改 Unreal Engine 虛幻遊戲引擎 -人物著色

\Assets\Character\Female\Head\Textures\F_Head_*.uasset
=> 維持原本

\Assets\Character\Female\Head\Textures\F_Head_*.uexp
=> 替換為純顏色的材質(全黃色)


84 加入
南
西南
W
西北
北
4
距离比赛开始剩余时间
1:00
Prison

修改 Unreal Engine 虛幻遊戲引擎 - 馬賽克地板

沙漠 - Maps\Desert\Art\LandscapeMaterial
Desert_Triplanar_Rock_Inst.uasset
=> /Game/Blueprints/Weapons/RecoilCurves/C_Recoil_SMG_Uzi.uasset

小島 - Maps\Erangel\Art
MI_BRO_Landscape.uasset
=> /Game/Blueprints/Weapons/RecoilCurves/C_Recoil_SMG_Uzi.uasset

透過載入錯誤的.uasset檔案，去除地板原始材質


西北 330 345 北 15 30 50 60 75 东 105 120 东南 150
61 生存
CHNE- 使用M416爆头击杀了 HumPiek
LOS PROSCRITOS
3:48
B6
B7
B8
M0
M1
15 , 15
kxploit - 3.8.22.52 - 33E90C

修改 Unreal Engine 虛幻遊戲引擎

Demo [人物上色+地板馬賽克 影片]

修改 Unreal Engine 虛幻遊戲引擎 - 完美無後座力

- TslGame\Content\Blueprints\Weapons\RecoilCurves\C_Recoil_AKM.uexp
  - 改這個對應的武器名稱

- Google 【C_Recoil_AKM】
  - https://battlegrounds.party/weapons/raw/C_Recoil_AKM.json

battlegrounds.party/weapons/raw/C_Recoil_AKM.json


```
{
    "C_Recoil_AKM": {
        "@Remaining": 4,
        "@SuperName": "Class",
        "@TemplateName": "Default__CurveVector",
        "ClassName": "CurveVector",
        "ExportName": "C_Recoil_AKM",
        "FloatCurves": [
            {
                "Keys": [
                    {
                        "StrucName": "RichCurveKey",
                        "value": {
                            "ArriveTangent": 0.1782974,
                            "ArriveTangentWeight": 0,
                            "InterpMode": 2,
                            "LeaveTangent": 0.1782941,
                            "LeaveTangentWeight": 0,
                            "StrucName": "FRichCurveKey",
                            "TangentMode": 1,
                            "TangentWeightMode": 0,
                            "Time": 0,
                            "Value": 0.13
                        }
                    },
                    {
                        "StrucName": "RichCurveKey",
                        "value": {
                            "ArriveTangent": 0.06788478,
                            "ArriveTangentWeight": 0,
                            "InterpMode": 2,
                            "LeaveTangent": 0.0678886,
                            "LeaveTangentWeight": 0,
                            "StrucName": "FRichCurveKey",
                            "TangentMode": 1,
                            "TangentWeightMode": 0,
                            "Time": 0.8,
                            "Value": 0.18
                        }
                    },
                    {
                        "StrucName": "RichCurveKey",
                        "value": {
                            "ArriveTangent": 0.3476593,
                            "ArriveTangentWeight": 0,
                            "InterpMode": 2,
                            "LeaveTangent": 0.347654045,
                            "LeaveTangentWeight": 0,
                            "StrucName": "FRichCurveKey",
```


C_Recoil_AKM.uexp

```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000
00000010
00000020
00000030
00000040
00000050
00000060
00000070
00000080  00 00 00 00 00 00 00 02  01 00 00 00 00 00 B8 1E
00000090  05 3E 98 93 36 3E 00 00  00 00 BB 92 36 3E 00 00   >˜"6>    »'6>
000000A0  00 00 02 01 00 CD CC 4C  3F EC 51 38 3E 2D 07 8B      ÍÌL?ìQ8>- ‹
000000B0  3D 00 00 00 00 2E 09 8B  3D 00 00 00 00 02 01 00  =     . ‹=
000000C0  9A 99 19 40 CD CC CC 3E  66 00 B2 3E 00 00 00 00  š™ @ÍÌÌ>f ²>
000000D0  B6 FF B1 3E 00 00 00 00  0A 00 00 00 00 00 00 00  ¶ÿ±>
000000E0  08 00 00 00 00 00 00 00  0E 00 00 00 00 00 00 00
000000F0  E5 00 00 00 01 00 00 00  0C 00 00 00 00 00 00 00  å
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110  00 09 00 00 00 00 00 00  00 03 00 00 00 00 00 00
00000120  00 BC 00 00 00 00 00 00  00 0E 00 00 00 00 00 00   ¼
00000130  00 00 05 00 00 00 09 00  00 00 00 00 00 00 0E 00
00000140  00 00 00 00 00 00 87 00  00 00 00 00 00 00 0D 00        ‡
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160  00 00 00 00 00 00 00 02  01 00 00 00 00 00 00 00
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180  00 00 02 01 00 00 00 00  00 00 00 00 00 00 00 00
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 02 01
000001A0  00 00 C0 3F 00 00 00 00  00 00 00 00 00 00 00 00    À?
000001B0  00 00 00 00 00 00 00 00  02 01 00 00 00 00 00 00
000001C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0  00 00 00 02 01 00 00 00  00 00 00 00 00 00 00 00
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0A 00
000001F0  00 00 00 00 00 00 08 00  00 00 00 00 00 00 0E 00
00000200  00 00 00 00 00 00 94 00  00 00 02 00 00 00 0C 00        ”
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000220  00 00 00 00 00 00 00 09  00 00 00 00 00 00 00 03
00000230  00 00 00 00 00 00 00 6B  00 00 00 00 00 00 00 0E         k
00000240  00 00 00 00 00 00 00 00  02 00 00 00 09 00 00 00
00000250  00 00 00 00 0E 00 00 00  00 00 00 00 36 00 00 00                6
```

```
 6  def float_to_hex(f):
 7      res =  hex(struct.unpack('<I', struct.pack('<f', f))[0])
 8      print '%s : %s' % (f , res)
 9
10  float_to_hex(0.1782974)
```

```
0.1782974 : 0x3e369398
```

battlegrounds.party/weapons/raw/C_Recoil_AKM.json


```
{
    "C_Recoil_AKM": {
        "@Remaining": 4,
        "@SuperName": "Class",
        "@TemplateName": "Default__CurveVector",
        "ClassName": "CurveVector",
        "ExportName": "C_Recoil_AKM",
        "FloatCurves": {
            "Keys": [
                {
                    "StrucName": "RichCurveKey",
                    "value": {
                        "ArriveTangent": 0.1782974,
                        "ArriveTangentWeight": 0,
                        "InterpMode": 2,
                        "LeaveTangent": 0.1782941,
                        "LeaveTangentWeight": 0,
                        "StrucName": "FRichCurveKey",
                        "TangentMode": 1,
                        "TangentWeightMode": 0,
                        "Time": 0,
                        "Value": 0.13
                    }
                },
                {
                    "StrucName": "RichCurveKey",
                    "value": {
                        "ArriveTangent": 0.06788478,
                        "ArriveTangentWeight": 0,
                        "InterpMode": 2,
                        "LeaveTangent": 0.0678886,
                        "LeaveTangentWeight": 0,
                        "StrucName": "FRichCurveKey",
                        "TangentMode": 1,
                        "TangentWeightMode": 0,
                        "Time": 0.8,
                        "Value": 0.18
                    }
                },
                {
                    "StrucName": "RichCurveKey",
                    "value": {
                        "ArriveTangent": 0.3476593,
                        "ArriveTangentWeight": 0,
                        "InterpMode": 2,
                        "LeaveTangent": 0.347654045,
                        "LeaveTangentWeight": 0,
                        "StrucName": "FRichCurveKey",
```


C_Recoil_AKM.uexp

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	08	00	00	00	00	00	00	00	0E	00	00	00	00	00	00	00
00000010	AF	00	00	00	00	00	00	00	0C	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	09	00	00	00	00	00	00	00	03	00	00	00	00	00	00
00000040	00	86	00	00	00	00	00	00	00	0E	00	00	00	00	00	00
00000050	00	00	03	00	00	00	09	00	00	00	00	00	00	00	0E	00
00000060	00	00	00	00	00	00	51	00	00	00	00	00	00	00	0D	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	02	01	00	00	00	00	00	B8	1E
00000090	05	3E	98	93	36	3E	00	00	00	00	BB	92	36	3E	00	00
000000A0	00	00	02	01	00	CD	CC	4C	3F	EC	51	38	3E	2D	07	8B
000000B0	3D	00	00	00	00	2E	09	8B	3D	00	00	00	00	02	01	00
000000C0	9A	99	19	40	CD	CC	CC	3E	66	00	B2	3E	00	00	00	00
000000D0	B6	FF	B1	3E	00	00	00	00	0A	00	00	00	00	00	00	00
000000E0	08	00	00	00	00	00	00	00	0E	00	00	00	00	00	00	00
000000F0	E5	00	00	00	01	00	00	00	0C	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	09	00	00	00	00	00	00	00	03	00	00	00	00	00	00
00000120	00	BC	00	00	00	00	00	00	00	0E	00	00	00	00	00	00
00000130	00	00	05	00	00	00	09	00	00	00	00	00	00	00	0E	00
00000140	00	00	00	00	00	00	87	00	00	00	00	00	00	00	0D	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	02	01	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	02	01	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	02	01
000001A0	00	00	C0	3F	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	02	01	00	00	00	00	00	00
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	02	01	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0A	00
000001F0	00	00	00	00	00	00	08	00	00	00	00	00	00	00	0E	00
00000200	00	00	00	00	00	00	94	00	00	00	02	00	00	00	0C	00
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000220	00	00	00	00	00	00	00	09	00	00	00	00	00	00	00	03
00000230	00	00	00	00	00	00	00	6B	00	00	00	00	00	00	00	0E
00000240	00	00	00	00	00	00	00	00	02	00	00	00	09	00	00	00
00000250	00	00	00	00	0E	00	00	00	00	00	00	00	36	00	00	00
00000260	00	00	00	00	0D	00	00	00	00	00	00	00	00	00	00	00

```
"__FloatCurves_1": {
        "Keys": [
            {
                "StrucName": "RichCurveKey",
                "value": {
                    "ArriveTangent": 0.609045565,
                    "ArriveTangentWeight": 0,
                    "InterpMode": 2,
                    "LeaveTangent": 0.6090472,
                    "LeaveTangentWeight": 0,
                    "StrucName": "FRichCurveKey",
                    "TangentMode": 1,
                    "TangentWeightMode": 0,
                    "Time": 0,
                    "Value": 0.55
                }
            },
            {
                "StrucName": "RichCurveKey",
                "value": {
                    "ArriveTangent": 0.06588007,
                    "ArriveTangentWeight": 0,
                    "InterpMode": 2,
                    "LeaveTangent": 0.0658768043,
                    "LeaveTangentWeight": 0,
                    "StrucName": "FRichCurveKey",
                    "TangentMode": 1,
                    "TangentWeightMode": 0,
                    "Time": 0.5,
                    "Value": 0.8
                }
            },
            {
                "StrucName": "RichCurveKey",
                "value": {
                    "ArriveTangent": 0.302177429,
                    "ArriveTangentWeight": 0,
                    "InterpMode": 2,
                    "LeaveTangent": 0.3021756,
                    "LeaveTangentWeight": 0,
                    "StrucName": "FRichCurveKey",
                    "TangentMode": 1,
                    "TangentWeightMode": 0,
                    "Time": 1.5,
                    "Value": 1
                }
            },
            {
```

???

???

???

???

???

C_Recoil_AKM.uexp

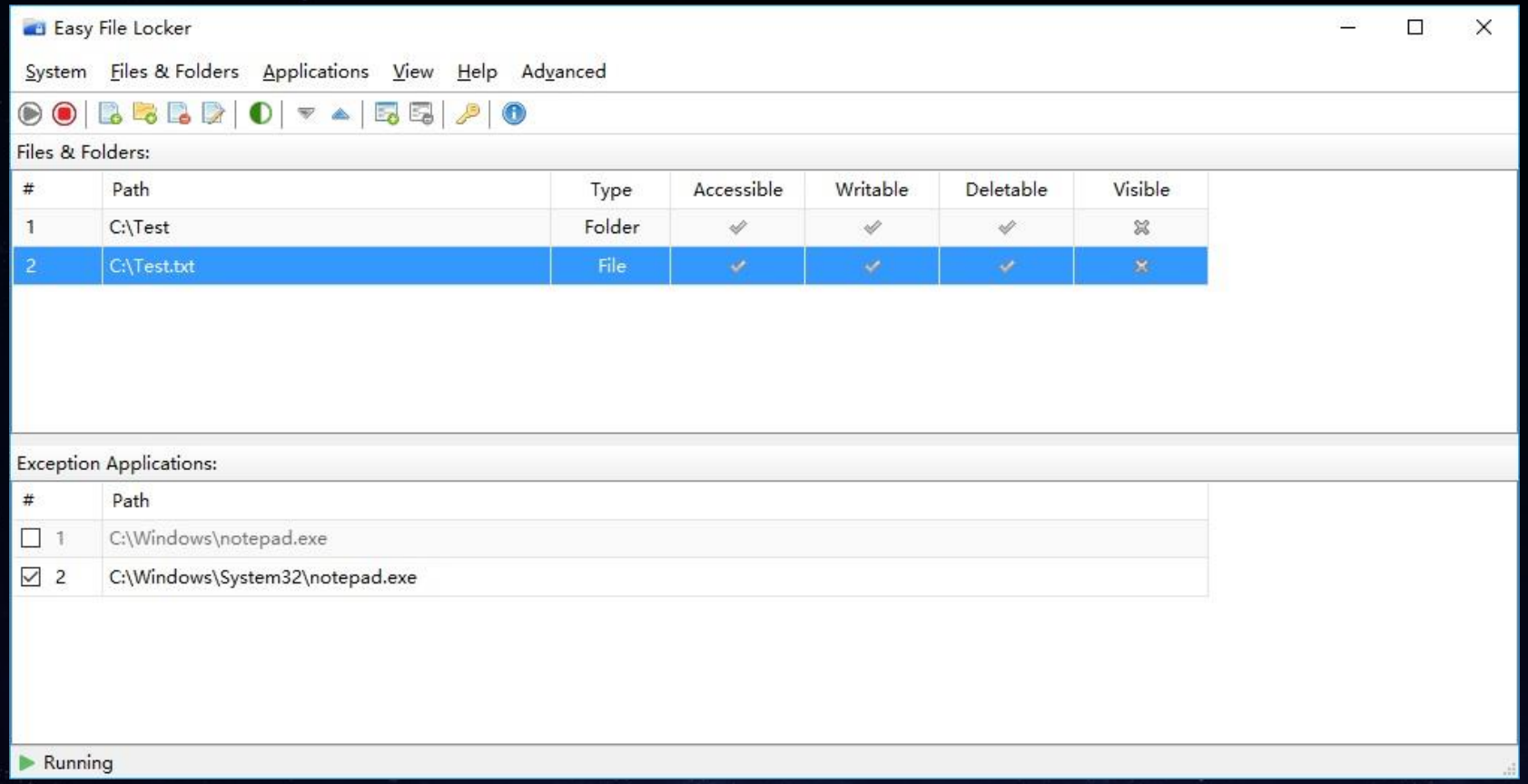
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	08	00	00	00	00	00	00	00	0E	00	00	00	00	00	00	00
00000010	AF	00	00	00	00	00	00	00	0C	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	09	00	00	00	00	00	00	00	03	00	00	00	00	00	00
00000040	00	86	00	00	00	00	00	00	00	0E	00	00	00	00	00	00
00000050	00	00	03	00	00	00	09	00	00	00	00	00	00	00	0E	00
00000060	00	00	00	00	00	00	51	00	00	00	00	00	00	00	0D	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	02	01	00	00	00	00	00	B8	1E
00000090	05	3E	98	93	36	3E	00	00	00	00	BB	92	36	3E	00	00
000000A0	00	00	02	01	00	CD	CC	4C	3F	EC	51	38	3E	2D	07	8B
000000B0	3D	00	00	00	00	2E	09	8B	3D	00	00	00	00	02	01	00
000000C0	9A	99	19	40	CD	CC	CC	3E	66	00	B2	3E	00	00	00	00
000000D0	B6	FF	B1	3E	00	00	00	00	0A	00	00	00	00	00	00	00
000000E0	08	00	00	00	00	00	00	00	0E	00	00	00	00	00	00	00
000000F0	E5	00	00	00	01	00	00	00	0C	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	09	00	00	00	00	00	00	00	03	00	00	00	00	00	00
00000120	00	BC	00	00	00	00	00	00	00	0E	00	00	00	00	00	00
00000130	00	00	05	00	00	00	09	00	00	00	00	00	00	00	0E	00
00000140	00	00	00	00	00	00	87	00	00	00	00	00	00	00	0D	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	02	01	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	02	01	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	02	01	00
000001A0	00	00	C0	3F	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	02	01	00	00	00	00	00	00
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	02	01	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0A	00
000001F0	00	00	00	00	00	00	08	00	00	00	00	00	00	00	0E	00
00000200	00	00	00	00	00	00	94	00	00	00	02	00	00	00	0C	00
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000220	00	00	00	00	00	00	00	09	00	00	00	00	00	00	00	03
00000230	00	00	00	00	00	00	00	6B	00	00	00	00	00	00	00	0E
00000240	00	00	00	00	00	00	00	00	02	00	00	00	09	00	00	00
00000250	00	00	00	00	0E	00	00	00	00	00	00	00	36	00	00	00
00000260	00	00	00	00	0D	00	00	00	00	00	00	00	00	00	00	00

修改 Unreal Engine 虛幻遊戲引擎 - 完美無後座力

修改 Unreal Engine 虛幻遊戲引擎

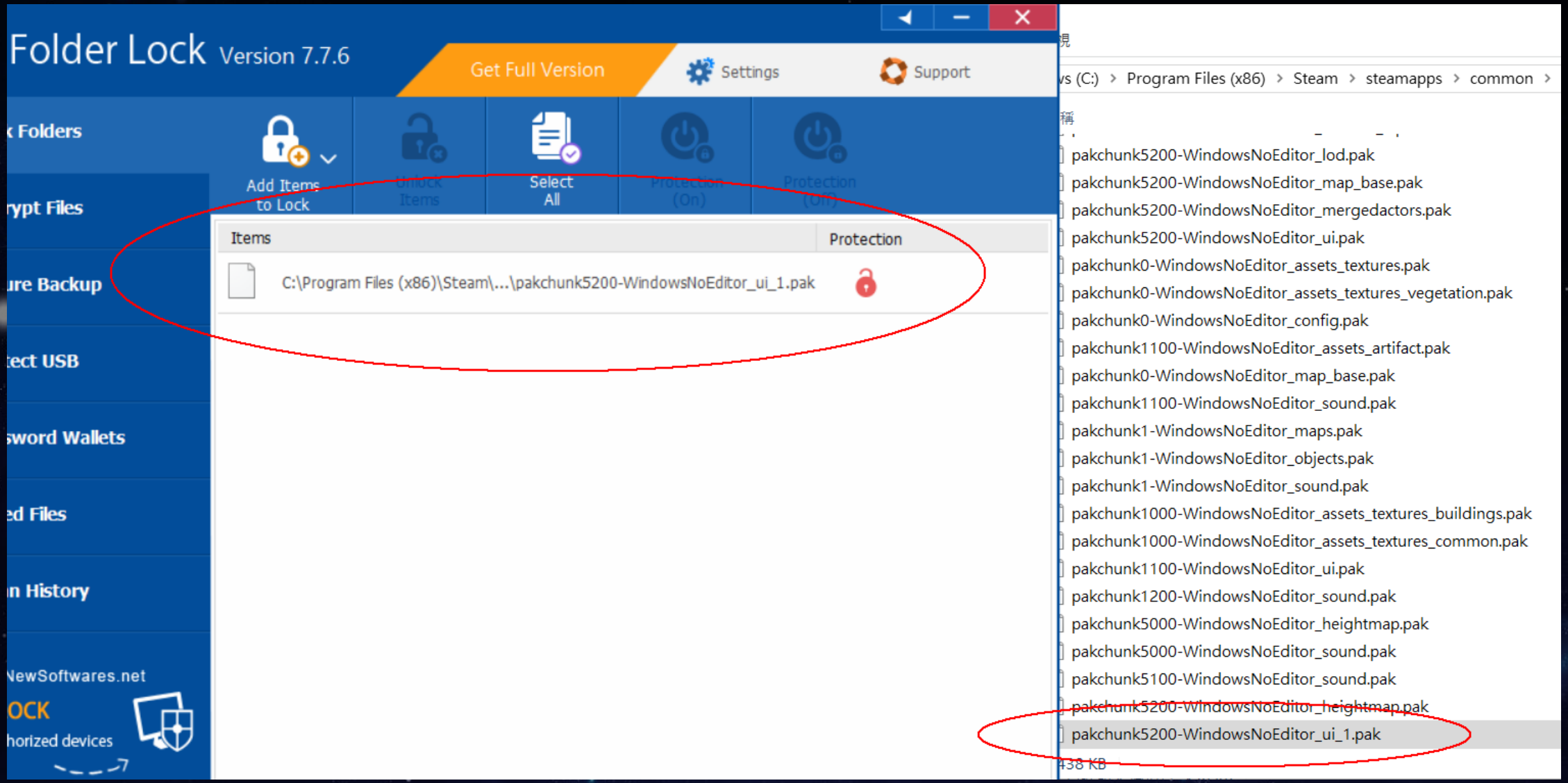
Demo [100%無後座力影片]

修改 Unreal Engine 虛幻遊戲引擎 - Bypass



- Easy File Locker：隱藏檔案 / 資料夾的工具
- 原理: Minifilter Drivers (微軟推薦實作方法)
- 三月初被公布，一直到六月中才列入黑名單

Make Bypass Greate again




人生最厲害
就是這個
BUT!

Make Bypass Greate again

帳戶警示 - 2018 年 6 月 27 日

PLAYERUNKNOWN'S BATTLEGROUNDS 已在 BattlEye 中以遊戲開發者的名義永久封鎖您。

您可前往封鎖歷史紀錄查看您 Steam 帳戶的遊戲封鎖狀態，以及受個別封鎖影響的遊戲列表。

有關遊戲封鎖的施行方式，請見遊戲封鎖一文。

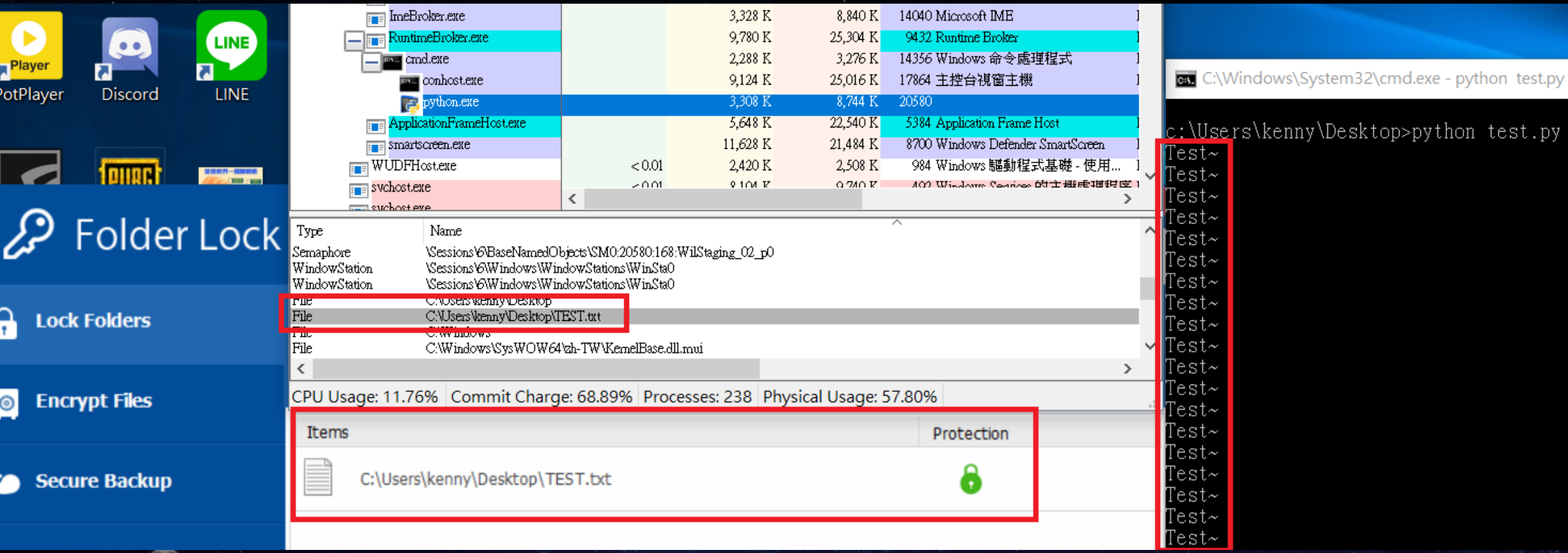
Make Bypass Greate again

TslGame.exe	17.59	1,867,516 K	1,060,892 K	3892 TslGame	Bluehole GinnoGames, Inc.	0x68

Type	Name	Handle	Access	Object Address
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Binaries\Win64	0x6D4	0x00100020	0xFFFF9C8D4F3304C0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Binaries\Win64\bgsecondary.dat	0x1788	0x0012019F	0xFFFF9C8D51C77A90
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor.pak	0x678	0x00120089	0xFFFF9C8D49351080
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor.pak	0xEB0	0x00120089	0xFFFF9C8D4E7E36D0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor.pak	0xEC4	0x00120089	0xFFFF9C8D4E7DFC50
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_asset_registry.pak	0x674	0x00120089	0xFFFF9C8D51BBFAF0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets.pak	0x670	0x00120089	0xFFFF9C8D3F232EF0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets.pak	0xDA8	0x00120089	0xFFFF9C8D4E830EF0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets.pak	0xEEC	0x00120089	0xFFFF9C8D50F2FEF0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_artifact.pak	0x66C	0x00120089	0xFFFF9C8D503D4C20
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_artifact.pak	0xECC	0x00120089	0xFFFF9C8D4E786EF0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures.pak	0x668	0x00120089	0xFFFF9C8D481E9CA0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures.pak	0xED0	0x00120089	0xFFFF9C8D4E784A80
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures_artifact.pak	0x664	0x00120089	0xFFFF9C8D51A8D5E0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures_buildings.pak	0x660	0x00120089	0xFFFF9C8D4D2EAA50
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures_buildings.pak	0xEC8	0x00120089	0xFFFF9C8D519169A0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures_common.pak	0x65C	0x00120089	0xFFFF9C8D4FB27080
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures_vegetation.pak	0x658	0x00120089	0xFFFF9C8D48090920
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_textures_vegetation.pak	0xEF4	0x00120089	0xFFFF9C8D4E85AAD0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_world.pak	0x654	0x00120089	0xFFFF9C8D51A72890
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_world.pak	0xEF0	0x00120089	0xFFFF9C8D4EEF8910
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_assets_world.pak	0xEFC	0x00120089	0xFFFF9C8D4E855EF0
File	C:\Program Files (x86)\Steam\steamapps\common\PUBG\TslGame\Content\Paks\pakchunk0-WindowsNoEditor_config.pak	0x650	0x00120089	0xFFFF9C8D50A73CF0

六月底 patch - PAK File Handle 處理

Make Bypass Greate again



最新流行的玩意兒

Demo 飛天車 [影片]

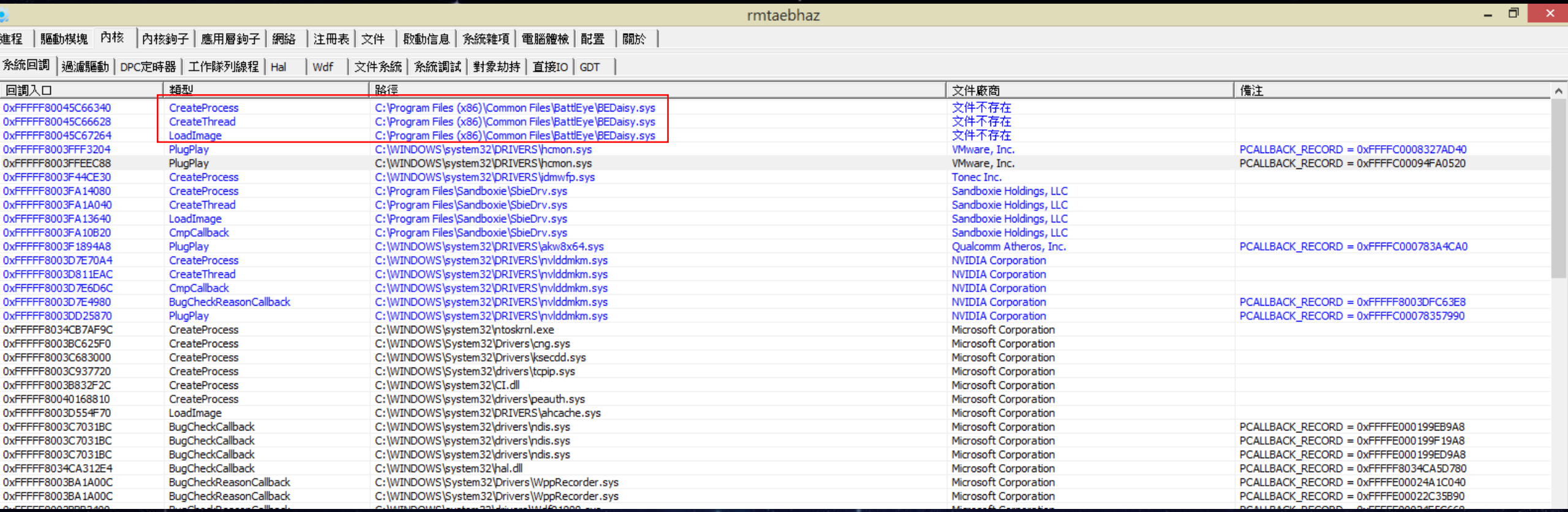

開車兜風 錯了嗎?
THE WIZARDING WORLD OF Harry Potter

04 分析遊戲保護 & Intel® 虛擬化

分析遊戲保護 - BattlEye

- BattlEye is 100% developed in Germany.
- BattlEye (BE) was founded by Bastian Suter in October 2004.
  - 八卦:作者也是做遊戲外掛出身
- 測試環境: Win10 x64

分析遊戲保護 – Kernel Mode

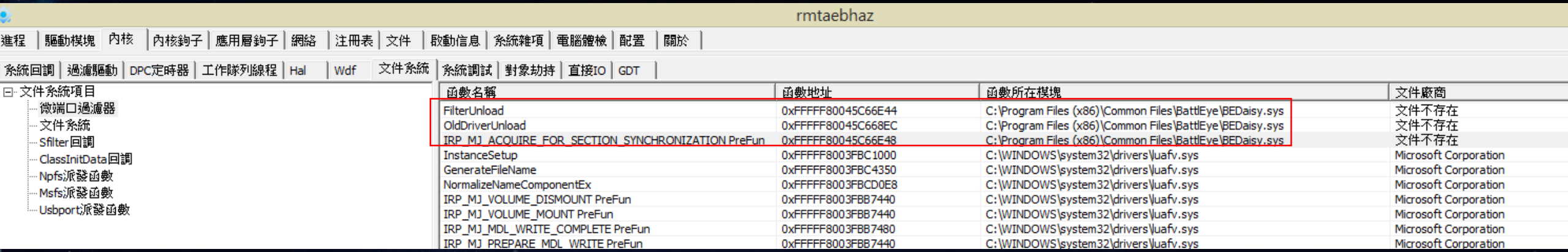


回調入口	類型	路徑	文件廠商	備注
0xFFFFF80045C66340	CreateProcess	C:\Program Files (x86)\Common Files\BattlEye\BEDaisy.sys	文件不存在	
0xFFFFF80045C66628	CreateThread	C:\Program Files (x86)\Common Files\BattlEye\BEDaisy.sys	文件不存在	
0xFFFFF80045C67264	LoadImage	C:\Program Files (x86)\Common Files\BattlEye\BEDaisy.sys	文件不存在	
0xFFFFF8003FFF3204	PlugPlay	C:\WINDOWS\system32\DRIVERS\hcmon.sys	VMware, Inc.	PCALLBACK_RECORD = 0xFFFFC0008327AD40
0xFFFFF8003FFEEC88	PlugPlay	C:\WINDOWS\system32\DRIVERS\hcmon.sys	VMware, Inc.	PCALLBACK_RECORD = 0xFFFFC00094FA0520
0xFFFFF8003F44CE30	CreateProcess	C:\WINDOWS\system32\DRIVERS\dmwfp.sys	Tonec Inc.	
0xFFFFF8003FA14080	CreateProcess	C:\Program Files\Sandboxie\SbieDrv.sys	Sandboxie Holdings, LLC	
0xFFFFF8003FA1A040	CreateThread	C:\Program Files\Sandboxie\SbieDrv.sys	Sandboxie Holdings, LLC	
0xFFFFF8003FA13640	LoadImage	C:\Program Files\Sandboxie\SbieDrv.sys	Sandboxie Holdings, LLC	
0xFFFFF8003FA10B20	CmpCallback	C:\Program Files\Sandboxie\SbieDrv.sys	Sandboxie Holdings, LLC	
0xFFFFF8003F1894A8	PlugPlay	C:\WINDOWS\system32\DRIVERS\akw8x64.sys	Qualcomm Atheros, Inc.	PCALLBACK_RECORD = 0xFFFFC000783A4CA0
0xFFFFF8003D7E70A4	CreateProcess	C:\WINDOWS\system32\DRIVERS\nvlddmkm.sys	NVIDIA Corporation	
0xFFFFF8003D811EAC	CreateThread	C:\WINDOWS\system32\DRIVERS\nvlddmkm.sys	NVIDIA Corporation	
0xFFFFF8003D7E6D6C	CmpCallback	C:\WINDOWS\system32\DRIVERS\nvlddmkm.sys	NVIDIA Corporation	
0xFFFFF8003D7E4980	BugCheckReasonCallback	C:\WINDOWS\system32\DRIVERS\nvlddmkm.sys	NVIDIA Corporation	PCALLBACK_RECORD = 0xFFFFF8003DFC63E8
0xFFFFF8003DD25870	PlugPlay	C:\WINDOWS\system32\DRIVERS\nvlddmkm.sys	NVIDIA Corporation	PCALLBACK_RECORD = 0xFFFFC00078357990
0xFFFFF8034CB7AF9C	CreateProcess	C:\WINDOWS\system32\ntoskrnl.exe	Microsoft Corporation	
0xFFFFF8003BC625F0	CreateProcess	C:\WINDOWS\System32\Drivers\cng.sys	Microsoft Corporation	
0xFFFFF8003C683000	CreateProcess	C:\WINDOWS\System32\Drivers\ksecdd.sys	Microsoft Corporation	
0xFFFFF8003C937720	CreateProcess	C:\WINDOWS\System32\drivers\tcpip.sys	Microsoft Corporation	
0xFFFFF8003B832F2C	CreateProcess	C:\WINDOWS\system32\CI.dll	Microsoft Corporation	
0xFFFFF8040168810	CreateProcess	C:\WINDOWS\system32\drivers\peauth.sys	Microsoft Corporation	
0xFFFFF8003D554F70	LoadImage	C:\WINDOWS\system32\DRIVERS\ahcache.sys	Microsoft Corporation	
0xFFFFF8003C7031BC	BugCheckCallback	C:\WINDOWS\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFE000199EB9A8
0xFFFFF8003C7031BC	BugCheckCallback	C:\WINDOWS\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFE000199F19A8
0xFFFFF8003C7031BC	BugCheckCallback	C:\WINDOWS\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFE000199ED9A8
0xFFFFF8034CA312E4	BugCheckCallback	C:\WINDOWS\system32\hal.dll	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF8034CA5D780
0xFFFFF8003BA1A00C	BugCheckReasonCallback	C:\WINDOWS\System32\Drivers\WppRecorder.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFE00024A1C040
0xFFFFF8003BA1A00C	BugCheckReasonCallback	C:\WINDOWS\System32\Drivers\WppRecorder.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFE00022C35B90

- CreateProcess_callback => 監控開啟的 Process
- CreateThread_callback => 監控開啟的 Thread
- LoadImage_callback => 監控載入的 Image

Kill All

分析遊戲保護 – Kernel Mode

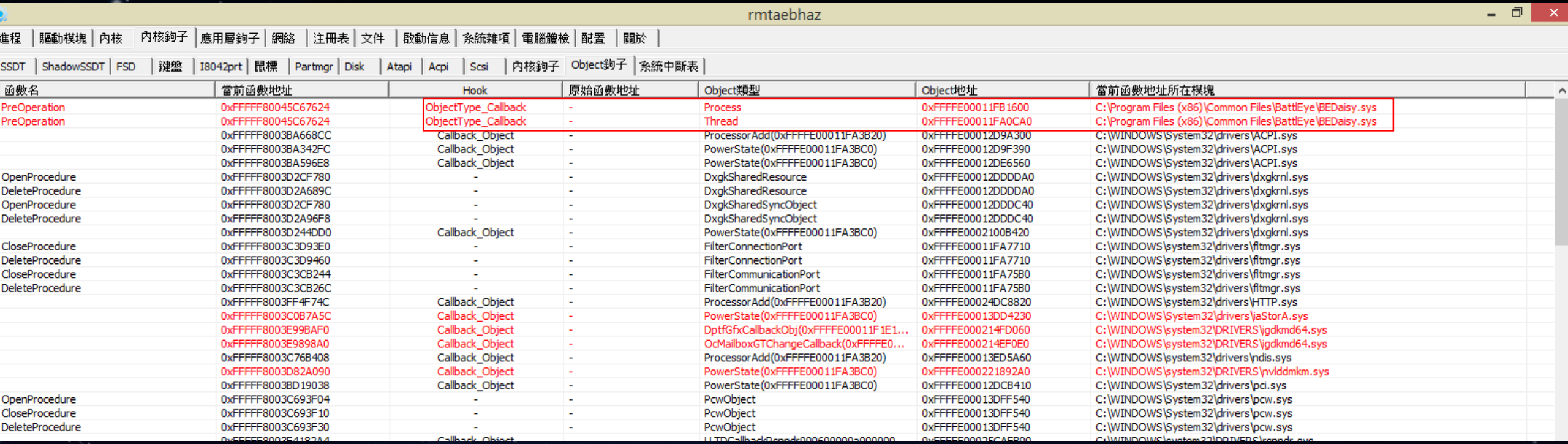


MiniFilter

- **IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION**
  - 偵測 Dll Inject

→ **Kill All**

分析遊戲保護 – Kernel Mode

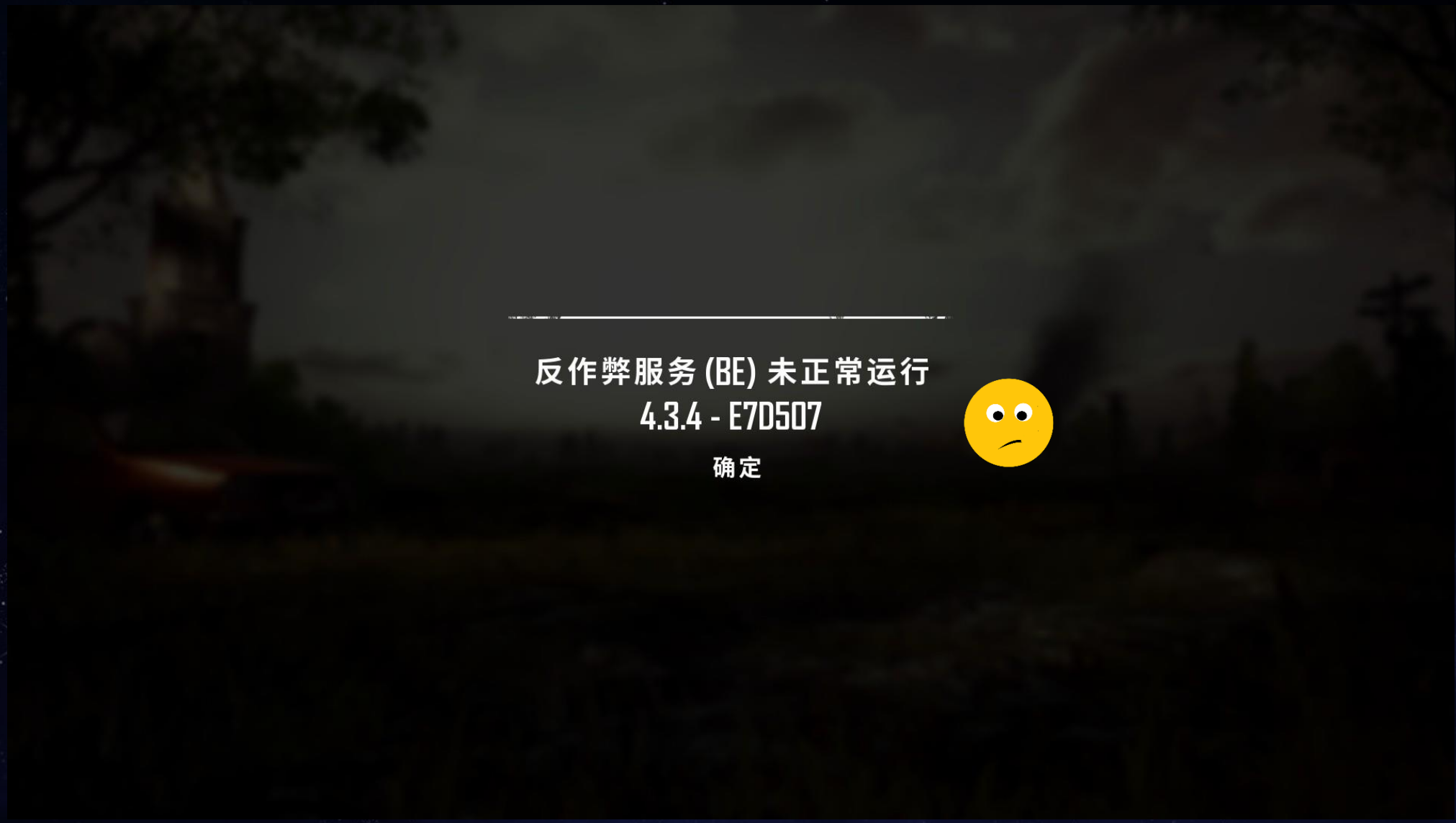


函數名	當前函數地址	Hook	原始函數地址	Object類型	Object地址	當前函數地址所在模塊
PreOperation	0xFFFFF80045C67624	ObjectType_Callback	-	Process	0xFFFFE00011FB1600	C:\Program Files (x86)\Common Files\BattlEye\BEDaisy.sys
PreOperation	0xFFFFF80045C67624	ObjectType_Callback	-	Thread	0xFFFFE00011FA0CA0	C:\Program Files (x86)\Common Files\BattlEye\BEDaisy.sys
	0xFFFFF8003BA668CC	Callback_Object	-	ProcessorAdd(0xFFFFE00011FA3B20)	0xFFFFE00012D9A300	C:\WINDOWS\System32\drivers\ACPI.sys
	0xFFFFF8003BA342FC	Callback_Object	-	PowerState(0xFFFFE00011FA3BC0)	0xFFFFE00012D9F390	C:\WINDOWS\System32\drivers\ACPI.sys
	0xFFFFF8003BA596E8	Callback_Object	-	PowerState(0xFFFFE00011FA3BC0)	0xFFFFE00012DE6560	C:\WINDOWS\System32\drivers\ACPI.sys
OpenProcedure	0xFFFFF8003D2CF780	-	-	DxgkSharedResource	0xFFFFE00012DDDDA0	C:\WINDOWS\System32\drivers\dxgkrnl.sys
DeleteProcedure	0xFFFFF8003D2A689C	-	-	DxgkSharedResource	0xFFFFE00012DDDDA0	C:\WINDOWS\System32\drivers\dxgkrnl.sys
OpenProcedure	0xFFFFF8003D2CF780	-	-	DxgkSharedSyncObject	0xFFFFE00012DDDC40	C:\WINDOWS\System32\drivers\dxgkrnl.sys
DeleteProcedure	0xFFFFF8003D2A96F8	-	-	DxgkSharedSyncObject	0xFFFFE00012DDDC40	C:\WINDOWS\System32\drivers\dxgkrnl.sys
	0xFFFFF8003D244DD0	Callback_Object	-	PowerState(0xFFFFE00011FA3BC0)	0xFFFFE0002100B420	C:\WINDOWS\System32\drivers\dxgkrnl.sys
CloseProcedure	0xFFFFF8003C3D93E0	-	-	FilterConnectionPort	0xFFFFE00011FA7710	C:\WINDOWS\system32\drivers\fltmgr.sys
DeleteProcedure	0xFFFFF8003C3D9460	-	-	FilterConnectionPort	0xFFFFE00011FA7710	C:\WINDOWS\system32\drivers\fltmgr.sys
CloseProcedure	0xFFFFF8003C3CB244	-	-	FilterCommunicationPort	0xFFFFE00011FA75B0	C:\WINDOWS\system32\drivers\fltmgr.sys
DeleteProcedure	0xFFFFF8003C3CB26C	-	-	FilterCommunicationPort	0xFFFFE00011FA75B0	C:\WINDOWS\system32\drivers\fltmgr.sys
	0xFFFFF8003FF4F74C	Callback_Object	-	ProcessorAdd(0xFFFFE00011FA3B20)	0xFFFFE00024DC8820	C:\WINDOWS\system32\drivers\HTTP.sys
	0xFFFFF8003C0B7A5C	Callback_Object	-	PowerState(0xFFFFE00011FA3BC0)	0xFFFFE00013DD4230	C:\WINDOWS\System32\drivers\jaStorA.sys
	0xFFFFF8003E99BAF0	Callback_Object	-	DptfGfxCallbackObj(0xFFFFE00011F1E1...	0xFFFFE000214FD060	C:\WINDOWS\system32\DRIVERS\igdkmd64.sys
	0xFFFFF8003E9898A0	Callback_Object	-	OcMailboxGTChangeCallback(0xFFFFE0...	0xFFFFE000214EF0E0	C:\WINDOWS\system32\DRIVERS\igdkmd64.sys
	0xFFFFF8003C76B408	Callback_Object	-	ProcessorAdd(0xFFFFE00011FA3B20)	0xFFFFE00013ED5A60	C:\WINDOWS\system32\drivers\ndis.sys
	0xFFFFF8003D82A090	Callback_Object	-	PowerState(0xFFFFE00011FA3BC0)	0xFFFFE000221892A0	C:\WINDOWS\system32\DRIVERS\nvlddmkm.sys
	0xFFFFF8003BD19038	Callback_Object	-	PowerState(0xFFFFE00011FA3BC0)	0xFFFFE00012DCB410	C:\WINDOWS\System32\drivers\pci.sys
OpenProcedure	0xFFFFF8003C693F04	-	-	PcwObject	0xFFFFE00013DFF540	C:\WINDOWS\System32\drivers\pcw.sys
CloseProcedure	0xFFFFF8003C693F10	-	-	PcwObject	0xFFFFE00013DFF540	C:\WINDOWS\System32\drivers\pcw.sys
DeleteProcedure	0xFFFFF8003C693F30	-	-	PcwObject	0xFFFFE00013DFF540	C:\WINDOWS\System32\drivers\pcw.sys

- **ObRegisterCallbacks Kernel API [微軟推薦]**
  - **Strip Process / Thread Handle**
    - **PROCESS_VM_OPERATION**
    - **PROCESS_VM_READ**
    - **PROCESS_VM_WRITE**
    - **PROCESS_DUP_HANDLE**
    - **...**

→ **Kill All...**

分析遊戲保護 – Kernel Mode



分析遊戲保護 – User Mode

ntdll.dll->DbgBreakPoint
ntdll.dll->DbgUiRemoteBreakin ➔ Anti Debuger

KERNEL32.DLL->LoadLibraryExW
KERNELBASE.dll->ResumeThread ➔ Anti Code Inject

USER32.dll->CreateWindowExW
d3d9.dll->Direct3DCreate9
d3d9.dll->Direct3DCreate9Ex
DDRAW.dll->DirectDrawCreate
dxgi.dll->CreateDXGIFactory ➔ Anti Directx Control

USER32.dll->GetCursorPos
USER32.dll->GetKeyState
USER32.dll->SetCursorPos ➔ Anti aoto mouse / kerboard

遊戲保護 – User Mode Bypass

騷年 - 老司機開車囉

遊戲保護 – User Mode Bypass

SetWinowsHookEx (WM_CALLWNDPROC , Hooker , Module , 0)

Global Inject

OBS Studio

```
int inject_library_safe_obf(DWORD thread_id, const wchar_t *dll,
                const char *set_windows_hook_ex_obf, uint64_t obf1)
{
        HMODULE user32 = GetModuleHandleW(L"USER32");
        set_windows_hook_ex_t set_windows_hook_ex;
```

TslGame.exe	20.94	1,807,856 K	1,027,204 K	10916 TslGame	Bluehole GinnoGames, Inc.	0x64

Name	Description	Company Name	Path
GFSDK_SSAO.win64.dll	GFSDK_SSAO.win64.dll		C:\Program Files (x86)\Steam\steamapps\common\PUBG\Engine\Binaries\ThirdParty\NVIDIA\GameWorks\GFSDK_SSAO\GFSDK_SSAO.win64.dll
glu32.dll	OpenGL 公用程式程式庫 DLL	Microsoft Corporation	C:\Windows\System32\glu32.dll
gpapi.dll	群組原則用戶端 API	Microsoft Corporation	C:\Windows\System32\gpapi.dll
hid.dll	Hid 使用者程式庫	Microsoft Corporation	C:\Windows\System32\hid.dll
Hook_x64.dll	SampleHIPS	Kenny	C:\Users\kenny\Desktop\SampleHIPS\Hook_x64.dll
icudtcoherent53.dll	ICU Data DLL	The ICU Project	C:\Program Files (x86)\Steam\steamapps\common\PUBG\Engine\Binaries\ThirdParty\CoherentUIGT\Win64\icudtcoherent53.dll
iertutil.dll	Internet Explorer 的執行階段公用程式	Microsoft Corporation	C:\Windows\System32\iertutil.dll
igc64.dll	Intel Graphics Shader Compiler for Intel(R)...	Intel Corporation	C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf_amd64_250db833a1cd577e\igc64.dll

遊戲保護 – User Mode Bypass

遊戲保護 – User Mode Bypass

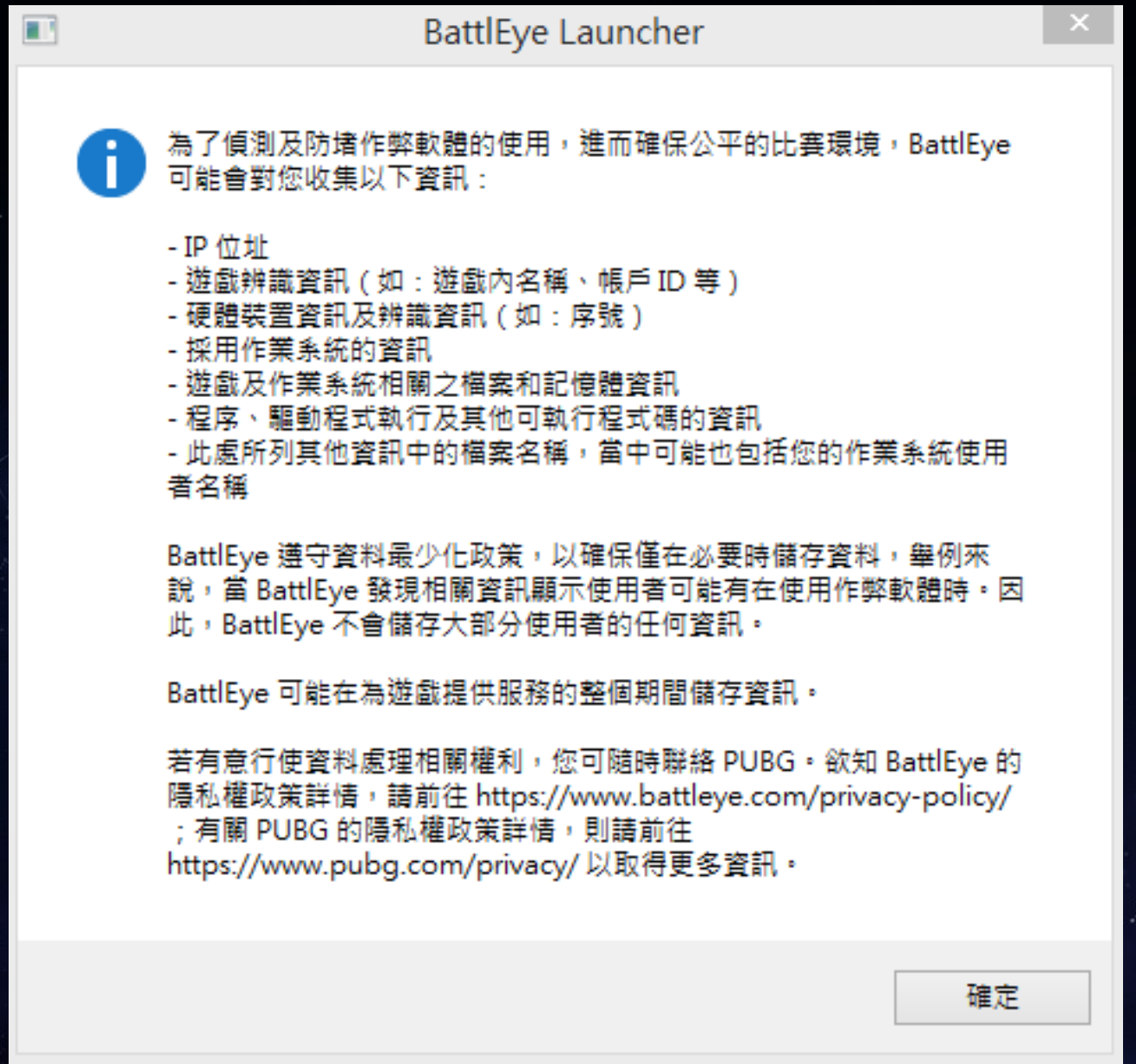
DII 都注進去了，接下來你懂得

遊戲保護 – Kernel Mode Bypass

- **Bypass ObRegisterCallbacks Handle Strip.**
- **Kernel API : MmCopyVirtualMemory**

```
NTSTATUS KeReadVirtualMemory(PEPROCESS Process, PVOID SourceAddress, PVOID TargetAddress, SIZE_T Size)
{
    SIZE_T Result;
    __try
    {
        if (NT_SUCCESS(MmCopyVirtualMemory(Process, SourceAddress, PsGetCurrentProcess(),
            TargetAddress, Size, KernelMode, &Result)))
            return STATUS_SUCCESS;
    }
    __except (EXCEPTION_EXECUTE_HANDLER)
    {
        //DbgPrintEx( 0,0,"KeReadVirtualMemory Exception");
    }
    return STATUS_ACCESS_DENIED;
}
```

分析遊戲保護 – 收集資料聲明

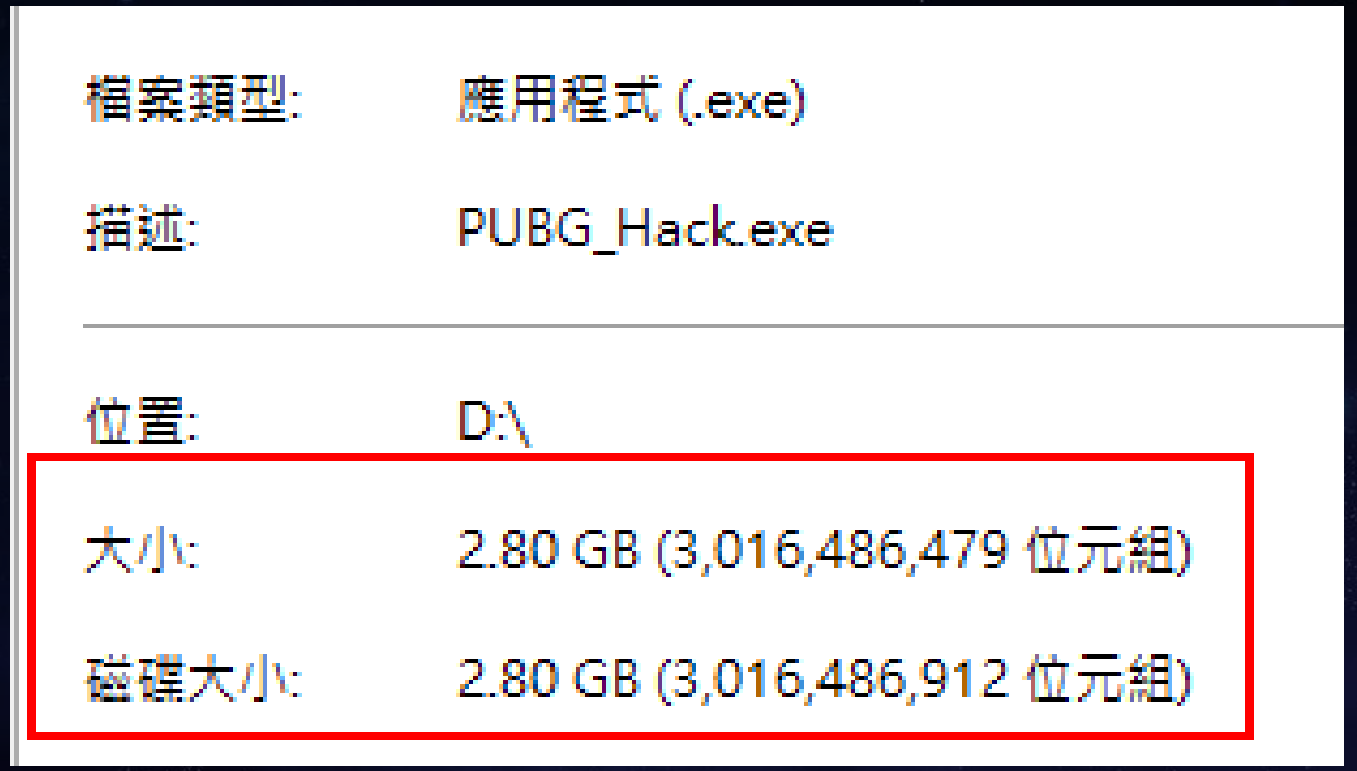


遊戲保護 – 對抗動態 & 靜態特徵掃描

- Vmprotect 虛擬保護殼 will help you.
  - 抹掉所有Strings
    - 「Bypass BattlEye」 -> 不抓你抓要抓誰?
  - 所有 Function 都用 VMP SDK 虛擬化保護
    - 模糊到你媽都認不出來 :P

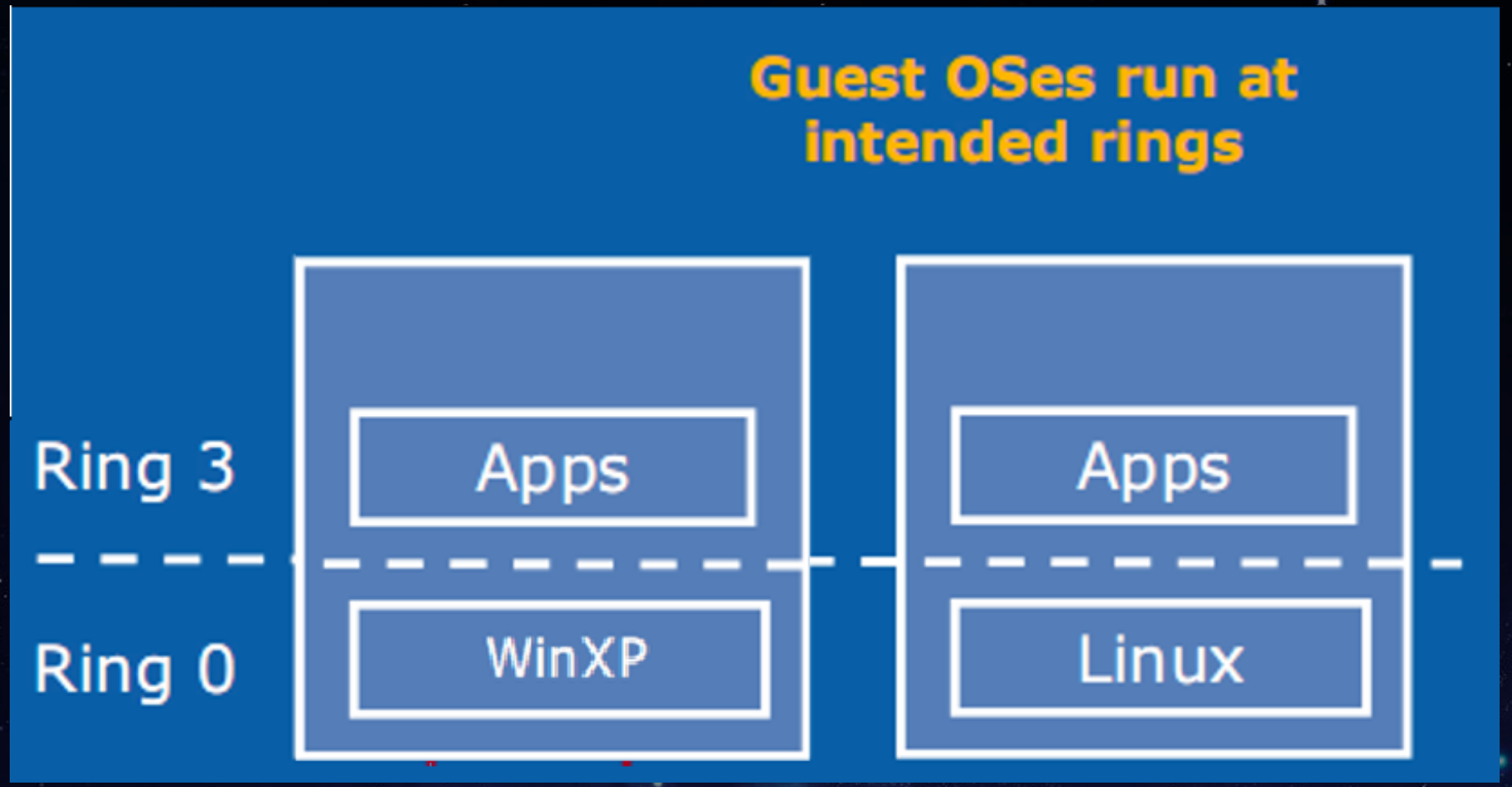
遊戲保護 – 對抗動態 & 靜態特徵掃描

- 對抗檔案上傳
- 簡單 / 有效 / 暴力
- 你看過檔案大小 3GB 的外掛嗎?

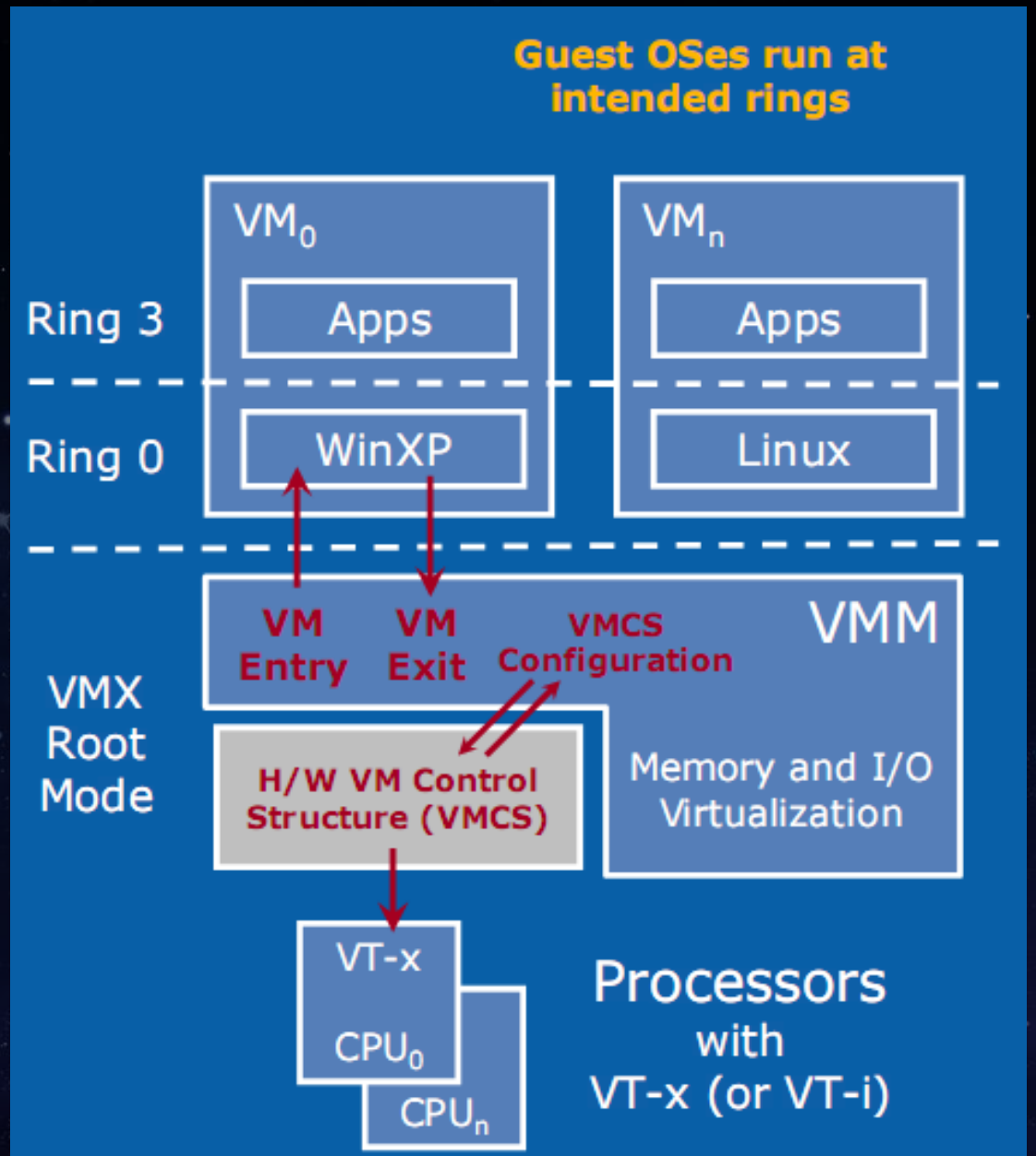


更強大的隱藏方法?

Intel® 虛擬化技術 (Intel® VT)



Intel® 虛擬化技術 (Intel® VT)



Intel® 虚擬化技術 (Intel® VT) - HyperPlatform

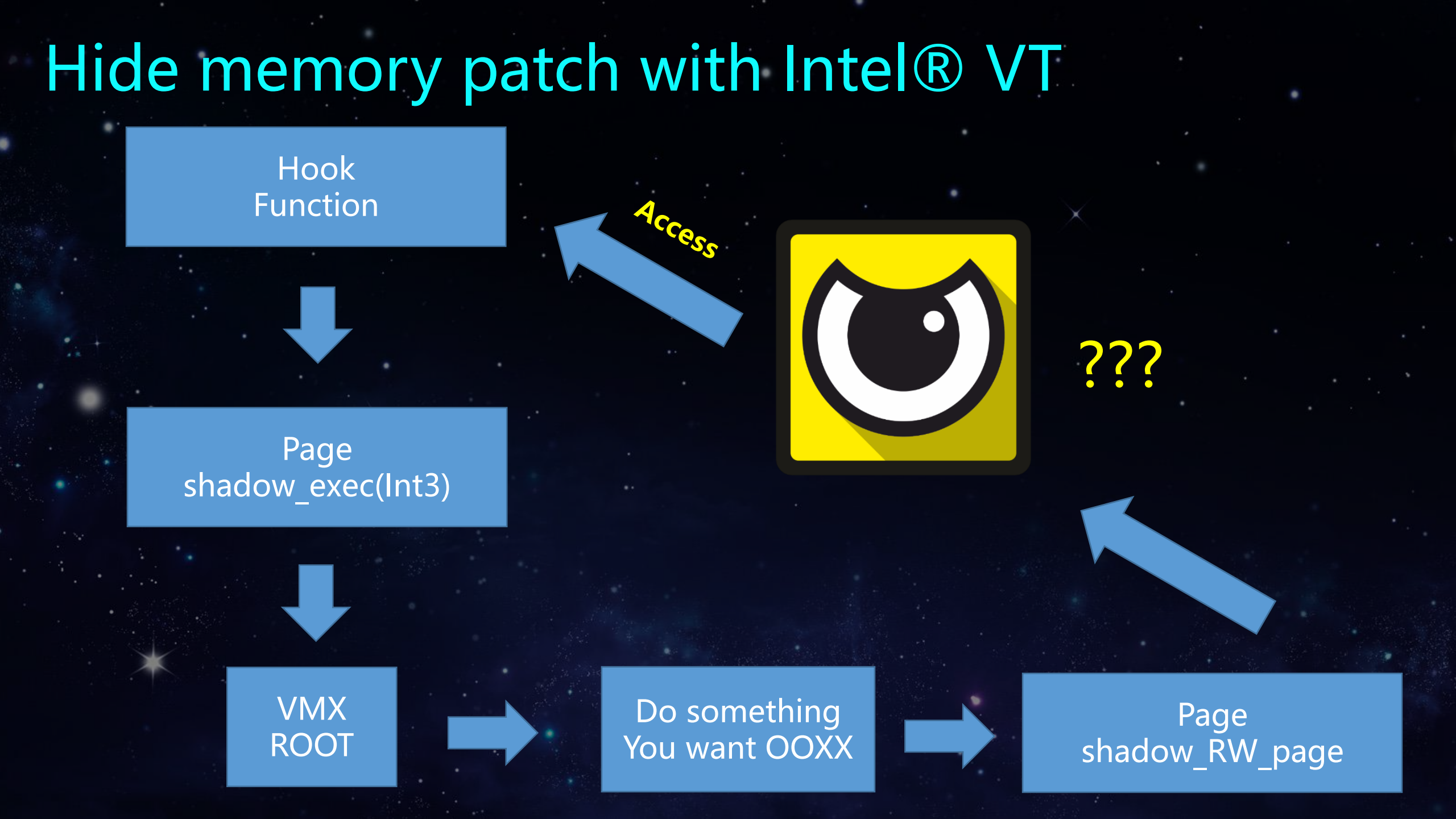
Satoshi Tanda

https://github.com/tandasat/HyperPlatform

Intel® 虛擬化技術 (Intel® VT) – 應用

- Analyzing kernel mode rootkit
- Virtual-machine-based sandbox
- Reverse-engineering the Windows kernel
- Hide memory patch from usermode & kernelmode

Hide memory patch with Intel® VT



Intel® 虛擬化技術 (Intel® VT)

實作 KernelMode SSDT Func Hook

- Bypass Anti Rootkit (PC Hunter / Poower Tool)
- Bypass Patch guard

Intel® 虛擬化技術 (Intel® VT)

Demo Intel VT Rootkit [影片]

DEMO 神仙大戰[影片]

Bluehole


不开挂的人生
一样强大
加入#绝地求生反外挂行动#,一同与外挂对抗到底!

傳承

30秒公司徵才


Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehen-derit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.
EPS 10
ABSTRACT GRAPHIC
vector Illustration
THANK YOU

Reference

https://www.deviantart.com/k9dogster/art/Pubg-Give-me-the-chicken-709157114
https://article-fd.zol-img.com.cn/t_s640x2000/g5/M00/0D/02/ChMkJlpLRdCIJ6FxAAHmzL3uzeUAAjvQwMEkFUAAebk514.jpg
https://www.g-cores.com/articles/22150
https://zh.wikipedia.org/wiki/DirectX
https://www.unknowncheats.me/forum/playerunknown-s-battlegrounds/283879-spectator-xrays.html
https://www.logitechg.com/zh-tw/product/g502-proteus-core-tunable-gaming-mouse
https://knowyourmeme.com/photos/348101-iddqd
https://dribbble.com/shots/1434596-God-Mode-Logo-Comp
https://www.hpfl.net/#!/online/forum/viewthread.php?f=2&t=3313
https://github.com/minglich/logitech-pubg
http://699pic.com/tupian-400218942.html
https://www.anandtech.com/show/2480/9
https://commons.wikimedia.org/wiki/File:Avant-Tower-Gaming-PC.png
http://pngimg.com/download/25963
https://hk.saowen.com/a/a87c5677fdc54937d112349e0e4675668a3270465970117b059ef255db59e8f6
https://en.wikipedia.org/wiki/Bluehole_(company)
http://www.wjbb.com/know/1599
https://sumtips.com/2018/06/control-youtube-playback-in-chrome-with-autohotkey.html
http://t.cj.sina.com.cn/articles/view/6431194824/p17f543ec800100dgh7?cre=tianyi&mod=pcpager_fintoutiao&loc=1&r=9&doct=0&rfunc=100&tj=none&tr=9
https://pets.ettoday.net/news/28563
https://emojiisland.com/products/100-perfect-emoji-icon
https://thehackernews.com/2017/06/ghosthook-windows-10-hacking.html
https://home.gamer.com.tw/creationDetail.php?sn=3389760
https://pixabay.com/zh/%E8%A1%A8%E6%83%85%E7%AC%A6%E5%8F%B7-%E8%84%B8-%E6%83%85%E6%84%9F-%E4%BC%A4%E5%BF%83-2792377/
http://hk.on.cc/hk/bkn/cnt/lifestyle/20160618/bkn-20160618162140072-0618_00982_001_cn.html