

那些年，我們一起寫的外掛

所以我到底為什麼會去寫外掛咧？

所以今天...？

- Hi, I am Inndy (木棍)
- 過去是個中二的少年
- 我們來聊聊外掛
- 可惜我沒有吃惡魔果實



MS-Memory Writer v1.0 alpha for MapleStory and HackShield 5.2.17.993+ by nimo1993.

檔案(File) 編輯(Edit) 說明(Help)



Nimo Table:

☐ 顯示16進位數值 (Show as hex value)

Lock 名稱(Name)	位址(Address)	型態(Type)	值(Value)

因為尚未完成，現在只有Auto Assemble Script可以寫入，鎖定Value功能不支援。

Program and GUI: nimo1993; HS-CRC Cracking: 大可, JaySecret, nimo1993; Assembler: Kgame Thanks to: Dark Byte. (依字母順序)

Click to attach MS. ▾ No MapleStory Attached! * Unsaved *

Me, and my past

2008 : PHP / JavaScript

2011 : 終於升級到 VB.NET

2013 : 好像很厲害的Python

AND KEEP ON!

2015 : 潮到出水的Ruby (with Rails)

2012 : C# / C++ Builder

2010 : VB6 & 飽受挫折的 C 語言

Delphi

Reversing

Java

VB6

PHP

Ruby

Web Security

Python

lisp

Linux

C#

Assembly

C

JavaScript

“做壞事是進步的原動力”

–Inndy, 2015

接下來讓我們幹一些壞事（？）

ID: MSDoggy開發者 Lv.189



[28690/29050]



[1205/1411]



[210019304/340440105]

- ☒ 30秒無敵
- ☒ 人物不退
- ☒ 降低損血量
- ☒ 自動補HP (PageUp)
- 7000
- ☒ 自動補MP (PageDown)
- 1000

You are the VIP user.

- ☒ 怪不反擊
- ☒ 超級笨怪
- ☒ 雙倍標彈箭
- ☐ 終極攻擊無延遲
- ☐ 完全無敵
- ☐ 全圖吸物
- ☐ 吸怪掛機

Inddy

I want VIP.

F12 顯示/隱藏表單

保護 普通 過濾 按鍵

儲存

載入

ID: MSDoggy開發者 Lv.189



[28690/29050]

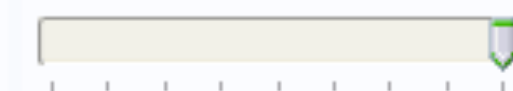


[1205/1411]



[210019304/340440105]

- ☒ 怪物變笨
- ☐ 定點跟隨(F4)
- 怪物跳動：
- 不跳
- 怪物擊退：
- 不退
- ☐ 移動加速(F2)

☐ 瞬間集滿

保護 普通 過濾 按鍵

儲存

載入

ID: MSDoggy開發者 Lv.189



[28690/29050]



[1205/1411]



[210019304/340440105]

- ☒ 物品過濾
- 2000000 // 紅色藥水
- 4280001 // 銀寶箱
- 1040004 // 藍修煉服
- 2061000 // 弩箭矢
- 2060000 // 箭矢
- 2440000 // 吃蟲桔小姐
- 2010009 // 青蘋果
- 4170025 // 英雄鑰匙
- 2940000 // 女媧的黃土副產
- 2440001 // 吃蟲寶石君
- 1002017 // 褐色舊魔法帽
- 1061029 // 紅夢褲
- 2512023 // 10階段智能藥水
- 2070009 // 木製陀螺
- 2512132 // 提昇的 4階段攻
- 4001701 // 重要線索
- 2512029 // 8階段幸運藥水白
- 2512156 // 提昇的 8階段力
- 2000019 // 超級藥水
- 2070005 // 雷之鏢
- 2512176 // 提昇的 8階段敏
- 2512006 // 9階段力量藥水白

偵測滑鼠指向物品 (F6)

移除物品請按Delete

保護 普通 過濾 按鍵

儲存

載入

ID: MSDoggy開發者 Lv.189



[28690/29050]



[1205/1411]



[210019304/340440105]

- ☐ 自動按鍵 (1) 秒
- ☒ 自動按鍵 (2) 240 秒
- ☒ 自動按鍵 (3) 180 秒
- ☒ 自動按鍵 (4) 240 秒
- ☒ 自動按鍵 (5) 180 秒
- ☒ 自動按鍵 (6) 240 秒
- ☒ 自動按鍵 (7) 114 秒
- ☒ 自動按鍵 (8) 240 秒
- ☒ 自動按鍵 (9) 360 秒

Doggy的貼心小提醒：

很杯具的本功能並不保證一

定能按到，所以請斟酌縮短

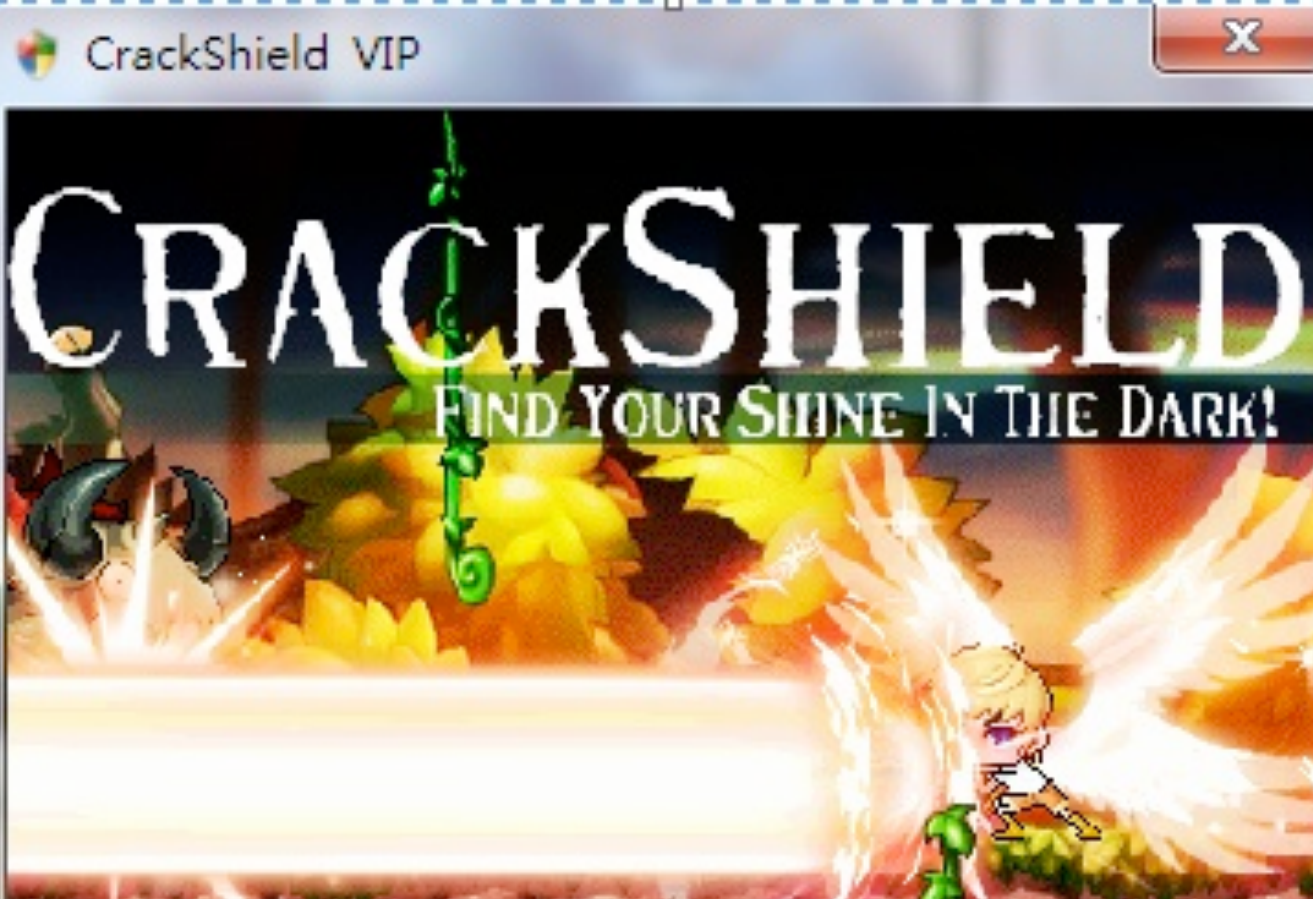
時間。

全部重按 (F3)

保護 普通 過濾 按鍵

儲存

載入



實用功能 | 自動按鍵 | 其他 | 掛機設置

自動補血補魔

☒ HP低於 5000 [Home]

☒ MP低於 500 [End]

☒ 怪物定點跟隨 ☒ 笨怪

☐ [F3]定怪 ☒ 遇GM斷線

☐ 終極無延遲二代

☒ 超級近戰無延遲+倍量魔水 ☒ 損血打折 ☒ 雙倍無限投器

☒ 無敵25秒 ☐ 滾筒/龍捲無延遲 ☒ 自動撿物 ☐ [F1]集氣秒放

☐ [F2]走路加速 ☐ 卡牌風暴無冷卻 ☒ 攻擊加速25%

☒ 幻影迴避65% ☒ 怪物不反擊 ☒ 怪物不擊退

自動全圖掛機模式[On]

CrackShield For Twms v149.1 V.I.P

授權給: 老趙

到期時間: 0/0/0

限制使用時間: 0分鐘

儲存 關閉遊戲



實用功能 | 自動按鍵 | 其他 | 掛機設置

☒ 按鍵A 間隔 20 秒 ☒ 按鍵E 間隔 40 秒

☒ 按鍵B 間隔 25 秒 ☒ 按鍵F 間隔 45 秒

☒ 按鍵C 間隔 30 秒 ☒ 按鍵G 間隔 50 秒

☒ 按鍵D 間隔 35 秒 ☒ 按鍵H 間隔 55 秒

☒ Delete放卡牌審判 40 張 ☒ 上線自動掛機

☐ 攻擊鍵(Ctrl) --無怪不放技

自動全圖掛機模式[On]

CrackShield For Twms v149.1 V.I.P

授權給: 老趙

到期時間: 0/0/0

限制使用時間: 0分鐘

儲存 關閉遊戲

你有用過這兩個外掛嗎？

比較強者我朋友和我的作品..

你會發現...

前者的視窗比例比較瘦長

因為那時候我的筆電只有1280 x 720

Game Hack

自動化、違反常理的遊戲行為



真是可愛的有違常理啊 <3



HACK

- ☒ 控怪走向 往左
- ☐ 怪物掉落
- ☒ 無敵笨怪

關閉遊戲 (C)

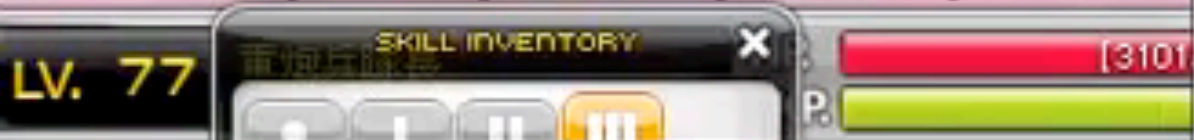
[卷軸] - 裝備屬性重置，讓你衝錯可重來；[保護卷軸] - 保證衝裝不會爆，高星高層就看它；[幸運日卷軸] - 衝卷成功率UP、神裝就此誕生！



全圖攻擊 + 攻擊加速



<人氣王勳章> Q半糖戀愛Q CHOM 4-2 Qo簡簡單單oQ 阿伯誠信收買



為了節省時間，動機機 速度播放

開外掛超賤的

幹，又是死外掛

我要檢舉你

路人A：所以你為什麼要開外掛？

(巴*特) 版主！！是外掛文快來刪除！

GM，有人開外掛啊！！

玩遊戲不能好好玩嗎？

因為遊戲玩不贏同學



所以只好開外掛



「二檔」

想想其實也是挺哀傷的



太哀傷了所以來隻貓吧！



等等，好像有什麼東西搞錯了...

開外掛的感覺就像是...

一個人拆了海軍總部



但是偶爾會被光速踢到



Oh... 我是說被GM鎖帳號

挖喔你會寫外掛耶

啊不就好棒棒厂厂

路人B：所以你為什麼要寫外掛？

我想要學外掛你可以教我嗎？

寫什麼外掛？破壞遊戲樂趣！

理由一：

自己的外掛自己寫，會寫外掛超帥的啊！

理由二：

身為一個 Hacker 就要勇於挑戰！

A close-up photograph of a Corgi puppy sitting on a light-colored paved surface. The puppy has a white blaze on its face, with brown and black patches around its eyes and on its ears. It is holding a single yellow leaf in its mouth. The background shows a dark wooden fence and a shadow of the puppy on the ground.

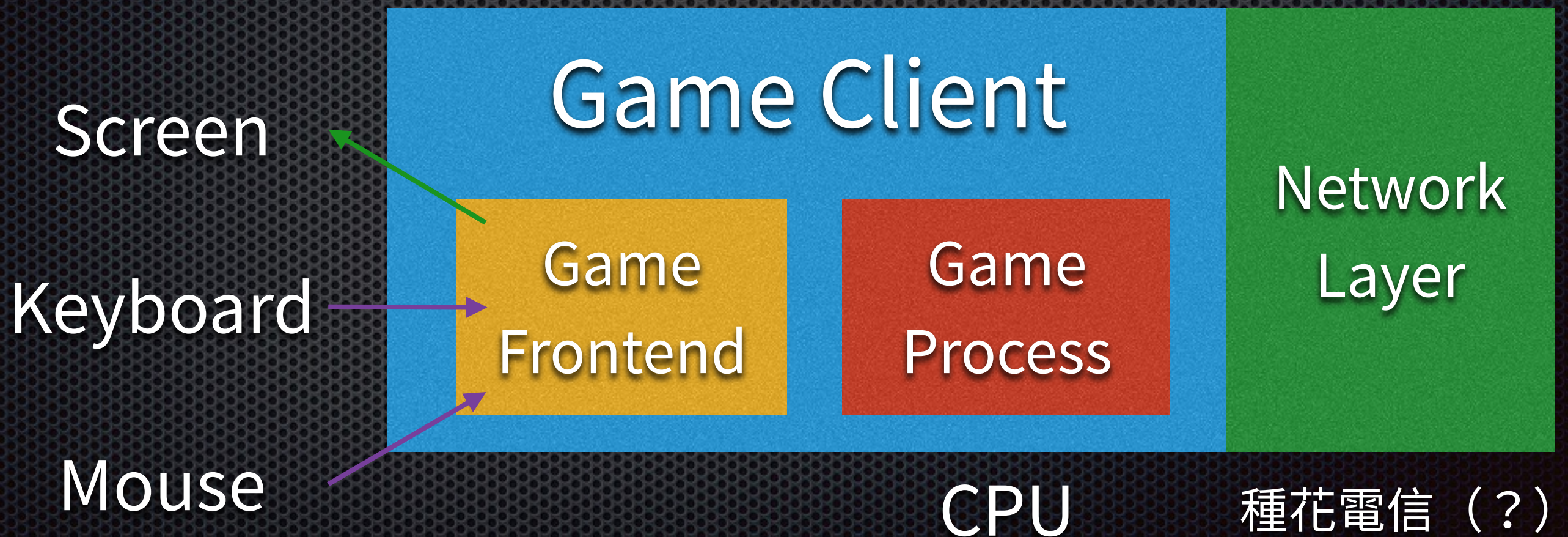
理由三：

你們都被遊戲玩，我要玩遊戲！

外掛的幾個層次



外掛的幾個層次



外掛的幾個層次

目標

按鍵精靈

自動化機器人

脫機外掛

比斯斯還多一種呢！



Mouse



CPU

種花電信（？）

外掛的幾個層次

- 按鍵精靈
 - Windows API : SendInput / PostMessage
- 自動化機器人
 - 影像辨識、流程控制、API Hook 達成後台操作
- 程式行為修改
 - Hook、Reversing
- 脫機外掛
 - Reversing (Decrypt Packet) 、Packet Analyze

外掛

反外掛

反反外掛

反反反外掛

所以到底是反還是不反？

崩 (𠂇 皿 𠂇) 潰

時代的眼淚

GG 的 GameGuard



後來一直到現在

Hackable HackShield



反反外掛

可是我就是想改

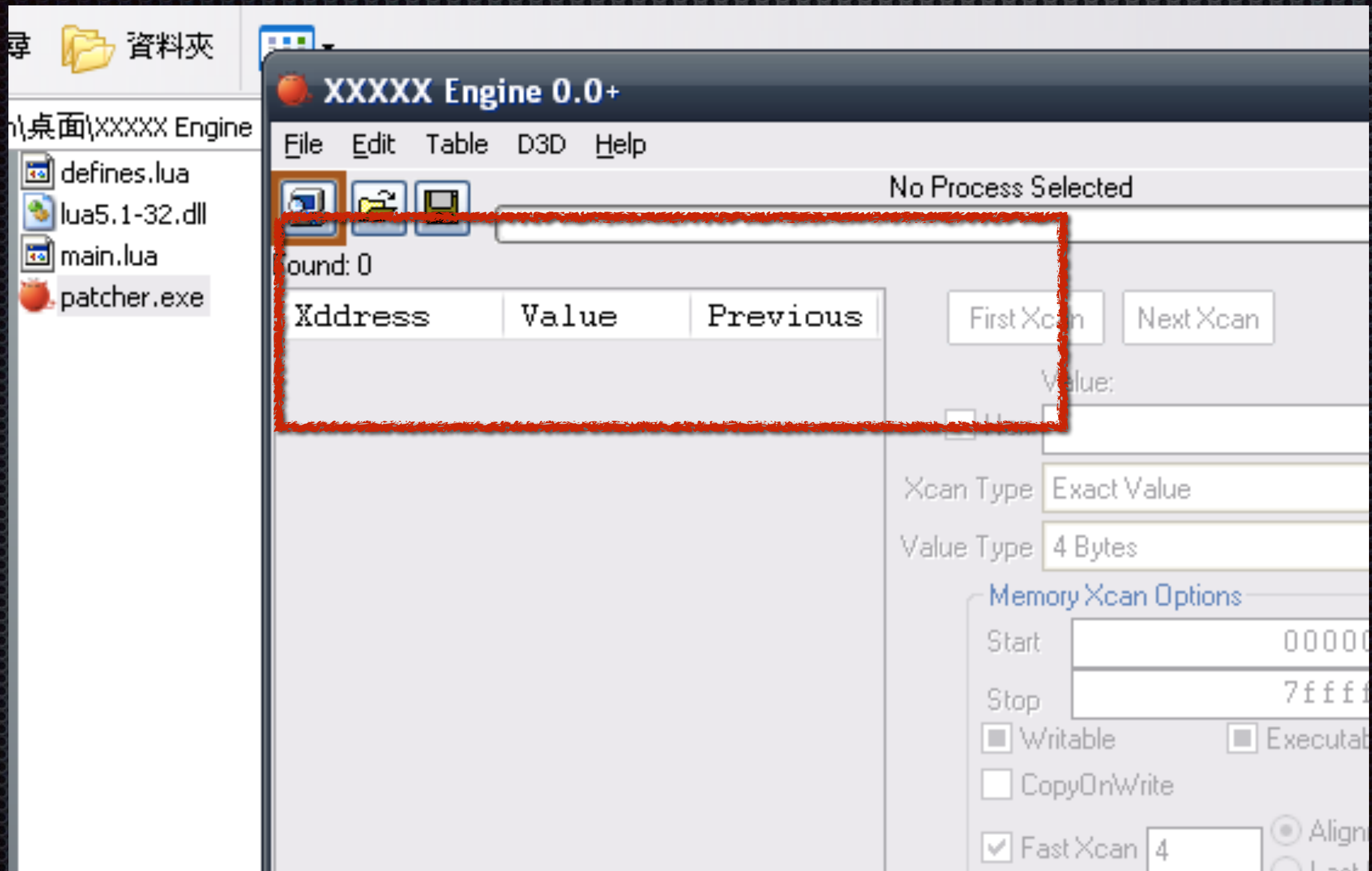
ImagePath 偽裝成工作管理員

Dark 在 2009 發現的，六年了還是能用，只有 x64 被修正

```
void fake_image_path(WCHAR *img_path) {  
    __asm {  
        // PEB  
        mov eax, fs:[0x30]  
        // _RTL_USER_PROCESS_PARAMETERS  
        mov eax, [eax+0x010]  
        // ImagePathName.Buffer  
        add eax, 0x3C  
        push img_path  
        pop [eax]  
    }  
}
```

ref: <http://www.hitcon.org/hit2009/download.htm>

ImagePath 偽裝其實不用那麼麻煩



patcher.exe ?

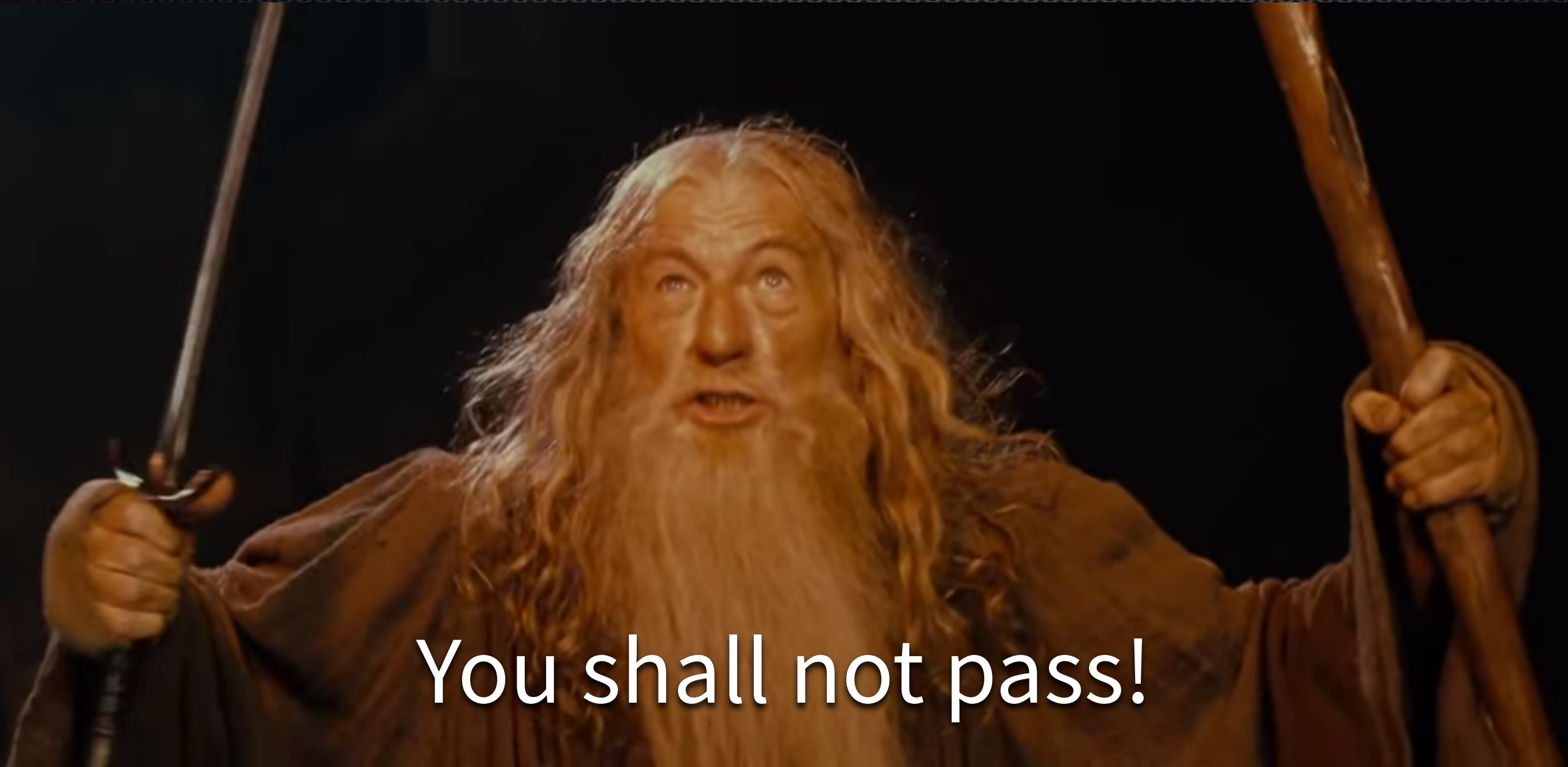
可以操作記憶體的程序白名單

也可以用taskmgr.exe

如果你需要自動按鍵...

```
int main()
{
    HWND game = FindWindow(NULL, "MapleStory");
    while(true)
    {
        PostMessage(game, WM_KEYDOWN, VK_CONTROL, 0);
        PostMessage(game, WM_KEYUP, VK_CONTROL, 0);
    }
}
```


HackShield says....



You shall not pass!

所以就把 lParam 參數修好

```
void PressKey(long KeyCode)
{
    unsigned char scan_code =
        MapVirtualKey(KeyCode, 0);

    PostMessage(MSHWND, WM_KEYDOWN, KeyCode,
        0x00000001 | scan_code << 16);

    PostMessage(MSHWND, WM_KEYUP, KeyCode,
        0xC0000001 | scan_code << 16);
}
```


我就是你，你就是我 — Inject DLL



```
graph TD; DLL[DLL] --> GameProcess[Game Process]
```

DLL

Game Process

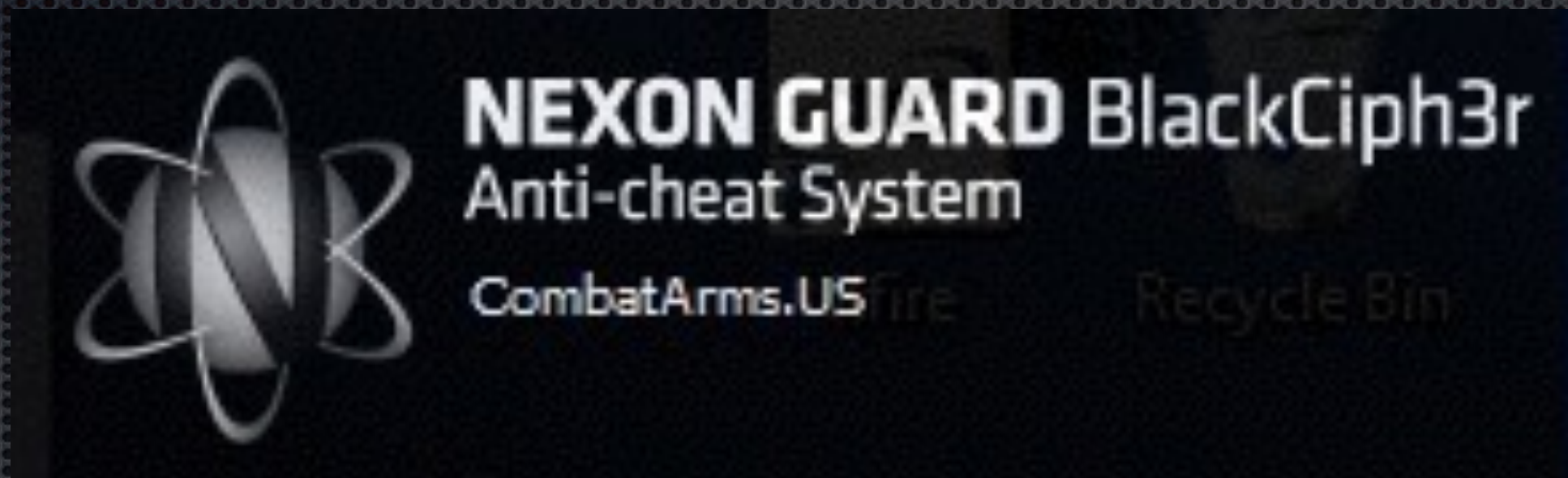
我就是你，你就是我 — Inject DLL

- 透過 LoadLibrary 可以載入 DLL，引用程式庫
- CreateRemoteThread — 在別人家裡面開 Thread
- 遊戲的記憶體就是我的記憶體！

反反反外掛

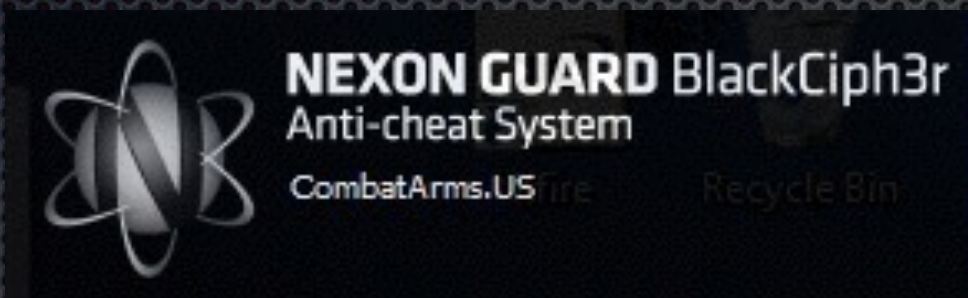
我就是不想讓你亂改

Nexon 自己開發了這東西



Lv. 3

HP : 2/10



Lv. 5

HP : 9/15

▶效果十分顯著！！才怪！！！！

(´・ω・`)

遊戲外掛產業與生態

其實就是黑產



玩家

遊戲廠商

外掛開發者

商人
交易平台



玩家

遊戲廠商

會被罵

外掛開發者

商人
交易平台



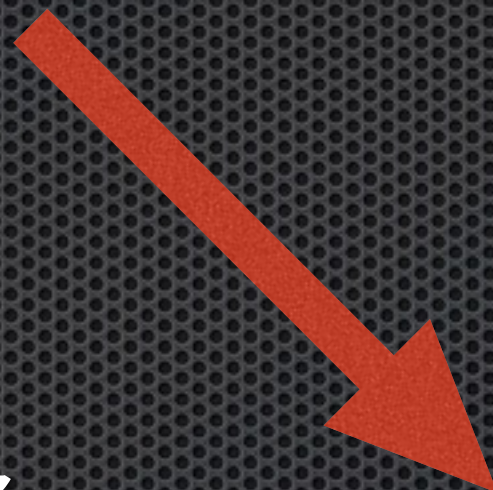
玩家

遊戲廠商

賺最多

外掛開發者

商人
交易平台



但是我沒有賺到錢

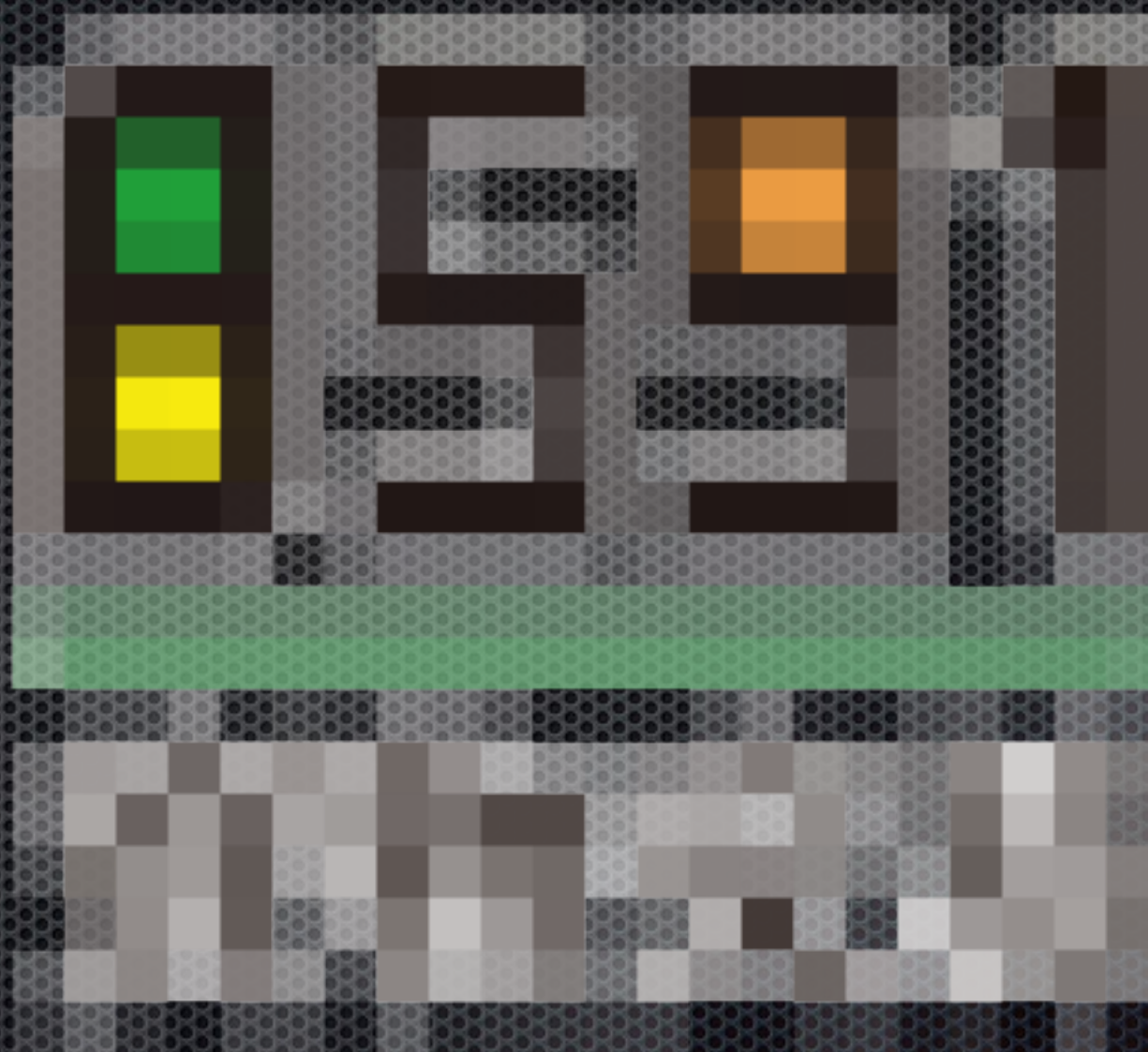
T____T

遊戲的黑色產業

- 遊戲幣對儲值點數的買賣
- 遊戲道具換現金
- 遊戲帳號（角色）買賣
- 代客練功、解任務、打Boss
- 販售外掛

台灣最大的交易平台

為了避免廣告嫌疑所以我打了馬賽克



因為該平台禁止交易外掛程式

我們需要一些掩人耳目的方法...

S18-51	已完成	12-14 17:54	新楓之谷 - 其他 龍蛋便宜賣	\$ 106
S18-06	已完成	12-14 17:54	新楓之谷 - 其他 龍蛋便宜賣	\$ 106
S18-58	已完成	12-14 17:54	新楓之谷 - 其他 龍蛋便宜賣	\$ 106
S18-35	已完成	12-13 22:18	新楓之谷 - 其他 龍蛋便宜賣	\$ 103
S18-54	已完成	12-13 20:36	新楓之谷 - 其他 龍蛋便宜賣	\$ 127
S18-98	已完成	12-13 20:35	新楓之谷 - 其他 龍蛋便宜賣	\$ 106

MultiMS Auth Manager

複製 貼上 # 加密 解密 輸出資料 上傳更新 資料存檔 備份資料 排序

用戶管理

硬體序號：4CuG/rkkTxv

客戶名稱：

購買管道：8591

備註資料：等待續費



新增



編輯

關鍵字：1Nw



搜尋



批量添加

用戶

硬體序號

客戶名稱

購買管道

備註資料

AAJY6	=	4	19	8591	等待續費
BDZw	=	T		Facebook	Unlimited
BDZw	:Dm9a8nbJComj...	9	12	8591	等待續費
BDZw	Z7avNM7XPWf	真	祥	Facebook	Free
BDZw	Z7avNNzYudK	真	祥	Facebook	Free
BDZw	mKJICC+z7Yh...	4	19	8591	等待續費
BDZw	gdOTO8Y=	z	06	永恆血色	
BDZw	Safc/TqLSaB05...	z	06	永恆血色	
BDZw	DotJoHTkzvG	z	06	永恆血色	
CMa//	pPE=	2	44	8591	等待續費
CPCrZ	=	8	55	8591	等待續費
CPCrZ	em+MV2o=	7	20	8591	等待續費
CPCrZ	UmpvjFdq	7	20	8591	等待續費
CPCrZ	DqYDqevD	3	山	Facebook	Unlimited
CPCrZ	06I=	c	32101	永恆血色	
CPCrZ	=	9	10	8591	等待續費
CPCrZ	o=	4	50	8591	等待續費
CPCrZ	!LvWTrWWjYr...	1	52	8591	等待續費
CPCrZ	!LvWTrWWjYr...	1	52	8591	等待續費
CPCrZ	jyfw=	6	35	8591	等待續費
CPCrZ	jyfw=	7	20	8591	等待續費
CPCrZ	WYXY=	1	821	其他	買過Doggy的
dBgGt	=	2	96	8591	等待續費
dBgGt	=	1	143	8591	等待續費
dBgGt	z9s=	1	940	8591	等待續費
dBgGt	=	3	誠	Facebook	
dBgGt	hU1hDIvR+	3		Facebook	Free
dBgGt	3Io=	9	06	8591	等待續費
dBgGt	=	6	27	8591	等待續費
dE9W.	Fw=	7	56	8591	等待續費
dE9W.	=	7	56	8591	等待續費
dE9W.	=	7	56	8591	等待續費
dKNJ7	qu3NsLc7jN	1	340	8591	等待續費
dKNJ7	{fQ=	9	42	8591	等待續費
dKNJ7		3	璋	Facebook	
dLpdV	eIM=	1	009	8591	等待續費
dMRv	eJRXy=	1	925	8591	等待續費

輸入輸入

遊戲多開賺的比外掛多 QAQ

- 那時候市面上的多開失效了 (Mutex)
- 另一個朋友研究出修改 HackShield 保護參數的方法
- 每次改版收費，那時候沒有打廣告但是生意很好
- 以前商人賺我錢，現在通通賺回來！

現在是農曆七月啊...

所以每天晚上十點

A group of four women are posing in matching outfits at what appears to be an auto show. They are wearing gold sequined halter-neck tops and black fringed shorts. The woman on the far left is partially obscured by the text. The woman next to her is smiling and pointing towards the camera. The woman on the right is also smiling. In the background, a white car is visible, and another woman in a white dress stands near it. A sign with the word 'Turbo' is visible on the right.

都會有複製人軍團出沒

其實就是打幣團上工了...

最後，跟大家說一個秘密！

學外掛可以救資安！

- ✧ 論壇經營學到社交工程
- ✧ 外掛技術接軌逆向工程，培養駭客思維
- ✧ 想要寫外掛就要學程式，學底層
- ✧ 賣外掛寫驗證，Web / Crypto 沒問題

Q & A