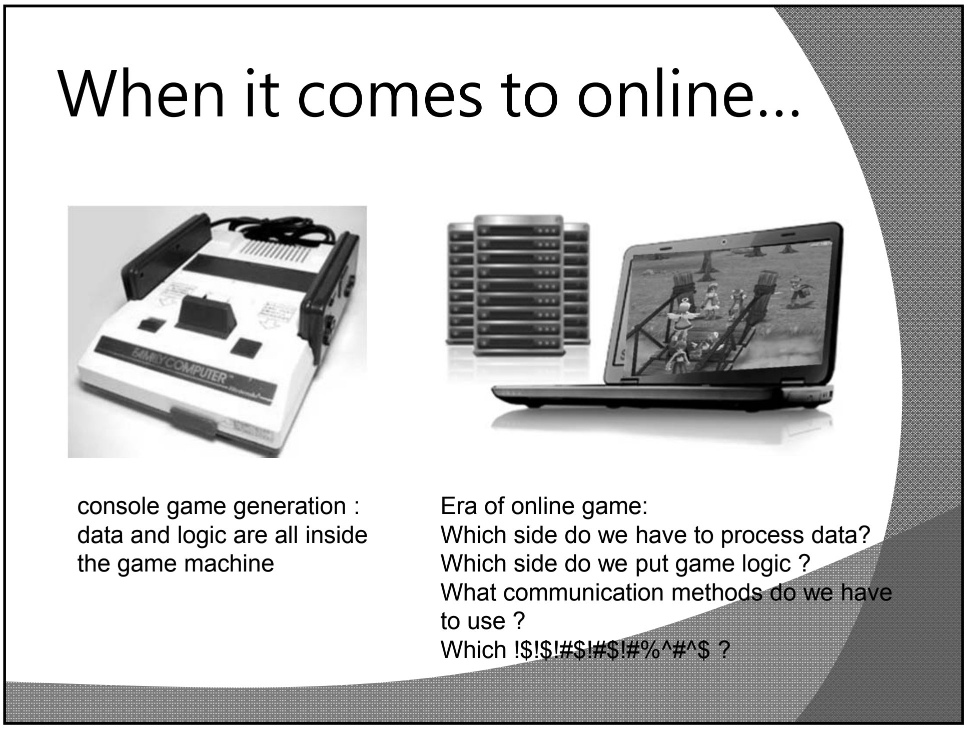
Story about fight against cyber gangsters

SPEARS AND SHIELDS ON ONLINE GAME

Seunghyun Seo a.k.a. truefinder

- KHDP
  - Board member of Korea Hacking Document Project
  - Team Syrinx won in World Information Security Olympia 2001
- HackersLab (3 years)
  - Pen-tester, administrator of drill.hackerslab.org
- Webzen (2 years)
  - Win32 Deverloper, Online game maker (MuOnline, SunOnline, …)
- NHN Japan (4 years)
  - Security Researcher, Major online game publisher (DragonNest, Tera, R2, Elsword, PachinkoDX, LUNA twinkle …)
- Japanese mobile giant (2012~)
  - Security Researcher, famous mobile game publisher

Online Game?
It’ s pretty tough here!

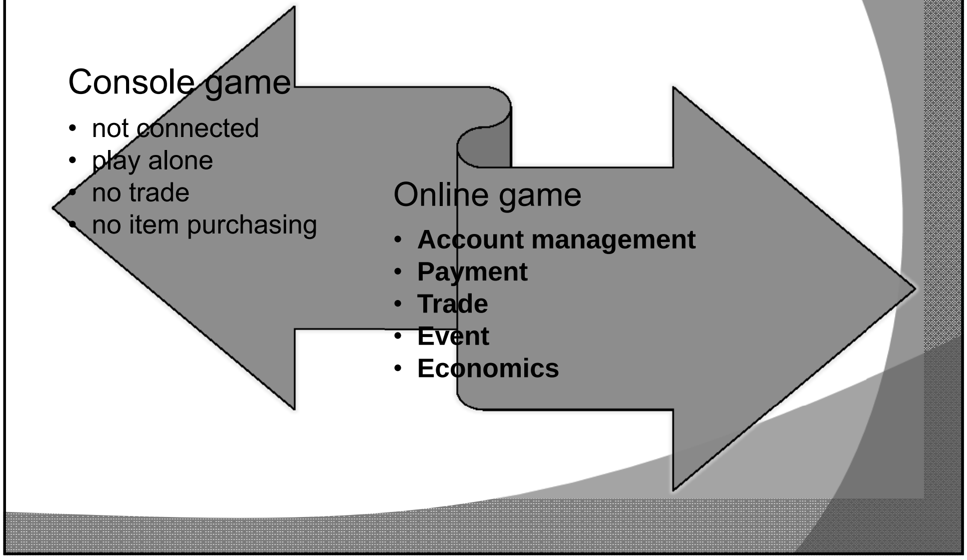


When it comes to online…

console game generation :
data and logic are all inside the game machine

Era of online game:
Which side do we have to process data?
Which side do we put game logic ?
What communication methods do we have to use ?
Which !$!$!#$!#$!#%^#^$?

Issues in online game?



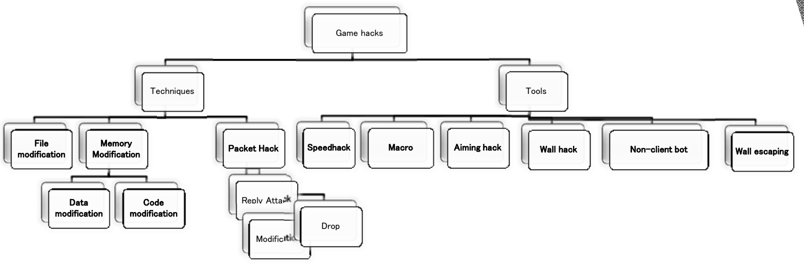
Console game

- not connected
- play alone
- no trade
- no item purchasing

Online game

- **Account management**
- **Payment**
- **Trade**
- **Event**
- **Economics**

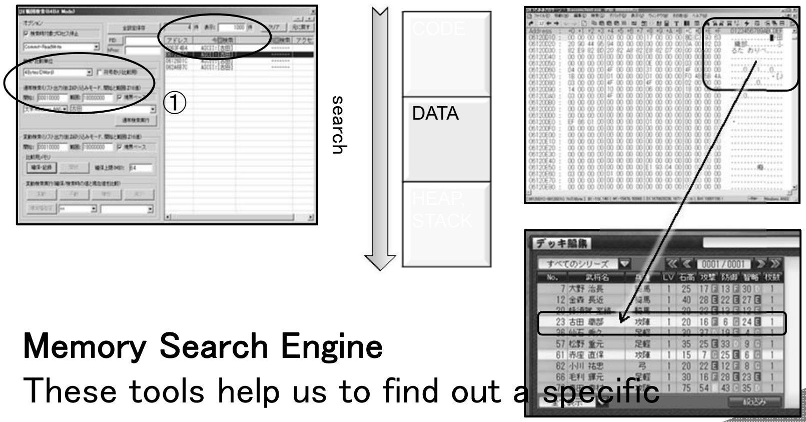
Technical overview of game hacks



Basics

Windows Memory Structure | Assembly | PE structure | Stack structure | Calling convention | DLL Injection | API Hook | Windows kernel | Debug | Anti-Reversing

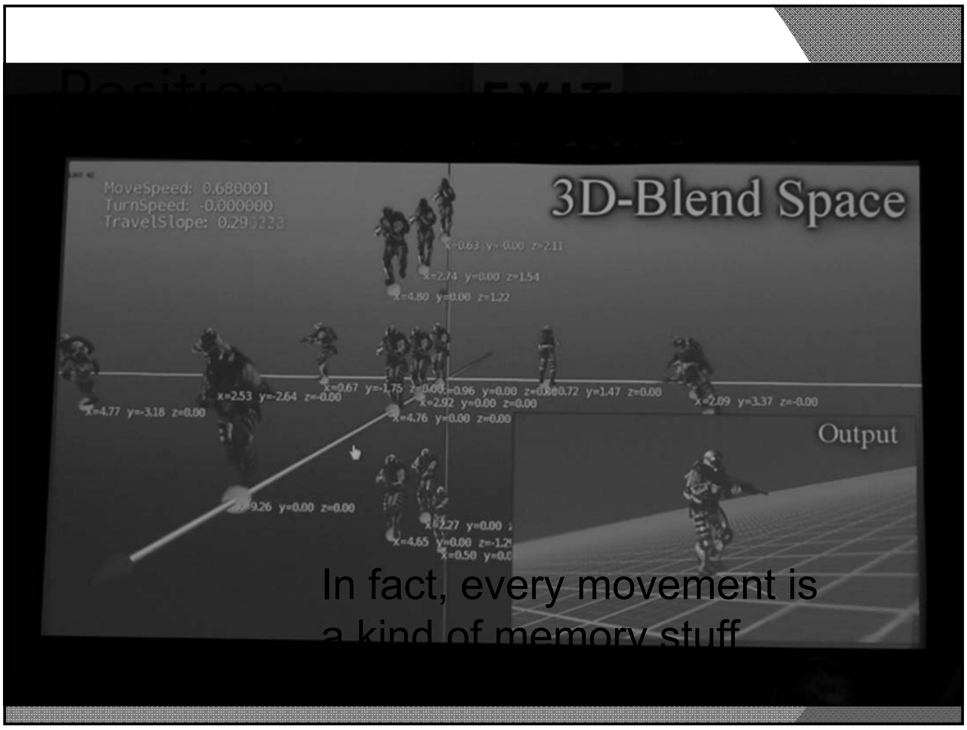
Hp, mp, money, exp …



Memory Search Engine

These tools help us to find out a specific value from game by skimming over its process memory

Position



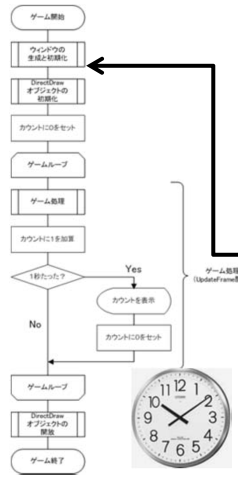
In fact, every movement is a kind of memory stuff

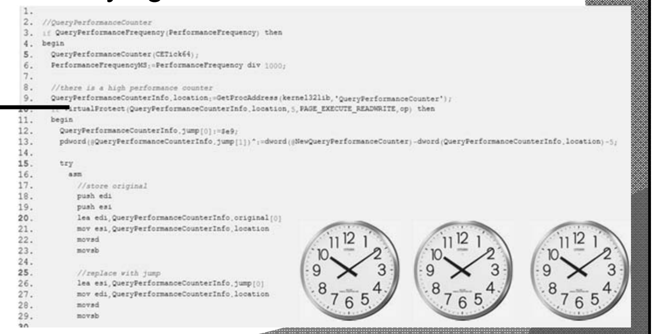
Nice view, ah !

~~~~~~@@@
송송이 : 우와
RedEye : 공참 79짜리 추옹 구해요
송송이 : 저거 강화하려고
송송이 : 마돌 무자게 썼겠다
천리지창 : 봉깃인데요 ㅠㅠㅋ
천리지창 : 마돌이아니고 ㅋ

Speed

FPS is frame per second, it means how many frames are processed per second, Speed hack makes this FPS faster, modifying time functions



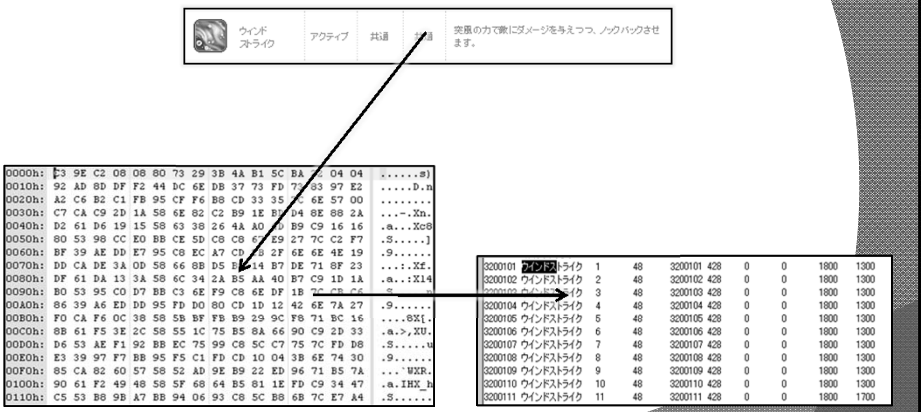


```

//QueryPerformanceCounter
if QueryPerformanceFrequency(PerformanceFrequency) then
begin
  QueryPerformanceCounter(CETick64);
  PerformanceFrequencyMS:=PerformanceFrequency div 1000;

  //there is a high performance counter
  QueryPerformanceCounterInfo.location:=GetProcAddress(kernel32lib,'QueryPerformanceCounter');
  if VirtualProtect(QueryPerformanceCounterInfo.location,5,PAGE_EXECUTE_READWRITE,op) then
  begin
    QueryPerformanceCounterInfo.jump[0]:=$e9;
    pdword(@QueryPerformanceCounterInfo.jump[1])^:=dword(@NewQueryPerformanceCounter)-dword(QueryPerformanceCounterInfo.location)-5;

    try
      asm
        //store original
        push edi
        push esi
        lea edi,QueryPerformanceCounterInfo.original[0]
        mov esi,QueryPerformanceCounterInfo.location
        movsd
        movsb

        //replace with jump
        lea esi,QueryPerformanceCounterInfo.jump[0]
        mov edi,QueryPerformanceCounterInfo.location
        movsd
        movsb

```
~~~~~~

files

There's a lot of interesting things when we break file encryption of game resource

Skill, item, monster, map, …



ウィンド ストライク	アクティブ	共通	共通	突風の力で敵にダメージを与えつつ、ノックバックさせます。

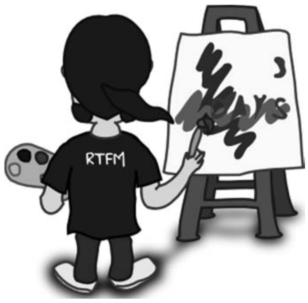
```
0000h: C3 9E C2 08 08 80 73 29 3B 4A B1 5C BA 22 04 04  ......s)
0010h: 92 AD 8D DF F2 44 DC 6E DB 37 73 FD 73 83 97 E2  .....D.n
0020h: A2 C6 B2 C1 FB 95 CF F6 B8 CD 33 35 7C 6E 57 00  ........
0030h: C7 CA C9 2D 1A 58 6E 82 C2 B9 1E BD D4 8E 88 2A  ...-.Xn.
0040h: D2 61 D6 19 15 58 63 38 26 4A A0 8D B9 C9 16 16  .a...Xc8
0050h: 80 53 98 CC E0 BB CE 5D C8 C8 67 E9 27 7C C2 F7  .S.....]
0060h: BF 39 AE DD E7 95 C8 EC A7 CD 2B 2F 6E 6E 4E 19  .9......
0070h: DD CA DE 3A 0D 58 66 8B D5 B5 14 B7 DE 71 8F 23  ...:.Xf.
0080h: DF 61 DA 13 3A 58 6C 34 2A B5 AA 40 B7 C9 1D 1A  .a..:X14
0090h: B0 53 95 C0 D7 BB C3 6E F9 C8 6E DF 1B 7C CB C6  .S.....n
00A0h: 86 39 A6 ED DD 95 FD D0 80 CD 1D 12 42 6E 7A 27  .9......
00B0h: F0 CA F6 0C 38 58 5B BF FB B9 29 9C F8 71 BC 16  ....8X[.
00C0h: 8B 61 F5 3E 2C 58 55 1C 75 B5 8A 66 90 C9 2D 33  .a.>,XU.
00D0h: D6 53 AE F1 92 BB EC 75 99 C8 5C C7 75 7C FD D8  .S.....u
00E0h: E3 39 97 F7 BB 95 F5 C1 FD CD 10 04 3B 6E 74 30  .9......
00F0h: 85 CA 82 60 57 58 52 AD 9E B9 22 ED 96 71 B5 7A  ...`WXR.
0100h: 90 61 F2 49 48 58 5F 68 64 B5 81 1E FD C9 34 47  .a.IHX_h
0110h: C5 53 B8 9B A7 BB 94 06 93 C8 5C B8 6B 7C E7 A4  .S......
```

3200101	ウインドストライク	1	48	3200101	428	0	0	1800	1300
3200102	ウインドストライク	2	48	3200102	428	0	0	1800	1300
3200103	ウインドストライク	3	48	3200103	428	0	0	1800	1300
3200104	ウインドストライク	4	48	3200104	428	0	0	1800	1300
3200105	ウインドストライク	5	48	3200105	428	0	0	1800	1300
3200106	ウインドストライク	6	48	3200106	428	0	0	1800	1300
3200107	ウインドストライク	7	48	3200107	428	0	0	1800	1300
3200108	ウインドストライク	8	48	3200108	428	0	0	1800	1300
3200109	ウインドストライク	9	48	3200109	428	0	0	1800	1300
3200110	ウインドストライク	10	48	3200110	428	0	0	1800	1300
3200111	ウインドストライク	11	48	3200111	428	0	0	1800	1700

Graphics

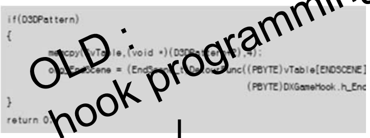
Direct3D Hook

You can be a great painter if you hook these graphic functions

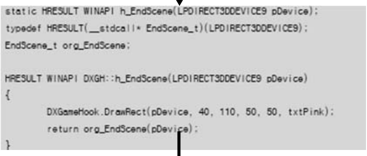


Direct3d

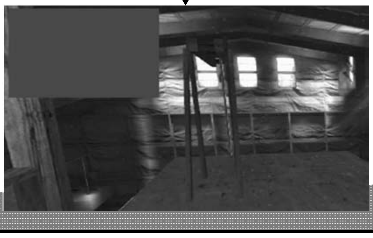
OLD :
hook programming



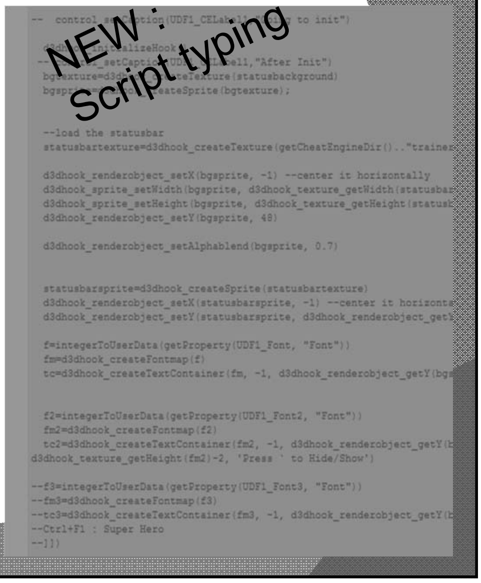
```
if(D3DPattern)
{
        memcpy(&vTable,(void *)(D3DPattern+2),4);
        org_EndScene = (EndScene_t)DetourFunc((PBYTE)vTable[ENDSCENE]
                                              (PBYTE)DXGameHook.h_End
}
return 0;
```



```
static HRESULT WINAPI h_EndScene(LPDIRECT3DDEVICE9 pDevice);
typedef HRESULT(__stdcall* EndScene_t)(LPDIRECT3DDEVICE9);
EndScene_t org_EndScene;

HRESULT WINAPI DXGH::h_EndScene(LPDIRECT3DDEVICE9 pDevice)
{
        DXGameHook.DrawRect(pDevice, 40, 110, 50, 50, txtPink);
        return org_EndScene(pDevice);
}
```

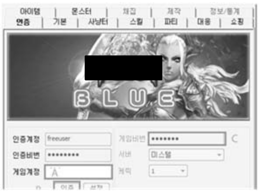


NEW :
Script typing

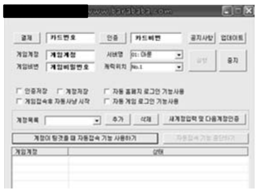


```
--  control_setCaption(UDF1_CELabel1,"Going to init")

  d3dhook_initializeHook()
 --control_setCaption(UDF1_CELabel1,"After Init")
  bgtexture=d3dhook_createTexture(statusbackground)
  bgsprite=d3dhook_createSprite(bgtexture);


  --load the statusbar
  statusbartexture=d3dhook_createTexture(getCheatEngineDir().."trainer

  d3dhook_renderobject_setX(bgsprite, -1) --center it horizontally
  d3dhook_sprite_setWidth(bgsprite, d3dhook_texture_getWidth(statusbar
  d3dhook_sprite_setHeight(bgsprite, d3dhook_texture_getHeight(statusb
  d3dhook_renderobject_setY(bgsprite, 48)

  d3dhook_renderobject_setAlphablend(bgsprite, 0.7)


  statusbarsprite=d3dhook_createSprite(statusbartexture)
  d3dhook_renderobject_setX(statusbarsprite, -1) --center it horizonta
  d3dhook_renderobject_setY(statusbarsprite, d3dhook_renderobject_getY

  f=integerToUserData(getProperty(UDF1_Font, "Font"))
  fm=d3dhook_createFontmap(f)
  tc=d3dhook_createTextContainer(fm, -1, d3dhook_renderobject_getY(bgs


  f2=integerToUserData(getProperty(UDF1_Font2, "Font"))
  fm2=d3dhook_createFontmap(f2)
  tc2=d3dhook_createTextContainer(fm2, -1, d3dhook_renderobject_getY(b
d3dhook_texture_getHeight(fm2)-2, 'Press ` to Hide/Show')

--f3=integerToUserData(getProperty(UDF1_Font3, "Font"))
--fm3=d3dhook_createFontmap(f3)
--tc3=d3dhook_createTextContainer(fm3, -1, d3dhook_renderobject_getY(b
--Ctrl+F1 : Super Hero
--]])
```

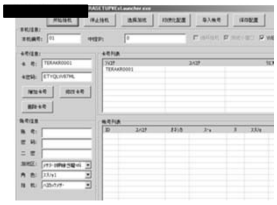
Automation


[redacted]

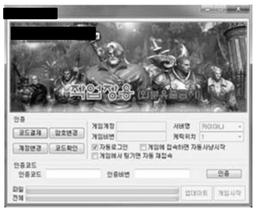
ブルー系, **Blue**


[redacted]

聖戦系, **Holy war**


[redacted]

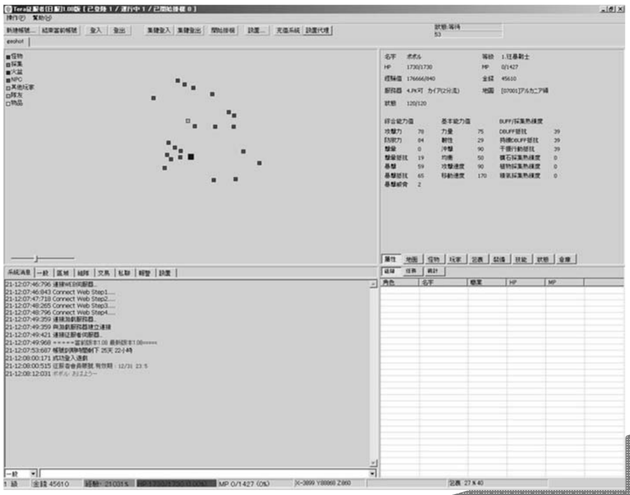
愛国者系, **Nationalist**


[redacted]

ハッピー系, **Happy**

This business is already a sort of red ocean,
There are many various malicious automation tools
having been developed for long time

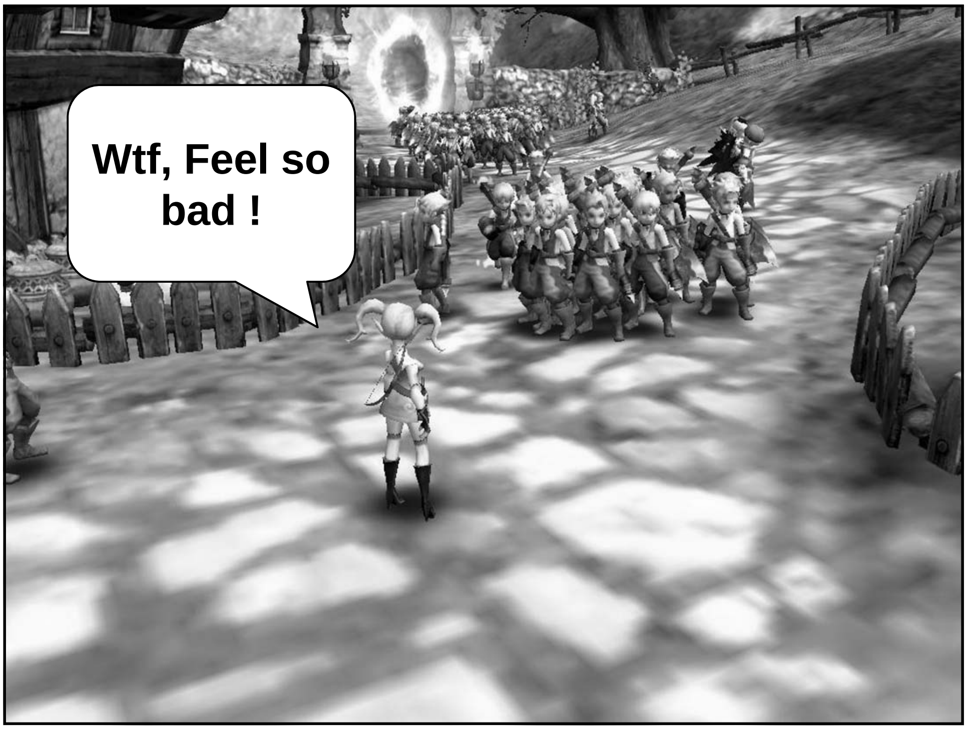
Beyond the automation



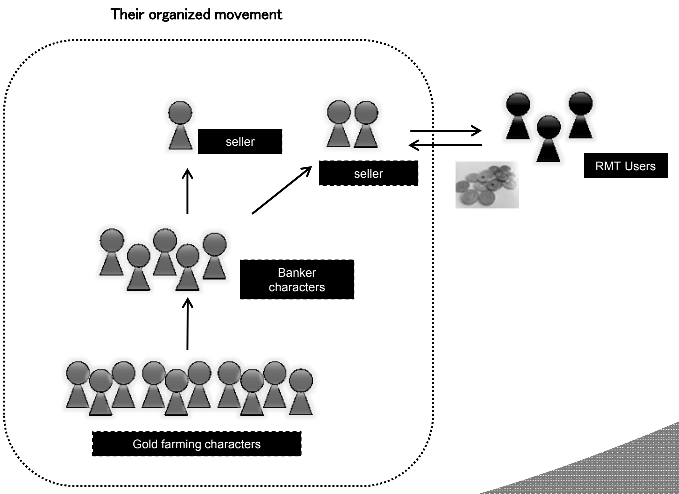
```
21-12:07:46:796 連接WEB伺服器..
21-12:07:46:843 Connect Web Step1.....
21-12:07:47:718 Connect Web Step2.....
21-12:07:48:265 Connect Web Step3.....
21-12:07:48:796 Connect Web Step4.....
21-12:07:49:359 連接游戲服務器..
21-12:07:49:359 與游戲服務器建立連接
21-12:07:49:421 連接征服者伺服器..
21-12:07:49:968 =====當前版本1.08 最新版本1.08=====
21-12:07:53:687 帳號剩餘時間剩下 26天 22小時
21-12:08:00:171 成功登入遊戲
21-12:08:00:515 征服者會員帳號 有效期：12/31 23:5
21-12:08:12:031 ボボル: おはよう～
```

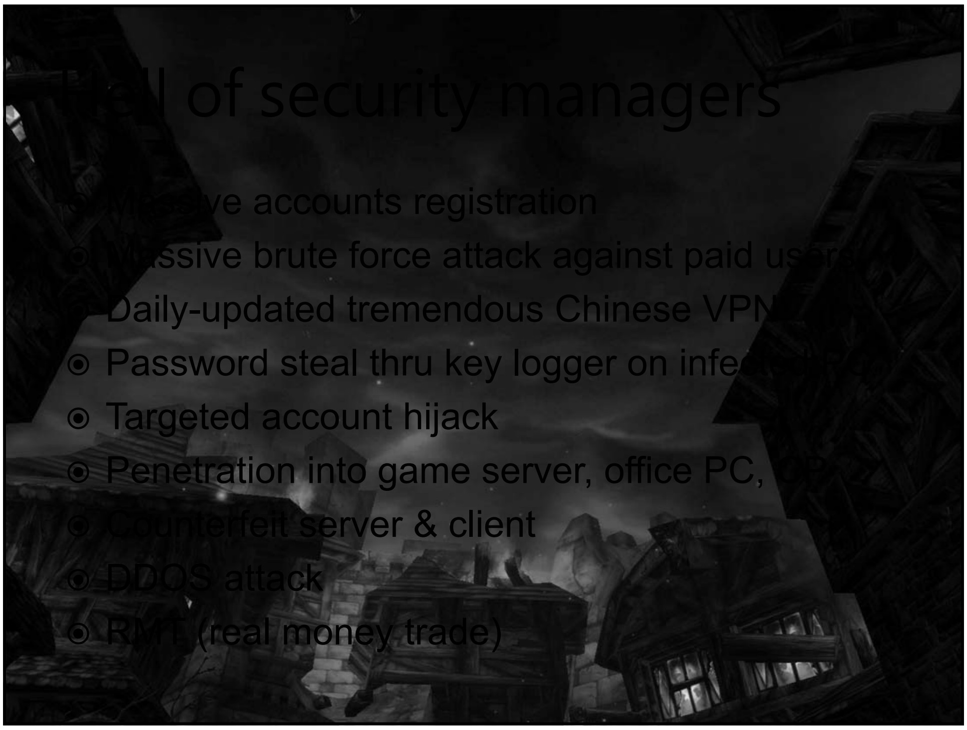
```
1 級  金錢 45610  經驗: 21031%  MP 0/1427 (0%)  X-3899 Y88868 Z860
```

征服者系, Conquer



Gangsters well organized

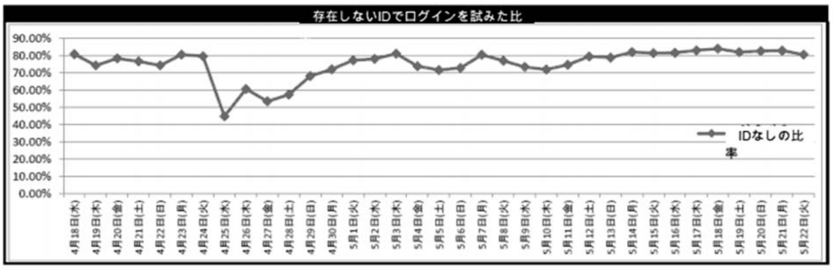




Hell of security managers

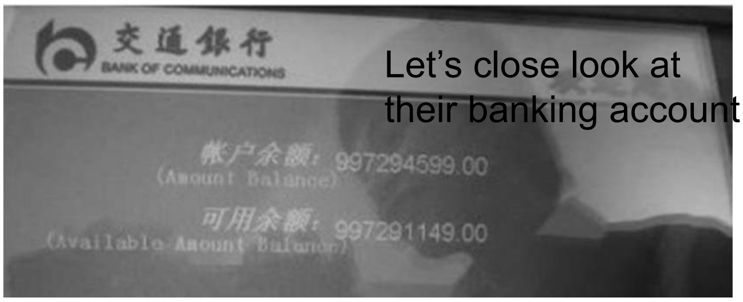
- ⊙ Massive accounts registration
- ⊙ Massive brute force attack against paid users
- ⊙ Daily-updated tremendous Chinese VPN
- ⊙ Password steal thru key logger on infected
- ⊙ Targeted account hijack
- ⊙ Penetration into game server, office PC, OP
- ⊙ Counterfeit server & client
- ⊙ DDOS attack
- ⊙ RMT (real money trade)

Brute force attack



80% of login tries came from Brute force attack , it's about 8,000,000 times per day.

Is it really serious？



交通银行
BANK OF COMMUNICATIONS

帐户余额：997294599.00
(Amount Balance)

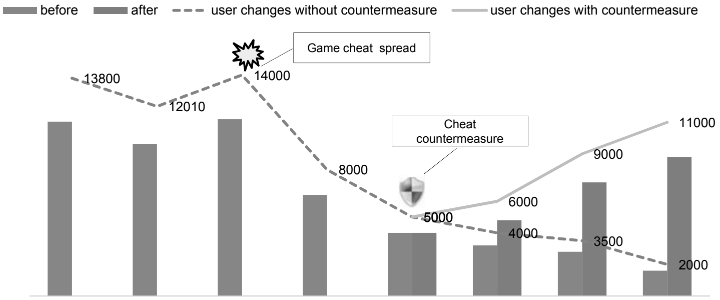
可用余额：997291149.00
(Available Amount Balance)

Let’s close look at their banking account

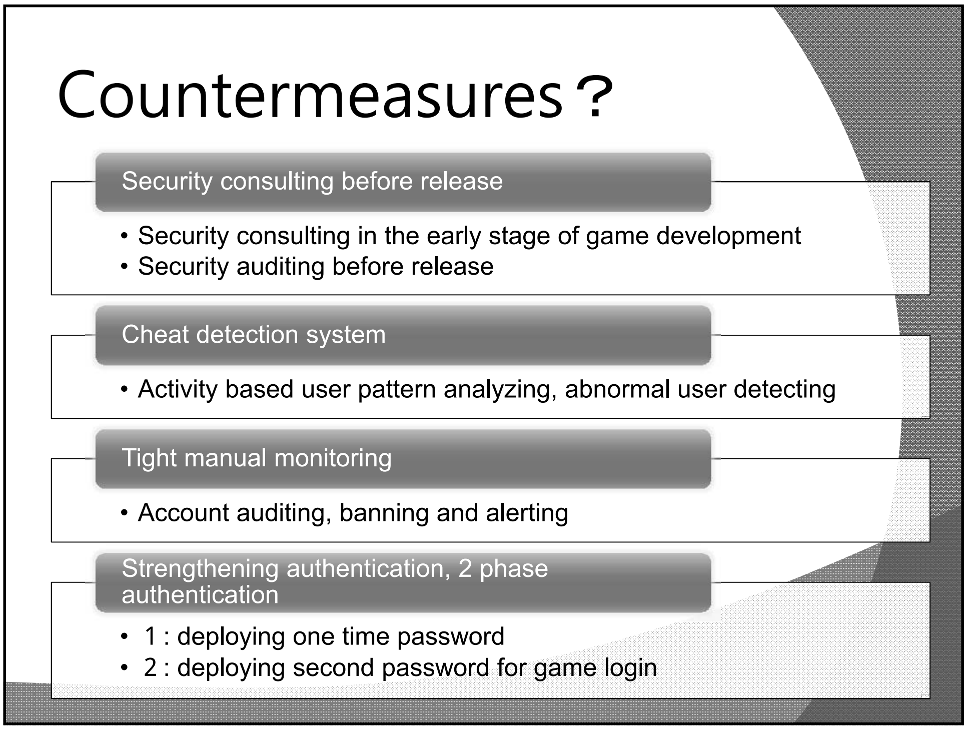
帳戸余額：Account balance
可用余額：Available amount balance

997,294,599.00元
→83,107,883円
->1,040,020 $

Impact on business and countermeasure before and after



2008 OOOO game, user number and sales changes



Countermeasures？

Security consulting before release

- Security consulting in the early stage of game development
- Security auditing before release

Cheat detection system

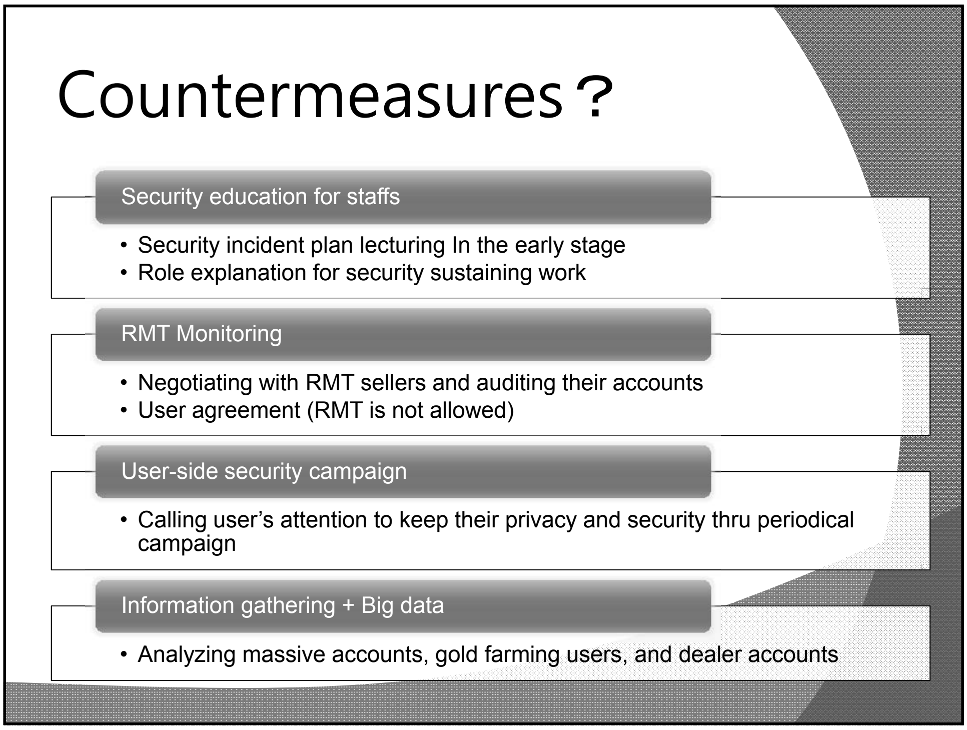
- Activity based user pattern analyzing, abnormal user detecting

Tight manual monitoring

- Account auditing, banning and alerting

Strengthening authentication, 2 phase authentication

- 1 : deploying one time password
- 2 : deploying second password for game login



Countermeasures？

Security education for staffs

- Security incident plan lecturing In the early stage
- Role explanation for security sustaining work

RMT Monitoring

- Negotiating with RMT sellers and auditing their accounts
- User agreement (RMT is not allowed)

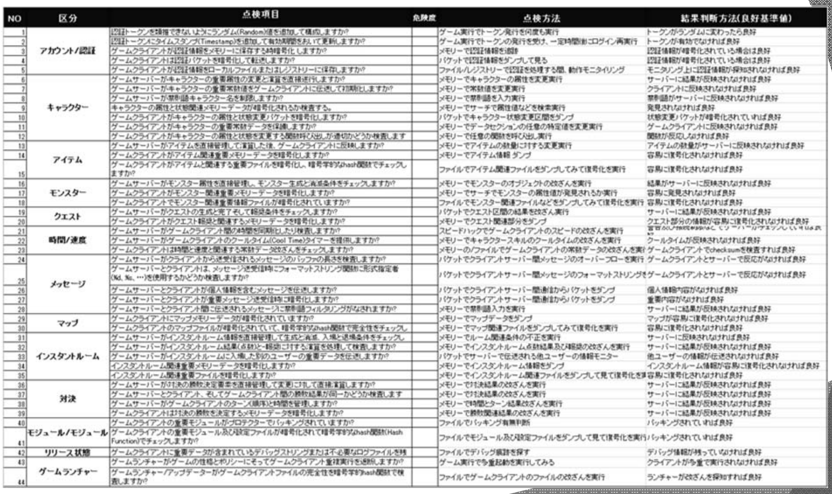
User-side security campaign

- Calling user’s attention to keep their privacy and security thru periodical campaign

Information gathering + Big data

- Analyzing massive accounts, gold farming users, and dealer accounts

Let’s fix all the bugs in detail!



NO	区分	点検項目	危険度	点検方法	結果判断方法(良好基準値)
1	アカウント/認証	認証トークンを類推できないようにランダム(Random)値を追加して構成しますか?		ゲーム実行でトークン発行を何度も実行	トークンがランダムに変わったら良好
2		認証トークンにタイムスタンプ(Timestamp)を追加して有効期間をおいて更新しますか?		ゲーム実行でトークンの発行を受け、一定時間後にログイン再実行	トークンが有効でなければ良好
3		ゲームクライアントが認証情報をメモリーに保存する時暗号化 しますか?		メモリーで認証情報を追跡	認証情報が暗号化されている場合は良好
4		ゲームクライアントは認証パケットを暗号化して転送しますか?		パケットで認証情報をダンプして見る	認証情報が暗号化されている場合は良好
5		ゲームクライアントが認証情報をローカルファイルまたはレジストリーに保存しますか?		ファイル/レジストリーで認証を処理する間、動作モニタイリング	モニタリング上に認証情報が探知されなければ良好
6	キャラクター	ゲームサーバーがキャラクターの重要属性の変更と演算を直接進行しますか?		メモリーでキャラクターの属性を変更実行	サーバーに結果が反映されなければ良好
7		ゲームサーバーがキャラクターの重要常数値をゲームクライアントに伝送して初期化しますか?		メモリーで常数値を変更実行	クライアントに反映されなければ良好
8		ゲームサーバーが禁則語キャラクター名を制限しますか?		メモリーで禁則語を入力実行	禁則語がサーバーに反映されなければ良好
9		キャラクターの属性と状態関連メモリーデータが暗号化されるか検査する。		メモリーでサーチで属性値などを検索実行	発見されなければ良好
10		ゲームクライアントがキャラクターの属性と状態変更パケットを暗号化しますか?		パケットでキャラクター状態変更区間をダンプ	状態変更パケットが暗号化されていれば良好
11		ゲームクライアントがキャラクターの重要常数データを保護しますか?		メモリーでデータセクションの任意の特定値を変更実行	ゲームクライアントに反映されなければ良好
12		ゲームクライアントがキャラクターの属性と状態を変更する関数呼び出しが適切かどうか検査します		メモリーで任意の関数を呼び出し実行	関数が反応しなければ良好
13	アイテム	ゲームサーバーがアイテムを直接管理して演算した後、ゲームクライアントに反映しますか?		メモリーでアイテムの数量に対する変更実行	アイテムの数量がサーバーに反映されなければ良好
14		ゲームクライアントがアイテム関連重要メモリーデータを暗号化しますか?		メモリーでアイテム情報 ダンプ	容易に復号化されなければ良好
15		ゲームクライアントがアイテムと関連する重要ファイルを暗号化し、暗号学的なhash関数でチェックしますか?		ファイルでアイテム関連ファイルをダンプしてみて復号化を実行	容易に復号化されなければ良好
16	モンスター	ゲームサーバーがモンスター属性を直接管理し、モンスター生成と消滅条件をチェックしますか?		メモリーでモンスターのオブジェクトの改ざんを実行	結果がサーバーに反映されなければ良好
17		ゲームクライアントがモンスター関連重要メモリーデータを暗号化しますか?		メモリーでサーチでモンスターの属性値が発見されるか実行	容易に発見されなければ良好
18		ゲームクライアントでモンスター関連重要情報ファイルが暗号化されていますか?		ファイルでモンスター関連ファイルなどをダンプしてみて復号化を実行	容易に復号化されなければ良好
19	クエスト	ゲームサーバーがクエストの生成と完了そして報奨条件をチェックしますか?		パケットでクエスト区間の結果を改ざん実行	サーバーに結果が反映されなければ良好
20		ゲームクライアントがクエスト報奨と関連するメモリーデータを暗号化しますか?		メモリーでクエスト関連部分をダンプ	クエスト部分の情報が容易に復号化されなければ良好
21	時間/速度	ゲームサーバーがゲームクライアント間の時間を同期化したり検査しますか?		スピードハックでゲームクライアントのスピードの改ざんを実行	[illegible]
22		ゲームサーバーがゲームクライアントのクールタイム(Cool Time)タイマーを提供しますか?		メモリーでキャラクタースキルのクールタイムの改ざんを実行	クールタイムが反映されなければ良好
23		ゲームクライアントは時間と速度と関連する常数データ改ざんをチェックしますか?		メモリーの/ファイルでゲームクライアントの常数データの改ざんを実	ゲームクライアントでchecksumを検査すれば良好
24	メッセージ	ゲームサーバーがクライアントから送受信されるメッセージのバッファの長さを検査しますか?		パケットでクライアントサーバー間メッセージのオーバーフローを実行	ゲームクライアントとサーバーで反応がなければ良好
25		ゲームサーバーとクライアントは、メッセージ送受信時にフォーマットストリング関数に形式指定者(%d, %s, …)を使用するかどうか検査しますか?		パケットでクライアントサーバー間メッセージのフォーマットストリングを	ゲームクライアントとサーバーで反応がなければ良好
26		ゲームサーバーとクライアントが個人情報を含むメッセージを伝送しますか?		パケットでクライアントサーバー間通信からパケットをダンプ	個人情報内容がなければ良好
27		ゲームサーバーとクライアントが重要メッセージ送受信時に暗号化しますか?		パケットでクライアントサーバー間通信からパケットをダンプ	重要内容がなければ良好
28		ゲームサーバーとクライアント間に伝送されるメッセージに禁則語フィルタリングがなされますか?		メモリーで禁則語入力を実行	サーバーに結果が反映されなければ良好
29	マップ	ゲームクライアントにマップメモリーデータが暗号化されていますか?		メモリーでマップデータをダンプ	マップが容易に復号化されなければ良好
30		ゲームクライアントのマップファイルが暗号化されていて、暗号学的なhash関数で完全性をチェックし		メモリーでマップ関連ファイルをダンプしてみて復号化を実行	容易に復号化されなければ良好
31	インスタントルーム	ゲームサーバーがインスタントルーム情報を直接管理して生成と消滅、入場と退場条件をチェックし		メモリーでルーム関連条件の不正を実行	サーバーに反映されなければ良好
32		ゲームサーバーがインスタントルーム結果(点数)と報奨に対する演算を処理して検査しますか?		メモリーでインスタントルーム点数結果及び報奨の改ざんを実行	サーバーに結果が反映されなければ良好
33		ゲームサーバーがインスタントルームに入場した別のユーザーの重要データを伝送しますか?		パケットでサーバーで伝送される他ユーザーの情報モニター	他ユーザーの情報が伝送されなければ良好
34		インスタントルーム関連重要メモリーデータを暗号化しますか?		メモリーでインスタントルーム情報をダンプ	インスタントルーム情報が容易に復号化されなければ良好
35		インスタントルーム関連重要ファイルを暗号化しますか?		メモリーでインスタントルーム関連ファイルをダンプして見て復号化を	容易に復号化されなければ良好
36	対決	ゲームサーバーが対決の勝敗決定要素を直接管理して変更に対して直接演算しますか?		メモリーで対決結果の改ざんを実行	サーバーに結果が反映されなければ良好
37		ゲームサーバーとクライアント、そしてゲームクライアント間の勝敗結果が同一かどうか検査します		メモリーで対決結果の改ざんを実行	サーバーに結果が反映されなければ良好
38		ゲームサーバーがゲームクライアントのターン(順序)と時間を管理しますか?		メモリーで時間とターン結果改ざんを実行	サーバーに結果が反映されなければ良好
39		ゲームクライアントは対決の勝敗を決定するメモリーデータを暗号化しますか?		メモリーで勝敗関連結果の改ざんを実行	サーバーに結果が反映されなければ良好
40	モジュール/モジュール	ゲームクライアントの重要モジュールがプロテクターでパッキングされていますか?		ファイルでパッキング有無判断	パッキングされていれば良好
41		ゲームクライアントの重要モジュール及び設定ファイルが暗号化されて暗号学的なhash関数(Hash Function)でチェックしますか?		ファイルでモジュール及び設定ファイルをダンプして見て復号化を実行	パッキングされていれば良好
42	リリース状態	ゲームクライアントに重要データが含まれているデバッグストリングまたは不必要なログファイルを残		ファイルでデバッグ痕跡を探す	デバッグ情報が残っていなければ良好
43	ゲームランチャー	ゲームランチャーがゲームの性格とポリシーにそってゲームクライアント重複実行を遮断しますか?		ゲーム実行で多重起動を実行してみる	クライアントが多重で実行されなければ良好
44		ゲームランチャー/アップデーターがゲームクライアントファイルの完全性を暗号学的hash関数で検査しますか?		ファイルでゲームクライアントのファイルの改ざんを実行	ランチャーが改ざんを探知すれば良好

Be smarter, he is a double spy

151294831(151294831) 2011/11/21 21:00:07
也不准备上了吗（もう辞めるつもりですか）
魔魔ず風魂(273307315) 2011/11/21 21:00:49
伤不起（もう耐えないですね。この懲戒対応の調子でいくと）
386054320(386054320) 2011/11/21 21:02:08
哦 忒狠了（そうですね。懲戒対応は厳しいすぎるですね）
魔魔ず風魂(273307315) 2011/11/21 21:02:29
满级的就给我剩下一个..（カンストしたキャラクタは一個だけ残ってますね。
他のは全部BANされました。）
151294831(151294831) 2011/11/21 21:02:48
我也是，只有一个满级的了（私も、カンストなのは一個だけ残されました。）
150414744(150414744) 2011/11/21 21:03:46
我17个剩2个
今天才30多的又两个
伤不起
卖外挂了
（私は17個のうち２個だけ残ってます。）
248873543(248873543) 2011/11/21 21:26:32
１３４５６７８９区收货！ 有出的TTT（ゲーム内マネを買収の宣伝）
438500585(438500585) 2011/11/21 22:14:20
坚持就是胜利（もうちょっと頑張ってください。多分これから良くなるかも）

Thank you