

**RE + VTube =  
Much harder  
than you'd  
think**

Still Hsu / Azaka Sekai 安坂星海

# whoami

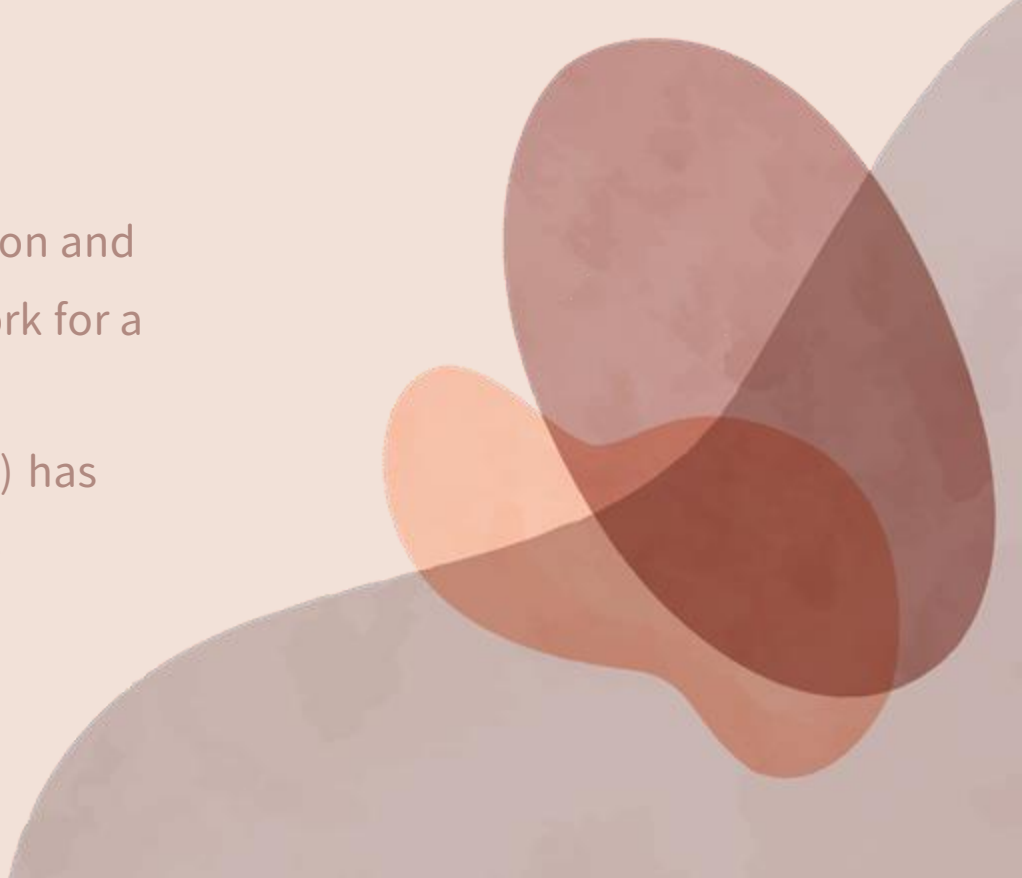
Still Hsu

- BEL, English @ NPTU
- Threat Intelligence Researcher @ TeamT5
- Active among infosec communities
- Windows internals + reverse engineering as hobby



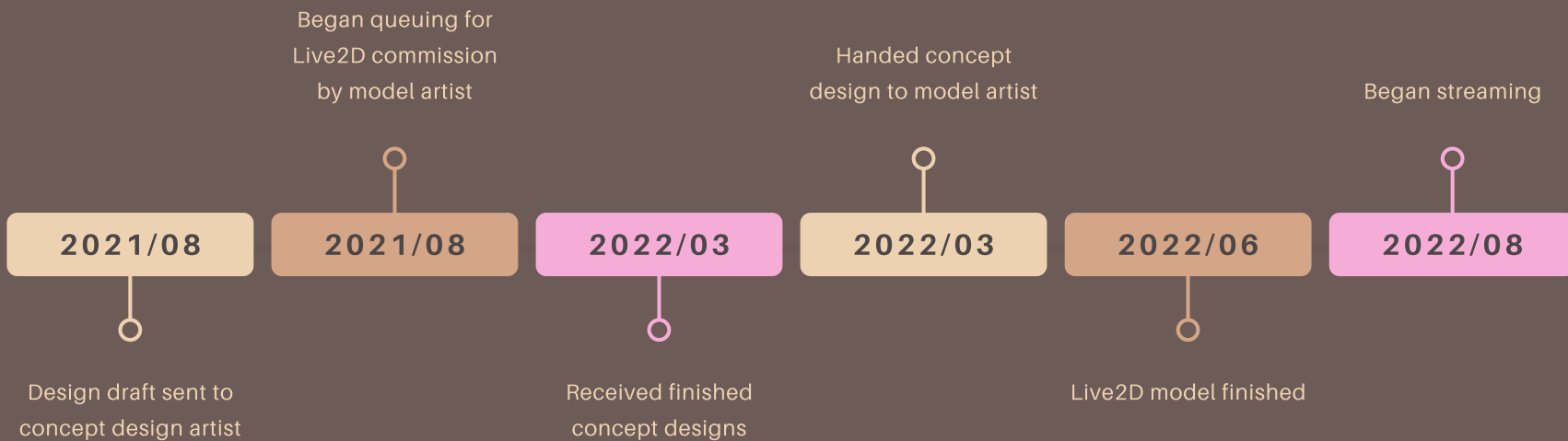
# So, like... What's this all about?

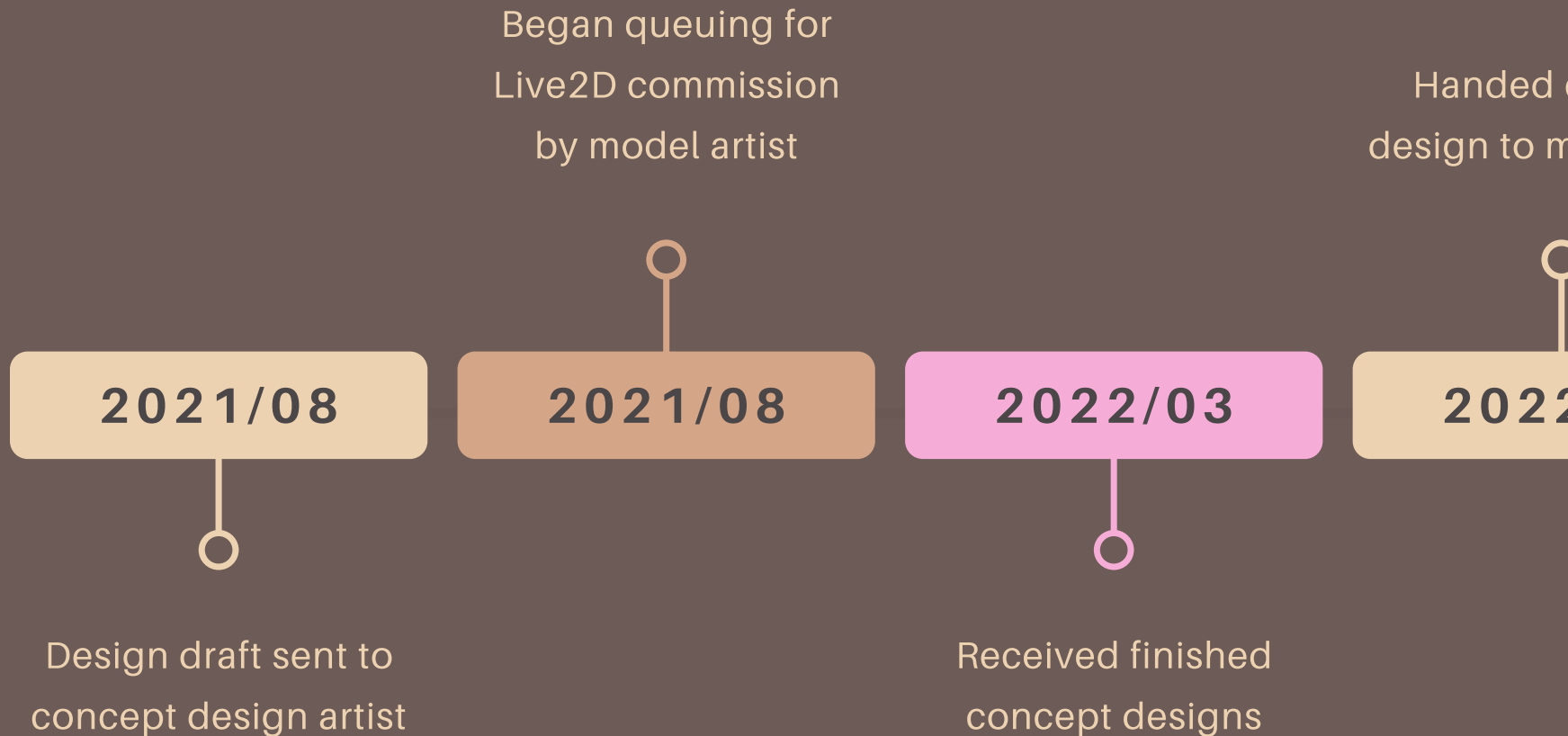
- Always wanted to stream
- Loved audio and video production and did dabble with professional work for a while
- Gender dysphoria (性別認同障礙) has been bothering me for a decade



# TIMELINE OF THINGS

A brief summary of all the complicated things





2022/03

Received finished  
concept designs

2022/03

Handed concept  
design to model artist

2022/06

Live2D model finished

2022/08

Began streaming

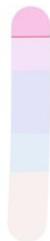
(丙)



IA



IB




(日) ver 2.

IA



IB





COOL

...but now what?





**Idk man**



# chat

malware\_guy: lmao this is like metal gear revengeance

AmiaLinara: yes

malware\_guy: he just wants to avenge nimue's death ig

AmiaLinara: lurking while exploring

AmiaLinara: i had to watch a guide too ya for some small stuff

AmiaLinara: oh i often get 1000% + LOL

malware\_guy: i'm gonna focus on some nim sample i'm working on, it was fun talking with you still! dropped a follow earlier

AmiaLinara: you need to really know to make some stronger etc

AmiaLinara: and overcap into amazing or brilliant





**Since we're at  
HITCON...**

No debugger

Library function Regular function Instruction Data Unexplored External symbol Lumina function

```

1 __int64 __fastcall sub_1400066D8(const WCHAR *a1, const WCHAR *a2)
2 {
3     HANDLE ProcessHeap; // rax
4     LPWSTR lpString1; // [rsp+20h] [rbp-138h] BYREF
5     __int64 v5[3]; // [rsp+28h] [rbp-130h] BYREF
6     LPVOID lpMem[10]; // [rsp+40h] [rbp-118h] BYREF
7     char v7[24]; // [rsp+90h] [rbp-C8h] BYREF
8     char v8[32]; // [rsp+B0h] [rbp-A8h] BYREF
9     DWORD p_code[8]; // [rsp+D0h] [rbp-88h] BYREF
10    char v10[104]; // [rsp+F0h] [rbp-68h] BYREF
11
12    lpString1 = sub_14000647C(0x104i64, 0x3000, 0x40);
13    lstrcpyW(lpString1, a1);
14    sub_140006564(lpString1);
15    lstrcatW(lpString1, a2);
16    qmemcpy(v7, Lockbit::ReadFile(p_code, lpString1, sizeof(v7)));
17    qmemcpy(v5, v7, sizeof(v5));
18    if ( v5[2] && LODWORD(v5[1]) )
19    {
20        qmemcpy(v8, v5, 0x18ui64);
21        if ( sub_1400042FC(v8, LODWORD(v8)) )
22        {
23            sub_140002AB0(&lpString1, 0x104i64);
24            lpMem[0] = sub_140005C00(a2);
25            qmemcpy(v10, lpMem, 0x48ui64);
26            if ( sub_140004DE8(v10) )
27            {
28                ProcessHeap = GetProcessHeap();
29                HeapFree(ProcessHeap, 0, lpMem[0]);
30                sub_140002AB0(&lpMem[7], LODWORD(lpMem[8]));
31                return LODWORD(lpMem[8]);
32            }
33            else
34            {
35                return 0i64;
36            }
37        }
38    }
39    {

```

X3B00D502: yo

X3B00D502: wtf is a malware analysis ?

X3B00D502: and why does the anime grill have no titties ?

TheDrifterX: Windows 98 🐼🐼

TheDrifterX: Oh sorry 95, looks similar

awesome\_goose34: you can just breakpoint on the NtAllocateVirtualMemory

awesome\_goose34: btw







**A LOT went wrong  
that stream...**

# Let's talk about what makes streaming difficult

You'd **HAVE TO** be entertaining 80%+.  
You'd **HAVE TO** be confident enough to show the viewers  
that you know what you're doing.  
The viewer **HAS TO** understand what's going on.

# Let's talk about what makes RE streams *even more* difficult

You can **ONLY** use TLP WHITE samples (quality differs).  
You **HAVE TO** be careful with what you say and show  
(company secrets).

**This is an entertainment-focused platform.**

# What went wrong with the stream?

- Lack of preparation
  - Difficult to tell what sample you're about to deal with is.
- Terribly boring
  - How *do* you make something as bland as reverse engineering fun?
- Confused viewers
  - They don't know what they're looking at – even for experienced RE players.



**awesome\_goose34:** what you're trying to do?

# Key takeaway

- Prepare your materials
  - Not necessarily finish REing the entire sample before the stream, but at least know what you're about to work with.
  - Understand “what exactly can the viewers learn out of this?”
- Maybe streaming isn't the best fit for RE
  - Cut it down to an entertaining video instead



**Bonus**



# I got banned on Twitter on Thursday.

...so the contacts at the end might not work.



# Latest Tweets

Retweets



What's happening?



Tweet

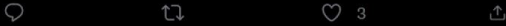
## Your account is permanently suspended

After careful review, we determined your account broke the [Twitter Rules](#). Your account is permanently in read-only mode, which means you can't Tweet, Retweet, or Like content. You won't be able to create new accounts. If you think we got this wrong, you can [submit an appeal](#).



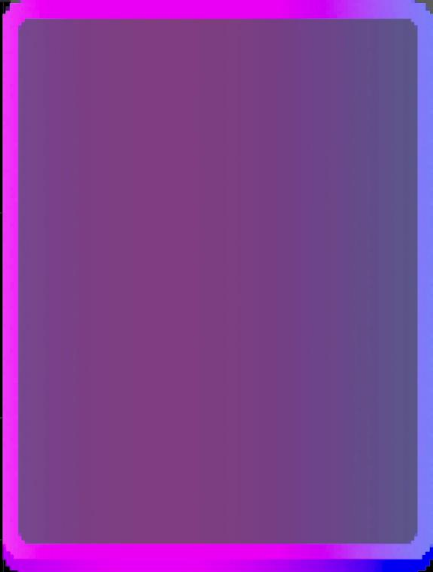
ラテ @Latte\_daruta2 · 2h

久しぶりに昼に起きた、ここ2日夕方まで寝てたからな...



Raccoons Hourly @raccoonhourly · 2h

Automated



Tweet

# THANKS

Contact me  
@StillAzureH (Twitter)  
@AzakaSekai (Twitter/Twitch)

CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#).

