# Adobe Flash Player Exploit

Atum

# About me

- Atum
  - @blue-lotus
  - @Tea Deliverers
  - @Peking University
- Keywords
  - Software Security, System Security
  - CTF PWNer, Weak Chicken
- lgcpku@gmail.com

# Difficulties to exploit adobe flash

- No Symbol
- AVM abstraction
- IE Sandbox

# Make symbol file

- Match symbol by AVMplus source code
- Match symbol by IDA FLIRT sig file
  - Identify compiler used by adobe flash
  - Use the same Compile Avmplus
  - Extract .sig file using IDA FLIRT
  - Load .sig file

# Debug without symbol

- By Access Breakpoint
  - Malloc block 1000 times， set a access breakpoint on arbitrary bloc， then free all blocks
  - Malloc block and fill with 0xdeadc0de, search 0xdeadc0de in mem and set a access breakpoint on it
  - Other techniques..
- Set break point on JavaScript engine
  - ExternalCall

# Exploit AVM

- Craft Arbitrary  RW by Spray Vector/ByteArray
- Spray Vector (Vector is protected since 2016)
    - Vector memory layout (length, xxxx,data)
- Spray ByteArray

# Exploit AVM

- Using Arbitrary to leak && Control flow hijack
- Control flow hijack
  - Change Vtable (Vtable is protected by CFG on Win10)
  - Change mmgc to bypass CFG on Win10
  - ROP+Vmprotect + shellcode

# Bypass IE sandbox

- Launch a local server and exploit again(if EPM enable, this skill cannot be used)
- NBNS spoofing