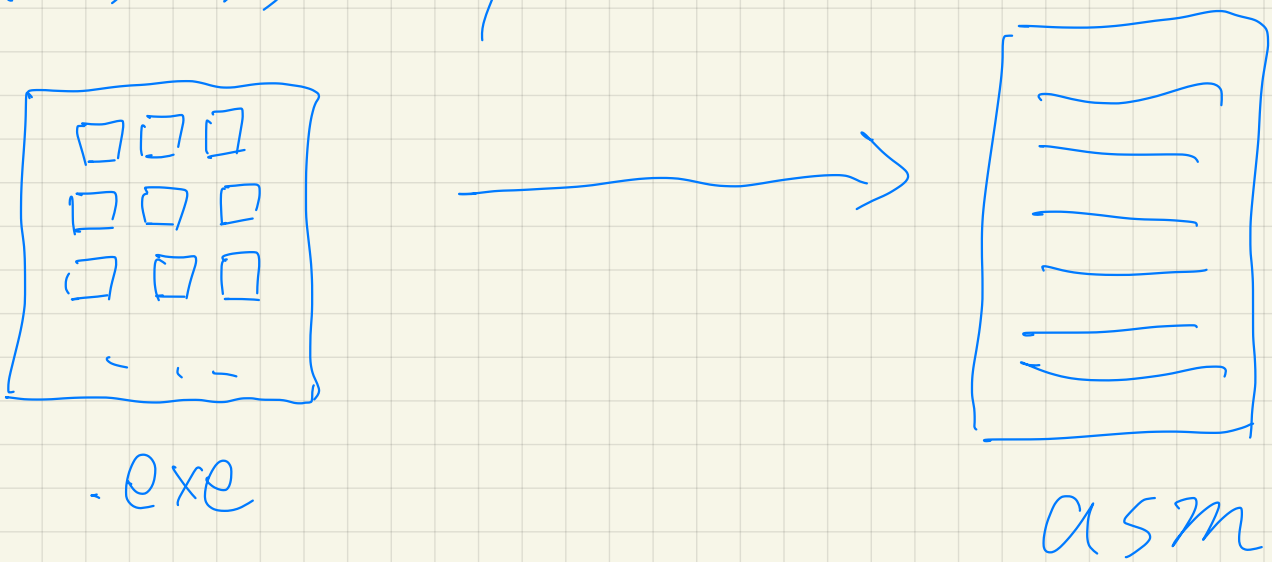
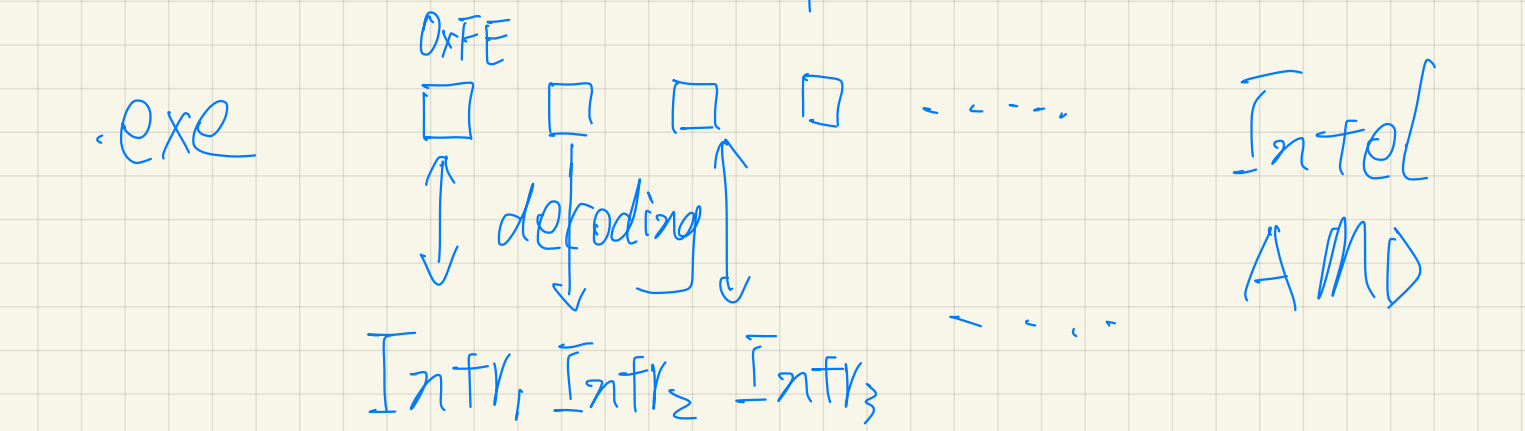
Disassembly :

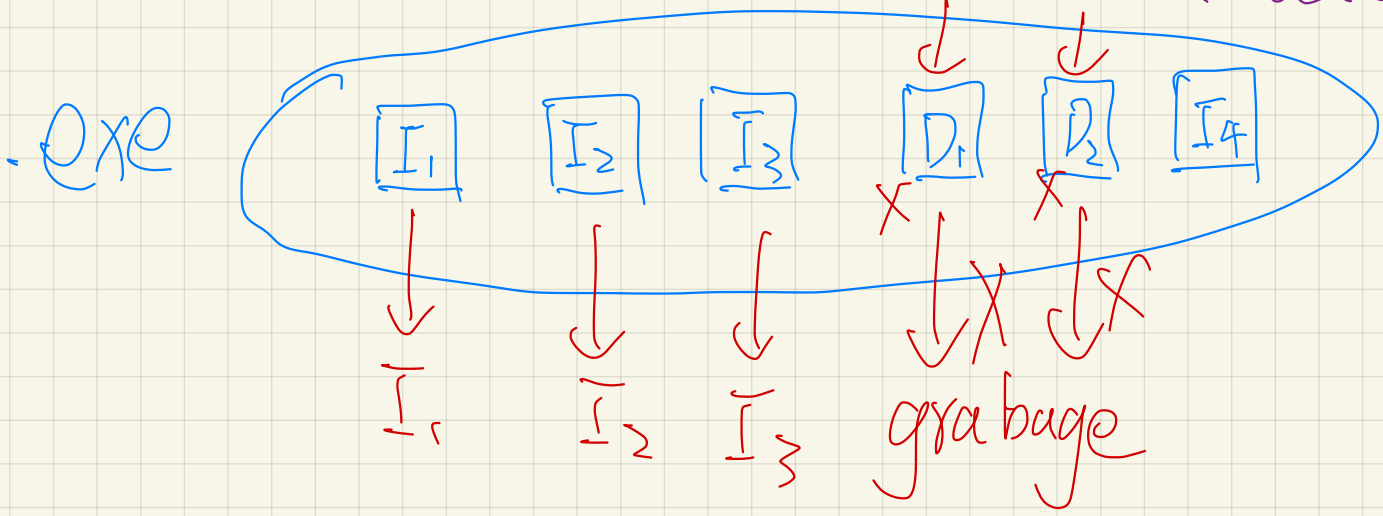


linear disassembly :

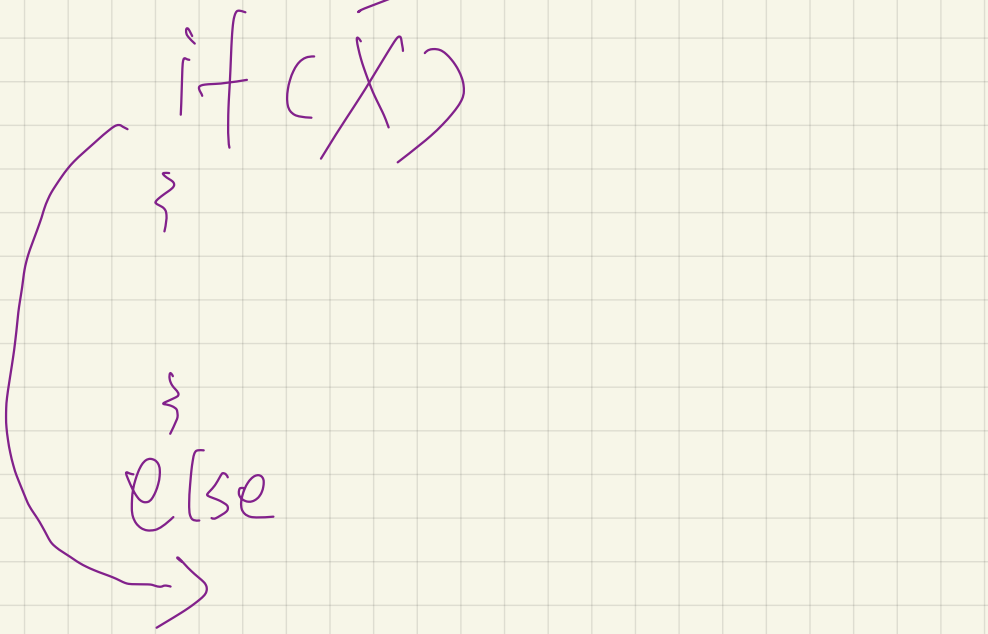


Instr ⟷ hex

embedded data



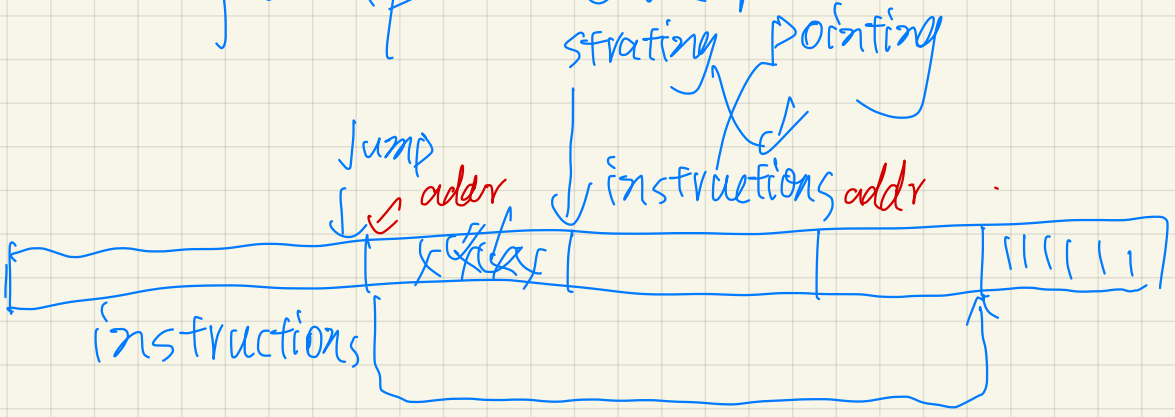
I must be a jump instruction



recursive disassembling

mimic CPU decode

jump over data bytes

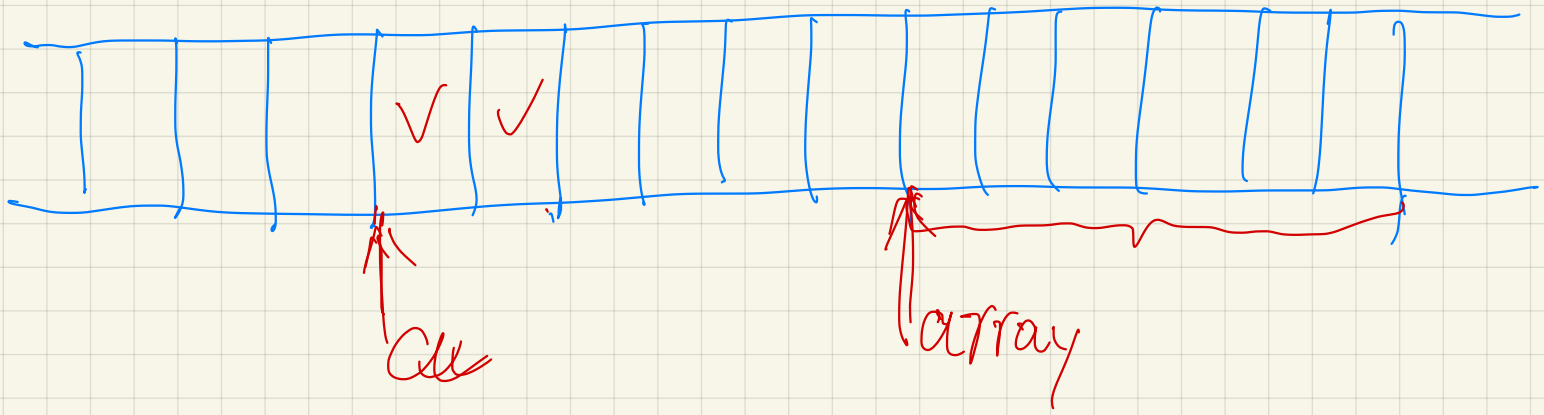


hybrid discussambly:

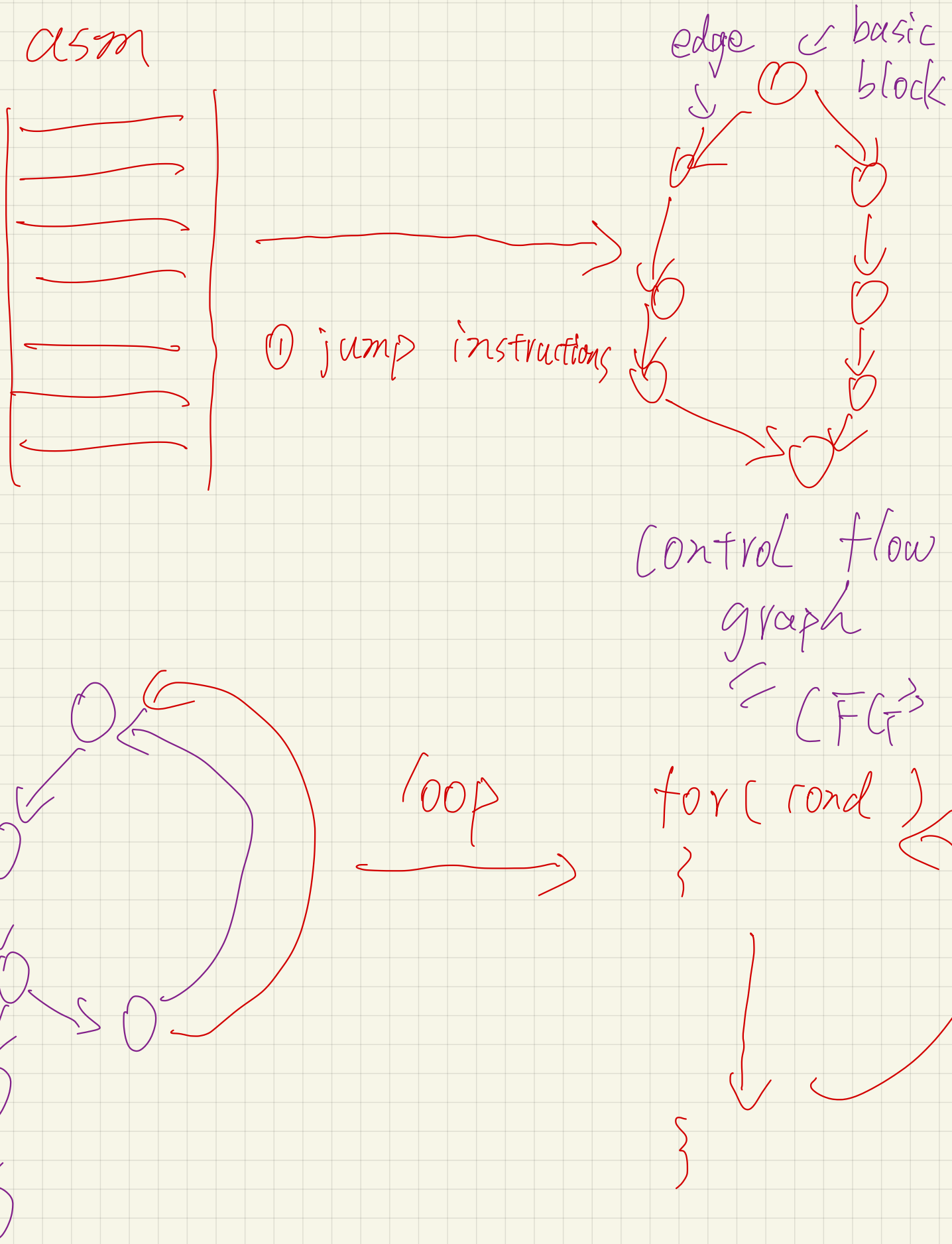
linear → recurisive

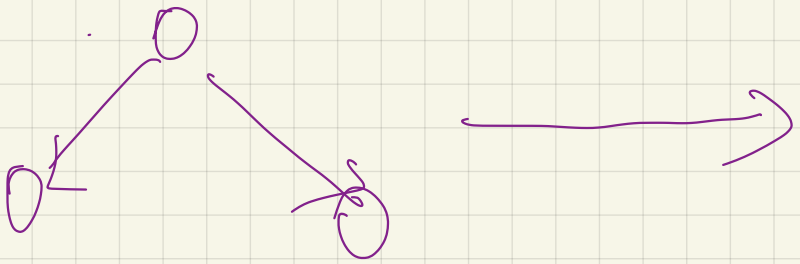
linear → recurive

Process Memory Space: 1D continues



simulate execution of asm code


asm
edge
basic block
① jump instructions
control flow graph
<CFG>
loop
for(cond)
{
}

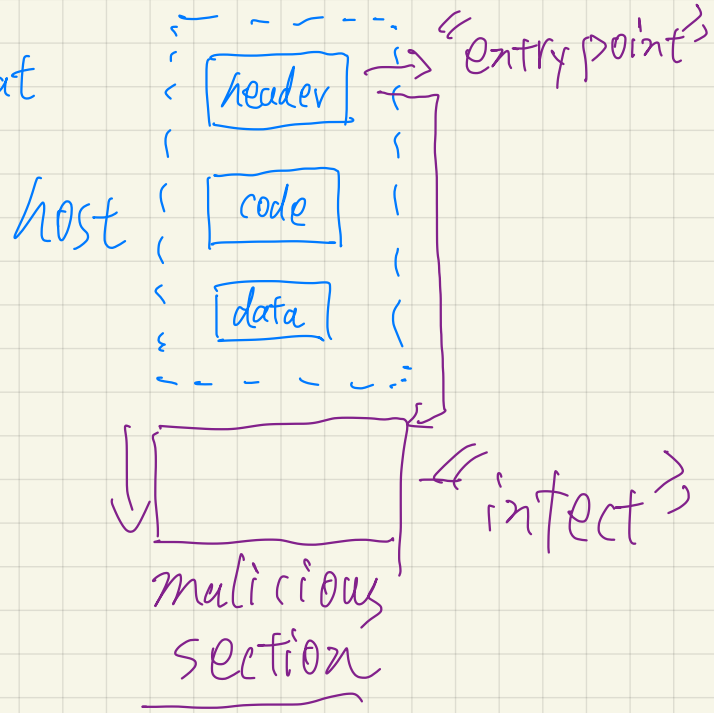


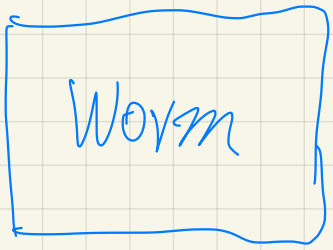
```
if (cond)
{

}
else
{

}
```

Virus

Worm

Format





standalone

spread:

host → floppy disk
host → usb drive
host → normal software

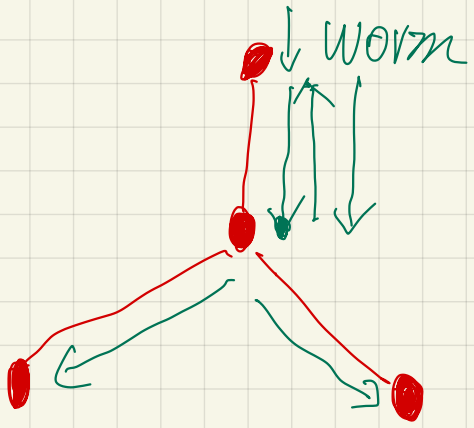
1. infect a host
2. wait for the host to be executed
3. look for new host to infect

self-propagation

→ email
→ url
→ network

1. look for vulnerable host machine
2. exploit
3. look for new vulnerable host machine

passive



bandwidth

CIA

historical into

1986

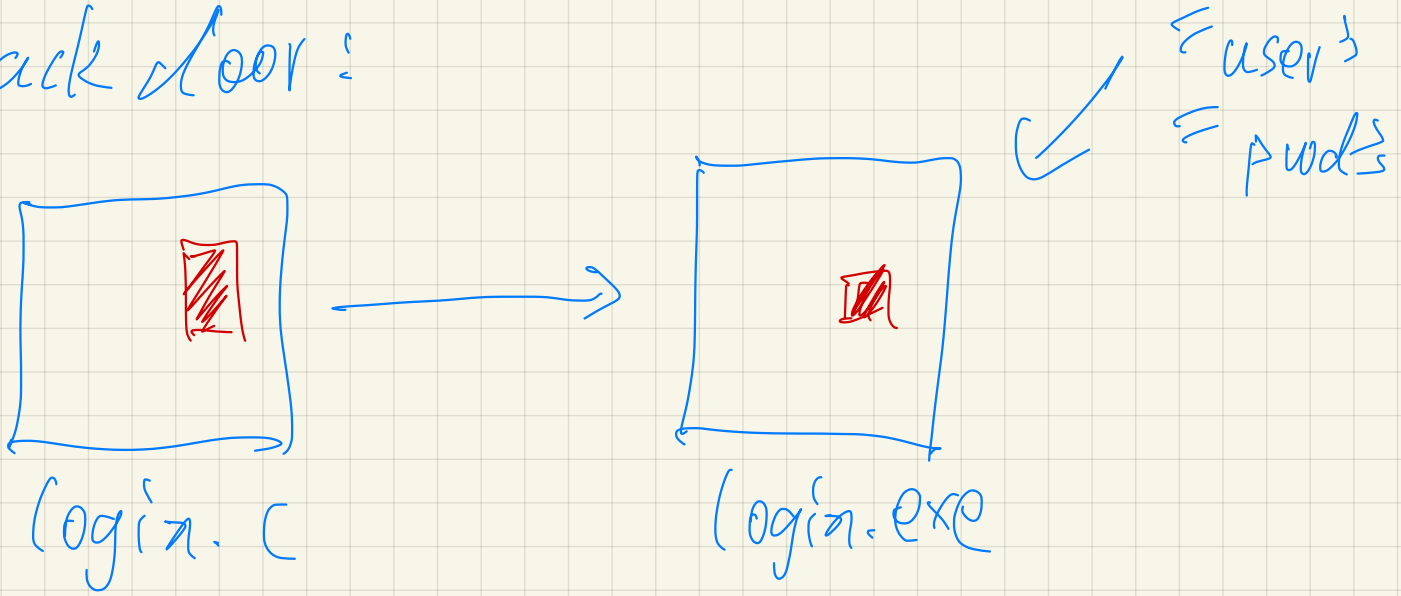
no harm

1988

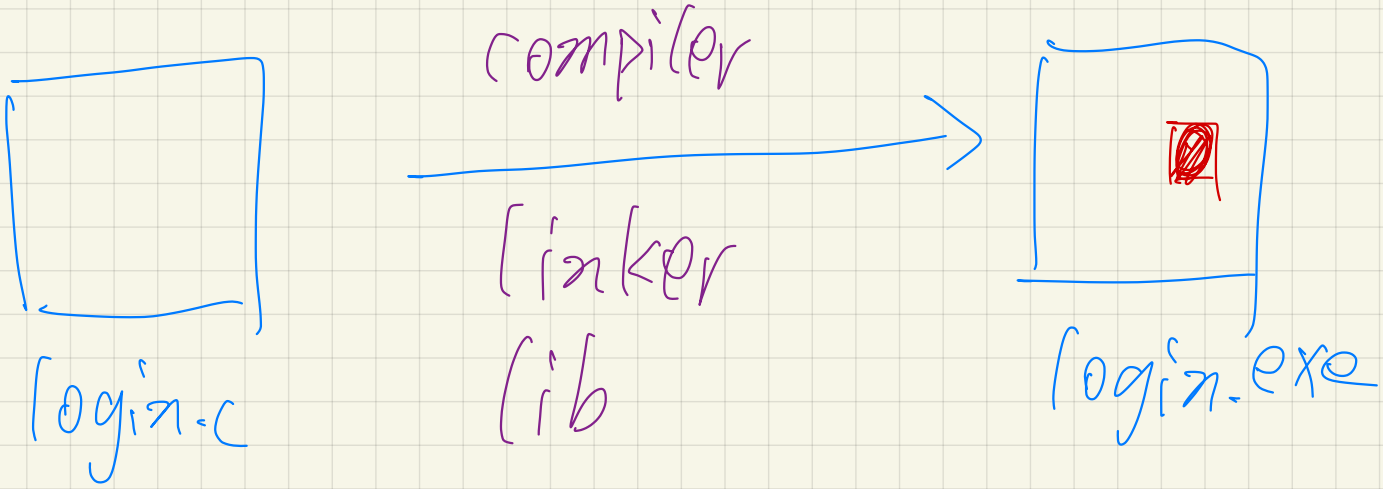
Morris Worm

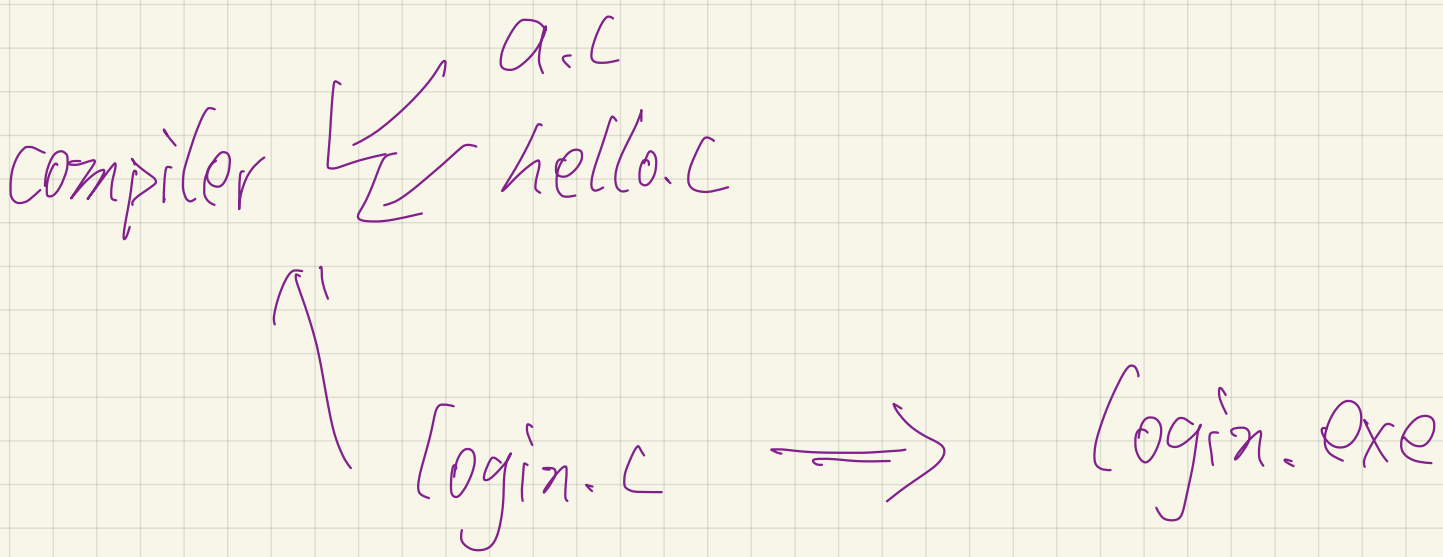
99 LOC

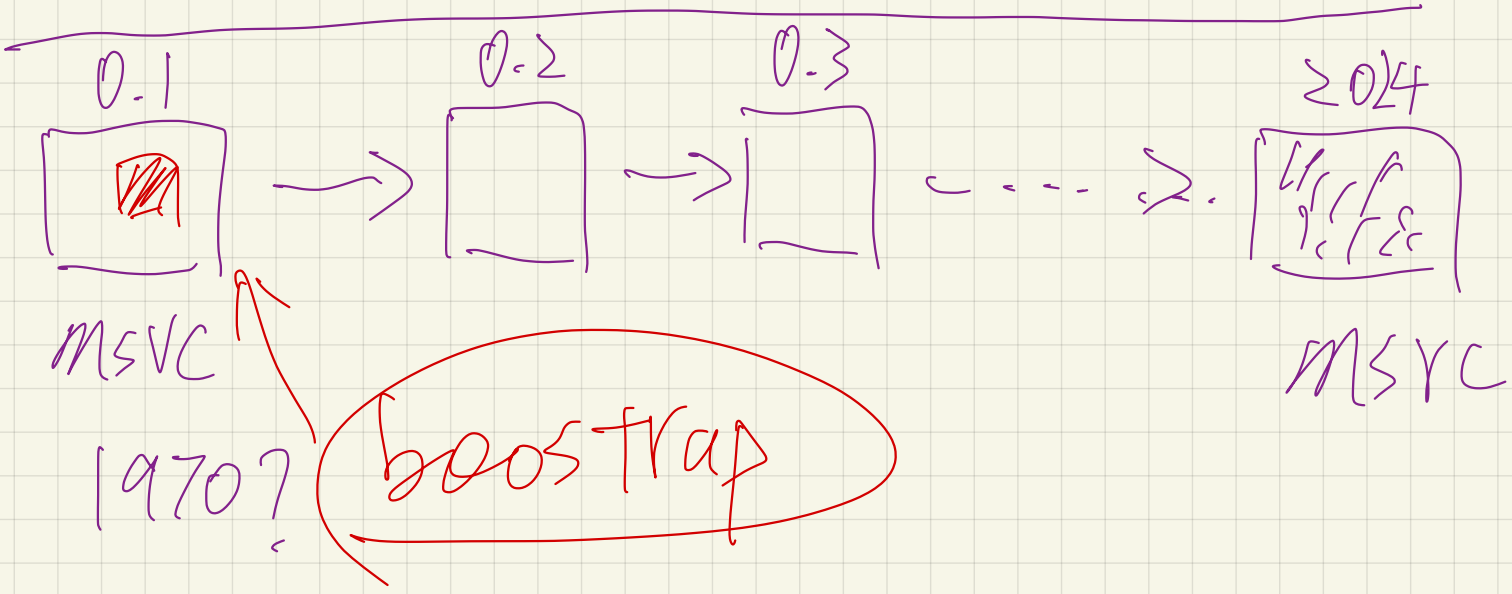
Back door :




```
if (name=="open door")
 {
        authenticate;

 }
else
 {
        pwd;
 }
```

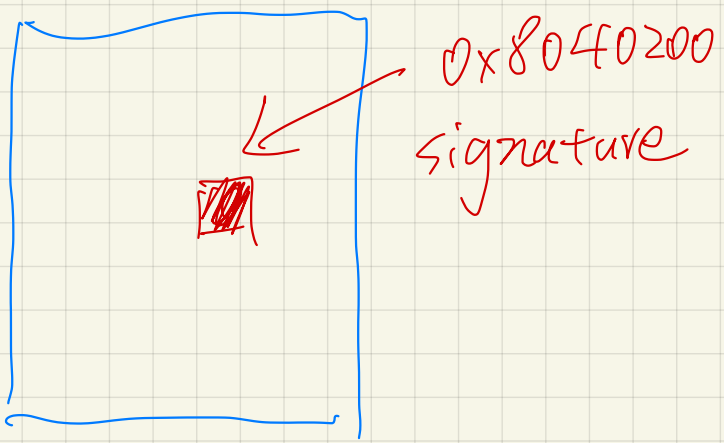

compiler
linker
lib
login.c
login.exe

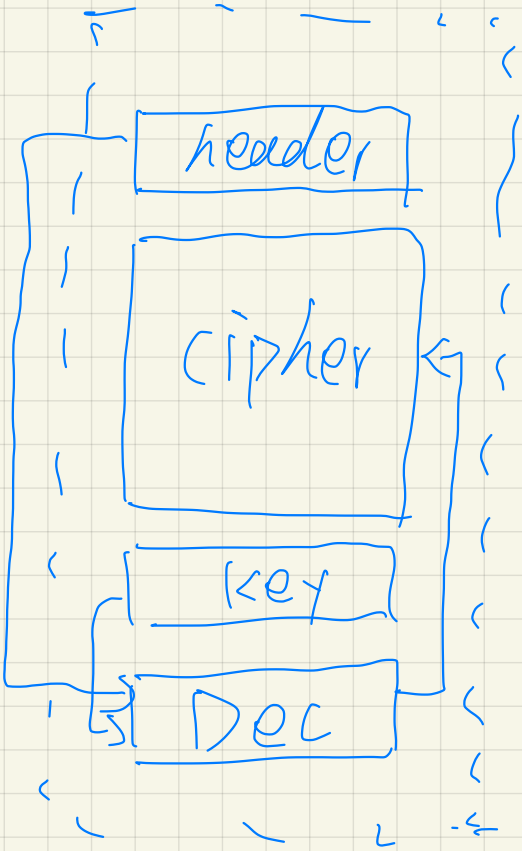

a.c
compiler
hello.c
login.c
login.exe


0.1
0.2
0.3
≥0.4
MSVC
1970
bootstrap
MSVC

Packed Malware:

Packer

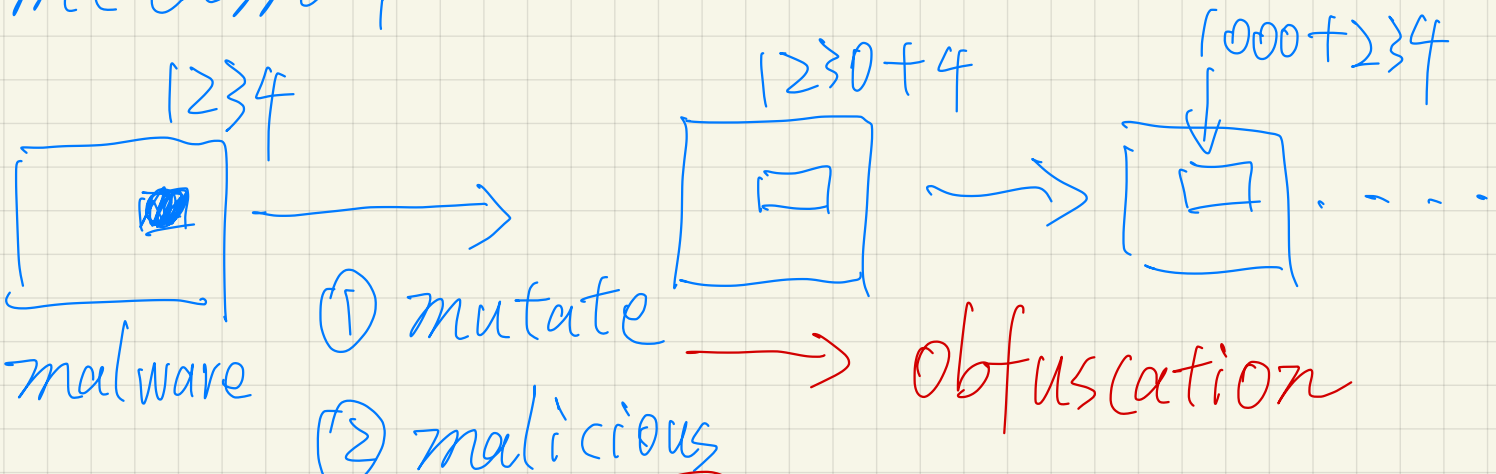




Packed malware

1. static signature ✗
2. Dynamic behavior ✓
3. memory shapshot ✓

metamorphic malware:



① mutate → obfuscation

② malicious

△ static sign ✗

△ dynamic behavior ✓