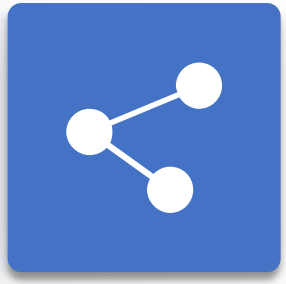
逆向基础

主讲人：immortal



What is Reverse Engineering?

Check Point
SOFTWARE TECHNOLOGIES LTD.

WIKIPEDIA

Reverse engineering is the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation.

aka: Reversing, RE, SRE

Why do it?

Check Point SOFTWARE TECHNOLOGIES LTD.

Discover Trade Secrets

Find Vulnerabilities

Academic Research (Yeah, right…)

Circumvent [Copy] Protection

Patch Binary and Alter Behavior

Pure Curiosity

Analyse Protocols

Sounds awesome, right?

```
for (Serial = 0, i = 0; i < strlen(UserName); i++) {
        CurChar = (int) UserName[i];
        Serial += CurChar;
        Serial = (((Serial << 1) && 0xFFFFFFFE) | |
((Serial >> 31) && 1));
        Serial = (((Serial * CurChar) + CurChar) ^
CurChar);
}
UserSerial = ~((UserSerial ^ 0x1337C0DE) -
0xBADC0DE5);
```

```
00401000 push ebp
00401001 mov ebp, esp
00401003 push ecx
00401004 push ecx
00401005 and dword ptr [ebp-4], 0
00401009 push esi
0040100A mov esi, [ebp+8]
0040100D push edi
0040100E push esi
0040100F call ds:[00402008h]
00401015 mov edi, eax
00401017 xor edx, edx
00401019 test edi, edi
0040101B jle 00401047h
0040101D movsx ecx, byte ptr [edx+esi]
00401021 add [ebp-4], ecx
00401024 mov [ebp-8], ecx
00401027 rol dword ptr [ebp-4], 1
0040102A mov eax, ecx
0040102C imul eax, [ebp-4]
00401030 mov [ebp-4], eax
00401033 mov eax, [ebp-8]
00401036 add [ebp-4], eax
00401039 xor [ebp-4], ecx
0040103C inc edx
0040103D cmp edx, edi
0040103F jl 0040101Dh
00401041 cmp dword ptr [ebp-4] 0
```

大海捞针：

- Opcode的平均大小：
  3bytes
- 平均一个可执行文件的大小：
  几百k到上兆不等
- 不止有可执行文件，还有驱动，库文件等等

- 程序的被动防护
  - 加壳
  - 混淆
- 程序的主动防护
  - 检测逆向工具
  - 反调试手段

ASPACK SOFTWARE

The Enigma Protector
Software Protection

So what do you need
in order to be
a good reverser?

工欲善其事，必先利其器

- 静态分析工具
  - 反编译器
  - Hex Editor (010Editor)
- 动态分析工具
  - Debugger

CONTENTS

1 ida

是汇编过程的逆过程，以机器语言为输入，输出结果是高级语言。

- 编译过程是有信息损失的
  机器语言中没有变量名或函数名，32位数据可以表示整数，指针，浮点数等，需要人工分析
- 编译是多对多的操作
  源程序可以通过很多不同的方式转换为汇编语言，而机器语言也可以通过许多方法转换成源程序。
- 反编译器非常依赖于语言和库
  用c代码的反编译器去处理Delphi编译器生成的二进制文件，可能会有很奇怪的结果。

THANK YOU