【GACTF】Checkin WriteUp

原创

古月浪子 于 2020-08-31 14:29:34 发布 274 收藏

文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/108312464

运行程序后隔了半秒才出现输入flag的提示，且用IDA搜索字符串搜索不到出现过的字符串，函数窗口中没有发现标准输出函数，猜测逻辑可能并非在C代码中

用OD附加后F9，直接退出，索性慢慢单步跟，一直到跟入sub_404920函数中

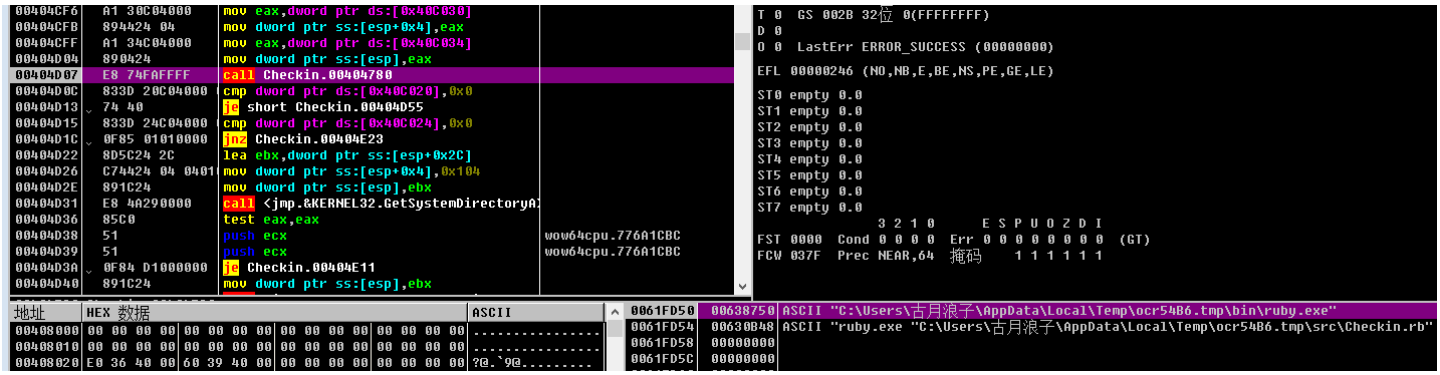
```
signed int __stdcall sub_404920(int a1, int a2, int a3, int a4)
{
  HANDLE v4; // eax
  void *v5; // esi
  DWORD v6; // eax
  int v7; // edi
  HANDLE v8; // eax
  void *v9; // ebx
  DWORD v10; // eax
  FILE *v12; // ebx
  DWORD nSize; // ST08_4
  const void *v14; // eax
  const void *v15; // ebp
  DWORD v16; // eax
  CHAR Buffer; // [esp+2Ch] [ebp-120h]

  sub_403F30();
  if ( !GetModuleFileNameA(0, Filename, 0x104u) )
  {
    v12 = &iob[16];
    fwrite("FATAL ERROR: ", 1u, 0xDu, &iob[16]);
    nSize = GetLastError();
    fprintf(&iob[16], "Failed to get executable name (error %lu).", nSize);
LABEL_7:
    fputc(10, v12);
    return -1;
  }
  sub_4039C0(Str);
  SetEnvironmentVariableA("OCRA_EXECUTABLE", Filename);
  SetConsoleCtrlHandler(HandlerRoutine, 1);
  v4 = CreateFileA(Filename, 0x80000000, 3u, 0, 3u, 0, 0);
  v5 = v4;
  if ( v4 == -1 )
```

发现与文件读写有关，继续OD跟踪，一直到标黄处

```
        fprintf(&iob[16], "Starting app in: %s", Str);
        fputc(10, &iob[16]);
        if ( dword_40C024 )
        {
          fwrite("**********", 1u, 0xAu, &iob[16]);
          fputc(10, &iob[16]);
        }
      }
    }
    sub_404780(dword_40C034, dword_40C030);
  }
  if ( dword_40C020 )
  {
    if ( dword_40C024 )
    {
      fprintf(&iob[16], "Deleting temporary installation directory %s", Str);
      fputc(10, &iob[16]);
    }
    if ( GetSystemDirectoryA(&Buffer, 0x104u) )
      SetCurrentDirectoryA(&Buffer);
    else
      SetCurrentDirectoryA("C:\\");
```

```
116|      sub_403F00(Str);
```

可以在栈窗口中看到被写入的文件的路径



程序被断在了这里，文件应该不可能被清理，资源管理器打开看看

直接在src目录里有一个Checkin.rb源代码

```ruby
require 'openssl'
require 'base64'



def aes_encrypt(key,encrypted_string)
 aes = OpenSSL::Cipher.new("AES-128-ECB")
 aes.encrypt
 aes.key = key
 cipher = aes.update(encrypted_string) << aes.final
 return Base64.encode64(cipher)
end

print "Enter flag: "
flag = gets.chomp

key = "Welcome_To_GACTF"
cipher = "4KeC/Oj1McI4TDIM2c9Y6ahahc6uhpPbpSgPWktXFLM=\n"

text = aes_encrypt(key,flag)
if cipher == text
 puts "good!"
else
 puts "no!"
end
```

直接能读出来加密算法、key、密文，随便找个网站解密即可

> GACTF{Have_a_wonderful_time!}