插入APC读写内存

原创

liuhaidon1992 于 2020-01-08 17:03:20 发布 417 收藏 2
分类专栏： Windows 文章标签： 读写内存


```
#include "ntddk.h"
#include "a_header.h"


NTKERNELAPI NTSTATUS PsLookupProcessByProcessId(HANDLE ProcessId, PEPROCESS *Process);
NTKERNELAPI VOID NTAPI KeStackAttachProcess(PEPROCESS Process, PKAPC_STATE ApcState);
NTKERNELAPI VOID NTAPI KeUnstackDetachProcess(PKAPC_STATE ApcState);

ULONG PID = 2340;
ULONG length = 6;
ULONGLONG address = 0x0725F102;

//插入APC温柔读内存
BOOLEAN APCReadProcessMemory()
{
 PEPROCESS pepro;
 LONG retdata = 0;
 KAPC_STATE ExitApc = { 0 };

 NTSTATUS st = PsLookupProcessByProcessId((HANDLE)PID, &pepro);
 if (!NT_SUCCESS(st))
 {
  return FALSE;
 }

 ObDereferenceObject(pepro);
 __try
 {
  KeStackAttachProcess(pepro, &ExitApc);
  ProbeForRead((CONST PVOID)address, length, sizeof(CHAR));
  RtlCopyMemory(&retdata, (PUCHAR)address, length);
  KeUnstackDetachProcess(&ExitApc);
  KdPrint(("读取的数据为:%x", retdata));
 }
 __except (EXCEPTION_EXECUTE_HANDLER)
 {
  KdPrint(("获取失败"));
  KeUnstackDetachProcess(&ExitApc);
  return FALSE;
 }
 return TRUE;
}
```

```
//插APC温柔写内存
BOOLEAN APCWriteProcessMemory()
{
 PEPROCESS pepro;
 KAPC_STATE kapc = { 0 };
 NTSTATUS st = PsLookupProcessByProcessId((HANDLE)PID, &pepro);
 if (!NT_SUCCESS(st))
 {
  return FALSE;
 }

 ObDereferenceObject(pepro);
 ULONG64 Cr0;
 __try
 {
  KeStackAttachProcess(pepro, &kapc);
  ProbeForWrite((CONST PVOID)address, length, sizeof(CHAR));
  _disable();
  Cr0 = __readcr0();
  Cr0 &= 0xfffffffffffeffff;
  __writecr0(Cr0);
  _enable();
  memcpy((PCHAR)address, "ffffff", length);
  _disable();
  Cr0 |= 10000;
  __writecr0(Cr0);
  _enable();
  KeUnstackDetachProcess(&kapc);
  KdPrint(("获取成功"));
 }
 __except (EXCEPTION_EXECUTE_HANDLER)
 {
  _disable();
  Cr0 |= 10000;
  __writecr0(Cr0);
  _enable();
  KeUnstackDetachProcess(&kapc);

  KdPrint(("获取失败"));
  return FALSE;
 }
 return TRUE;
}
```