

Forum:[Hack Forums](#)

Thread: [\[TUT\] C Read/Write Memory Of A Process From Kernel Mode](#)

Zer0Memo0ry - November 7, 2016, 6:11 am

This code is made working using the undocumented API Function "MmCopyVirtualMemory" in ntoskrnl.exe, which allows the manipulation of a usermode process. These functions are designed to be working like regular WPM/RPM functions, except they operate from ring0.

This method works for regular x64 processes and for WOW64 Processes (x86) regardless of the architecture of the system.

Github: github.com/Zer0Memory/KernelReadWriteMemory

Code NTSTATUS NTAPI MmCopyVirtualMemory

```
(  
PEPROCESS SourceProcess,  
PVOID SourceAddress,  
PEPROCESS TargetProcess,  
PVOID TargetAddress,  
SIZE_T BufferSize,  
KPROCESSOR_MODE PreviousMode,  
PSIZE_T ReturnSize  
);
```

```
NTSTATUS KeReadVirtualMemory(PEPROCESS Process, PVOID SourceAddress, PVOID  
TargetAddress, SIZE_T Size)  
{  
    PSIZE_T Bytes;  
    if (NT_SUCCESS(MmCopyVirtualMemory(Process, SourceAddress, PsGetCurrentProcess(),  
        TargetAddress, Size, KernelMode, &Bytes)))  
    {  
        return STATUS_SUCCESS;  
    }  
    return STATUS_ACCESS_DENIED;  
}
```

```
NTSTATUS KeWriteVirtualMemory(PEPROCESS Process, PVOID SourceAddress, PVOID  
TargetAddress, SIZE_T Size)  
{  
    PSIZE_T Bytes;  
    if (NT_SUCCESS(MmCopyVirtualMemory(PsGetCurrentProcess(), SourceAddress, Process,  
        TargetAddress, Size, KernelMode, &Bytes))) {  
        return STATUS_SUCCESS;  
    }  
    return STATUS_ACCESS_DENIED;  
}
```

PEPROCESS Handle can be obtained with:

```
Code HANDLE ProcessId = 1032 // for example from taskmanager
PEPROCESS Process;
PsLookupProcessByProcessId(ProcessId, &Process);
```

paggarotti - November 7, 2016, 12:45 pm

pretty nice, would be surprised if anyone on here could actually put it to good use except all the shitty vb.net malware.

Zer0Memo0ry - November 7, 2016, 1:36 pm

(Nov 7, 2016 01:45 PM)paggarotti Wrote: [\[CITE\]](#) pretty nice, would be surprised if anyone on here could actually put it to good use except all the shitty vb.net malware.

Yup, people on hackforums should focus less on "skid stuff" like kali linux or ddossing shit, and focus instead on lower level on programming and the actual security and exploits and so forth.

Kernel module programming is interesting area.

paggarotti - November 7, 2016, 1:49 pm

(Nov 7, 2016 02:36 PM)Zer0Memo0ry Wrote: [\[CITE\]](#) Yup, people on hackforums should focus less on "skid stuff" like kali linux or ddossing shit, and focus instead on lower level on programming and the actual security and exploits and so forth.

Kernel module programming is interesting area.

totally agree, though shame all public forums and communities are mostly filled with absolute trash, it's good to see actual skill and talent from time to time, there were some pretty great malware communities with skilled people around some years back that would of appreciated your work very much.

Zer0Memo0ry - November 9, 2016, 8:48 am

(Nov 7, 2016 02:49 PM)paggarotti Wrote: [\[CITE\]](#) totally agree, though shame all public forums and communities are mostly filled with absolute trash, it's good to see actual skill and talent from time to time, there were some pretty great malware communities with skilled people around some years back that would of appreciated your work very much.

That's true. I am glad though that there are some really good underground forums on the darkweb which are totally different from these toxic script kiddy communities. Hell & Kickass Forums are both great.

View - November 11, 2016, 1:16 pm

Thanks for the share!!!!!!!!!!!!

Zer0Memo0ry - November 12, 2016, 7:36 am

(Nov 11, 2016 02:16 PM)Nonstop223 Wrote: [\[CITE\]](#) Thanks for the share!!!!!!!!!!!!
No problem =)

private.member - February 13, 2017, 9:18 am

Thanks for the share!!!!!!!!!!!!