

Forum: [Hack Forums](#)

Thread: [Process termination from Windows krnl](#)

Cheddar Cheese - October 21, 2019, 4:23 pm

Hi

Easy peazy way to terminate processes when you are in the kernel on Windows

1. PsLookupProcessByProcessId
2. ObOpenObjectByPointer
3. ZwTerminateProcess

^^ order of API calls required. That's it!

```
Code PEBPROCESS pProcess;
HANDLE hProcess;
if (NT_SUCCESS(PsLookupProcessByProcessId((HANDLE)processid, &pProcess)))
{
    if (NT_SUCCESS(ObOpenObjectByPointer(pProcess, 0, NULL, 0, *PsProcessType,
KernelMode, &hProcess)))
    {
        ZwTerminateProcess(hProcess, 0);
    }
}
```

If you are in the kernel then with this method you will also be able to kill many AV processes but it won't get around ELAM so you need dkom for that one m8.

enjoy the read & gl

Nyugen3 - October 22, 2019, 8:44 am

Cheddar, you do not need to use ObOpenObjectByPointer and ZwTerminateProcess!

Once you have found the pointer address to the process's _EPROCESS structure, you can use PsTerminateProcess directly. PsTerminateProcess is not exported so you would have to find the address to it.

RBF Tools - November 2, 2019, 5:43 pm

Hello friend do you have any contact information about the User Wikipedia ? his account had been closed and i was in a conversation with him, really need to talk to him i saw you visited his account so maybe you know how to contact him?

thanks in advance