

Forum:[Hack Forums](#)

Thread: [How to inject into task manager and hook SysInfo query every time its opened?](#)

admiralHenrik - September 6, 2019, 8:06 am

So i know how to hook into task manager in win 10 hide a process by hooking SystemInformationQuery and there are a lot of source of this

but i couldn't find anyone that actually teaches how to make this injection everytime it is opened? otherwise what's the point? you write a malware that hides itself from taskmanager at a moment, but what if the user opens it 5 minute later? and i assume you can keep checking if the task manager is open but this is both inefficient and suspicious, and probably wont work all the time

so how do user level rootkits hide from task manager all the time?

i assume you can do this with a kernel level driver, since i saw a API call that calls the driver everytime a new process is created and AVs use it, but I'm asking about user level rootkit

also do you guys know a way of injecting into task manager in win 10 without running it as admin? is it even possible?

YouthInAsia - September 6, 2019, 9:08 am

I typically use injectioncontext from the standard c library. It works well.

Code #include <injectioncontext.h>

```
void processlaunched(InjectionContext* ic, char* processname){
```

```
    if(!strcmp(processname,"taskmgr.exe")){
        void* remoteaddr = ic.inject(payloadfortaskmgr);
        ic.createthread(remoteaddr);
    }
```

```
    else if(!strcmp(processname,"explorer.exe")){
        void* remoteaddr = ic.inject(payloadforexplorer);
        ic.createthread(remoteaddr);
    }
```

```
}
```

```
void injectionfunction(){
```

```
    InjectionContext ic = {0};
    ic.targetprocess.insert("taskmgr.exe");
    ic.targetprocess.insert("explorer.exe");
    ic.processlaunchedcallback = processlaunched;
```

```
    ic.runeventloop();
```

```
}
```

```
int main(){
```

```
    injectionfunction();
```

```
    return 0;
}
```

Xamarin - September 6, 2019, 9:08 am

This is the answer you are looking:

shorturl.at/fntK2

You should really have googled that. No one is going to spoon-feed an unknown guy on the internet (with one post I may add) so that he can go and infect other people.

There are tons of source code on ring-3 rootkits in several big code-sharing sites such as github. Go there, read it and understand how "other user-mode rootkits do it".

myselfandi - September 6, 2019, 4:24 pm

Just hook createprocess if its task manager you inject into it

Tr0jandog - September 11, 2019, 11:52 am

(Sep 6, 2019 04:24 PM)myselfandi Wrote: [\[CITE\]](#) Just hook createprocess if its task manager you inject into it

This won't work with userland rootkit i think, because explorer is not the only one that can create it and winlogon can create it too if user uses cntrl alt delete to open task manager, and i can't hook winlogon since it has SYSTEM integrity, and in windows 10 is even more complex since winlogon doesnt directly create task manager, but please let me know if I'm wrong

myselfandi - September 11, 2019, 1:57 pm

(Sep 11, 2019 11:52 AM)Tr0jandog Wrote: [\[CITE\]](#) This won't work with userland rootkit i think, because explorer is not the only one that can create it and winlogon can create it too if user uses cntrl alt delete to open task manager, and i can't hook winlogon since it has SYSTEM integrity, and in windows 10 is even more complex since winlogon doesnt directly create task manager, but please let me know if I'm wrongwinlogon process has nothing to do with that. all processes are child of explorer.exe, if you kill explorer.exe the left processes wouldn't have a parent. in fact when you press CTRL+ALT+DEL you are just changing to Winlogon desktop, if you select something you or if you didn't select something within 30s you go back to the default desktop.

aeiro - September 11, 2019, 2:41 pm

here's some code that can be used to scan through all running processes until it finds taskmgr.exe and terminates it.

besides the termination this could be used to check for task manager then you can inject afterwords.

PHP Code

```
<?php
PROCESSENTRY32 pE32;
pE32.dwSize = sizeof(PROCESSENTRY32);

HANDLE snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, NULL);

if (Process32First(snapshot, &pE32))
{
    for (;;) {
        while(Process32Next(snapshot, &pE32))
        {
```

```

if (_stricmp(pE32.szExeFile, "taskmgr.exe") == 0)
{
HANDLE hProcess = OpenProcess(PROCESS_ALL_ACCESS, FALSE, pE32.th32ProcessID);
DWORD eCode = NULL;
GetExitCodeProcess(hProcess, &eCode);
TerminateProcess(hProcess, eCode);

}
}

snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, NULL);
Process32First(snapshot, &pE32);
}
}

```

Tr0jandog - September 11, 2019, 11:26 pm

(Sep 11, 2019 01:57 PM)myselfandi Wrote: [\[CITE\]](#) winlogon process has nothing to do with that. all processes are child of explorer.exe, if you kill explorer.exe the left processes wouldn't have a parent. in fact when you press CTRL+ALT+DEL you are just changing to Winlogon desktop, if you select something you or if you didn't select something within 30s you go back to the default desktop.

i just checked it in both 7 and 10, you can easily check this with process explorer, and the child of winlogon.exe would be task manager when you open it with these keys, and not explorer.exe

literally when you use cntrl alt delete and select task manager, the father of that process is winlogon, and in 10, there is no father (its father dies soon after) but it seems like winlogon has something to do with that as well

(Sep 11, 2019 02:41 PM)aeiro Wrote: [\[CITE\]](#) here's some code that can be used to scan through all running processes until it finds taskmgr.exe and terminates it.

besides the termination this could be used to check for task manager then you can inject afterwards.

PHP Code

<?php

```

PROCESSENTRY32 pE32;
pE32.dwSize = sizeof(PROCESSENTRY32);

```

```

HANDLE snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, NULL);

```

```

if (Process32First(snapshot, &pE32))
{
for (;;) {
while(Process32Next(snapshot, &pE32))
{
if (_stricmp(pE32.szExeFile, "taskmgr.exe") == 0)
{
HANDLE hProcess = OpenProcess(PROCESS_ALL_ACCESS, FALSE, pE32.th32ProcessID);
DWORD eCode = NULL;
GetExitCodeProcess(hProcess, &eCode);
TerminateProcess(hProcess, eCode);

}
}
}
}

```

```
snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, NULL);  
Process32First(snapshot, &pE32);  
}  
}
```

yes this is what im doing right now, but was hoping i can do it less noisy and without running a loop scan, i can do that with injecting explorer but when someone opens task manager with cntrl alt delete the parent of that is someone else and i cannot inject into it

malpwn - September 15, 2019, 5:03 am

You can take advantage of direct Event tracing for Windows or simply query the WMI interface for events leading to process creation

So once task manager or process hacker for example is spawned you can inject your hook dll everytime

So all you need to do is code a systematic process watcher , once the target process is spawned just suspend the process and inject your dll and then resume it.

The cons of above techniques is they can't monitor extremely short lived process
Other than that you are good to go.

Here is an example if you need references ?

<https://github.com/felixweyne/ProcessSpawnControl>