

Forum:[Hack Forums](#)

Thread: [Adding to startup problem](#)

ThePacketBaron - April 18, 2015, 11:05 am

So I am learning c++ and I was playing around with adding registry keys to make programs get added to startup. However I came across something which puzzled me slightly. When I used the normal way of adding something to startup in c++ it only got added when I ran it as admin. The thing that puzzled me is the fact that a lot of malware can add things to startup without requiring any admin priv's what so ever, using the same method of startup. Can someone please explain this? (I am assuming this thread is gonna be full of people whining about me being an idiot but I figure I may as well ask) Here is the code below:

PHP Code

```
<?php
#include<windows.h>
#include<string.h>
int main()
{
    HKEY hkey;
    DWORD dwDisposition;

    RegOpenKeyEx(HKEY_LOCAL_MACHINE,"Software\\Microsoft\\Windows\\CurrentVersion\\Run",0
,KEY_ALL_ACCESS ,&hkey);
    const unsigned char path[150] = "C:\\Windows\\system32\\notepad.exe";
    RegSetValueEx(hkey,"Test Startup",0,1,path,sizeof(path));
    return 0;
}
```

sqsgkrldwg - April 18, 2015, 11:59 am

Hi,

I love your thread.
I never tested to overcome those things.

Here is a paper that will help you :
<http://www.exploit-db.com/bypassing-uac-with-user-privilege-under-windows-vista7-mirror/>

It's from 2010, but the idea is here. I think the only solution is to take advantage of exploits.

I will try it, this things interest me.

Edit : I'm off topic.

See this instead : <http://stackoverflow.com/a/15937683>

Masm4ever - April 18, 2015, 12:02 pm

No surprise. Normal non-admin users should never be allowed to fumble with Run keys (there are several). This is a really basic security design thing. Just tell your users to install your proggy as

admin, this will solve your problem. Unless you are a wannabe malware writer, of course.

ThePacketBaron - April 18, 2015, 2:51 pm

Thanks a lot guys, your posts have been very helpful to me :D Adding to HKEY_CURRENT_USER made it work however all the posts were very insightful. Thanks guys :)

santoryu - April 26, 2015, 12:21 pm

Well, it's all about accessing the system32 folder . Windows won't allow you to access that folder unless you run the executable file as admin.

hint : copy the your executable file you want to run at startup in a folder like %programdata% and set the register key with the equivalent path

0xDEAD10CC - April 26, 2015, 1:12 pm

I think you're confused about the fact that there is malware that doesn't use the registry for startup persistence either, because that is not the only way, and neither is the shell:startup folder. It's also the easiest to detect.

Xch4ng3 - April 26, 2015, 3:51 pm

I just had to remove 50+ low quality posts from this thread because some members don't understand the concept of "don't feed the troll", especially when responding to an account that has the suffix v129.

Anyone entertaining trolls will be held equally responsible. Trolls and shit posters only get giggles when YOU respond. Do the smart thing, report the posts, let staff deal with them.