Any way of getting the flag is valid. I will describe two of the ways you can do it, but any way you manage to get the flag is completely valid.

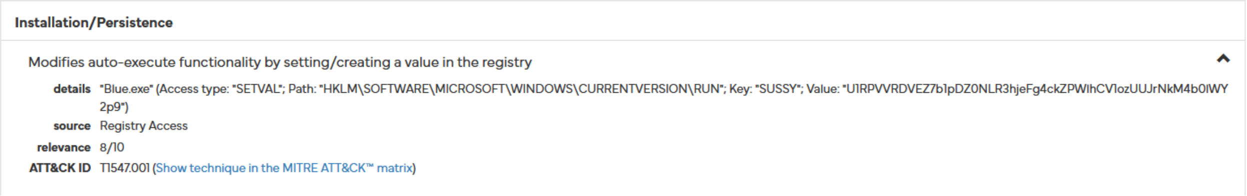
When run, this executable changes a registry key and then causes a blue screen of death (BSOD). You need to get the value of the registry key before the program blue screens.

Easy Solution

The easiest way to get the flag is using an online sandbox, such as https://any.run/, https://www.hybrid-analysis.com/, or https://tria.ge/. Any.run and tria.ge are both free but require you to sign up. Hybrid-analysis allows you to run samples without signing up.

After you upload the file to hybrid-analysis, you can scroll down and click one of the Falcon Sandbox Reports, with the Windows 11 and Windows 10 results containing the necessary information.

These Falcon reports will give a variety of information, which you will have to look through to find the flag. The flag will be located under the Installation/Persistence dropdown, as shown below.

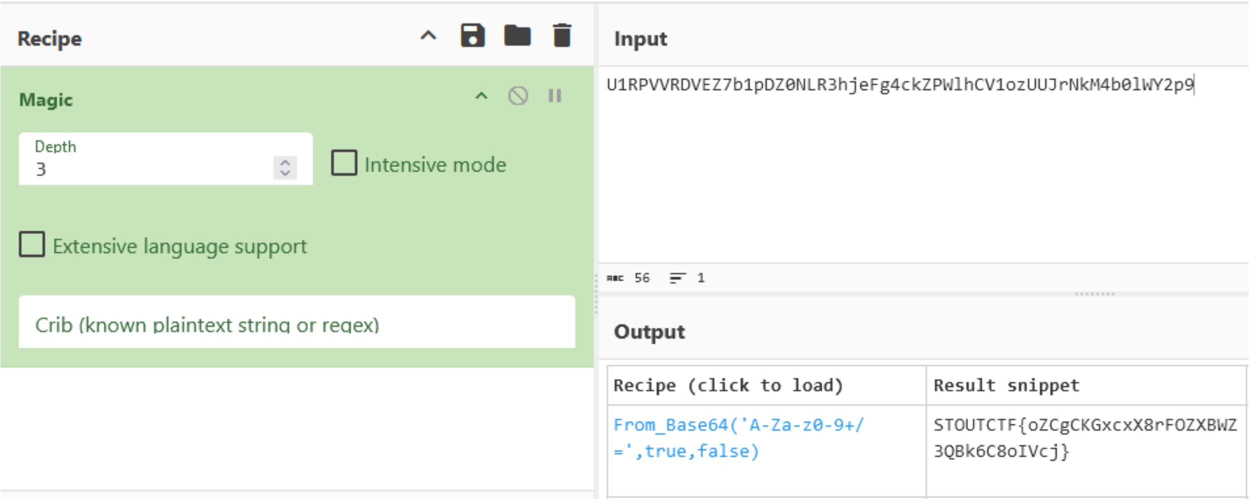


Installation/Persistence

Modifies auto-execute functionality by setting/creating a value in the registry

details	"Blue.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"; Key: "SUSSY"; Value: "U1RPVVRDVEZ7b1pDZ0NLR3hjeFg4ckZPWlhCV1ozUUJrNkM4b0lWY2p9")
source	Registry Access
relevance	8/10
ATT&CK ID	T1547.001 (Show technique in the MITRE ATT&CK™ matrix)

You can then copy the value and decode it using whatever tool you prefer. I used CyberChef (https://gchq.github.io/CyberChef/), with the “Magic” recipe to decode and get the flag.



Depth: 3

□ Intensive mode

□ Extensive language support

Input

```
U1RPVVRDVEZ7b1pDZ0NLR3hjeFg4ckZPWlhCV1ozUUJrNkM4b0lWY2p9
```

Output

Recipe (click to load)	Result snippet
From_Base64('A-Za-z0-9+/=',true,false)	STOUTCTF{oZCgCKGxcxX8rFOZXBWZ3QBk6C8oIVcj}

Hard Solution

The hard solution is the manual way of getting the flag. For this, I used x64dbg, ProcMon (Sysinternals Process Monitor), regedit.exe, and of course, CyberChef. When performing analysis this way, make sure to only do it within the safety of a virtual machine, so that you don't damage your own operating system. Here are the high-level steps to finding the flag manually:

1. To start, open ProcMon and filter by the name of the executable.
2. (Optional) Unpack the executable. The file was packed using UPX and can be unpacked using the command "upx -d Blue.exe"/. The challenge is possible whether or not you unpack it, but it will be slightly easier if you do unpack it.
3. Next, load the executable into a debugger.
4. Step through the executable and watch what happens in ProcMon. At some point, the executable will create a new registry key located at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, a common spot for malware to register persistence.
    a. The registry key will be named "sussy", with the value "U1RPVVRDVEZ7b1pDZ0NLR3hjeFg4ckZPWlhCV1ozUUJrNkM4b0lWY2p9".
    b. If ProcMon doesn't directly show the value, the built-in Windows tool regedit.exe can be used to retrieve the value.
5. Decode the string using any tool you want, such as CyberChef, show above.