# Contents



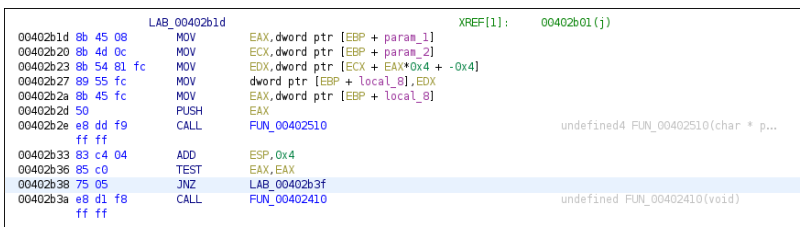
# 1 Homework

## 1.1 HW7

### 1.1.1 Lab 9-1

1. Question 1 To get the malware to install, we need to reach `0x00402600`. Within this function, there are function calls to `OpenSCManagerA`, `ChangeServiceConfigA`, `CreateServiceA`, `CopyFileA`, and registry modifications.

   To get to the install function, we would need to run this malware with 3 arguments. We need a password as one of these arguments along with `"-in"` as the first argument. To decipher this password, we can take a look at `0x00402510`. The password must be 4 characters long. After analyzing the funciton, we see that the passcode is `"abcd"`.




   We can also patch `0x00402B38` by changing `jnz` to `jz` to bypass any password check.

   We can install the malware by executing it with the arguments `"Lab09-01.exe -in abcd"`.

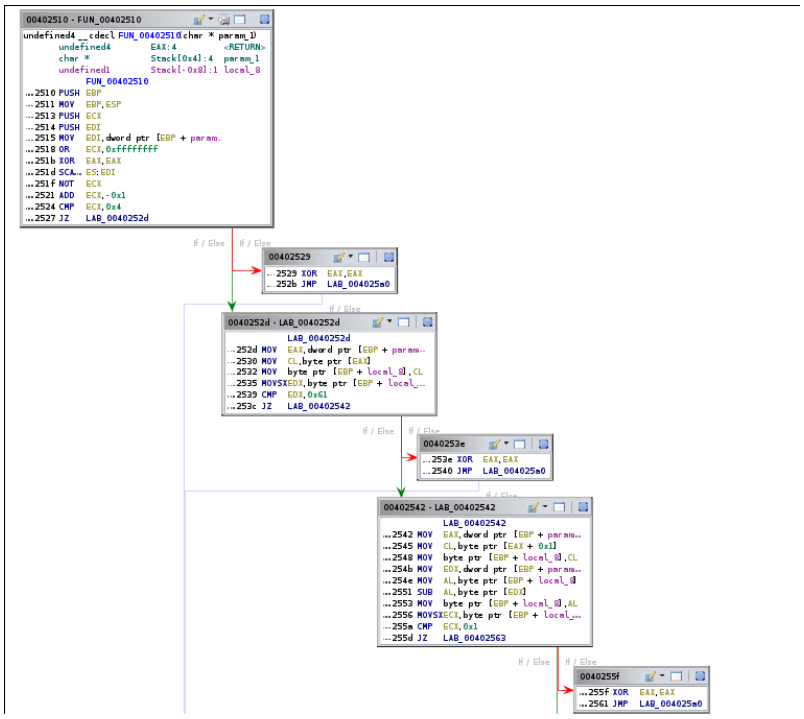
2. Question 2 There are 4 command-line options for the program.

   (a) `"-in"`: installs

   (b) `"-re"`: uninstalls

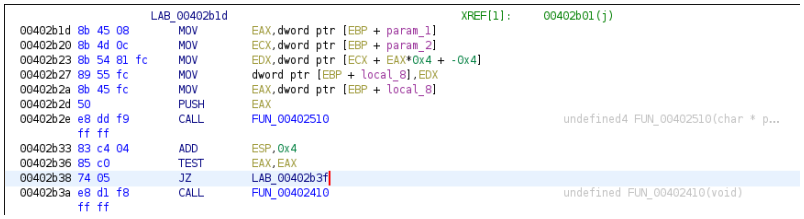
   (c) `"-cc"`: prints our registry

(d) `"-c"`: sets registry value



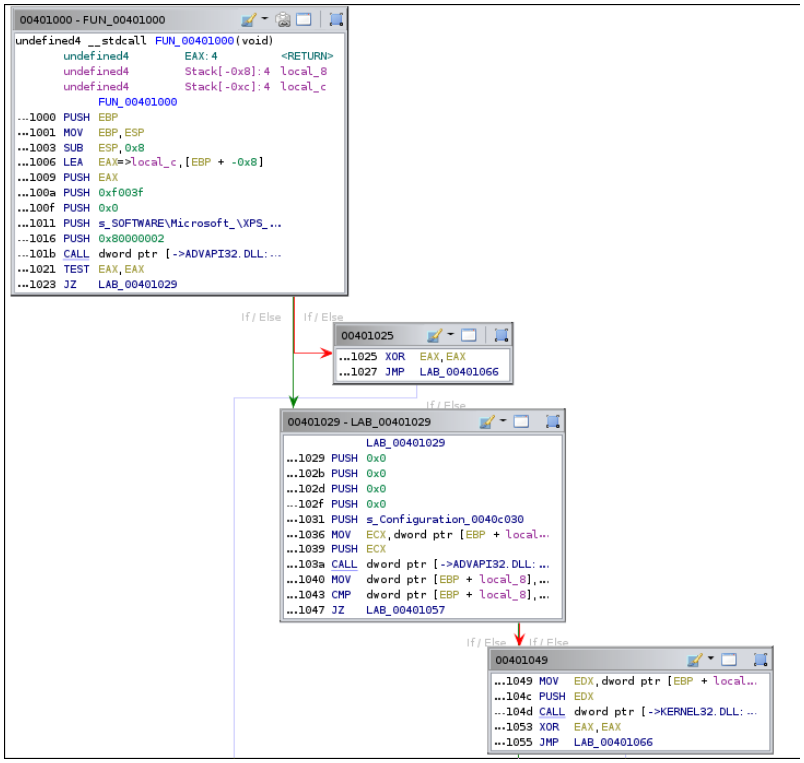

Analyzing the function, we can find what the password to the installer, `"abcd"`.

3. Question 3 To Patch the program so that it doesnt require a password, we need to patch 0x00402B38 from `jnz` to `jz`.




Changing `75` to `74` will change the instruction from `jnz` to `jz`.

4. Question 4

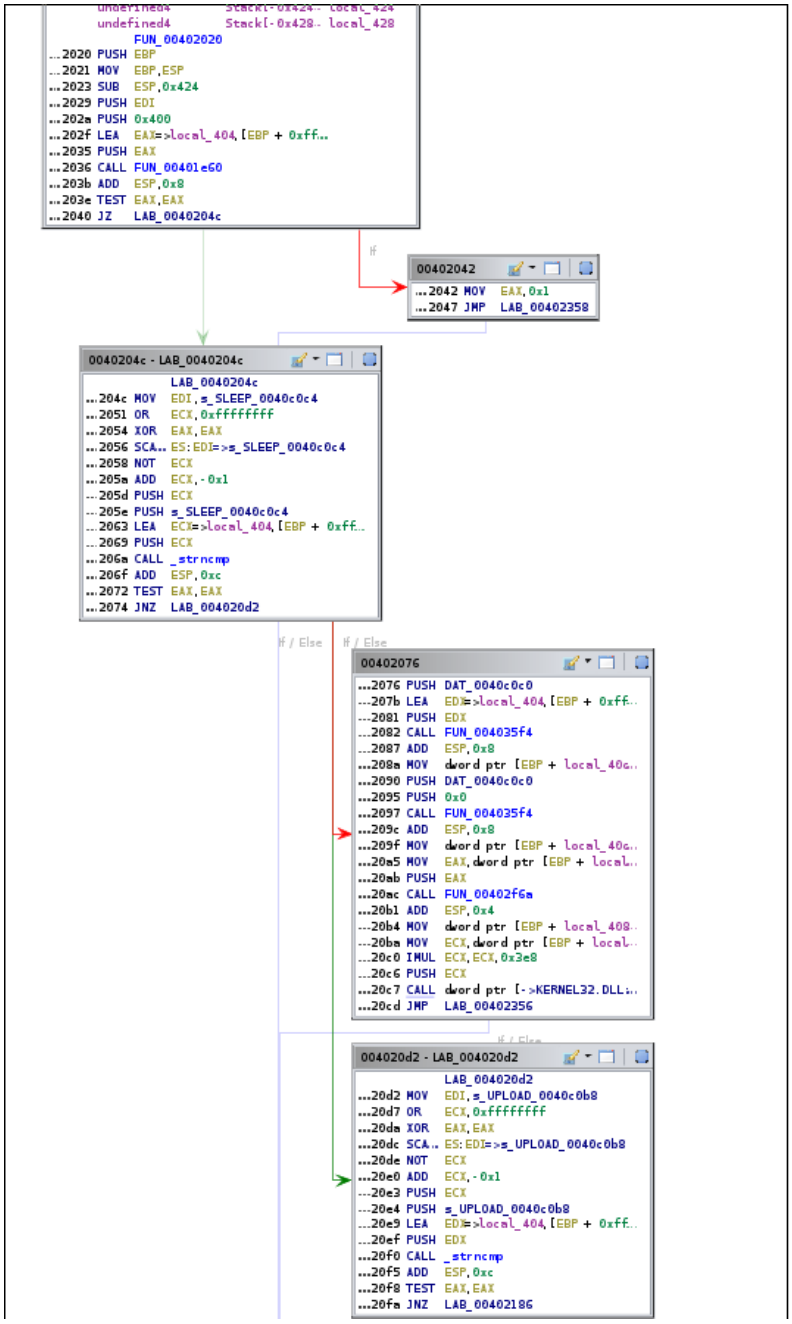



One possible way of detecting the malware is by checking if any registry values were added. These registry keys are added to create persistance.

```
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\ImagePath: "%SYSTEMROOT%\system32\Lab09-01_patched.exe"
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\DisplayName: "Lab09-01_patched Manager Service"
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\Lab09-01_patched\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00
HKLM\SYSTEM\CurrentControlSet\Services\Lab09-01_patched\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\Lab09-01_patched\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\Lab09-01_patched\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\Lab09-01_patched\ImagePath: "%SYSTEMROOT%\system32\Lab09-01_patched.exe"
HKLM\SYSTEM\CurrentControlSet\Services\Lab09-01_patched\DisplayName: "Lab09-01_patched Manager Service"
HKLM\SYSTEM\CurrentControlSet\Services\Lab09-01_patched\ObjectName: "LocalSystem"
```

We can check for these registry keys as a way of detecting whether a computer has been infected or not

5. Question 5




Taking a look at 0x00402020, we can see that there are multiple different tasks the malware does

(a) Sleep

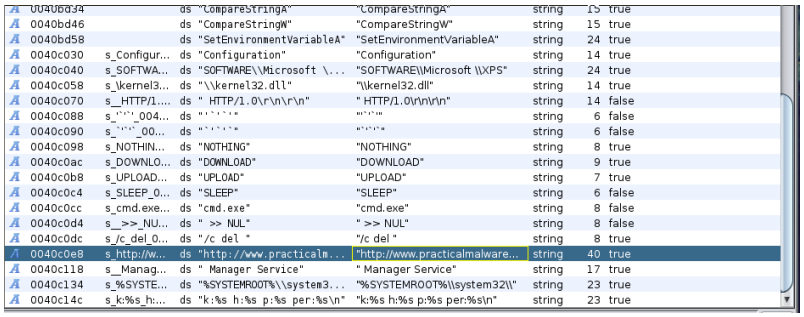
(b) Upload

(c) Download

(d) Execute

(e) Do nothing

6. Question 6



| | | | | | | |
|---|---|---|---|---|---|---|
| 0040bd46 | | ds | "CompareStringW" | "CompareStringW" | string | 15 true |
| 0040bd58 | | ds | "SetEnvironmentVariableA" | "SetEnvironmentVariableA" | string | 24 true |
| 0040c030 | s_Configur... | ds | "Configuration" | "Configuration" | string | 14 true |
| 0040c040 | s_SOFTWA... | ds | "SOFTWARE\\Microsoft \... | "SOFTWARE\\Microsoft \\XPS" | string | 24 true |
| 0040c058 | s_\kernel3... | ds | "\\kernel32.dll" | "\\kernel32.dll" | string | 14 true |
| 0040c070 | s__HTTP/1.... | ds | " HTTP/1.0\r\n\r\n" | " HTTP/1.0\r\n\r\n" | string | 14 false |
| 0040c088 | s_``_004... | ds | "``" | "``" | string | 6 false |
| 0040c090 | s_``_00... | ds | "``" | "``" | string | 6 false |
| 0040c098 | s_NOTHIN... | ds | "NOTHING" | "NOTHING" | string | 8 true |
| 0040c0ac | s_DOWNLO... | ds | "DOWNLOAD" | "DOWNLOAD" | string | 9 true |
| 0040c0b8 | s_UPLOAD... | ds | "UPLOAD" | "UPLOAD" | string | 7 true |
| 0040c0c4 | s_SLEEP_0... | ds | "SLEEP" | "SLEEP" | string | 6 false |
| 0040c0cc | s_cmd.exe... | ds | "cmd.exe" | "cmd.exe" | string | 8 false |
| 0040c0d4 | s_>>_NU... | ds | " >> NUL" | " >> NUL" | string | 8 false |
| 0040c0dc | s_/c_del_0... | ds | "/c del " | "/c del " | string | 8 true |
| 0040c0e8 | s_http://w... | ds | "http://www.practicalm... | "http://www.practicalmalware... | string | 40 true |
| 0040c118 | s__Manag... | ds | " Manager Service" | " Manager Service" | string | 17 true |
| 0040c134 | s_%SYSTE... | ds | "%SYSTEMROOT%\\system3... | "%SYSTEMROOT%\\system32\\" | string | 23 true |
| 0040c14c | s_k:%s_h:... | ds | "k:%s h:%s p:%s per:%s\n" | "k:%s h:%s p:%s per:%s\n" | string | 23 true |

We can see in the strings, there is a website stored in the program, `"http://www.practicalmalwareanalysis.com"`. Using wireshark, we see that the malware is trying to receive commands from the website

### 1.1.2 Lab 9-2