Lab 7 Solutions - The Case of Joon Malware

Lab 7 - The case of Joon malware

Analyze the sample ***blob.exe*** and answer the below questions

- Does the malware have references to the downloader API calls?
- What is the API call used by the malware to download the file?
- What is the name of the domain from where malware downloads malicious component?
- What is the name of the executable that it downloads?
- What is the full path on the disk where downloaded malware is dropped?
- How does it execute the downloaded file?
- Based on your analysis, what is the functionality of the malware?

Answers

01. Does the malware have references to the downloader API calls?

To look at references to API calls, first Run ***x32dbg.exe*** as Administrator and load ***blob.exe.*** Now right-click anywhere in the disassembly (CPU) window (with the executable loaded), then select **Search for | Current Module |Intermodular calls**; this will populate the ***references window*** with the references to all of the API calls in the program. In the references window, you can see the downloader API calls ***URLDownloadToFile()*** and ***ShellExecute()***

```
004006D8    call dword ptr ds:[<&ExitProcess>]
00402002    call dword ptr ds:[<&GetModuleHandleA>]
00402016    call dword ptr ds:[<&FindResourceA>]
00402029    call dword ptr ds:[<&LoadResource>]
0040203C    call dword ptr ds:[<&SizeofResource>]
0040204D    call dword ptr ds:[<&LockResource>]
00402069    call dword ptr ds:[<&RtlMoveMemory>]
00402075    call dword ptr ds:[<&FreeResource>]
00402087    call dword ptr ds:[<&GetTempPathA>]
00402097    call dword ptr ds:[<&lstrcatA>]
004020A2    call dword ptr ds:[<&DeleteFileA>]
004020B8    call dword ptr ds:[<&URLDownloadToFileA>]
004020D0    call dword ptr ds:[<&ShellExecuteA>]
004020D8    call dword ptr ds:[<&ExitProcess>]
```

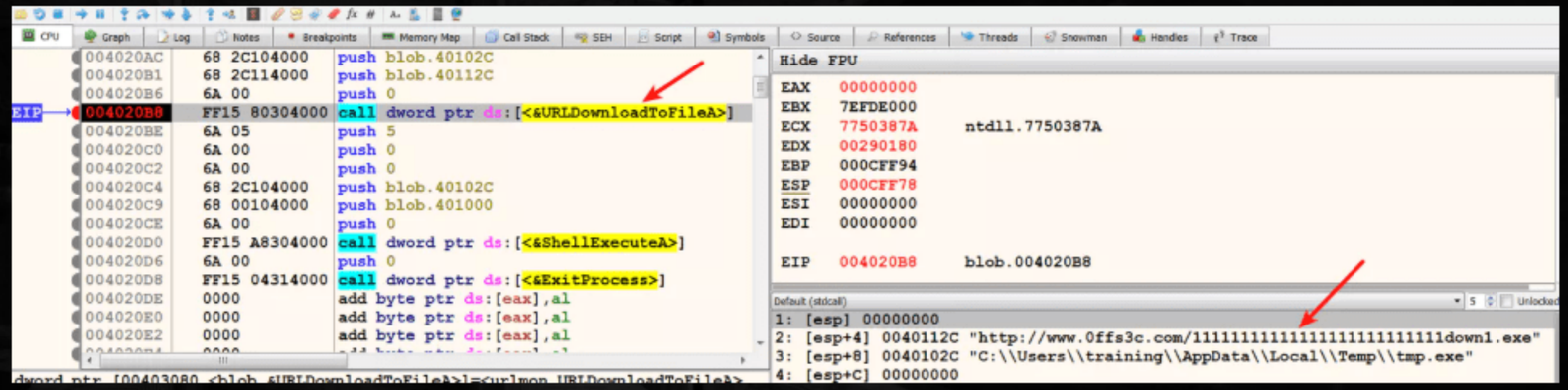
02. What is the API call used by the malware to download the file?

URLDownloadToFile() is the API call used by the malware to download the file. MSDN documentation for this API call suggests that this function can be used to downloads bits from the Internet and save them to a file.

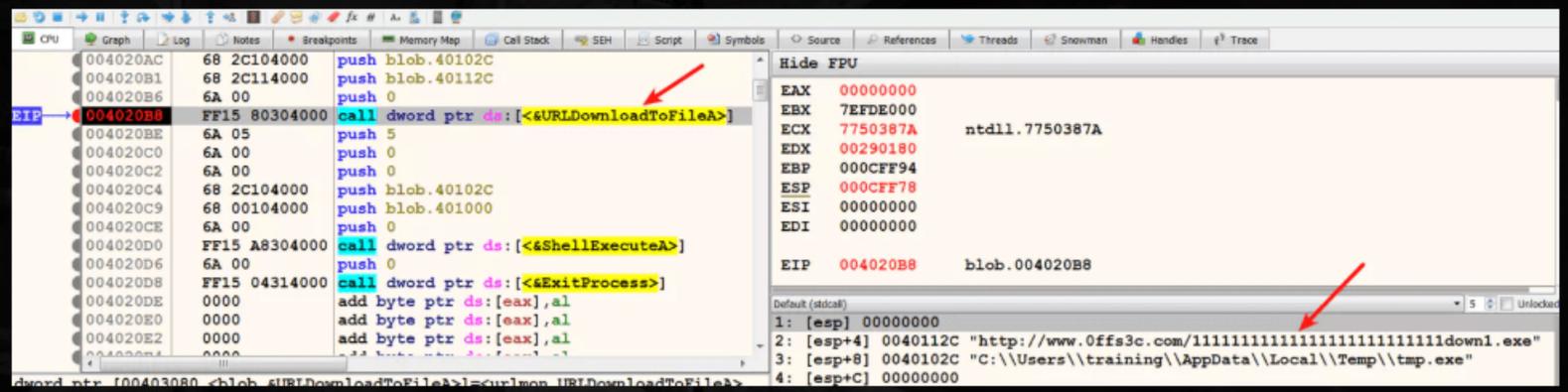
03. What is the name of the domain from where malware downloads malicious component?

To answer this question, you need to find the reference to ***URLDownloadToFile()*** in the code. To do that highlight the function ***URLDownloadToFile()*** in the ***references window***, right click and select ***Follow in Disassembler,*** this shows the reference to the code where the api call is used.

At this point, you can set the breakpoint (***F2***) on the instructions where ***UrlDownloadToFileA()*** will be called and run the code, the execution should pause before the API Call as shown in the screenshot



MSDN documentation for this function shows that the second parameter to this function will contain the URL from where the malicious component will be downloaded.. Examining the second parameter in the stack window shows the URL (& the name of the domain). In this case, the malware downloads an executable "***111111111111111111111111111down1.exe***" from the domain "www[.]offs3c[.]com"; as shown in the screenshot.

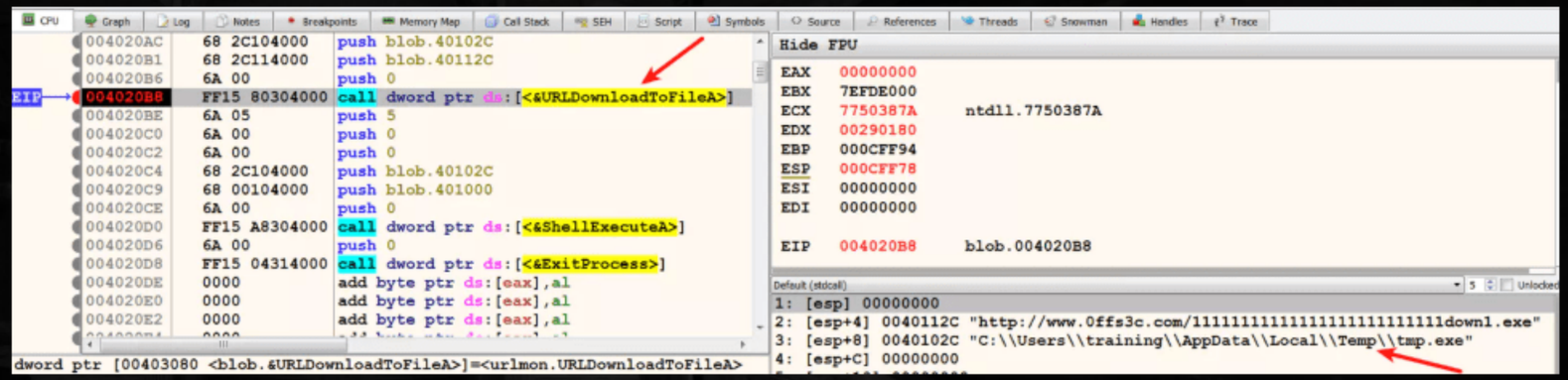


04. What is the name of the executable that it downloads from the domain?

Examining the second parameter shows the name of the executable. In this case, the name of the executable that it downloads from the C2 domain is "***111111111111111111111111111down1.exe***"

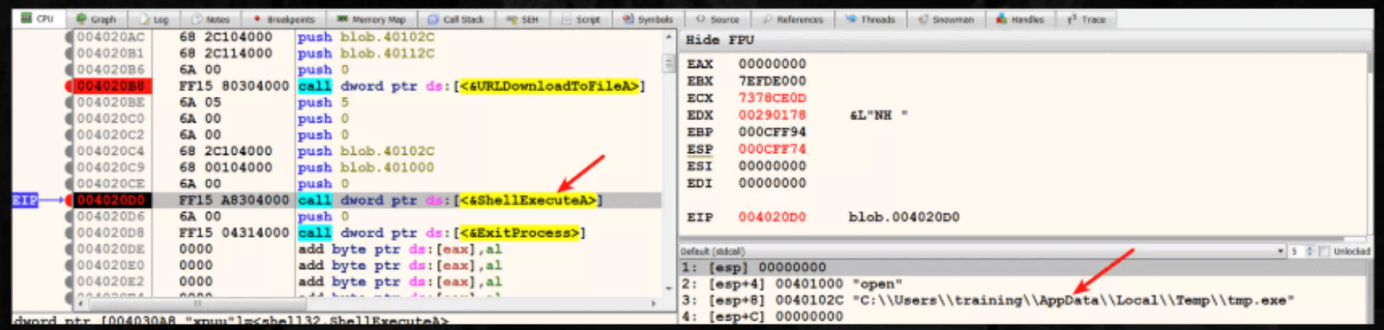
05. What is the full path on the disk where downloaded malware is dropped?

As per the MSDN documentation, the third parameter to the function will give the full path on the disk. Examining the third parameter shows the full path where the downloaded executable will be saved. In this case, the downloaded file is saved as "***tmp.exe***" in the ***%TEMP%*** folder



06. How does it execute the downloaded file?

The malware executes the downloaded file by calling the ***ShellExecute()*** function. The malware passes the full path to the executable as the third parameter to the ***ShellExecute()*** function. When the ***ShellExecute()*** function is called it will execute the file (***tmp.exe***) from the ***%TEMP%*** folder



07. Based on your analysis, what is the functionality of the malware?

Based on the analysis the malware downloads an executable and executes it on the system. This malware is a downloader.