Malware Analysis Report [dofoil.exe]

Prepared by: Sameer Patil

Mentors: Amit Malik & Monnappa KA

[SecurityXploded Student Mentorship Programme]

General Information

- File name: dofoil.exe
- MD5: fbeb99d329cbaa396b148d37a32aae97
- SHA-1: 57747fd86269fa547a94e47d565a71285993e284
- File Size: 281 KB
- First submission on: 19-9-2012
- Identified as: TrojanDownloader:Win32/Dofoil.R [Microsoft]
  Trojan-Spy.Win32.Zbot.eqmk [Kaspersky Lab]
  PWS-Zbot.gen.ala [McAfee]
  TrojWare.Win32.Injector.VDK [Comodo]

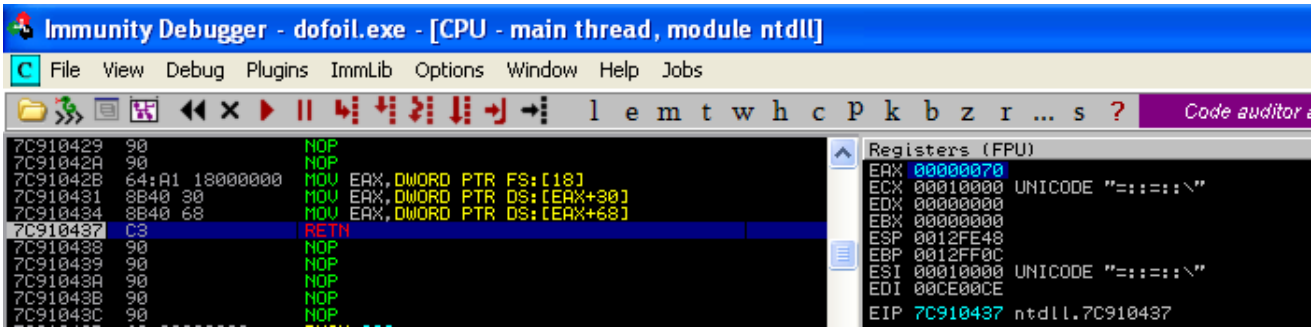
Analysis Overview:

Dofoil.exe is a Trojan dropper. It downloads and installs other programs without user consent. This may include installation of more powerful and latest malwares by the author. The Trojan also modifies the registry to trigger its execution at system startup itself. Its a very carefully written malware which also uses multiple anti-detection techniques.

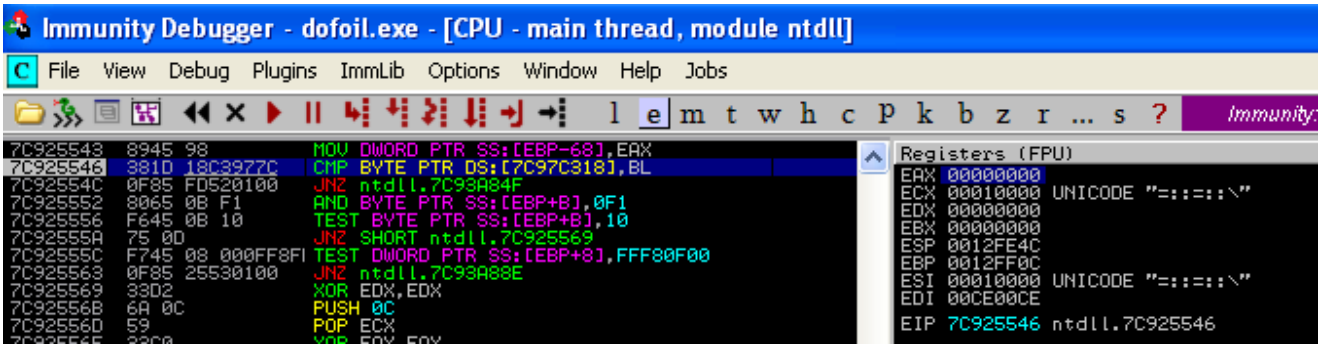
Technical Analysis

1. The malwares deploys several debugger detection techniques to hide its activities.

   a. One of them is the use of “PEB.NTGlobalFlag” which is present at offset 0x68 of PEB. The flag is set 0 if no debugger is running. If any debugger is running its value is 0x70 which signifies the following flags are set:
   FLG_HEAP_ENABLE_TAIL_CHECK (0x10)
   FLG_HEAP_ENABLE_FREE_CHECK (0x20)
   FLG_HEAP_VALIDATE_PARAMETERS (0x40)

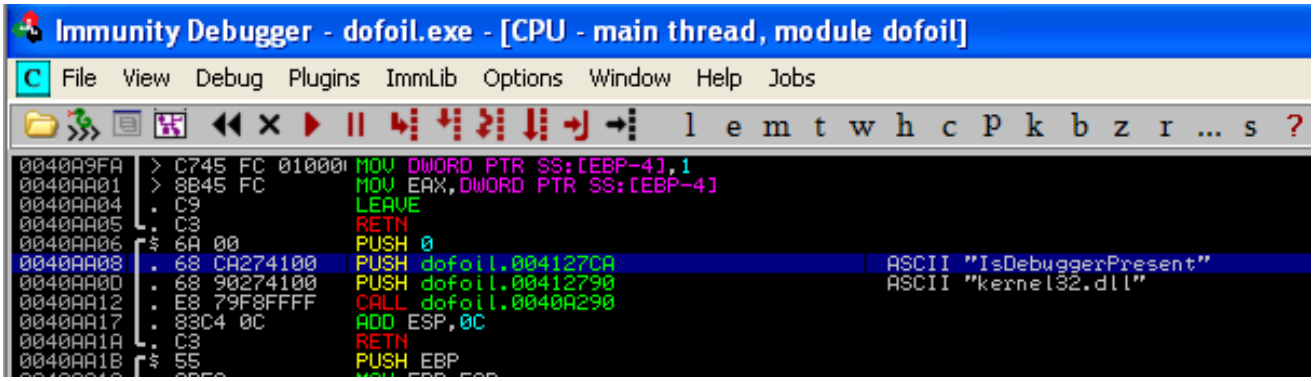


   This check can be bypassed by manually changing the value stored in EAX from “00000070” to 0.



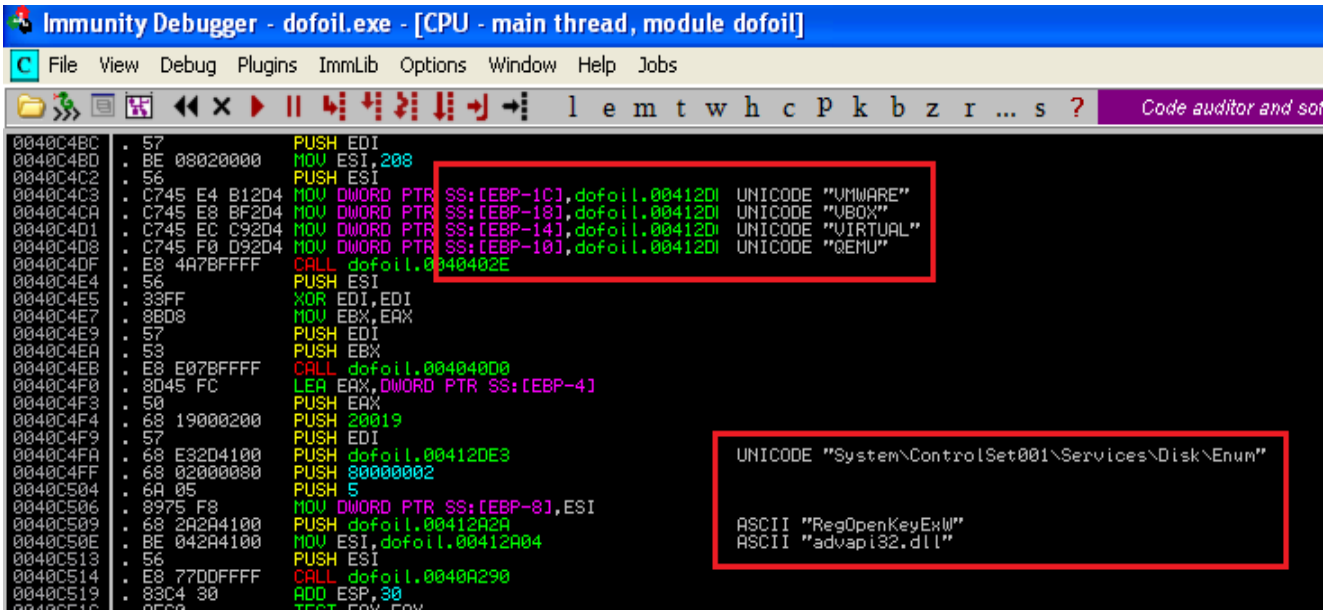
   b. Another method used is “Kernel32.IsDebuggerPresent” API as shown below. Here also we make the value of EAX register as 0 to bypass the protection.

.

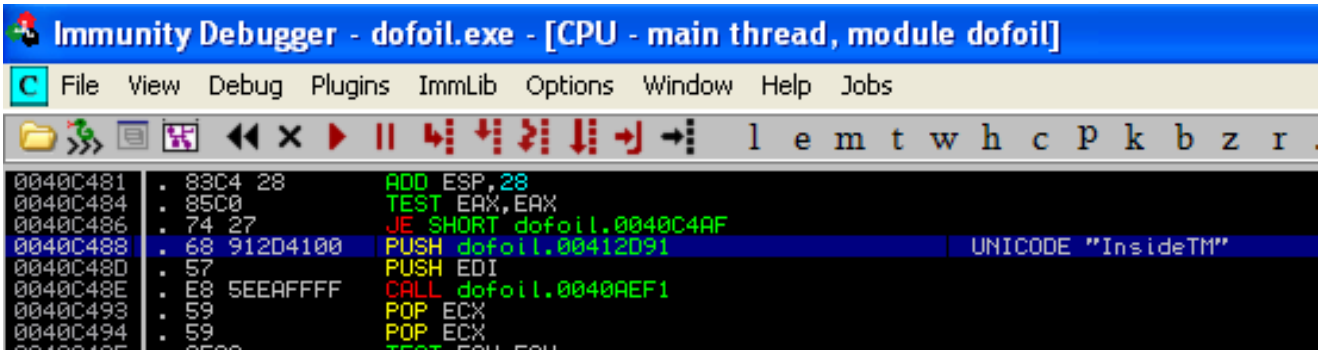


2. After we bypass these tests the malware unpacks itself and generates more code at different locations in memory.

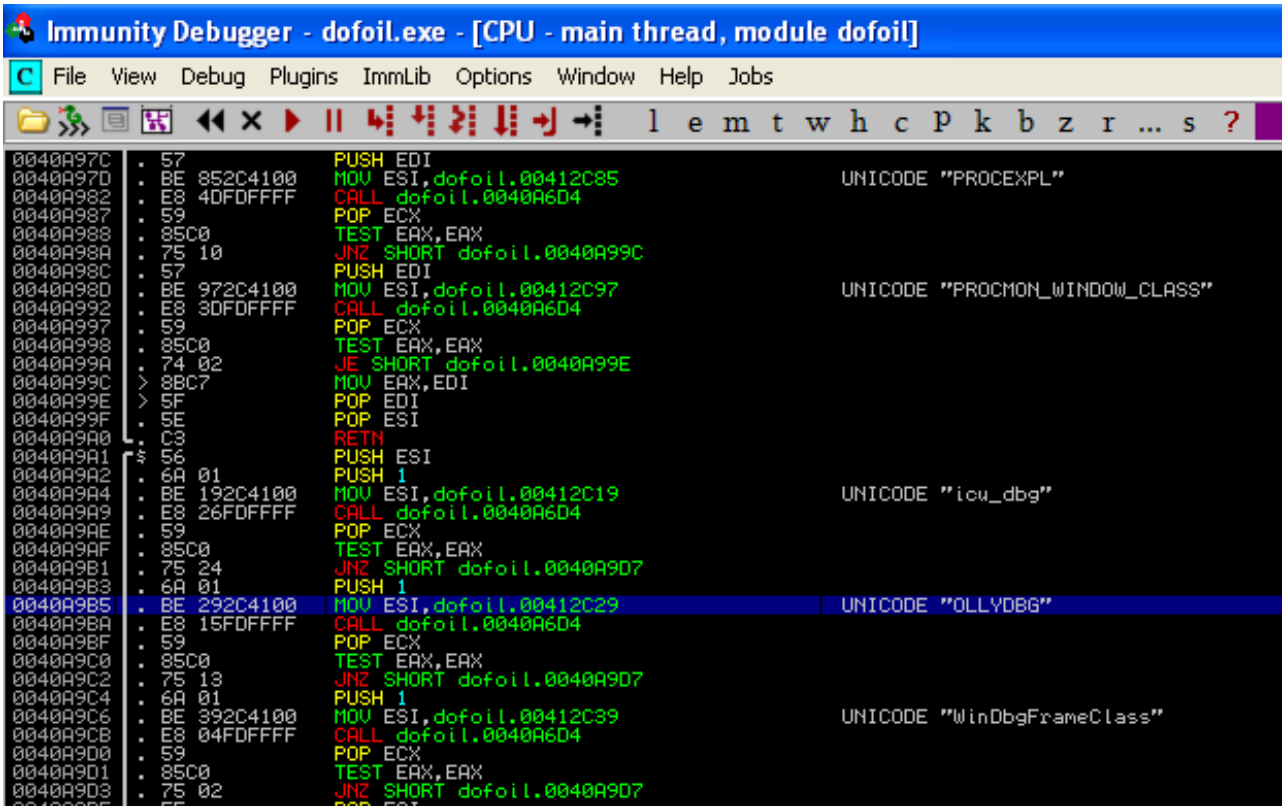
   a. After unpacking, it tries to find out whether the malware is being run inside an emulator. It accesses the registry through “Advapi32.RegOpenKeyExW” API and looks for keys present in “System\ControlSet001\Services\Disk\Enum”. Enum key stores values for the various drives present in the system. The malware checks for the presence of emulators through strings like vmware, vbox, virtual, qemu etc.

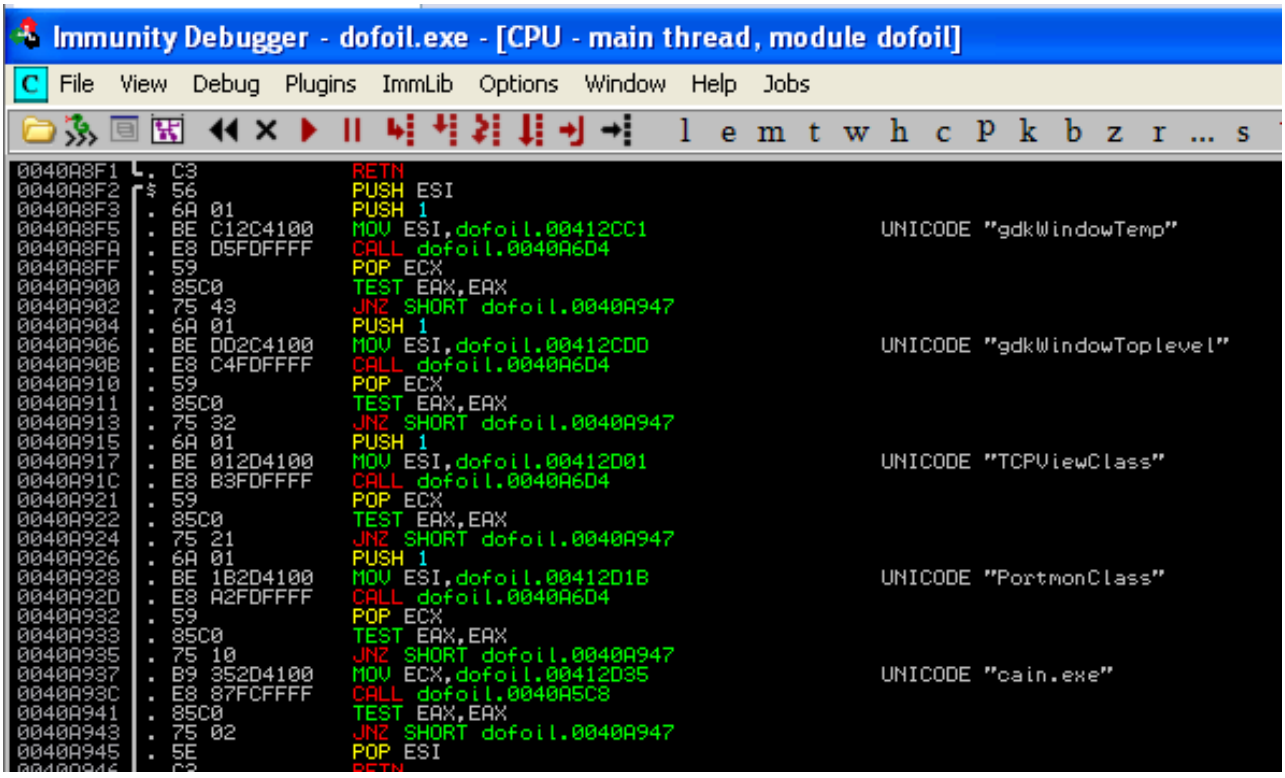


   b. It also checks whether malware is being run inside Anubis Sandbox by searching for the string “InsideTM”.



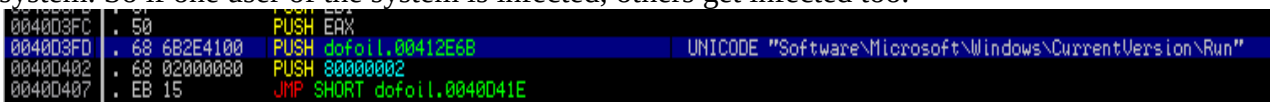
   c. Further anti-analysis techniques check for various other reverse-engineering softwares like OllyDbg, Process Explorer, Process Monitor, WinDbg, Cain & Abel, TCPView, Portmon etc.


Immunity Debugger - dofoil.exe - [CPU - main thread, module dofoil]
File View Debug Plugins ImmLib Options Window Help Jobs
0040A97C . 57 PUSH EDI
0040A97D . BE 852C4100 MOV ESI,dofoil.00412C85 UNICODE "PROCEXPL"
0040A982 . E8 4DFDFFFF CALL dofoil.0040A6D4
0040A987 . 59 POP ECX
0040A988 . 85C0 TEST EAX,EAX
0040A98A . 75 10 JNZ SHORT dofoil.0040A99C
0040A98C . 57 PUSH EDI
0040A98D . BE 972C4100 MOV ESI,dofoil.00412C97 UNICODE "PROCMON_WINDOW_CLASS"
0040A992 . E8 3DFDFFFF CALL dofoil.0040A6D4
0040A997 . 59 POP ECX
0040A998 . 85C0 TEST EAX,EAX
0040A99A . 74 02 JE SHORT dofoil.0040A99E
0040A99C > 8BC7 MOV EAX,EDI
0040A99E > 5F POP EDI
0040A99F . 5E POP ESI
0040A9A0 . C3 RETN
0040A9A1 $ 56 PUSH ESI
0040A9A2 . 6A 01 PUSH 1
0040A9A4 . BE 192C4100 MOV ESI,dofoil.00412C19 UNICODE "icu_dbg"
0040A9A9 . E8 26FDFFFF CALL dofoil.0040A6D4
0040A9AE . 59 POP ECX
0040A9AF . 85C0 TEST EAX,EAX
0040A9B1 . 75 24 JNZ SHORT dofoil.0040A9D7
0040A9B3 . 6A 01 PUSH 1
0040A9B5 . BE 292C4100 MOV ESI,dofoil.00412C29 UNICODE "OLLYDBG"
0040A9BA . E8 15FDFFFF CALL dofoil.0040A6D4
0040A9BF . 59 POP ECX
0040A9C0 . 85C0 TEST EAX,EAX
0040A9C2 . 75 13 JNZ SHORT dofoil.0040A9D7
0040A9C4 . 6A 01 PUSH 1
0040A9C6 . BE 392C4100 MOV ESI,dofoil.00412C39 UNICODE "WinDbgFrameClass"
0040A9CB . E8 04FDFFFF CALL dofoil.0040A6D4
0040A9D0 . 59 POP ECX
0040A9D1 . 85C0 TEST EAX,EAX
0040A9D3 . 75 02 JNZ SHORT dofoil.0040A9D7


Immunity Debugger - dofoil.exe - [CPU - main thread, module dofoil]
File View Debug Plugins ImmLib Options Window Help Jobs
0040A8F1 . C3 RETN
0040A8F2 $ 56 PUSH ESI
0040A8F3 . 6A 01 PUSH 1
0040A8F5 . BE C12C4100 MOV ESI,dofoil.00412CC1 UNICODE "gdkWindowTemp"
0040A8FA . E8 D5FDFFFF CALL dofoil.0040A6D4
0040A8FF . 59 POP ECX
0040A900 . 85C0 TEST EAX,EAX
0040A902 . 75 43 JNZ SHORT dofoil.0040A947
0040A904 . 6A 01 PUSH 1
0040A906 . BE DD2C4100 MOV ESI,dofoil.00412CDD UNICODE "gdkWindowToplevel"
0040A90B . E8 C4FDFFFF CALL dofoil.0040A6D4
0040A910 . 59 POP ECX
0040A911 . 85C0 TEST EAX,EAX
0040A913 . 75 32 JNZ SHORT dofoil.0040A947
0040A915 . 6A 01 PUSH 1
0040A917 . BE 012D4100 MOV ESI,dofoil.00412D01 UNICODE "TCPViewClass"
0040A91C . E8 B3FDFFFF CALL dofoil.0040A6D4
0040A921 . 59 POP ECX
0040A922 . 85C0 TEST EAX,EAX
0040A924 . 75 21 JNZ SHORT dofoil.0040A947
0040A926 . 6A 01 PUSH 1
0040A928 . BE 1B2D4100 MOV ESI,dofoil.00412D1B UNICODE "PortmonClass"
0040A92D . E8 A2FDFFFF CALL dofoil.0040A6D4
0040A932 . 59 POP ECX
0040A933 . 85C0 TEST EAX,EAX
0040A935 . 75 10 JNZ SHORT dofoil.0040A947
0040A937 . B9 352D4100 MOV ECX,dofoil.00412D35 UNICODE "cain.exe"
0040A93C . E8 87FCFFFF CALL dofoil.0040A5C8
0040A941 . 85C0 TEST EAX,EAX
0040A943 . 75 02 JNZ SHORT dofoil.0040A947
0040A945 . 5E POP ESI

3. There are lots of strings dumped in the memory which can tell what the malware does.

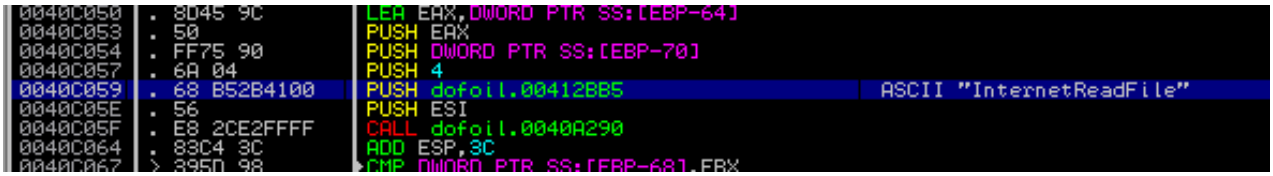
   a. Modifies the registry key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" to add its existence during system startup. This key maintains configurations for all the users of the system. So if one user of the system is infected, others get infected too.



   b. Modifies the userinit.exe file to run the malware process when the user logs in. Userinit.exe runs various logon scripts, re-establishes network connections and also starts explorer.exe.

   Further it also checks the registry to find whether Winlogon runs userinit.exe after the user logs in.

   c. It downloads other malicious files from the internet by using "Wininet.InternetReadFile" API.



   d. Possibly it also performs local DNS poisoning by modifying the "hosts" file. This may trick the user into opening malicious websites instead of genuine sites.