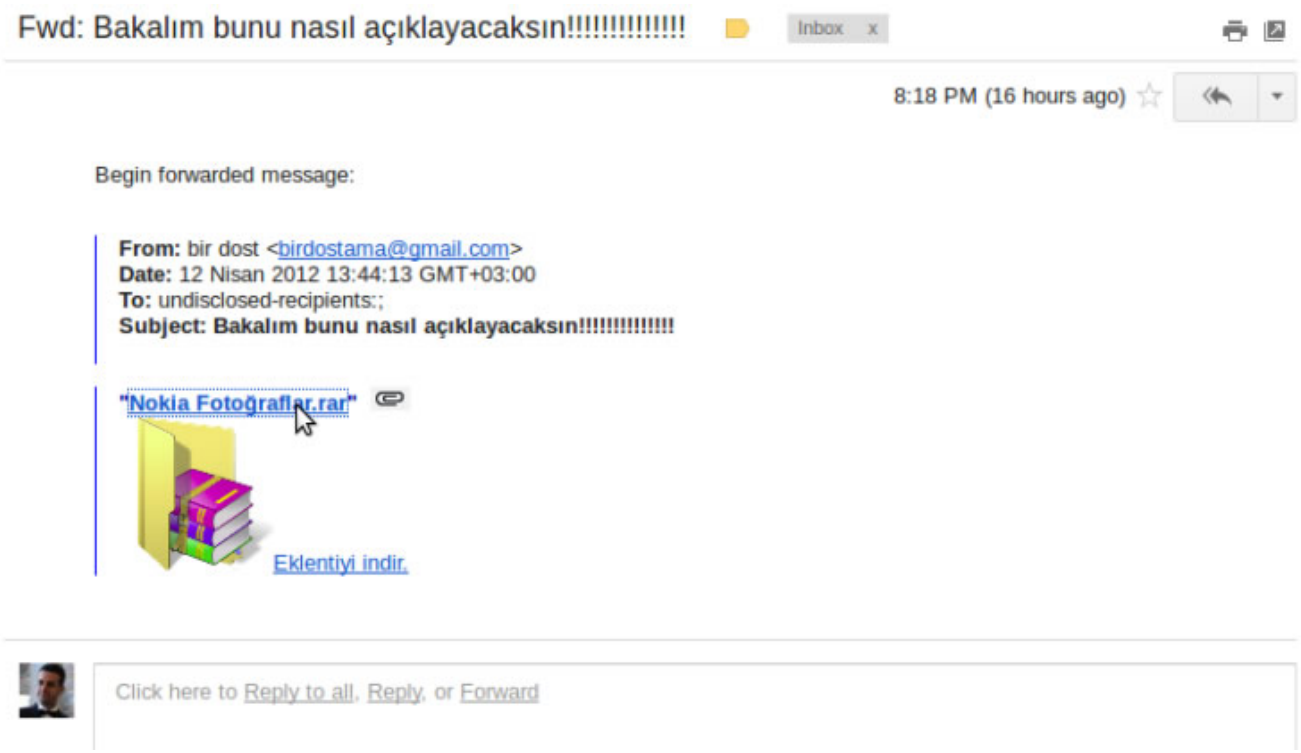
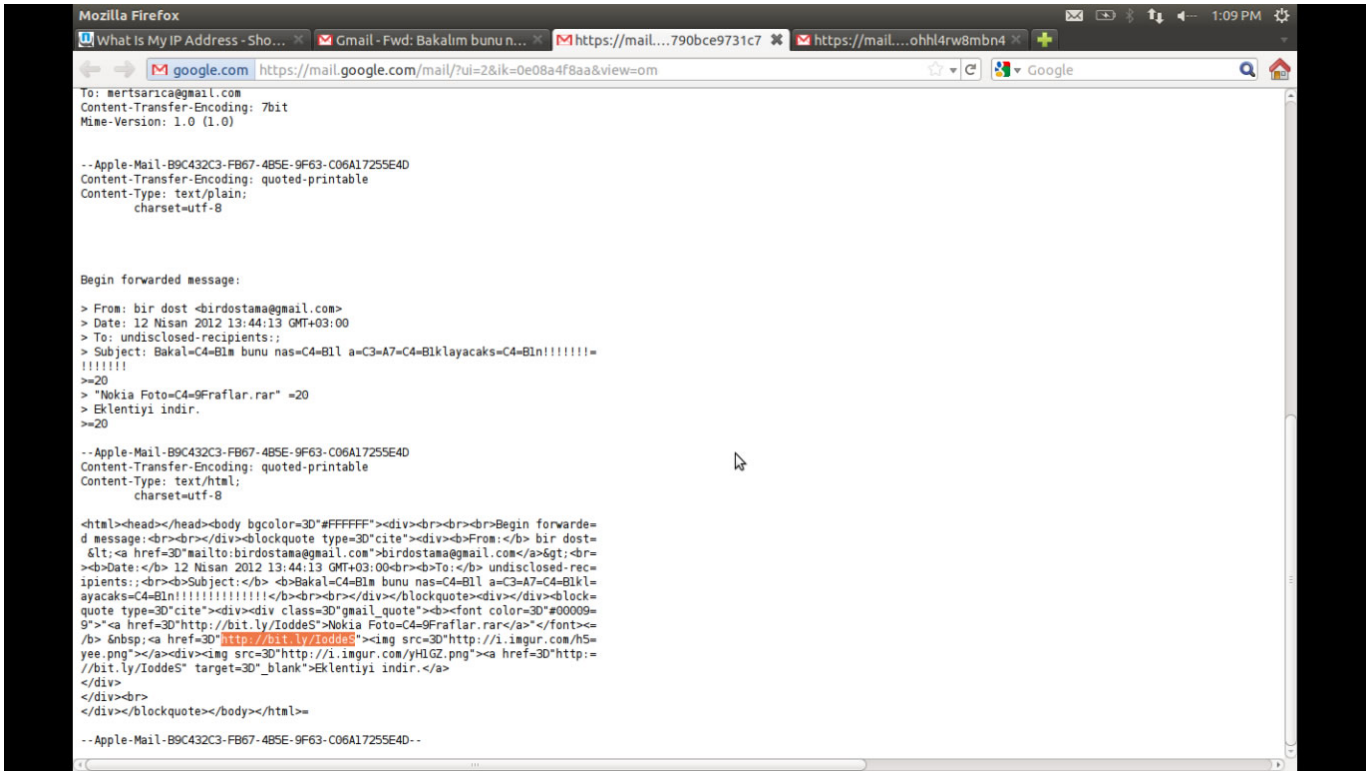
Anti Analiz

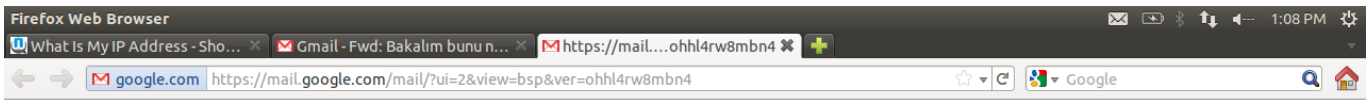
written by Mert SARICA | 23 April 2012

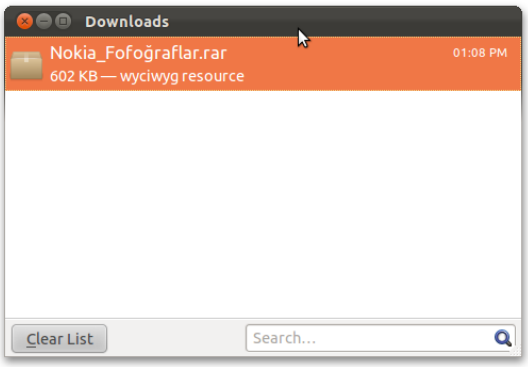
Yakın bir arkadaşım ile 12 Nisan tarihinde Namık Kemal Üniversitesi'ne bağlı Çorlu Mühendislik Fakültesi'nde gerçekleşen İnternet Haftası etkinliğinden dönerken bana 1 saat önce kendisine ulaşan e-postayı gösterdi. E-postanın konu başlığı ("Bakalım bunu nasıl açıklayacaksın!!!!) ve içeriği ("Nokia Fotoğraflar.rar") şüpheli olduğu için arkadaşıma e-postayı bana göndermesini ilettikten sonra mümkün olan en kısa zamanda analiz için işe koyuldum.



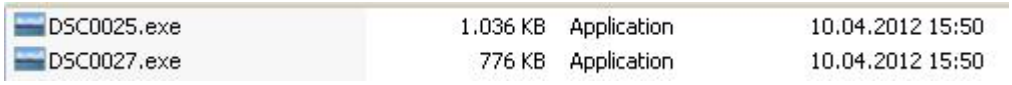
Gelen e-posta SPAM kategorisin girmediği için direk gelen kutusuna gelmişti. E-posta, HTML içeriğe sahip olduğu için eklenti adı ve eklentiye ait resim güzel bir şekilde konumlandırılmıştı ve bu nedenle dikkatsiz bir kullanıcı tarafından ilk bakışta eklentinin Gmail'de olduğu düşünülebilirdi. E-postanın başlık bilgilerine (headers) dikkatlice bakılınca HTML kodlar ve eklentinin bulunduğu kısaltılmış (bit.ly) web adresi dikkat çekiyordu.



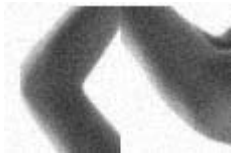




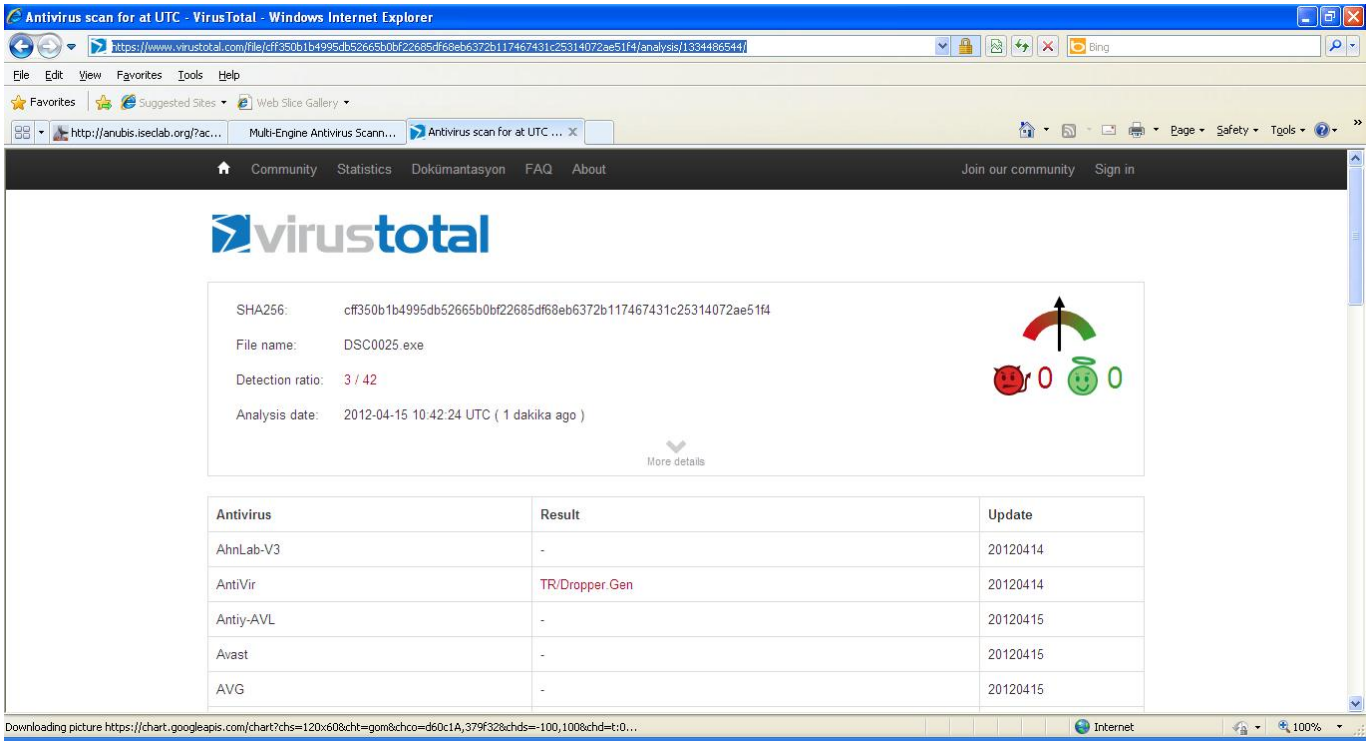
Nokia_Fofoğraflar.rar dosyasını indirip açtıktan sonra içinden çıkan 2 yazılımın (DSC0025.exe ve DSC0027.exe) PE başlık bilgilerinde yer alan zaman damgaları 10.04.2012 12:47:51 tarihini gösteriyordu.

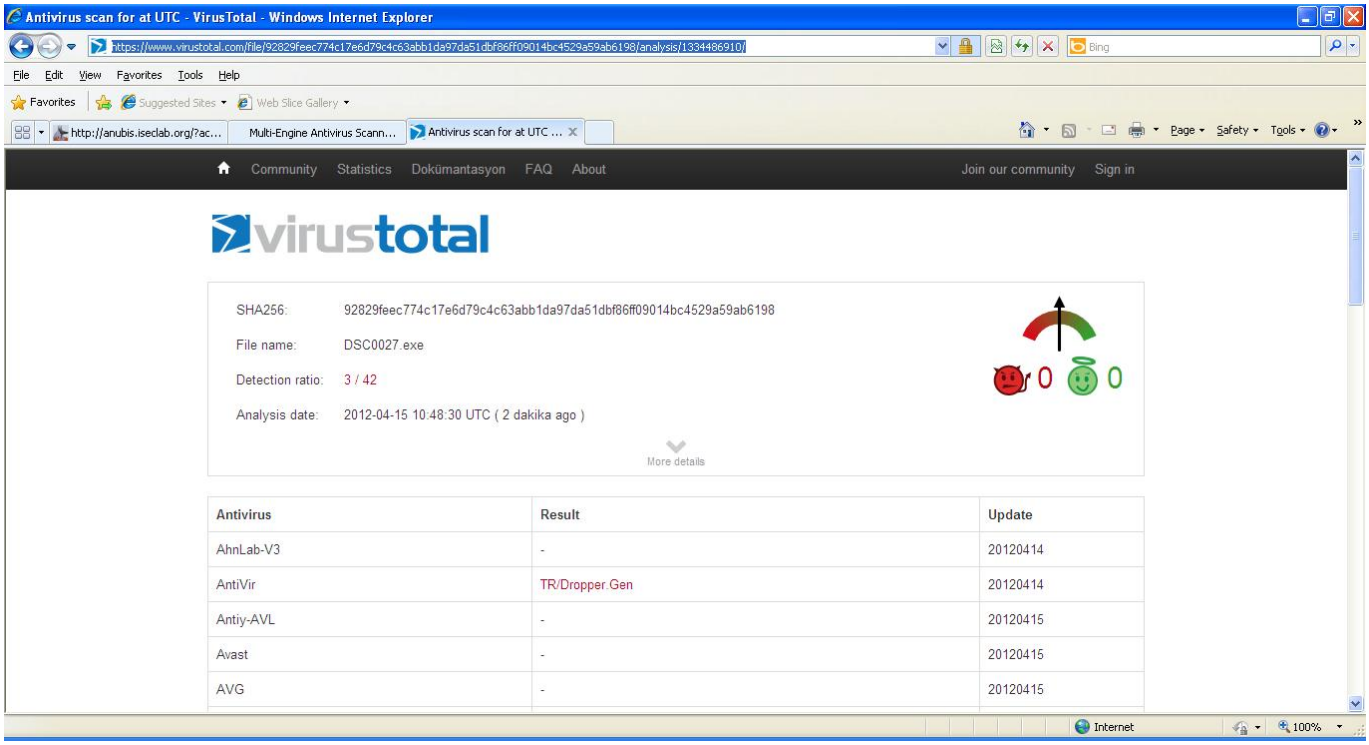


İki yazılımın ortak özelliklerinden biri çalıştırılır çalıştırılmaz ekrana aşağıdaki resmi çıkartıyor olmasıydı.



Bu iki yazılımın kullanmış olduğum antivirüs yazılımı tarafından tespit edilmemiş olması zararlı yazılım oluşturan kişiler arasında sıkça tercih edilen Crypter (şifreleme) aracı ile yazılımların oluşturulduğu şüphesini uyandırdı.
Virustotal üzerinden 42 farklı Antivirüs yazılımı ile bu iki yazılımı tarattığımda sadece 2 tanesi bu zararlı yazılımları tanıyabiliyordu.

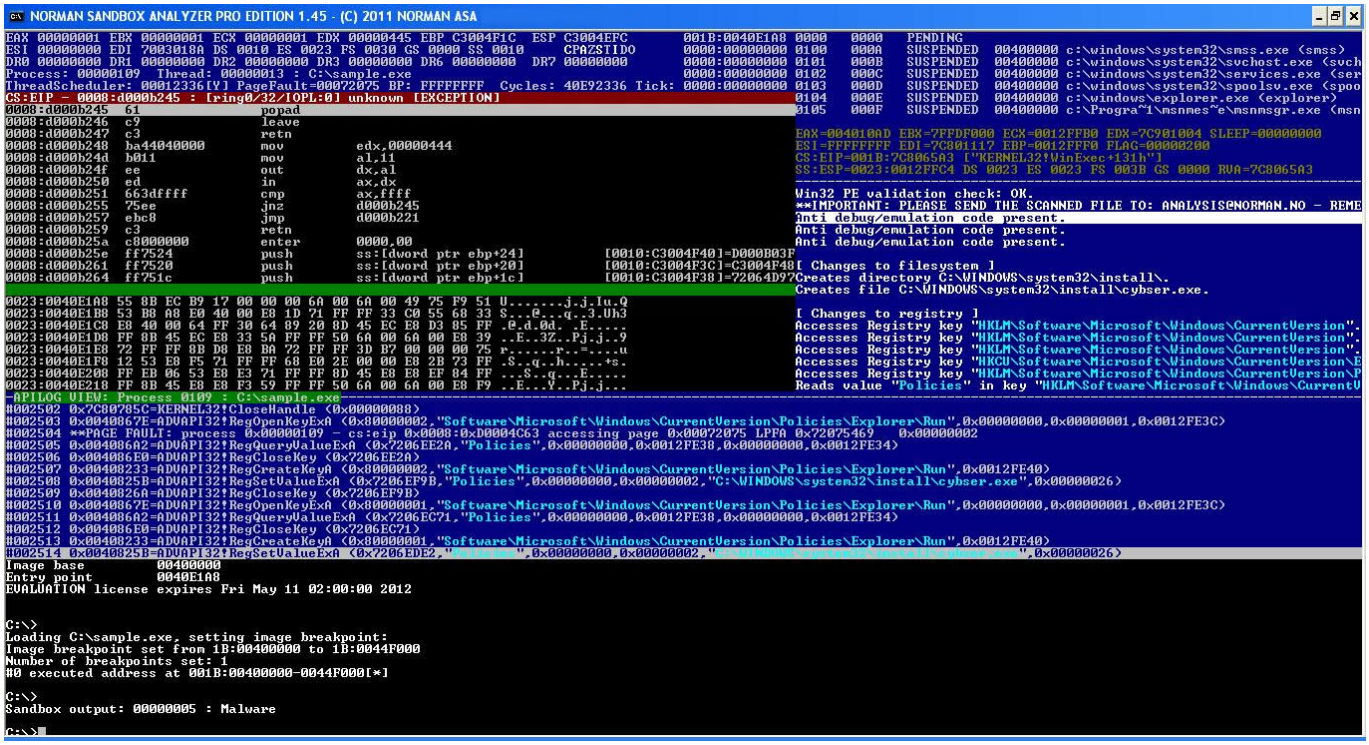




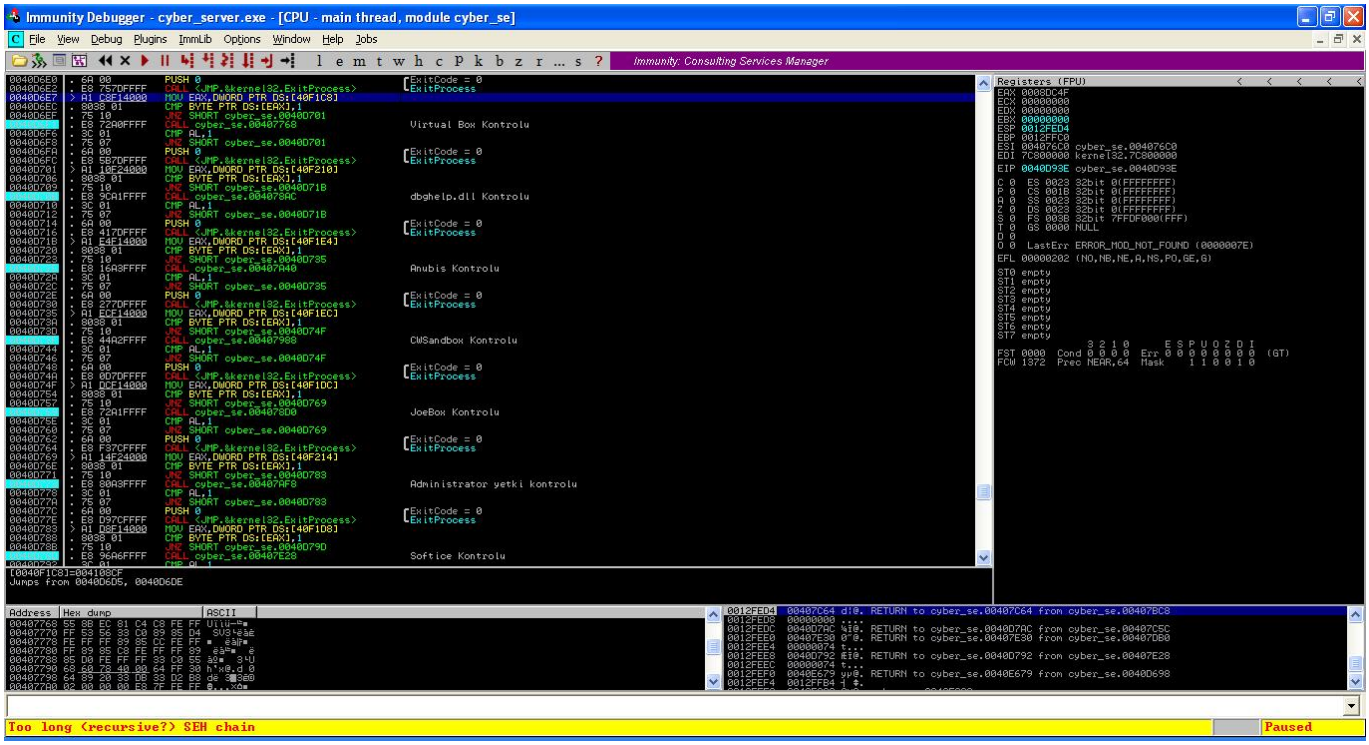
Boyutu diğerine kıyasla daha ufak olan DSC0027.exe yazılımını sanal makine içinde Immunity Debugger aracı ile dinamik olarak analiz ettiğimde yazılımın 2004 yılından kalma Flux RAT olduğunu (flServ.exe adı altında çalışmaktadır), kendinisini explorer.exe içine enjekte ettiğini ve Vodafone 3G IP bloğunda yer alan 46.155.243.4 dinamik ip adresi (*****.zapto.org) ile 2001 numaralı bağlantı noktası üzerinden haberleşmeye çalıştığı rahatlıkla anlaşılıyordu.

Ancak DSC0027.exe adındaki diğer zararlı yazılımı incelediğimde sanal makine içinde çalışmadığı gibi Anubis ve benzeri online kum havuzu (sandbox) hizmetleri tarafından da analiz edilemiyordu. Günümüzde çoğu zararlı yazılımı oluşturan ana yazılımların oluşturdukları zararlı yazılımın sanal makinelerde ve kum havuzu araçlarında çalıştırılmaya karşı ek kontroller barındırdığı düşünüldüğünde çalışmamasının başka bir nedeni olabileceğini pek düşünmemiştim.

Norman Malware Debugger PRO aracı ile zararlı yazılımı incelediğimde az önce bahsetmiş olduğum kontrollerin yazılım üzerinde mevcut olduğuna dair bilgilendirme mesajları ile karşılaştım.



Zararlı yazılımı Immunity Debugger ile detaylı olarak incelediğimde bu yazılımın aslında CyberGate RAT (cyber_server.exe adı altında çalışmaktadır) olduğu ve Norman Malware Debugger PRO aracının belirtmiş olduğu gibi üzerinde birçok anti analiz kodlarını (vmware, virtualbox, anubis, debugger vb.) yer aldığı açıkça görülüyordu.



Sandboxie Kontrolu

00407888 /$ 53 PUSH EBX

```
00407889 |. 33DB XOR EBX,EBX
0040788B |. 68 A0784000 PUSH cyber_se.004078A0 ; /pModule = "SbieDll.dll"
00407890 |. E8 1FDCFFFF CALL ; \GetModuleHandleA
00407895 |. 85C0 TEST EAX,EAX
00407897 |. 74 02 JE SHORT cyber_se.0040789B
00407899 |. B3 01 MOV BL,1
0040789B |> 8BC3 MOV EAX,EBX
0040789D |. 5B POP EBX
0040789E \. C3 RETN
```

ThreatExpert Kontrolu

```
004078AC /$ 53 PUSH EBX
004078AD |. 33DB XOR EBX,EBX
004078AF |. 68 C4784000 PUSH cyber_se.004078C4 ; /pModule = “dbghelp.dll”
004078B4 |. E8 FBDBFFFF CALL ; \GetModuleHandleA
004078B9 |. 85C0 TEST EAX,EAX
004078BB |. 74 02 JE SHORT cyber_se.004078BF
004078BD |. B3 01 MOV BL,1
004078BF |> 8BC3 MOV EAX,EBX
004078C1 |. 5B POP EBX
004078C2 \. C3 RETN
```

Sandbox Kontrolu

55274-640-2673064-23950 – JoeBox

```
004078D0 /$ 53 PUSH EBX
004078D1 |. 81C4 F4FEFFFF ADD ESP,-10C
004078D7 |. 33DB XOR EBX,EBX
004078D9 |. 54 PUSH ESP ; /pHandle
004078DA |. 6A 01 PUSH 1 ; |Access
004078DC |. 6A 00 PUSH 0 ; |Reserved = 0
004078DE |. 68 38794000 PUSH cyber_se.00407938 ; |Subkey =
“Software\Microsoft\Windows\CurrentVersion”
004078E3 |. 68 02000080 PUSH 80000002 ; |hKey = HKEY_LOCAL_MACHINE
004078E8 |. E8 EFDAFFFF CALL ; \RegOpenKeyExA
004078ED |. 85C0 TEST EAX,EAX
004078EF |. 75 32 JNZ SHORT cyber_se.00407923
004078F1 |. C74424 04 0101>MOV DWORD PTR SS:[ESP+4],101
004078F9 |. 8D4424 04 LEA EAX,DWORD PTR SS:[ESP+4]
004078FD |. 50 PUSH EAX ; /pBufSize
```

```
004078FE |. 8D4424 0C LEA EAX,DWORD PTR SS:[ESP+C] ; |
00407902 |. 50 PUSH EAX ; |Buffer
00407903 |. 6A 00 PUSH 0 ; |pValueType = NULL
00407905 |. 6A 00 PUSH 0 ; |Reserved = NULL
00407907 |. 68 64794000 PUSH cyber_se.00407964 ; |ValueName = “ProductId”
0040790C |. 8B4424 14 MOV EAX,DWORD PTR SS:[ESP+14] ; |
00407910 |. 50 PUSH EAX ; |hKey
00407911 |. E8 CEDAFFFF CALL ; \RegQueryValueExA
00407916 |. 8D4424 08 LEA EAX,DWORD PTR SS:[ESP+8]
0040791A |. 3D 70794000 CMP EAX,cyber_se.00407970 ; ASCII
“55274-640-2673064-23950”
0040791F |. 75 02 JNZ SHORT cyber_se.00407923
00407921 |. B3 01 MOV BL,1
00407923 |> 8B0424 MOV EAX,DWORD PTR SS:[ESP]
00407926 |. 50 PUSH EAX ; /hKey
00407927 |. E8 88DAFFFF CALL ; \RegCloseKey
0040792C |. 8BC3 MOV EAX,EBX
0040792E |. 81C4 0C010000 ADD ESP,10C
00407934 |. 5B POP EBX
00407935 \. C3 RETN
```

76487-644-3177037-23510 – CWSandbox

```
00407988 /$ 53 PUSH EBX
00407989 |. 81C4 F4FEFFFF ADD ESP,-10C
0040798F |. 33DB XOR EBX,EBX
00407991 |. 54 PUSH ESP ; /pHandle
00407992 |. 6A 01 PUSH 1 ; |Access
00407994 |. 6A 00 PUSH 0 ; |Reserved = 0
00407996 |. 68 F0794000 PUSH cyber_se.004079F0 ; |Subkey =
“Software\Microsoft\Windows\CurrentVersion”
0040799B |. 68 02000080 PUSH 80000002 ; |hKey = HKEY_LOCAL_MACHINE
004079A0 |. E8 37DAFFFF CALL ; \RegOpenKeyExA
004079A5 |. 85C0 TEST EAX,EAX
004079A7 |. 75 32 JNZ SHORT cyber_se.004079DB
004079A9 |. C74424 04 0101>MOV DWORD PTR SS:[ESP+4],101
004079B1 |. 8D4424 04 LEA EAX,DWORD PTR SS:[ESP+4]
004079B5 |. 50 PUSH EAX ; /pBufSize
004079B6 |. 8D4424 0C LEA EAX,DWORD PTR SS:[ESP+C] ; |
004079BA |. 50 PUSH EAX ; |Buffer
```

```
004079BB |. 6A 00 PUSH 0 ; |pValueType = NULL
004079BD |. 6A 00 PUSH 0 ; |Reserved = NULL
004079BF |. 68 1C7A4000 PUSH cyber_se.00407A1C ; |ValueName = “ProductId”
004079C4 |. 8B4424 14 MOV EAX,DWORD PTR SS:[ESP+14] ; |
004079C8 |. 50 PUSH EAX ; |hKey
004079C9 |. E8 16DAFFFF CALL ; \RegQueryValueExA
004079CE |. 8D4424 08 LEA EAX,DWORD PTR SS:[ESP+8]
004079D2 |. 3D 287A4000 CMP EAX,cyber_se.00407A28 ; ASCII
“76487-644-3177037-23510”
004079D7 |. 75 02 JNZ SHORT cyber_se.004079DB
004079D9 |. B3 01 MOV BL,1
004079DB |> 8B0424 MOV EAX,DWORD PTR SS:[ESP]
004079DE |. 50 PUSH EAX ; /hKey
004079DF |. E8 D0D9FFFF CALL ; \RegCloseKey
004079E4 |. 8BC3 MOV EAX,EBX
004079E6 |. 81C4 0C010000 ADD ESP,10C
004079EC |. 5B POP EBX
004079ED \. C3 RETN
```

```
76487-337-8429955-22614 – Anubis
00407A40 /$ 53 PUSH EBX
00407A41 |. 81C4 F4FEFFFF ADD ESP,-10C
00407A47 |. 33DB XOR EBX,EBX
00407A49 |. 54 PUSH ESP ; /pHandle
00407A4A |. 6A 01 PUSH 1 ; |Access
00407A4C |. 6A 00 PUSH 0 ; |Reserved = 0
00407A4E |. 68 A87A4000 PUSH cyber_se.00407AA8 ; |Subkey =
“Software\Microsoft\Windows\CurrentVersion”
00407A53 |. 68 02000080 PUSH 80000002 ; |hKey = HKEY_LOCAL_MACHINE
00407A58 |. E8 7FD9FFFF CALL ; \RegOpenKeyExA
00407A5D |. 85C0 TEST EAX,EAX
00407A5F |. 75 32 JNZ SHORT cyber_se.00407A93
00407A61 |. C74424 04 0101>MOV DWORD PTR SS:[ESP+4],101
00407A69 |. 8D4424 04 LEA EAX,DWORD PTR SS:[ESP+4]
00407A6D |. 50 PUSH EAX ; /pBufSize
00407A6E |. 8D4424 0C LEA EAX,DWORD PTR SS:[ESP+C] ; |
00407A72 |. 50 PUSH EAX ; |Buffer
00407A73 |. 6A 00 PUSH 0 ; |pValueType = NULL
00407A75 |. 6A 00 PUSH 0 ; |Reserved = NULL
```

```
00407A77 |. 68 D47A4000 PUSH cyber_se.00407AD4 ; |ValueName = “ProductId”
00407A7C |. 8B4424 14 MOV EAX,DWORD PTR SS:[ESP+14] ; |
00407A80 |. 50 PUSH EAX ; |hKey
00407A81 |. E8 5ED9FFFF CALL ; \RegQueryValueExA
00407A86 |. 8D4424 08 LEA EAX,DWORD PTR SS:[ESP+8]
00407A8A |. 3D E07A4000 CMP EAX,cyber_se.00407AE0 ; ASCII
“76487-337-8429955-22614”
00407A8F |. 75 02 JNZ SHORT cyber_se.00407A93
00407A91 |. B3 01 MOV BL,1
00407A93 |> 8B0424 MOV EAX,DWORD PTR SS:[ESP]
00407A96 |. 50 PUSH EAX ; /hKey
00407A97 |. E8 18D9FFFF CALL ; \RegCloseKey
00407A9C |. 8BC3 MOV EAX,EBX
00407A9E |. 81C4 0C010000 ADD ESP,10C
00407AA4 |. 5B POP EBX
00407AA5 \. C3 RETN

IsDebuggerPresent
00407BC8 /$ 53 PUSH EBX
00407BC9 |. 56 PUSH ESI
00407BCA |. 57 PUSH EDI
00407BCB |. 55 PUSH EBP
00407BCC |. 33DB XOR EBX,EBX
00407BCE |. 68 FC7B4000 PUSH cyber_se.00407BFC ; /FileName = “kernel32.dll”
00407BD3 |. E8 14D9FFFF CALL ; \LoadLibraryA
00407BD8 |. 8BF8 MOV EDI,EAX
00407BDA |. 85FF TEST EDI,EDI
00407BDC |. 74 17 JE SHORT cyber_se.00407BF5
00407BDE |. 68 0C7C4000 PUSH cyber_se.00407C0C ; /ProcNameOrOrdinal
00407BE3 |. 57 PUSH EDI ; |hModule
00407BE4 |. E8 E3D8FFFF CALL ; \GetProcAddress
00407BE9 |. 8BE8 MOV EBP,EAX ; kernel32.IsDebuggerPresent
00407BEB |. 89EE MOV ESI,EBP
00407BED |. 85ED TEST EBP,EBP
00407BEF |. 74 04 JE SHORT cyber_se.00407BF5
00407BF1 |. FFD6 CALL ESI
00407BF3 |. 8BD8 MOV EBX,EAX
00407BF5 |> 8BC3 MOV EAX,EBX
00407BF7 |. 5D POP EBP
```

```
00407BF8 |. 5F POP EDI
00407BF9 |. 5E POP ESI
00407BFA |. 5B POP EBX
00407BFB \. C3 RETN
```

Virtual PC

```
00407726 0F DB 0F ; Virtual PC Kontrolü
00407727 3F DB 3F ; CHAR '?'
00407728 07 DB 07
```

VMWare

```
004076CD . B8 68584D56 MOV EAX,564D5868
004076D2 . BB 12F76C3C MOV EBX,3C6CF712
004076D7 . B9 0A000000 MOV ECX,0A
004076DC . 66:BA 5856 MOV DX,5658
```

VirtualBox

```
00407768 /$ 55 PUSH EBP
00407769 |. 8BEC MOV EBP,ESP
0040776B |. 81C4 C8FEFFFF ADD ESP,-138
00407771 |. 53 PUSH EBX
00407772 |. 56 PUSH ESI
00407773 |. 33C0 XOR EAX,EAX
00407775 |. 8985 D4FEFFFF MOV DWORD PTR SS:[EBP-12C],EAX
0040777B |. 8985 CCFEFFFF MOV DWORD PTR SS:[EBP-134],EAX
00407781 |. 8985 C8FEFFFF MOV DWORD PTR SS:[EBP-138],EAX
00407787 |. 8985 D0FEFFFF MOV DWORD PTR SS:[EBP-130],EAX
0040778D |. 33C0 XOR EAX,EAX
0040778F |. 55 PUSH EBP
00407790 |. 68 60784000 PUSH cyber_se.00407860
00407795 |. 64:FF30 PUSH DWORD PTR FS:[EAX]
00407798 |. 64:8920 MOV DWORD PTR FS:[EAX],ESP
0040779B |. 33DB XOR EBX,EBX
0040779D |. 33D2 XOR EDX,EDX
0040779F |. B8 02000000 MOV EAX,2
004077A4 |. E8 7FFEFFFF CALL cyber_se.00407628
004077A9 |. 8BF0 MOV ESI,EAX
004077AB |. C785 D8FEFFFF >MOV DWORD PTR SS:[EBP-128],128
004077B5 |. EB 70 JMP SHORT cyber_se.00407827
004077B7 |> 8D85 D0FEFFFF /LEA EAX,DWORD PTR SS:[EBP-130]
```

```
004077BD |. 8D95 FCFEFFFF |LEA EDX,DWORD PTR SS:[EBP-104]
004077C3 |. B9 04010000 |MOV ECX,104
004077C8 |. E8 1BC2FFFF |CALL cyber_se.004039E8
004077CD |. 8B85 D0FEFFFF |MOV EAX,DWORD PTR SS:[EBP-130]
004077D3 |. 8D95 D4FEFFFF |LEA EDX,DWORD PTR SS:[EBP-12C]
004077D9 |. E8 12F5FFFF |CALL cyber_se.00406CF0
004077DE |. 8B85 D4FEFFFF |MOV EAX,DWORD PTR SS:[EBP-12C]
004077E4 |. 50 |PUSH EAX
004077E5 |. 8D95 C8FEFFFF |LEA EDX,DWORD PTR SS:[EBP-138]
004077EB |. B8 78784000 |MOV EAX,cyber_se.00407878 ; ASCII “VBoxService.exe”
004077F0 |. E8 FBF4FFFF |CALL cyber_se.00406CF0
004077F5 |. 8B85 C8FEFFFF |MOV EAX,DWORD PTR SS:[EBP-138]
004077FB |. E8 14C4FFFF |CALL cyber_se.00403C14
00407800 |. 8BD0 |MOV EDX,EAX
00407802 |. 8D85 CCFEFFFF |LEA EAX,DWORD PTR SS:[EBP-134]
00407808 |. E8 63C1FFFF |CALL cyber_se.00403970
0040780D |. 8B85 CCFEFFFF |MOV EAX,DWORD PTR SS:[EBP-134]
00407813 |. 5A |POP EDX
00407814 |. E8 E3C4FFFF |CALL cyber_se.00403CFC
00407819 |. 85C0 |TEST EAX,EAX
0040781B |. 7E 0A |JLE SHORT cyber_se.00407827
0040781D |. 56 |PUSH ESI ; /hObject
0040781E |. E8 D1DBFFFF |CALL ; \CloseHandle
00407823 |. B3 01 |MOV BL,1
00407825 |. EB 1B |JMP SHORT cyber_se.00407842
00407827 |> 8D95 D8FEFFFF LEA EDX,DWORD PTR SS:[EBP-128]
0040782D |. 8BC6 |MOV EAX,ESI
0040782F |. E8 34FEFFFF |CALL cyber_se.00407668
00407834 |. 85C0 |TEST EAX,EAX
00407836 |.^0F85 7BFFFFFF \JNZ cyber_se.004077B7
0040783C |. 56 PUSH ESI ; /hObject
0040783D |. E8 B2DBFFFF CALL ; \CloseHandle
00407842 |> 33C0 XOR EAX,EAX
00407844 |. 5A POP EDX
00407845 |. 59 POP ECX
00407846 |. 59 POP ECX
00407847 |. 64:8910 MOV DWORD PTR FS:[EAX],EDX
0040784A |. 68 67784000 PUSH cyber_se.00407867
0040784F |> 8D85 C8FEFFFF LEA EAX,DWORD PTR SS:[EBP-138]
```

```
00407855 |. BA 04000000 MOV EDX,4
0040785A |. E8 3DBFFFFF CALL cyber_se.0040379C
0040785F \. C3 RETN
```

Softice Kontrolu

```
00407DB0 /$ 53 PUSH EBX
00407DB1 |. 33DB XOR EBX,EBX
00407DB3 |. 6A 00 PUSH 0 ; /hTemplateFile = NULL
00407DB5 |. 68 80000000 PUSH 80 ; |Attributes = NORMAL
00407DBA |. 6A 03 PUSH 3 ; |Mode = OPEN_EXISTING
00407DBC |. 6A 00 PUSH 0 ; |pSecurity = NULL
00407DBE |. 6A 03 PUSH 3 ; |ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
00407DC0 |. 68 000000C0 PUSH C0000000 ; |Access = GENERIC_READ|GENERIC_WRITE
00407DC5 |. 68 E07D4000 PUSH cyber_se.00407DE0 ; |FileName = “\\.\SICE”
00407DCA |. E8 45D6FFFF CALL ; \CreateFileA
00407DCF |. 83F8 FF CMP EAX,-1
00407DD2 |. 74 08 JE SHORT cyber_se.00407DDC
00407DD4 |. 50 PUSH EAX ; /hObject
00407DD5 |. E8 1AD6FFFF CALL ; \CloseHandle
00407DDA |. B3 01 MOV BL,1
00407DDC |> 8BC3 MOV EAX,EBX
00407DDE |. 5B POP EBX
00407DDF \. C3 RETN
00407DE0 . 5C 5C 2E 5C 53>ASCII “\\.\SICE”,0
00407DE9 00 DB 00
00407DEA 00 DB 00
00407DEB 00 DB 00
00407DEC /$ 53 PUSH EBX
00407DED |. 33DB XOR EBX,EBX
00407DEF |. 6A 00 PUSH 0 ; /hTemplateFile = NULL
00407DF1 |. 68 80000000 PUSH 80 ; |Attributes = NORMAL
00407DF6 |. 6A 03 PUSH 3 ; |Mode = OPEN_EXISTING
00407DF8 |. 6A 00 PUSH 0 ; |pSecurity = NULL
00407DFA |. 6A 03 PUSH 3 ; |ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
00407DFC |. 68 000000C0 PUSH C0000000 ; |Access = GENERIC_READ|GENERIC_WRITE
00407E01 |. 68 1C7E4000 PUSH cyber_se.00407E1C ; |FileName = “\\.\NTICE”
00407E06 |. E8 09D6FFFF CALL ; \CreateFileA
00407E0B |. 83F8 FF CMP EAX,-1
00407E0E |. 74 08 JE SHORT cyber_se.00407E18
```

```
00407E10 |. 50 PUSH EAX ; /hObject
00407E11 |. E8 DED5FFFF CALL ; \CloseHandle
00407E16 |. B3 01 MOV BL,1
00407E18 |> 8BC3 MOV EAX,EBX
00407E1A |. 5B POP EBX
00407E1B \. C3 RETN
00407E1C . 5C 5C 2E 5C 4E>ASCII “\\.\NTICE”,0
```

SyserDebugger Kontrolu

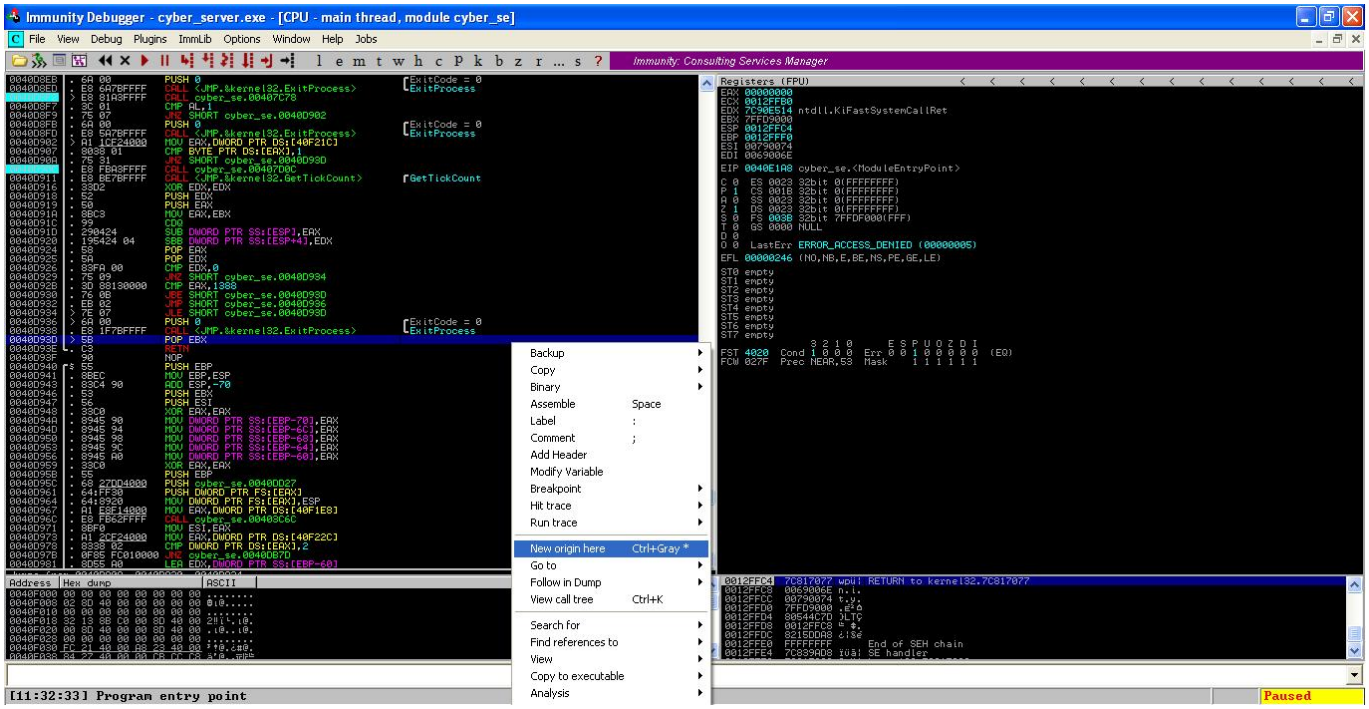
```
00407D53 . B8 847D4000 MOV EAX,cyber_se.00407D84 ; ASCII “\\.\Syser”
00407D58 . E8 C7FFFFFF CALL cyber_se.00407D24
00407D5D . 84C0 TEST AL,AL
00407D5F . 75 1C JNZ SHORT cyber_se.00407D7D
00407D61 . B8 907D4000 MOV EAX,cyber_se.00407D90 ; ASCII “\\.\SyserDbgMsg”
00407D66 . E8 B9FFFFFF CALL cyber_se.00407D24
00407D6B . 84C0 TEST AL,AL
00407D6D . 75 0E JNZ SHORT cyber_se.00407D7D
00407D6F . B8 A07D4000 MOV EAX,cyber_se.00407DA0 ; ASCII “\\.\SyserBoot”
```

TickCount

```
0040D7C5 |. E8 0A7DFFFF CALL ; [GetTickCount
0040D7CA |. 8BD8 MOV EBX,EAX
0040D7CC |. B8 04774000 MOV EAX,cyber_se.00407704 ; Entry address
0040D7D1 |. E8 16A5FFFF CALL cyber_se.00407CEC ; ?
0040D7D6 |. 84C0 TEST AL,AL
….
0040D911 |. E8 BE7BFFFF CALL ; [GetTickCount
0040D916 |. 33D2 XOR EDX,EDX
0040D918 |. 52 PUSH EDX
0040D919 |. 50 PUSH EAX
0040D91A |. 8BC3 MOV EAX,EBX
0040D91C |. 99 CDQ
0040D91D |. 290424 SUB DWORD PTR SS:[ESP],EAX
0040D920 |. 195424 04 SBB DWORD PTR SS:[ESP+4],EDX
0040D924 |. 58 POP EAX
0040D925 |. 5A POP EDX
0040D926 |. 83FA 00 CMP EDX,0
0040D929 |. 75 09 JNZ SHORT cyber_se.0040D934
0040D92B |. 3D 88130000 CMP EAX,1388
```

```
0040D930 |. 76 0B JBE SHORT cyber_se.0040D93D
0040D932 |. EB 02 JMP SHORT cyber_se.0040D936
0040D934 |> 7E 07 JLE SHORT cyber_se.0040D93D
0040D936 |> 6A 00 PUSH 0 ; /ExitCode = 0
0040D938 |. E8 1F7BFFFF CALL ; \ExitProcess
```

Piyasada yer alan çoğu zararlı yazılımın yıllardır aynı anti analiz kodlarını içerdiği düşünüldüğünde bu kodlar üzerinde bol bol pratik yapmış olan zararlı yazılım analisti için bu kontrolleri tespit etmek ve aşmak sadece birkaç dakika sürmektedir.



Bu tür kodların kullanım amacı her ne kadar zararlı yazılım analistinin işini zorlaştırmak olsa da motive olmuş bir zararlı yazılım analistini bu tür kontroller ile durdurmak hiçbir zaman mümkün değildir.

Bu vesileyle herkesin 23 Nisan Ulusal Egemenlik ve Çocuk Bayramı’nı kutlar bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…