






Anubis - Analysis Report



Analysis Report for DHL_print_label_bf46d.exe

MD5: 8960322225b6a842bad87a285f028f5f

Summary:

Description	Risk
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	 medium
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	 high
Performs Registry Activities: The executable reads and modifies register values. It also creates and monitors register keys.	 low

Dependency overview:

 **DHL_print_label_bf46d.exe** C:\DHL_print_label_bf46d.exe

Analysis reason: Primary Analysis Subject

 **Explorer.EXE** C:\WINDOWS\Explorer.EXE

Analysis reason: DHL_print_label_bf46d.exe injected a remote thread into this process

Table of Contents:

1. General Information.....	4
2. DHL_print_label_bf46d.exe.....	4
a) Registry Activities.....	4
b) File Activities.....	5
c) Process Activities.....	5
d) Other Activities.....	5
3. Explorer.EXE.....	6
a) Registry Activities.....	7
b) File Activities.....	7
c) Other Activities.....	8



1. General Information

Information about Anubis' invocation

Time needed:	240 s
Report created:	10/17/09, 00:29:37 UTC
Termination reason:	Timeout
Program version:	1.72.0

1.a) - Network Activity

HTTP Conversations:

From ANUBIS:1038 to 91.213.72.226:80 - [mmsfoundssystem.ru]

Request: GET /public/controller.php?action=bot&entity_list=&uid=&first=1&guid=2893656641&v=15&rnd=8520045

Response: 200 "OK"

Unknown UDP Traffic:

From ANUBIS:1025 to 192.168.0.1:53

State: Normal establishment and termination - Transferred outbound Bytes: 35 - Transferred inbound Bytes: 97

2. DHL_print_label_bf46d.exe

General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	DHL_print_label_bf46d.exe
MD5:	8960322225b6a842bad87a285f028f5f
SHA-1:	e8998eaf92a6e993018fe41079cf3b946c37193a
File Size:	23552
Command Line:	"C:\DHL_print_label_bf46d.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\gdi32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\advapi32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000

Ikarus Virus Scanner

Trojan.Win32.Bredolab (Sig-Id:1281816)

2.a) DHL_print_label_bf46d.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs		1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAAppCompat	0	3
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1



2.b) DHL_print_label_bf46d.exe - File Activities

Files Deleted:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM2.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp

Files Created:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM2.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM5.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM54EA3A.TMP

Files Read:

C:\WINDOWS\system32\kernel32.dll
 C:\WINDOWS\system32\ntdll.dll

Files Modified:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM2.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM54EA3A.TMP

Files Renamed:

Old Filename	New Filename
C:\DHL_print_label_bf46d.exe	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM5.tmp

File System Control Communication:

File	Control Code	Times
C:\	0x00090028	1

Memory Mapped Files:

File Name
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM2.tmp
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp
C:\WINDOWS\system32\ntoskrnl.exe
c:\dhl_print_label_bf46d.exe

2.c) DHL_print_label_bf46d.exe - Process Activities

Remote Threads Created:

Affected Process

C:\WINDOWS\explorer.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\explorer.exe

2.d) DHL_print_label_bf46d.exe - Other Activities

Windows SEH exceptions:

Description	Times
Exception 0x80000003 (STATUS_BREAKPOINT) at 0x40d65b	1



3. Explorer.EXE

General information about this executable

Analysis Reason:	DHL_print_label_bf46d.exe injected a remote thread into this process
Filename:	Explorer.EXE
MD5:	12896823fb95bfb3dc9b46bcaedc9923
SHA-1:	9d2bf84874abc5b6e9a2744b7865c193c08d362f
File Size:	1033728
Command Line:	C:\WINDOWS\Explorer.EXE
Process-status at analysis end:	alive
Exit Code:	0

Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\BROWSEUI.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\SHDOCVW.dll	0x7E290000	0x00171000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\appHelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\cscur.dll	0x77A20000	0x00054000
C:\WINDOWS\System32\CSCDLL.dll	0x76600000	0x0001D000
C:\WINDOWS\system32\themeui.dll	0x5BA60000	0x00071000
C:\WINDOWS\system32\MSIMG32.dll	0x76380000	0x00005000
C:\WINDOWS\system32\xpsp2res.dll	0x00BC0000	0x002C5000
C:\WINDOWS\system32\actxprxy.dll	0x71D40000	0x0001B000
C:\WINDOWS\system32\msutb.dll	0x5FC10000	0x00033000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000



Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\LINKINFO.dll	0x76980000	0x00008000
C:\WINDOWS\system32\ntshrui.dll	0x76990000	0x00025000
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\webcheck.dll	0x74B30000	0x00046000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\stobject.dll	0x76280000	0x00021000
C:\WINDOWS\system32\BatMeter.dll	0x74AF0000	0x0000A000
C:\WINDOWS\system32\POWRPROF.dll	0x74AD0000	0x00008000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\msi.dll	0x7D1E0000	0x002BC000
C:\WINDOWS\system32\NETSHELL.dll	0x76400000	0x001A5000
C:\WINDOWS\system32\credui.dll	0x76C00000	0x0002E000
C:\WINDOWS\system32\dot3api.dll	0x478C0000	0x0000A000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\dot3dlg.dll	0x736D0000	0x00006000
C:\WINDOWS\system32\OneX.DLL	0x5DCA0000	0x00028000
C:\WINDOWS\system32\eappcfg.dll	0x745B0000	0x00022000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\eappprxy.dll	0x5DCD0000	0x0000E000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\System32\drprov.dll	0x75F60000	0x00007000
C:\WINDOWS\System32\ntlanman.dll	0x71C10000	0x0000E000
C:\WINDOWS\System32\NETUI0.dll	0x71CD0000	0x00017000
C:\WINDOWS\System32\NETUI1.dll	0x71C90000	0x00040000
C:\WINDOWS\System32\NETRAP.dll	0x71C80000	0x00007000
C:\WINDOWS\System32\davclnt.dll	0x75F70000	0x0000A000
C:\WINDOWS\system32\browsecl.dll	0x71600000	0x00012000
C:\WINDOWS\system32\MLANG.dll	0x75CF0000	0x00091000
C:\WINDOWS\system32\IMM32.dll	0x76390000	0x0001D000

3.a) Explorer.EXE - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MENUORDER\START MENU\	Order	0x08000000020000000002000001000000003000000d200000000000000c400

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAM\MUICACHE\	@C:\WINDOWS\system32\xpsp1res.dll	Set Program Access and Defaults	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAM\MUICACHE\	@shell32.dll,-22075	Windows Catalog	7
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Startup	C:\Documents and Settings\Administrator\Start Menu\Programs\Startup	2

3.b) Explorer.EXE - File Activities



Files Deleted:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM54EA3A.TMP
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM6.tmp

Files Created:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM6.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM7.tmp
 C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\isqsys32.exe

Files Read:

C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
 C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini
 C:\Documents and Settings\All Users\Start Menu\desktop.ini
 C:\WINDOWS\system32\kernel32.dll
 C:\WINDOWS\system32\ntdll.dll

Files Modified:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM6.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM7.tmp
 C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\isqsys32.exe

Memory Mapped Files:

File Name

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM54EA3A.TMP
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM6.tmp
 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM7.tmp

Directories Monitored:

Directory	Watch subtree	Notify Filter	Count
C:\Documents and Settings\Administrator\Start Menu	1	File Name Change,Directory Name Change,Name Change	5

3.c) Explorer.EXE - Other Activities

Mutexes Created:

_SYSTEM_4D2EF3A_

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_LBUTTON (1)	14