Relatorio
Ver_Postcards_card_ec_id_7318.exe■

Tempo de analise: 210 segundos

Nome:

Ver_Postcards_card_ec_id_7318.exe

MD5 hash:

9d57a4ad8530751a2358b8e4c3334948

Tipo de arquivo:

PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Metadata Colhida

Required CPU type 80386

Required OS 4.00 - Win 95 or NT 4

Subsystem Windows GUI

Flags:

Relocation info stripped from file

File is executable

Line numbers stripped from file

Local symbols stripped from file

Machine based on 32-bit-word architecture

Processed/created with:
Seems to be linked with Microsoft linker 6.0

Seems to be linked with Microsoft linker 6.0

Bibliotecas em tempo de carregamento:

MSVBVM60.DLL

Arquivo Compactado:

None

Processos Criados:

iexplore.exe - 2524
iexplore.exe - 2888
Ver_Postcards_card_ec_id_7318.exe - 2484

Arquivos Criados:

C:\Users\ANALIS~1\AppData\Local\Temp\~DF75CB7885D4538170.TMP
C:\Users\ANALIS~1\AppData\Local\Temp\~DFCE2E3A89F700C1CC.TMP
C:\Users\ANALIS~1\AppData\Local\Temp\~DFE5CC20E14FFB5355.TMP
C:\textbackslash Users\analiseMalware\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active
C:\Windows\System32\drivers\etc\hosts

Arquivos Apagados:

C:\Users\ANALIS~1\AppData\Local\Temp\~DFE5CC20E14FFB5355.TMP
C:\Windows\System32\drivers\etc\hosts

Arquivos Modificados:

C:\Users\ANALIS~1\AppData\Local\Temp
C:\Users\ANALIS~1\AppData\Local\Temp\Low
C:\Users\ANALIS~1\AppData\Local\Temp\~DFE5CC20E14FFB5355.TMP
C:\Users\analiseMalware\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active
C:\Users\analiseMalware\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8EBD3022-A14A-11E2-B921-0800273EDF98}.dat
C:\Users\analiseMalware\AppData\Local\Microsoft\Windows\History\History.IE5
C:\Users\analiseMalware\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\analiseMalware\AppData\Local\Microsoft\Windows\History\Low
C:\Users\analiseMalware\AppData\Local\Temp
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Windows\Cookies
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Windows\IETldCache\Low
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Windows\PrivacIE
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
C:\Users\analiseMalware\AppData\Roaming\Microsoft\Windows\PrivacIE\index.dat
C:\Windows\System32\drivers\etc
C:\Windows\System32\drivers\etc\hosts

Chaves de registro alteradas:

HKEY_USERS\S-1-5-21-76576680-606660151-3285115108-1000\Software\Microsoft\Internet Explorer\Recovery\AdminActive
HKEY_USERS\S-1-5-21-76576680-606660151-3285115108-1000\Software\Microsoft\Internet Explorer\SQM\PIDs

Bibliotecas:

Arquivo Ver_Postcards_card_ec_id_7318.exe:

```
\Analise\Artefatos\Ver_Postcards_card_ec_id_7318.exe
\Windows\SysWOW64\KernelBase.dll
\Windows\SysWOW64\RpcRtRemote.dll
\Windows\SysWOW64\advapi32.dll
\Windows\SysWOW64\clbcatq.dll
\Windows\SysWOW64\cryptbase.dll
\Windows\SysWOW64\cryptsp.dll
\Windows\SysWOW64\dwmapi.dll
\Windows\SysWOW64\gdi32.dll
\Windows\SysWOW64\imm32.dll
\Windows\SysWOW64\kernel32.dll
\Windows\SysWOW64\lpk.dll
\Windows\SysWOW64\msctf.dll
\Windows\SysWOW64\msvbvm60.dll
\Windows\SysWOW64\msvcrt.dll
\Windows\SysWOW64\ntdll.dll
\Windows\SysWOW64\ole32.dll
\Windows\SysWOW64\oleaut32.dll
\Windows\SysWOW64\rpcrt4.dll
\Windows\SysWOW64\rsaenh.dll
\Windows\SysWOW64\sechost.dll
\Windows\SysWOW64\sspicli.dll
\Windows\SysWOW64\sxs.dll
\Windows\SysWOW64\user32.dll
\Windows\SysWOW64\usp10.dll
\Windows\SysWOW64\uxtheme.dll
\Windows\System32\apisetschema.dll
\Windows\System32\ntdll.dll
\Windows\System32\wow64.dll
\Windows\System32\wow64cpu.dll
\Windows\System32\wow64win.dll
```

Arquivo iexplore.exe:

```
Explorer\ieproxy.dll
Explorer\iexplore.exe
Explorer\sqmapi.dll
\Windows\SysWOW64\ExplorerFrame.dll
\Windows\SysWOW64\IPHLPAPI.DLL
\Windows\SysWOW64\KernelBase.dll
\Windows\SysWOW64\RpcRtRemote.dll
\Windows\SysWOW64\SensApi.dll
\Windows\SysWOW64\WSHTCPIP.DLL
\Windows\SysWOW64\WindowsCodecs.dll
\Windows\SysWOW64\Wldap32.dll
\Windows\SysWOW64\advapi32.dll
\Windows\SysWOW64\apphelp.dll
\Windows\SysWOW64\cfgmgr32.dll
\Windows\SysWOW64\clbcatq.dll
\Windows\SysWOW64\comdlg32.dll
\Windows\SysWOW64\cryptbase.dll
\Windows\SysWOW64\cryptsp.dll
```

```
\Windows\SysWOW64\devobj.dll
\Windows\SysWOW64\dnsapi.dll
\Windows\SysWOW64\dui70.dll
\Windows\SysWOW64\duser.dll
\Windows\SysWOW64\dwmapi.dll
\Windows\SysWOW64\gdi32.dll
\Windows\SysWOW64\ieframe.dll
\Windows\SysWOW64\iertutil.dll
\Windows\SysWOW64\ieui.dll
\Windows\SysWOW64\imm32.dll
\Windows\SysWOW64\kernel32.dll
\Windows\SysWOW64\lpk.dll
\Windows\SysWOW64\mlang.dll
\Windows\SysWOW64\msctf.dll
\Windows\SysWOW64\mshtml.dll
\Windows\SysWOW64\msimg32.dll
\Windows\SysWOW64\msvcrt.dll
\Windows\SysWOW64\mswsock.dll
\Windows\SysWOW64\netprofm.dll
\Windows\SysWOW64\nlaapi.dll
\Windows\SysWOW64\normaliz.dll
\Windows\SysWOW64\npmproxy.dll
\Windows\SysWOW64\nsi.dll
\Windows\SysWOW64\ntdll.dll
\Windows\SysWOW64\ntmarta.dll
\Windows\SysWOW64\ole32.dll
\Windows\SysWOW64\oleacc.dll
\Windows\SysWOW64\oleaut32.dll
\Windows\SysWOW64\profapi.dll
\Windows\SysWOW64\propsys.dll
\Windows\SysWOW64\psapi.dll
\Windows\SysWOW64\rasadhlp.dll
\Windows\SysWOW64\rasapi32.dll
\Windows\SysWOW64\rasman.dll
\Windows\SysWOW64\rpcrt4.dll
\Windows\SysWOW64\rsaenh.dll
\Windows\SysWOW64\rtutils.dll
\Windows\SysWOW64\sechost.dll
\Windows\SysWOW64\secur32.dll
\Windows\SysWOW64\setupapi.dll
\Windows\SysWOW64\shell32.dll
\Windows\SysWOW64\shlwapi.dll
\Windows\SysWOW64\sspicli.dll
\Windows\SysWOW64\sxs.dll
\Windows\SysWOW64\urlmon.dll
\Windows\SysWOW64\user32.dll
\Windows\SysWOW64\usp10.dll
\Windows\SysWOW64\uxtheme.dll
\Windows\SysWOW64\version.dll
\Windows\SysWOW64\wininet.dll
\Windows\SysWOW64\winnsi.dll
\Windows\SysWOW64\ws2_32.dll
\Windows\SysWOW64\wship6.dll
\Windows\SysWOW64\xmllite.dll
\Windows\System32\apisetschema.dll
\Windows\System32\ntdll.dll
\Windows\System32\wow64.dll
```

```
\Windows\System32\wow64cpu.dll
\Windows\System32\wow64win.dll
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16661_none_420fe3fa2b81
```

Arquivo iexplore.exe:

```
Explorer\IEShims.dll
Explorer\ieproxy.dll
Explorer\iexplore.exe
Explorer\sqmapi.dll
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
\Windows\SysWOW64\DWrite.dll
\Windows\SysWOW64\IPHLPAPI.DLL
\Windows\SysWOW64\KernelBase.dll
\Windows\SysWOW64\RpcRtRemote.dll
\Windows\SysWOW64\SensApi.dll
\Windows\SysWOW64\WSHTCPIP.DLL
\Windows\SysWOW64\WindowsCodecs.dll
\Windows\SysWOW64\Wldap32.dll
\Windows\SysWOW64\advapi32.dll
\Windows\SysWOW64\apphelp.dll
\Windows\SysWOW64\cfgmgr32.dll
\Windows\SysWOW64\clbcatq.dll
\Windows\SysWOW64\comdlg32.dll
\Windows\SysWOW64\crypt32.dll
\Windows\SysWOW64\cryptbase.dll
\Windows\SysWOW64\cryptsp.dll
\Windows\SysWOW64\d2d1.dll
\Windows\SysWOW64\d3d10.dll
\Windows\SysWOW64\d3d10_1.dll
\Windows\SysWOW64\d3d10_1core.dll
\Windows\SysWOW64\d3d10core.dll
\Windows\SysWOW64\d3d10warp.dll
\Windows\SysWOW64\devobj.dll
\Windows\SysWOW64\dnsapi.dll
\Windows\SysWOW64\dwmapi.dll
\Windows\SysWOW64\dxgi.dll
\Windows\SysWOW64\gdi32.dll
\Windows\SysWOW64\ieframe.dll
\Windows\SysWOW64\iertutil.dll
\Windows\SysWOW64\imm32.dll
\Windows\SysWOW64\jscript9.dll
\Windows\SysWOW64\kernel32.dll
\Windows\SysWOW64\lpk.dll
\Windows\SysWOW64\mlang.dll
\Windows\SysWOW64\msasn1.dll
\Windows\SysWOW64\msctf.dll
\Windows\SysWOW64\mshtml.dll
\Windows\SysWOW64\msimtf.dll
\Windows\SysWOW64\msvcp100.dll
\Windows\SysWOW64\msvcr100.dll
\Windows\SysWOW64\msvcrt.dll
\Windows\SysWOW64\mswsock.dll
\Windows\SysWOW64\nlaapi.dll
```

```
\Windows\SysWOW64\normaliz.dll
\Windows\SysWOW64\nsi.dll
\Windows\SysWOW64\ntdll.dll
\Windows\SysWOW64\ntmarta.dll
\Windows\SysWOW64\ole32.dll
\Windows\SysWOW64\oleacc.dll
\Windows\SysWOW64\oleaut32.dll
\Windows\SysWOW64\profapi.dll
\Windows\SysWOW64\propsys.dll
\Windows\SysWOW64\psapi.dll
\Windows\SysWOW64\rasadhlp.dll
\Windows\SysWOW64\rasapi32.dll
\Windows\SysWOW64\rasman.dll
\Windows\SysWOW64\rpcrt4.dll
\Windows\SysWOW64\rsaenh.dll
\Windows\SysWOW64\rtutils.dll
\Windows\SysWOW64\sechost.dll
\Windows\SysWOW64\secur32.dll
\Windows\SysWOW64\setupapi.dll
\Windows\SysWOW64\shell32.dll
\Windows\SysWOW64\shlwapi.dll
\Windows\SysWOW64\sspicli.dll
\Windows\SysWOW64\sxs.dll
\Windows\SysWOW64\urlmon.dll
\Windows\SysWOW64\user32.dll
\Windows\SysWOW64\usp10.dll
\Windows\SysWOW64\uxtheme.dll
\Windows\SysWOW64\version.dll
\Windows\SysWOW64\wininet.dll
\Windows\SysWOW64\winnsi.dll
\Windows\SysWOW64\wintrust.dll
\Windows\SysWOW64\ws2_32.dll
\Windows\SysWOW64\wship6.dll
\Windows\System32\apisetschema.dll
\Windows\System32\ntdll.dll
\Windows\System32\wow64.dll
\Windows\System32\wow64cpu.dll
\Windows\System32\wow64win.dll
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600.16661_none_ebfb56996c
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16661_none_420fe3fa2b81
```