# DarunGrim3 Installation & Usage Guide

## *Prerequisites*

### Must-have

IDA 5.6
We tested current release of DarunGrim3 on IDA 5.6. Any other versions are not officially supported yet. Further support for other versions will come soon after more testing. You can always try yourself if it works, though. Theoretically there will not be any major problems with any IDA upper 5.0.

### Optional

If you are going to use python source code for execution, you need to install following Python distribution and Python modules. The other versions might work, but this is the exact packages we tested. This Python and Python module installation is not necessary if you are using the compiled package we provide.

***Python 2.6.5***
http://www.python.org/ftp/python/2.6.5/python-2.6.5.msi

***SQLAlchemy 0.6.3***
http://www.sqlalchemy.org/download.html

***CherryPy 3.1.2***
http://download.cherrypy.org/cherrypy/3.1.2/

***Mechanize 0.2.2***
http://wwwsearch.sourceforge.net/mechanize/

***BeautifulSoup 3.1.0***
http://www.crummy.com/software/BeautifulSoup/

***Mako 0.3.4***
http://www.makotemplates.org/download.html

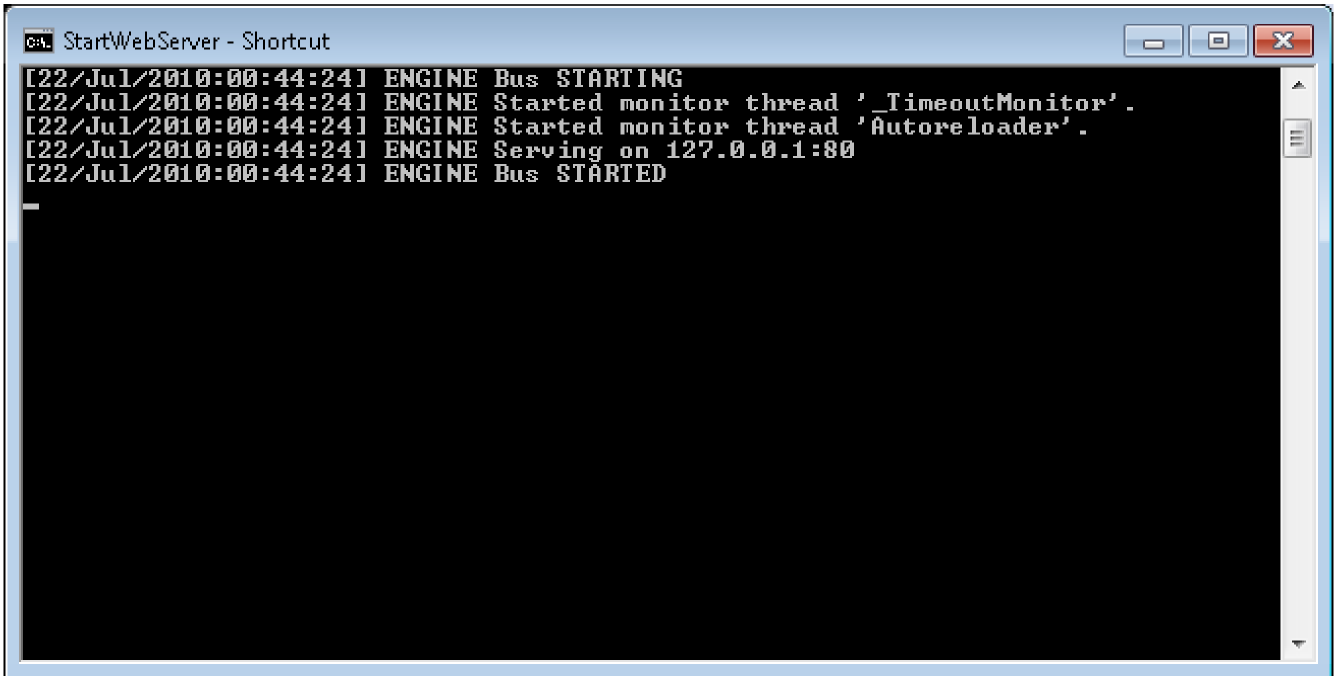
## *Web Browser*

Any web browser will work except lynx, but we found that Mozilla Firefox is the best in rendering the results as we intended. IE is good, but sometimes it needs you some patience displaying big size table.

## Starting the DarunGrim3 Server

Start DarunGrim3Server.exe from binary directory. If you're trying python source code distribution, execute DarunGrim3Server.py from the source directory.

If you start the server, you will see the Darungrim3 Webserver starting.



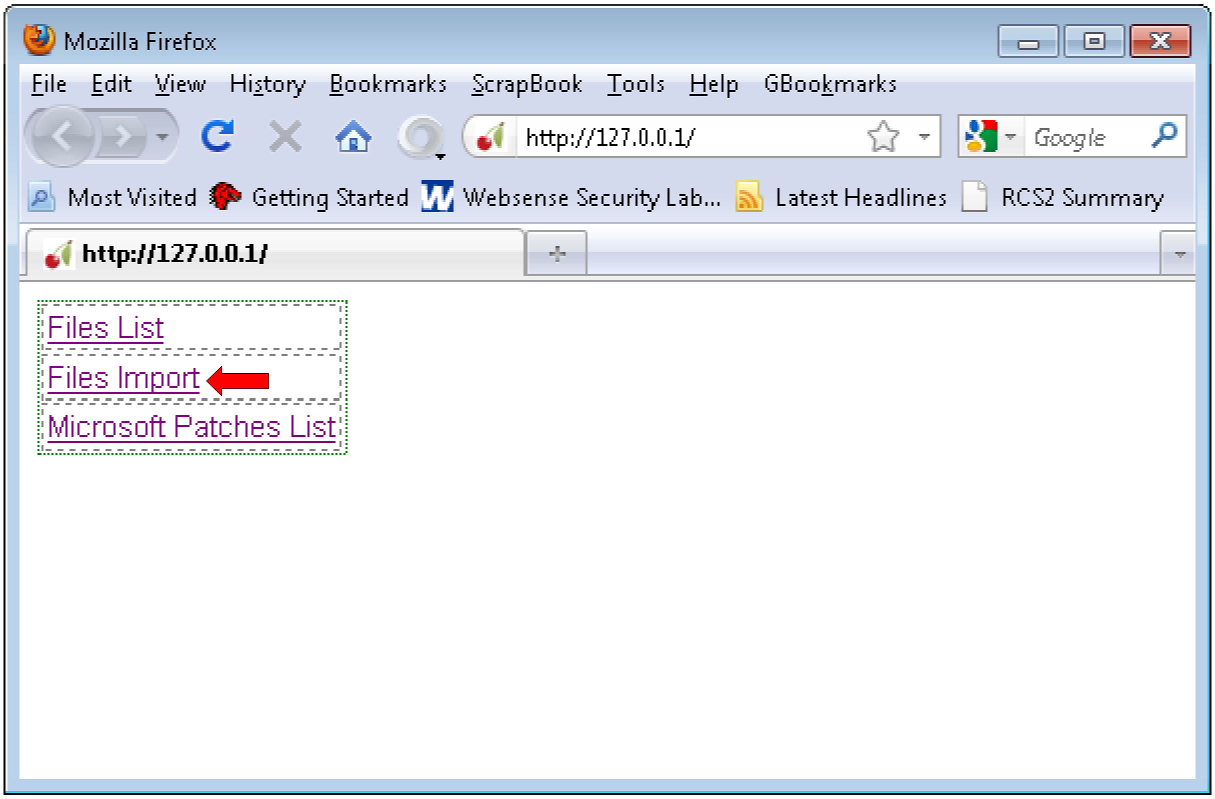
```
[22/Jul/2010:00:44:24] ENGINE Bus STARTING
[22/Jul/2010:00:44:24] ENGINE Started monitor thread '_TimeoutMonitor'.
[22/Jul/2010:00:44:24] ENGINE Started monitor thread 'Autoreloader'.
[22/Jul/2010:00:44:24] ENGINE Serving on 127.0.0.1:80
[22/Jul/2010:00:44:24] ENGINE Bus STARTED
```

The default binding TCP port is 80. You can change the port by editing DarunGrim3.cfg in the line looks like following.

```
[Global]
Port = 80
```

## Main Menu

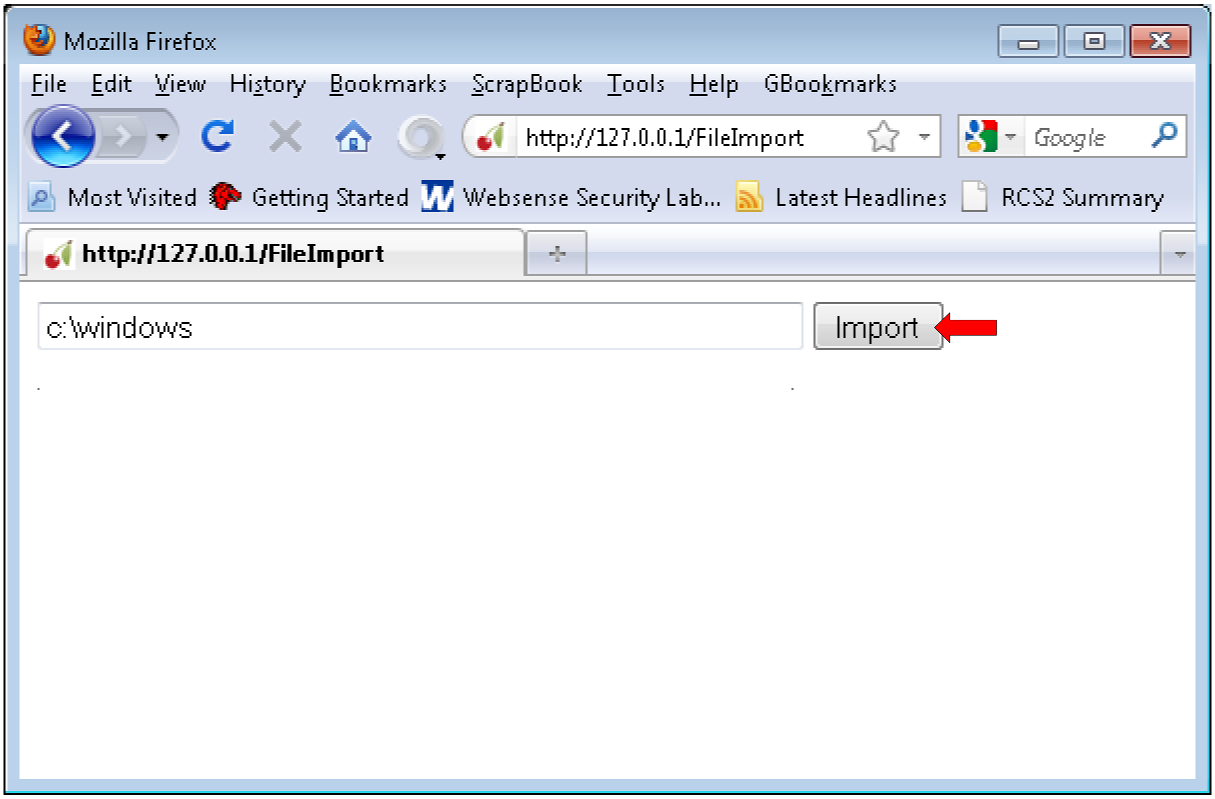
You can see the first page with 3 menus. With first run, there will not be anything to analyze.So you need to import files first. Click “Files Import” link.


Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/
Google
Most Visited Getting Started Websense Security Lab... Latest Headlines RCS2 Summary
http://127.0.0.1/
Files List
Files Import
Microsoft Patches List

# Importing

You will see an input box, you can put any local folder name to import PE files. I recommend testing by importing “c:\windows” directory which contains pretty much every system files.

If you click “import”, it will start importing files. If the process takes too long, the session will be timed out. But when it times out, don't reload the page because it will trigger the import action again which is unnecessary.



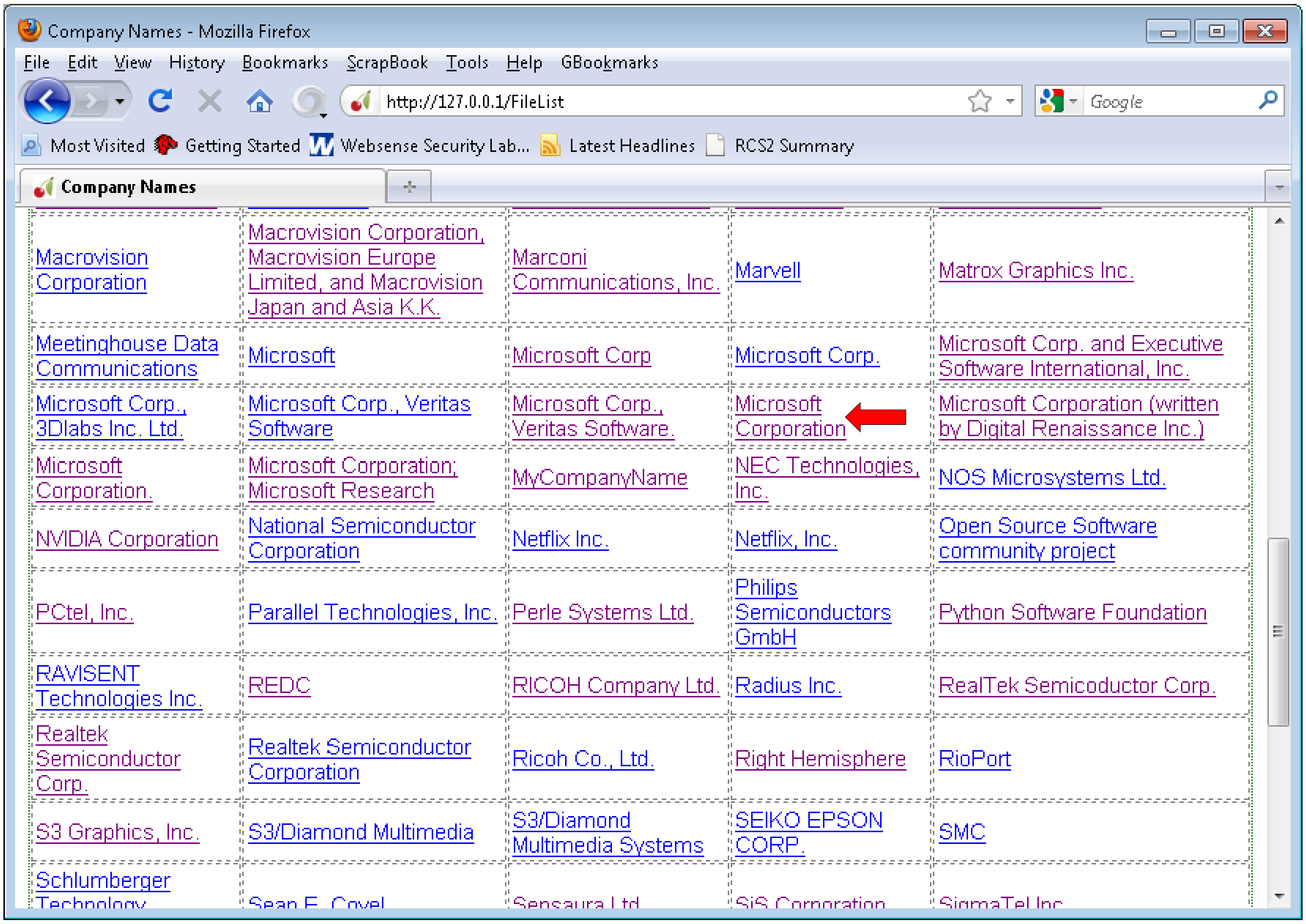
http://127.0.0.1/FileImport

c:\windows

# List of Company Names

You go back to main menu, by connecting to the root URI and select “Files List” menu. It will display the company names of the all the files.

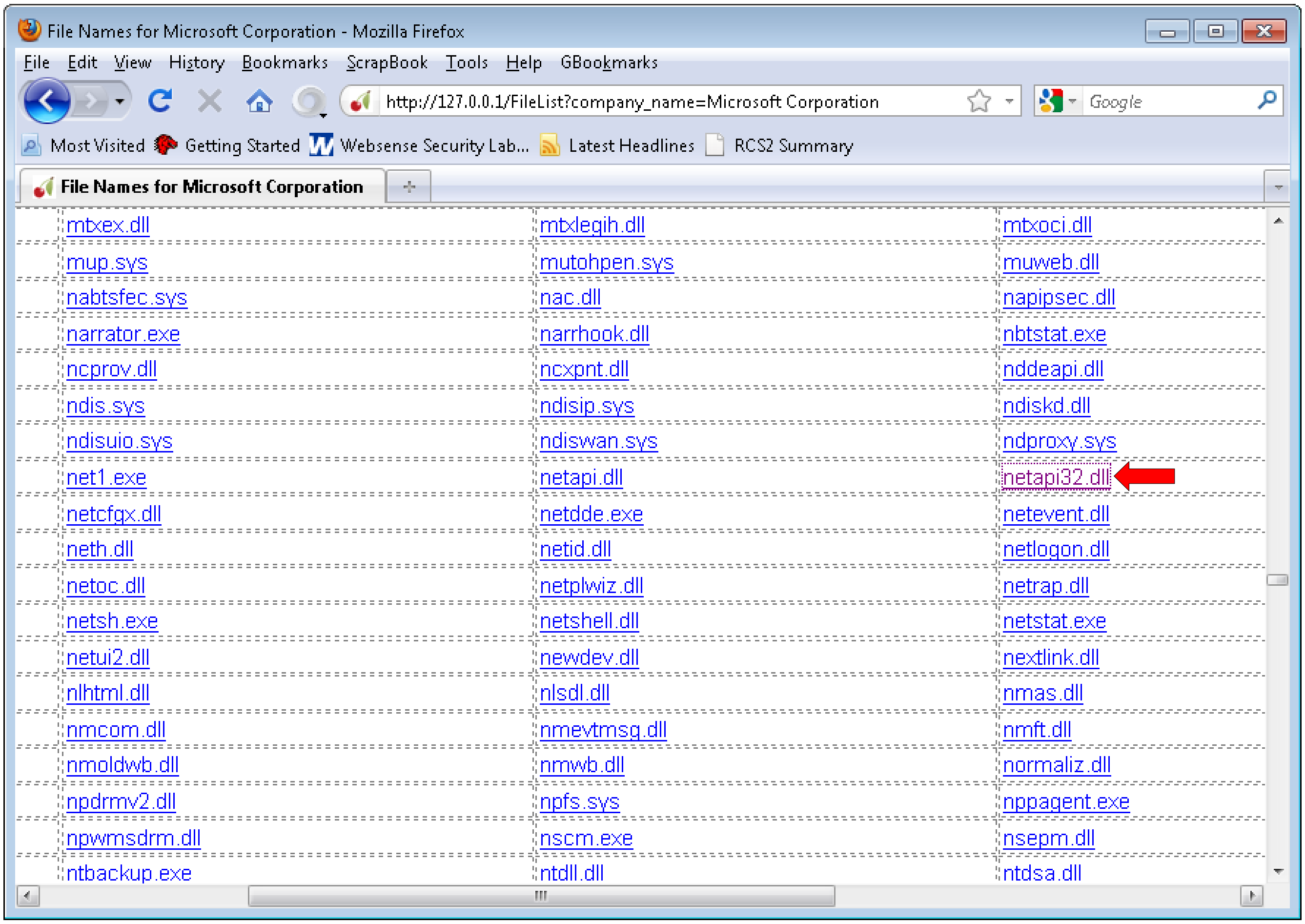
Probably you might be interested in patches from Microsoft, Adobe or Sun. For example, to check Microsoft's binaries, just click “Microsoft Corporation” link.


Company Names - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/FileList
Google
Most Visited
Getting Started
Websense Security Lab...
Latest Headlines
RCS2 Summary
Company Names

| | | | | |
|---|---|---|---|---|
| Macrovision Corporation | Macrovision Corporation, Macrovision Europe Limited, and Macrovision Japan and Asia K.K. | Marconi Communications, Inc. | Marvell | Matrox Graphics Inc. |
| Meetinghouse Data Communications | Microsoft | Microsoft Corp | Microsoft Corp. | Microsoft Corp. and Executive Software International, Inc. |
| Microsoft Corp., 3Dlabs Inc. Ltd. | Microsoft Corp., Veritas Software | Microsoft Corp., Veritas Software. | Microsoft Corporation | Microsoft Corporation (written by Digital Renaissance Inc.) |
| Microsoft Corporation. | Microsoft Corporation; Microsoft Research | MyCompanyName | NEC Technologies, Inc. | NOS Microsystems Ltd. |
| NVIDIA Corporation | National Semiconductor Corporation | Netflix Inc. | Netflix, Inc. | Open Source Software community project |
| PCtel, Inc. | Parallel Technologies, Inc. | Perle Systems Ltd. | Philips Semiconductors GmbH | Python Software Foundation |
| RAVISENT Technologies Inc. | REDC | RICOH Company Ltd. | Radius Inc. | RealTek Semicoductor Corp. |
| Realtek Semiconductor Corp. | Realtek Semiconductor Corporation | Ricoh Co., Ltd. | Right Hemisphere | RioPort |
| S3 Graphics, Inc. | S3/Diamond Multimedia | S3/Diamond Multimedia Systems | SEIKO EPSON CORP. | SMC |
| Schlumberger Technology | Sean E. Covel | Sensaura Ltd | SiS Corporation | SigmaTel Inc |

## List of Files

The next page will display every files that were collected under the selected company name.  You just need to click the name of the file you are interested in. I want to diff netapi32.dll for the analysis example. The file is known for having good history of vulnerabilities.



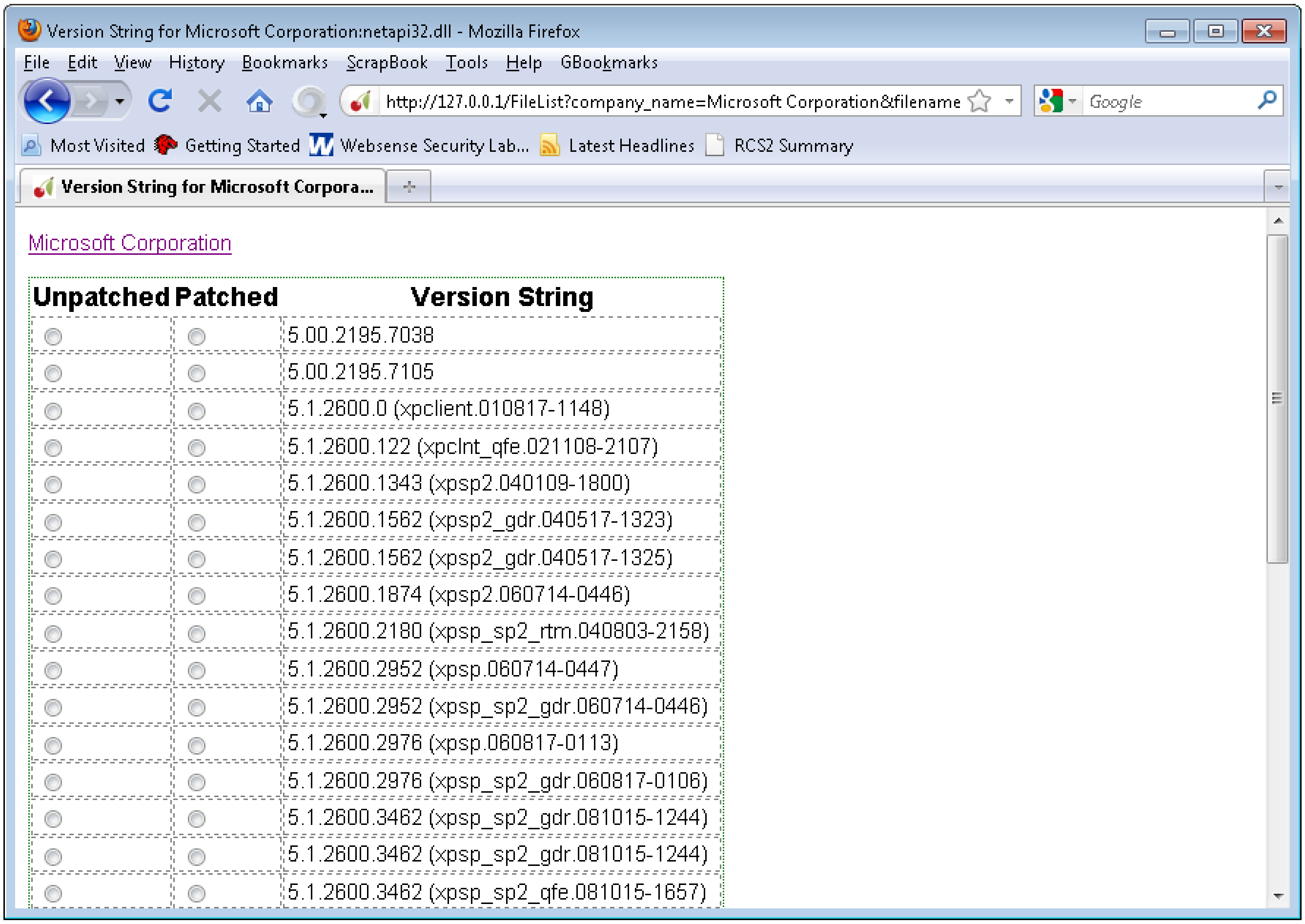
http://127.0.0.1/FileList?company_name=Microsoft Corporation

| | | |
|---|---|---|
| mtxex.dll | mtxlegih.dll | mtxoci.dll |
| mup.sys | mutohpen.sys | muweb.dll |
| nabtsfec.sys | nac.dll | napipsec.dll |
| narrator.exe | narrhook.dll | nbtstat.exe |
| ncprov.dll | ncxpnt.dll | nddeapi.dll |
| ndis.sys | ndisip.sys | ndiskd.dll |
| ndisuio.sys | ndiswan.sys | ndproxy.sys |
| net1.exe | netapi.dll | netapi32.dll |
| netcfgx.dll | netdde.exe | netevent.dll |
| neth.dll | netid.dll | netlogon.dll |
| netoc.dll | netplwiz.dll | netrap.dll |
| netsh.exe | netshell.dll | netstat.exe |
| netui2.dll | newdev.dll | nextlink.dll |
| nlhtml.dll | nlsdl.dll | nmas.dll |
| nmcom.dll | nmevtmsg.dll | nmft.dll |
| nmoldwb.dll | nmwb.dll | normaliz.dll |
| npdrmv2.dll | npfs.sys | nppagent.exe |
| npwmsdrm.dll | nscm.exe | nsepm.dll |
| ntbackup.exe | ntdll.dll | ntdsa.dll |

## List of Version strings  for the file

It will display all the different versions of the file that were collected from the system. It'll display many different versions of the same file. This is possible because when installing patches, Microsoft usually leaves original file in some directory. So by just collecting binaries from a machine that is fully patched, you have a good chances of collecting many versions of the patched files.

You can choose the versions you want to compare with by clicking the radio buttons.

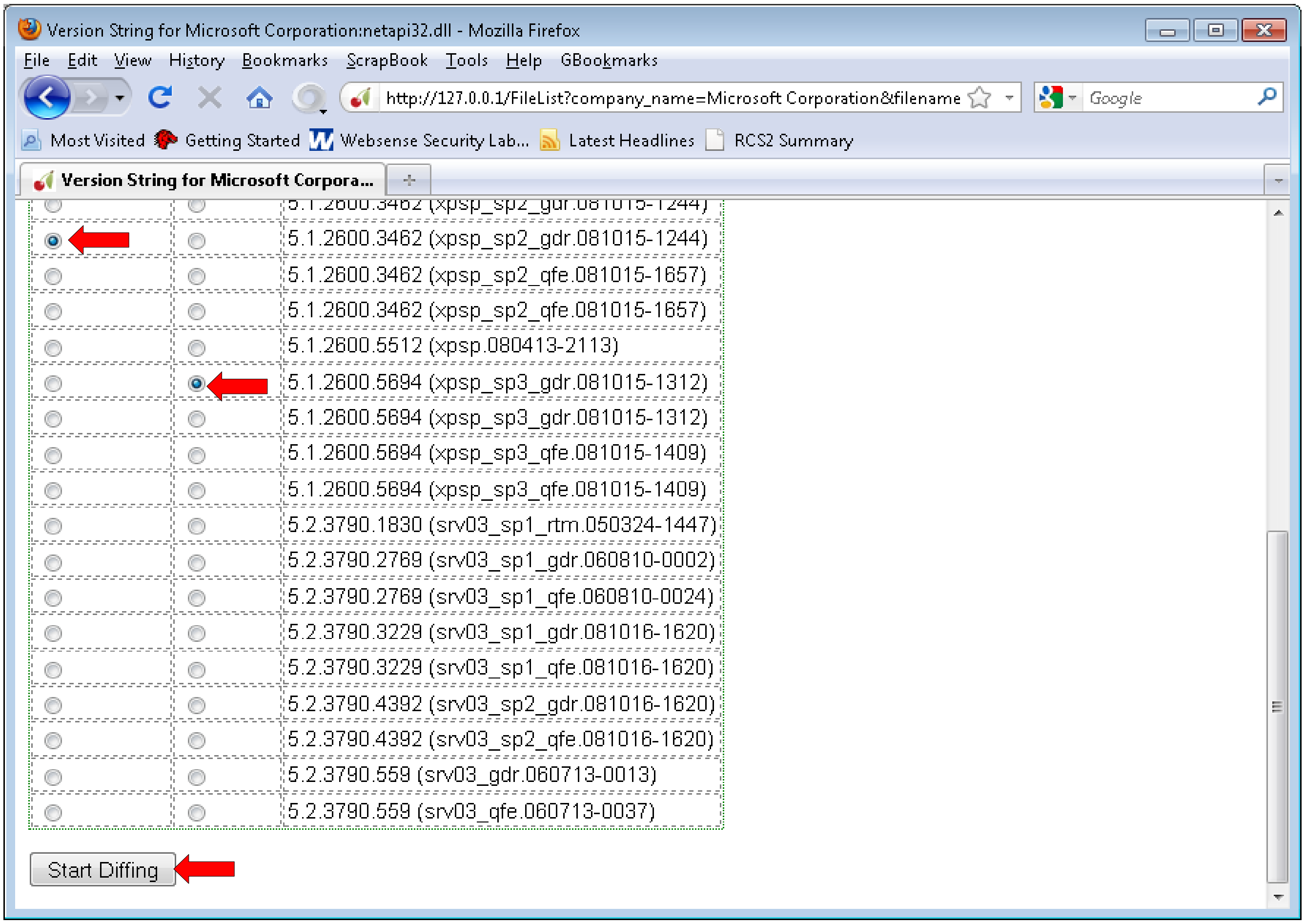

Version String for Microsoft Corporation:netapi32.dll - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/FileList?company_name=Microsoft Corporation&filename
Google
Most Visited Getting Started Websense Security Lab... Latest Headlines RCS2 Summary
Version String for Microsoft Corpora...

Microsoft Corporation

| Unpatched | Patched | Version String |
|---|---|---|
| ○ | ○ | 5.00.2195.7038 |
| ○ | ○ | 5.00.2195.7105 |
| ○ | ○ | 5.1.2600.0 (xpclient.010817-1148) |
| ○ | ○ | 5.1.2600.122 (xpclnt_qfe.021108-2107) |
| ○ | ○ | 5.1.2600.1343 (xpsp2.040109-1800) |
| ○ | ○ | 5.1.2600.1562 (xpsp2_gdr.040517-1323) |
| ○ | ○ | 5.1.2600.1562 (xpsp2_gdr.040517-1325) |
| ○ | ○ | 5.1.2600.1874 (xpsp2.060714-0446) |
| ○ | ○ | 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158) |
| ○ | ○ | 5.1.2600.2952 (xpsp.060714-0447) |
| ○ | ○ | 5.1.2600.2952 (xpsp_sp2_gdr.060714-0446) |
| ○ | ○ | 5.1.2600.2976 (xpsp.060817-0113) |
| ○ | ○ | 5.1.2600.2976 (xpsp_sp2_gdr.060817-0106) |
| ○ | ○ | 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) |
| ○ | ○ | 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) |
| ○ | ○ | 5.1.2600.3462 (xpsp_sp2_qfe.081015-1657) |

# Initiating Diffing Process

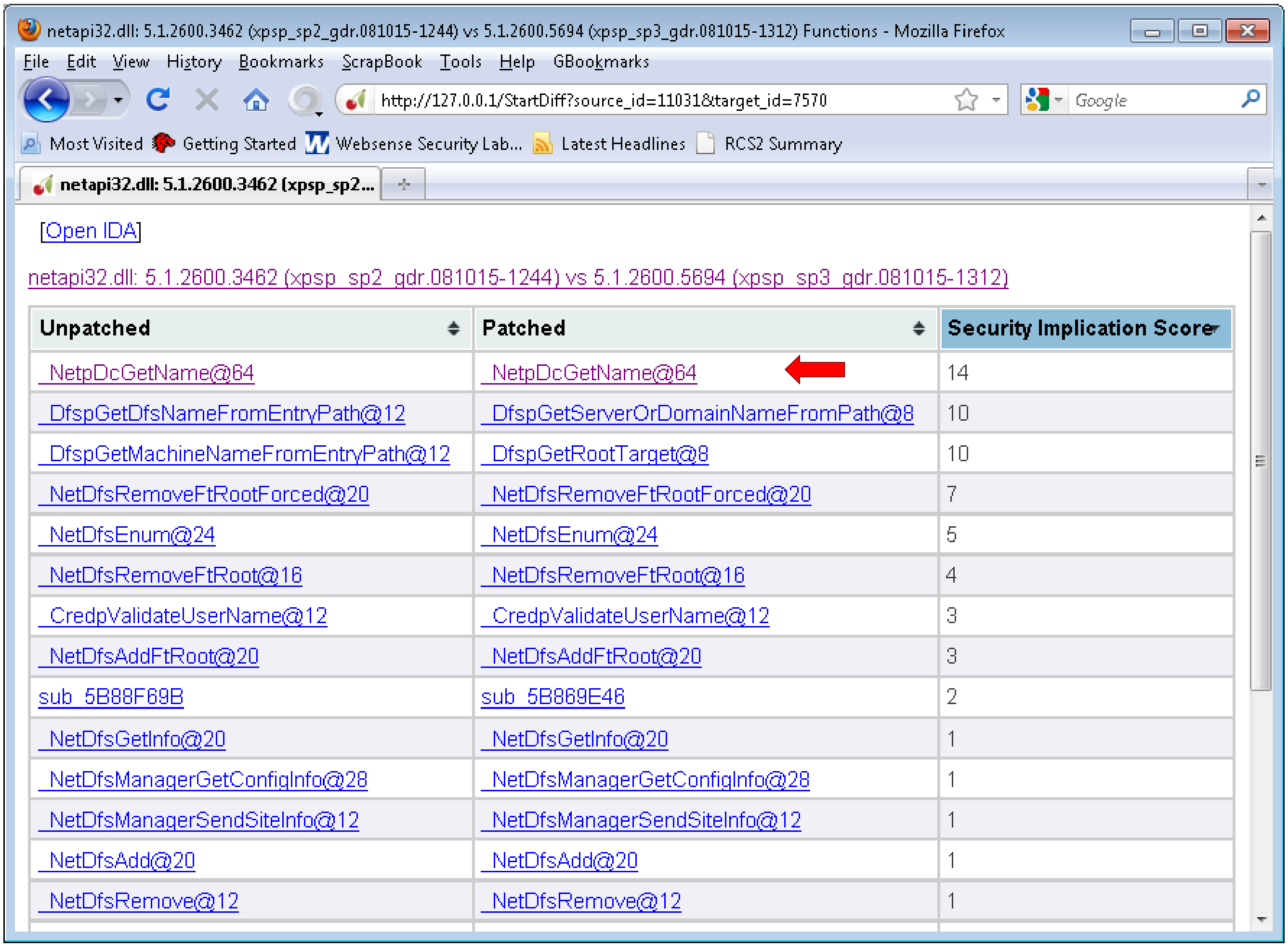
After choosing the files to compare, press “Starting Diffing” button.


Version String for Microsoft Corporation:netapi32.dll - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/FileList?company_name=Microsoft Corporation&filename
Google
Most Visited Getting Started Websense Security Lab... Latest Headlines RCS2 Summary
Version String for Microsoft Corpora...

| | | |
|---|---|---|
| ○ | ○ | 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) |
| ● | ○ | 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) |
| ○ | ○ | 5.1.2600.3462 (xpsp_sp2_qfe.081015-1657) |
| ○ | ○ | 5.1.2600.3462 (xpsp_sp2_qfe.081015-1657) |
| ○ | ○ | 5.1.2600.5512 (xpsp.080413-2113) |
| ○ | ● | 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312) |
| ○ | ○ | 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312) |
| ○ | ○ | 5.1.2600.5694 (xpsp_sp3_qfe.081015-1409) |
| ○ | ○ | 5.1.2600.5694 (xpsp_sp3_qfe.081015-1409) |
| ○ | ○ | 5.2.3790.1830 (srv03_sp1_rtm.050324-1447) |
| ○ | ○ | 5.2.3790.2769 (srv03_sp1_gdr.060810-0002) |
| ○ | ○ | 5.2.3790.2769 (srv03_sp1_qfe.060810-0024) |
| ○ | ○ | 5.2.3790.3229 (srv03_sp1_gdr.081016-1620) |
| ○ | ○ | 5.2.3790.3229 (srv03_sp1_qfe.081016-1620) |
| ○ | ○ | 5.2.3790.4392 (srv03_sp2_gdr.081016-1620) |
| ○ | ○ | 5.2.3790.4392 (srv03_sp2_qfe.081016-1620) |
| ○ | ○ | 5.2.3790.559 (srv03_gdr.060713-0013) |
| ○ | ○ | 5.2.3790.559 (srv03_qfe.060713-0037) |

# Analysis Results

It takes few minutes to finish the analysis. After that you can see the list of functions that has been modified. You can sort by the columns like “Security Implication Score”



netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312) Functions - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/StartDiff?source_id=11031&target_id=7570
Google
Most Visited Getting Started Websense Security Lab... Latest Headlines RCS2 Summary
netapi32.dll: 5.1.2600.3462 (xpsp_sp2...

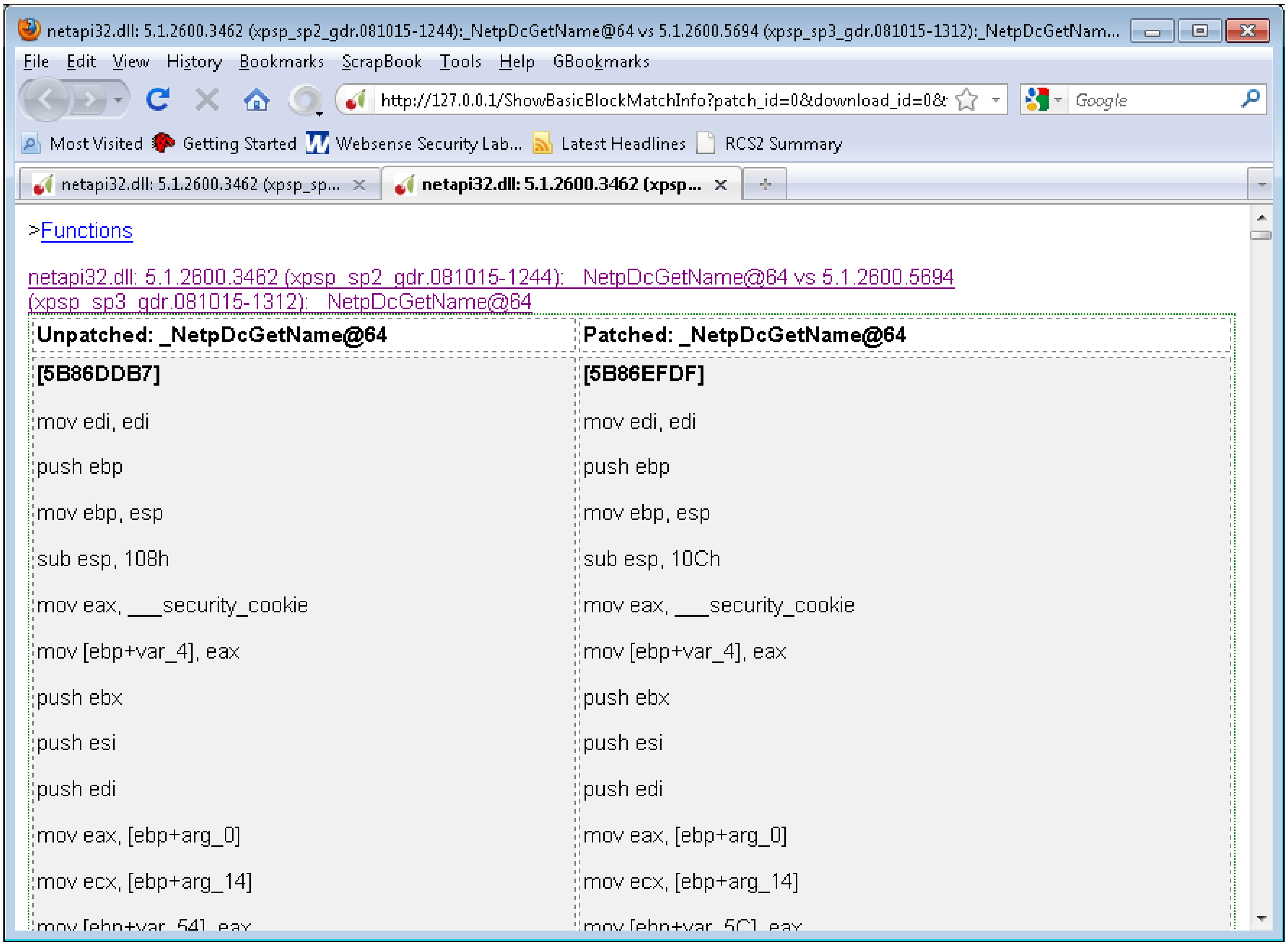
[Open IDA]

netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312)

| Unpatched | Patched | Security Implication Score |
|---|---|---|
| _NetpDcGetName@64 | _NetpDcGetName@64 | 14 |
| _DfspGetDfsNameFromEntryPath@12 | _DfspGetServerOrDomainNameFromPath@8 | 10 |
| _DfspGetMachineNameFromEntryPath@12 | _DfspGetRootTarget@8 | 10 |
| _NetDfsRemoveFtRootForced@20 | _NetDfsRemoveFtRootForced@20 | 7 |
| _NetDfsEnum@24 | _NetDfsEnum@24 | 5 |
| _NetDfsRemoveFtRoot@16 | _NetDfsRemoveFtRoot@16 | 4 |
| _CredpValidateUserName@12 | _CredpValidateUserName@12 | 3 |
| _NetDfsAddFtRoot@20 | _NetDfsAddFtRoot@20 | 3 |
| sub_5B88F69B | sub_5B869E46 | 2 |
| _NetDfsGetInfo@20 | _NetDfsGetInfo@20 | 1 |
| _NetDfsManagerGetConfigInfo@28 | _NetDfsManagerGetConfigInfo@28 | 1 |
| _NetDfsManagerSendSiteInfo@12 | _NetDfsManagerSendSiteInfo@12 | 1 |
| _NetDfsAdd@20 | _NetDfsAdd@20 | 1 |
| _NetDfsRemove@12 | _NetDfsRemove@12 | 1 |

### *Function Level Analysis*

If you click the function names from the previous view, you can get to the function analysis page like following scrrenshot. It will show the result side-by-side. Left side is unpatched function and right side is patched one.


netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244):_NetpDcGetName@64 vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312):_NetpDcGetNam...
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/ShowBasicBlockMatchInfo?patch_id=0&download_id=0&
Google
Most Visited
Getting Started
Websense Security Lab...
Latest Headlines
RCS2 Summary
netapi32.dll: 5.1.2600.3462 (xpsp_sp...
netapi32.dll: 5.1.2600.3462 (xpsp...

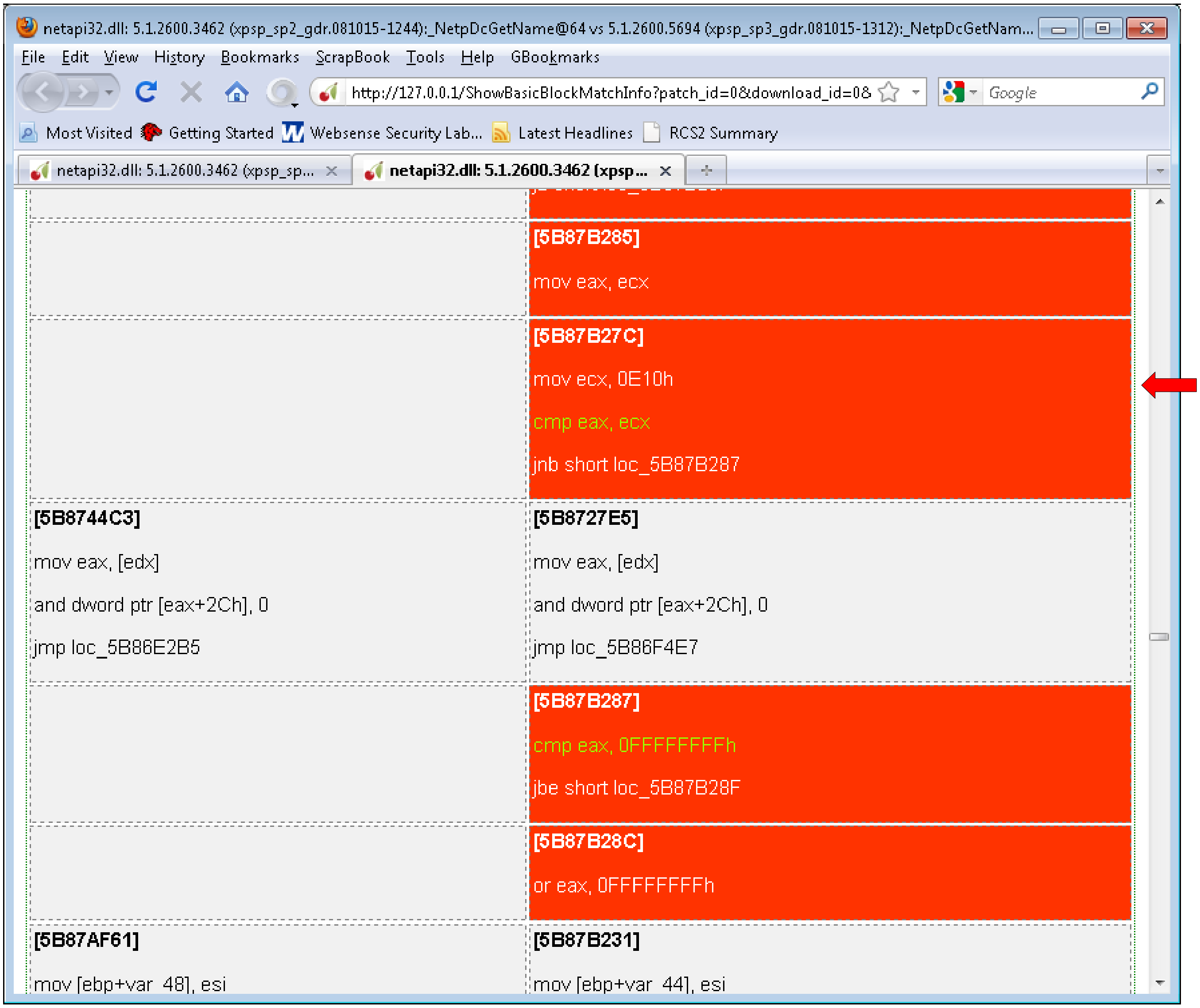
>Functions

netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244):_NetpDcGetName@64 vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312):_NetpDcGetName@64

| **Unpatched: _NetpDcGetName@64** | **Patched: _NetpDcGetName@64** |
|---|---|
| **[5B86DDB7]**<br>mov edi, edi<br>push ebp<br>mov ebp, esp<br>sub esp, 108h<br>mov eax, ___security_cookie<br>mov [ebp+var_4], eax<br>push ebx<br>push esi<br>push edi<br>mov eax, [ebp+arg_0]<br>mov ecx, [ebp+arg_14]<br>mov [ebp+var_54], eax | **[5B86EFDF]**<br>mov edi, edi<br>push ebp<br>mov ebp, esp<br>sub esp, 10Ch<br>mov eax, ___security_cookie<br>mov [ebp+var_4], eax<br>push ebx<br>push esi<br>push edi<br>mov eax, [ebp+arg_0]<br>mov ecx, [ebp+arg_14]<br>mov [ebp+var_5C], eax |

## *Reading the Results*

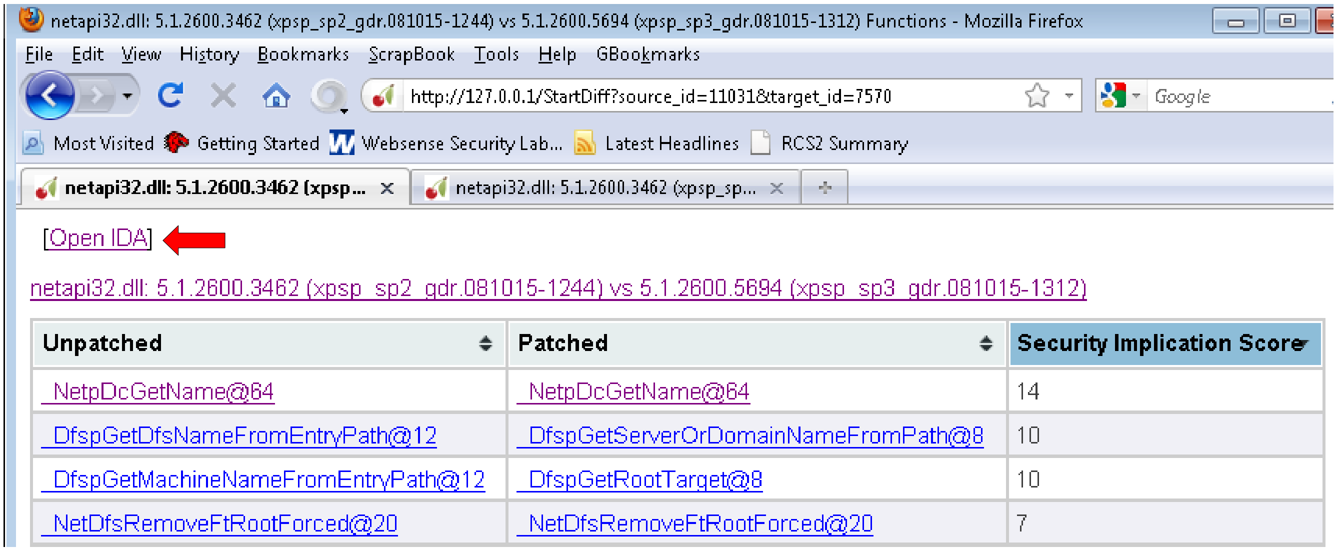
The red blocks on the right side are inserted blocks.


netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244):_NetpDcGetName@64 vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312):_NetpDcGetNam...
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/ShowBasicBlockMatchInfo?patch_id=0&download_id=0&
Google
Most Visited
Getting Started
Websense Security Lab...
Latest Headlines
RCS2 Summary
netapi32.dll: 5.1.2600.3462 (xpsp_sp...
netapi32.dll: 5.1.2600.3462 (xpsp...

| | |
|---|---|
| | **[5B87B285]**<br>mov eax, ecx |
| | **[5B87B27C]**<br>mov ecx, 0E10h<br>cmp eax, ecx<br>jnb short loc_5B87B287 |
| **[5B8744C3]**<br>mov eax, [edx]<br>and dword ptr [eax+2Ch], 0<br>jmp loc_5B86E2B5 | **[5B8727E5]**<br>mov eax, [edx]<br>and dword ptr [eax+2Ch], 0<br>jmp loc_5B86F4E7 |
| | **[5B87B287]**<br>cmp eax, 0FFFFFFFFh<br>jbe short loc_5B87B28F |
| | **[5B87B28C]**<br>or eax, 0FFFFFFFFh |
| **[5B87AF61]**<br>mov [ebp+var_48], esi | **[5B87B231]**<br>mov [ebp+var_44], esi |

## *IDA View*

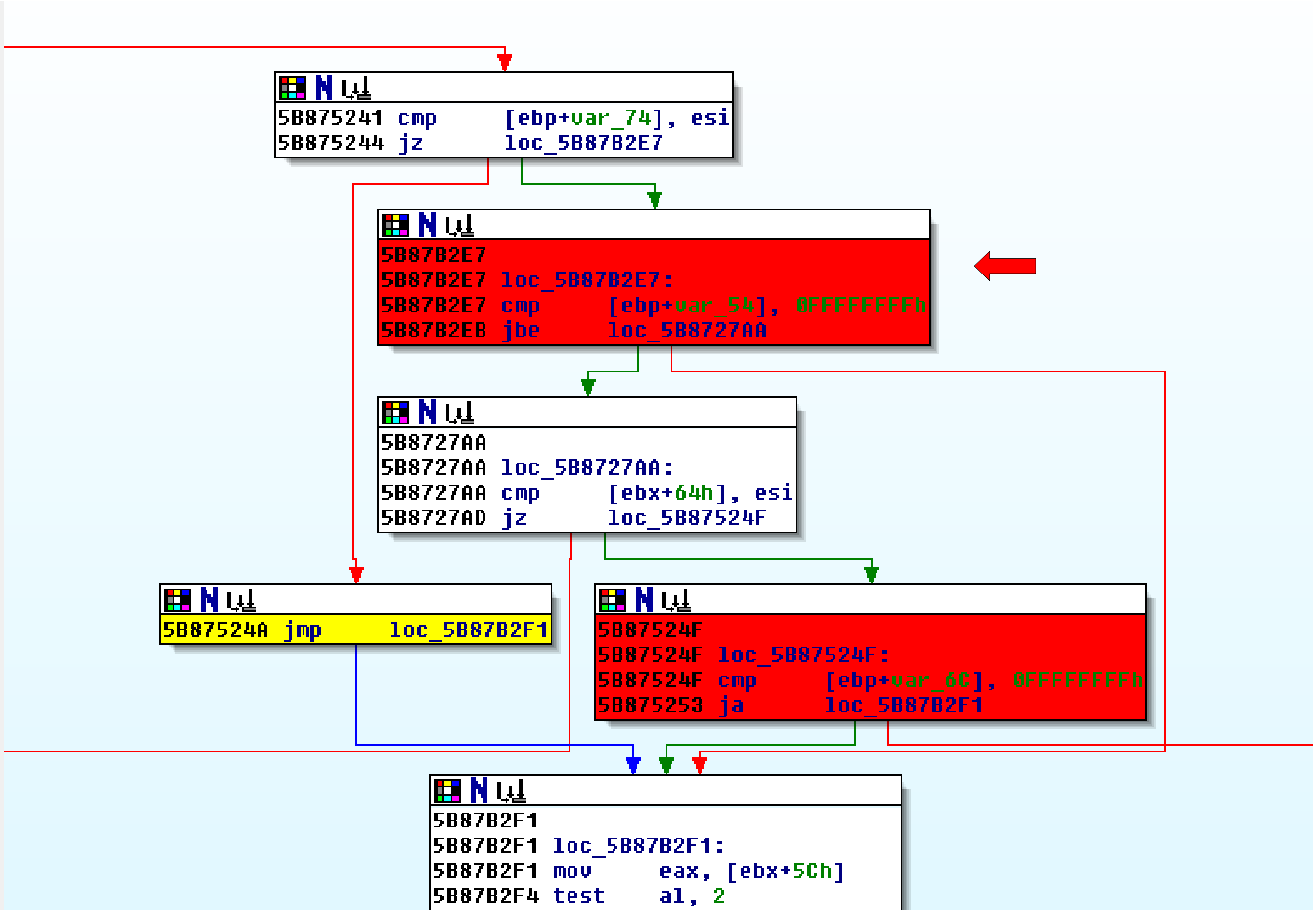
From the functions list view, you can click "Open IDA" link and it will open the IDA views. And if you click each functions list, the IDA view will be automatically refreshed to the matching position and the color code will be applied to each of them.


netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312) Functions - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help GBookmarks
http://127.0.0.1/StartDiff?source_id=11031&target_id=7570
Google
Most Visited
Getting Started
Websense Security Lab...
Latest Headlines
RCS2 Summary
netapi32.dll: 5.1.2600.3462 (xpsp...
netapi32.dll: 5.1.2600.3462 (xpsp_sp...

[Open IDA]

netapi32.dll: 5.1.2600.3462 (xpsp_sp2_gdr.081015-1244) vs 5.1.2600.5694 (xpsp_sp3_gdr.081015-1312)

| Unpatched | Patched | Security Implication Score |
|---|---|---|
| NetpDcGetName@64 | NetpDcGetName@64 | 14 |
| DfspGetDfsNameFromEntryPath@12 | DfspGetServerOrDomainNameFromPath@8 | 10 |
| DfspGetMachineNameFromEntryPath@12 | DfspGetRootTarget@8 | 10 |
| NetDfsRemoveFtRootForced@20 | NetDfsRemoveFtRootForced@20 | 7 |



```
5B875241 cmp     [ebp+var_74], esi
5B875244 jz      loc_5B87B2E7
```

```
5B87B2E7
5B87B2E7 loc_5B87B2E7:
5B87B2E7 cmp     [ebp+var_54], 0FFFFFFFFh
5B87B2EB jbe     loc_5B8727AA
```

```
5B8727AA
5B8727AA loc_5B8727AA:
5B8727AA cmp     [ebx+64h], esi
5B8727AD jz      loc_5B87524F
```

```
5B87524A jmp     loc_5B87B2F1
```

```
5B87524F
5B87524F loc_5B87524F:
5B87524F cmp     [ebp+var_6C], 0FFFFFFFFh
5B875253 ja      loc_5B87B2F1
```

```
5B87B2F1
5B87B2F1 loc_5B87B2F1:
5B87B2F1 mov     eax, [ebx+5Ch]
5B87B2F4 test    al, 2
```

## Configuration

Main configuration file name is “DarunGrim3.cfg”

```
[Global]
Port = 80
[Directories]
BinariesStorage = Binaries
MicrosoftBinariesStorage = Binaries\Microsoft
DGFDirectory = Output
IDAPath = C:\Program Files (x86)\ida\idag.exe
DatabaseName = index.db
PatchTemporaryStore = Temp
```

The default binaries storage folder name is “Binaries”. You can configure this by modifying “BinariesStorage” value.

The default Output folder name is “Output”. You can configure this by modifying “DGFDirectory” value.

You can also configure IDA path name by changing “IDAPath” value.

## Further details

If you need more information or help, visit http://www.darungrim.org or shoot me a mail to oh.jeongwook@gmail.com. Any bug reporting or feature requests are appreciated.