|  |  |
| --- | --- |
| M:\SlimCharles\Resources\Images\MRIBadgeFullLarge.png | svchost.exe **( 1480 )** |
| M:\SlimCharles\Resources\Images\MRIBadgeEmptyLarge.png |  |
| M:\SlimCharles\Resources\Images\MRIBadgeHalfLarge.png |  |

**Process Details**

|  |  |
| --- | --- |
| **Username:** | NT Authority\System |
| **Path:** | C:\WINDOWS\system32 |
| **Parent:** | services.exe (644) |
| **Parent Process Path:** | C:\WINDOWS\system32 |
| **Arguments:** | “C:\INDOWS\\system32\\lsass.exe” |
| **Start Time:** | 7/17/2010 4:13:39 PM |
| **Kernel Time Elapsed:** | 00:00:00 |
| **User Time Elapsed:** | 00:00:00 |
| **SID:** | S-1-5-18 |
| **SID Type:** | SidTypeWellKnownGroup |
| **Hidden:** | True |
| **Malware Rating Index:** | 95 |

**Malware Risk Index Hits**

|  |  |
| --- | --- |
| M:\SlimCharles\Resources\Images\MRIBadgeFullSmall.png | This Process was spawned from an unexpected location: “\windows\system32\dllcache”. (see MRI configuration for a list of processes and their expected paths) |
| M:\SlimCharles\Resources\Images\MRIBadgeEmptySmall.png | [Comment]: Process was spawned by an unexpected user: “EXPERIAN-354642\Administrator” (see MRI configuration for a list of processes and their expected users) |
| M:\SlimCharles\Resources\Images\MRIBadgeHalfSmall.png | [False Positive]: This Process was spawned with unexpected arguments: “C:\WINDOWS\system32\dllcache\svchost.exe” (see MRI configuration for list of processes and their expected arguments) |
| M:\SlimCharles\Resources\Images\MRIBadgeFullSmall.png | [User Injected]: This looks like so and so malware. |

**Named Memory Sections**

|  |  |  |
| --- | --- | --- |
| M:\SlimCharles\Resources\Images\Negative.png | Negative Factors | 40% |
| M:\SlimCharles\Resources\Images\Positive.png | Positive Factors | 48% |
| M:\SlimCharles\Resources\Images\Ignored.png | Ignored Factors | 0% |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Trust Status | | Count | Name |
| M:\SlimCharles\Resources\Images\Positive.png | Digitally Signed and Verified | 5 | C:\WINDOWS\system32\dllcache\svchost.exe |
| M:\SlimCharles\Resources\Images\Positive.png | Found in 70% of all Processes | 6 | C:\WINDOWS\system32\unicode.nls |
| M:\SlimCharles\Resources\Images\Negative.png | User untrusted | 7 | C:\WINDOWS\system32\locale.nls |
| M:\SlimCharles\Resources\Images\Ignored.png | Ignored | 8 | C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat |