Beyond good ol' Run key, Part 24

Ability to load a DLL of your choice anytime someone is connecting to the internet is something that definitely deserves some attention. This is why I will describe here yet another obscure mechanism that can be abused for malicious purposes. Courtesy of Winsock 2 library (ws2_32.dll).

When Winsock library connects to the internet it 'talks' to various service providers and probes them for connectivity services. It's actually pretty complex and I won't pretend that I fully understand what's going on there yet there is one thing which this library does that I do understand 🙂

At some stage it attempts to load a DLL as specified by the following Registry key:

```
HKLM\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\AutodialDLL
```

This key is quite obscure and Microsoft only describes it in a context of a very old vulnerability MS06-041.

Turns out that the AutodialDLL entry points to a DLL that WinSock will load anytime it connects to the internet.

The DLL needs to export 3 functions:

- WSAttemptAutodialAddr
- WSAttemptAutodialName
- WSNoteSuccessfulHostentLookup

The result of loading the following registry key:

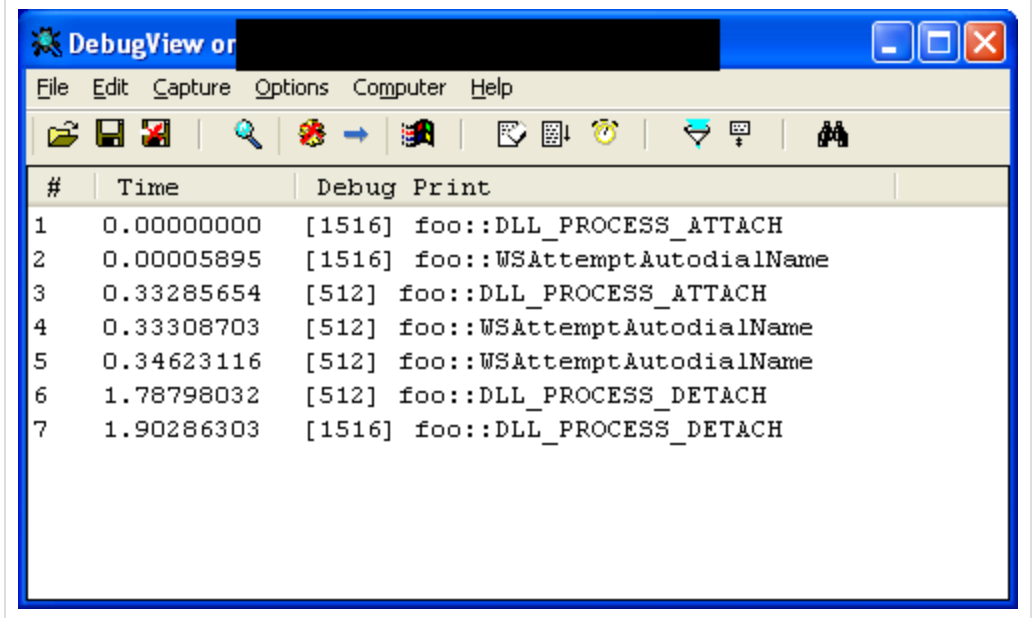
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Paramete
```

and dropping the file

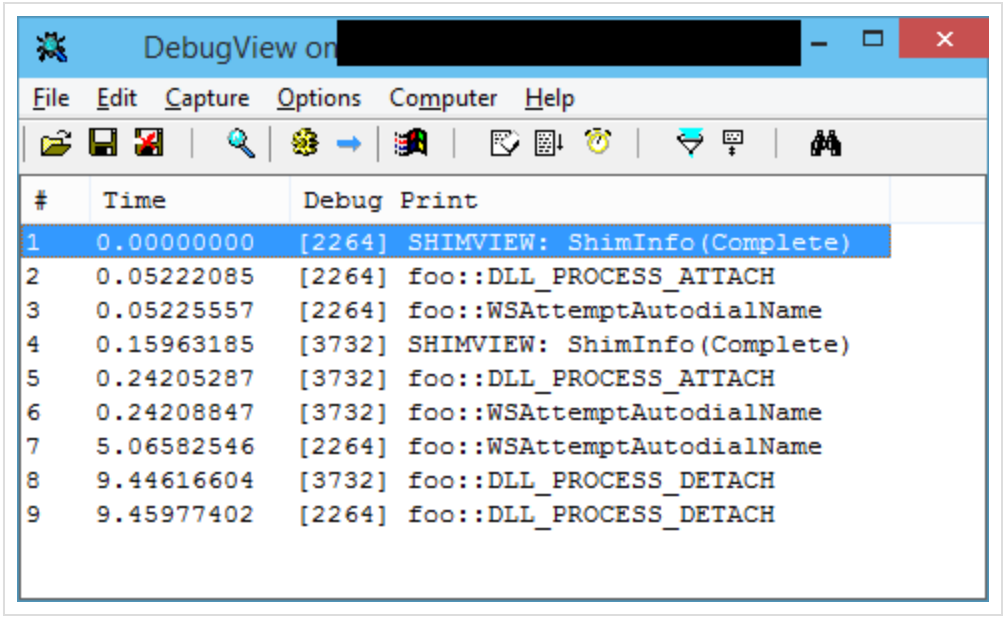
```
c:\temp\foo.dll
```

(the DLL exports the aforementioned APIs) can be seen below:



The screenshot was taken from a Windows XP system – I simply opened and closed Internet Explorer.

Of course, it works on Windows 10 too – just access to HKLM is slightly more difficult 🙄



This entry was posted in **Anti-Forensics**, **Autostart (Persistence)**, **Compromise Detection**, **Forensic Analysis**, **Malware Analysis** by **adam**. Bookmark the **permalink**.