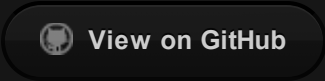


# ./ persistence-info.github.io



## Autodial DLL

### Location:

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

### Classification:

| Criteria         | Value                        |
|------------------|------------------------------|
| Permissions      | Admin                        |
| Security context | System <sup>1</sup>          |
| Persistence type | Registry                     |
| Code type        | DLL                          |
| Launch type      | Automatic <sup>2</sup>       |
| Impact           | Non-destructive <sup>3</sup> |
| OS version       | All OS versions              |
| Dependencies     | OS only                      |
| Toolset          | Scriptable                   |

### Description:

When winsock library connects to the internet it ‘talks’ to various service providers and probes them for connectivity services. [...] 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
```

## References:

<https://www.hexacorn.com/blog/2015/01/13/beyond-good-ol-run-key-part-24/>

## Credits:

[@Hexacorn](#)

## See also:

## Remarks:

1. Requires confirmation but it should be possible ↵
2. Requires confirmation ↵
3. Requires confirmation ↵