



## ODDVAR MOE'S BLOG

Notes from My adventures with Windows security

# PERSISTENCE USING RUNONCEEX – HIDDEN FROM AUTORUNS.EXE

TL;DR

# RunOnceEx



The string values within a  
...RunOnceEx\000  
xsection contain the commands that should be run for the section. The format is:

```
"  
  DllFileName|  
  FunctionName|  
  CommandLineArguments"
```

-or-

```
"||  
  command parameters"
```

For example:

```
"Line1" = "||my.exe -quiet -url http://www.microsoft.com/"
```

```
"Line2" = "shdocvw.dll|DllRegisterServer"
```

Line1 runs the "my.exe -quiet -url http://www.microsoft.com/" command line. Line2 runs the DllRegisterServer function in Shdocvw.dll.

## RunOnceEx with ||Executable.exe



RunOnceEx with DLLFile|Function



Autoruns - Sysinternals: [www.sysinternals.com](http://www.sysinternals.com)

File Entry Options Help

Filter:

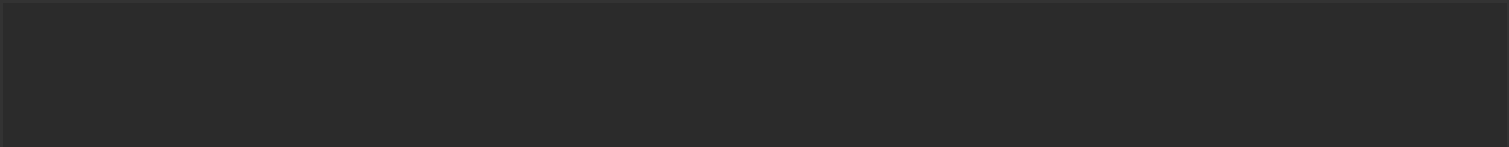
Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI

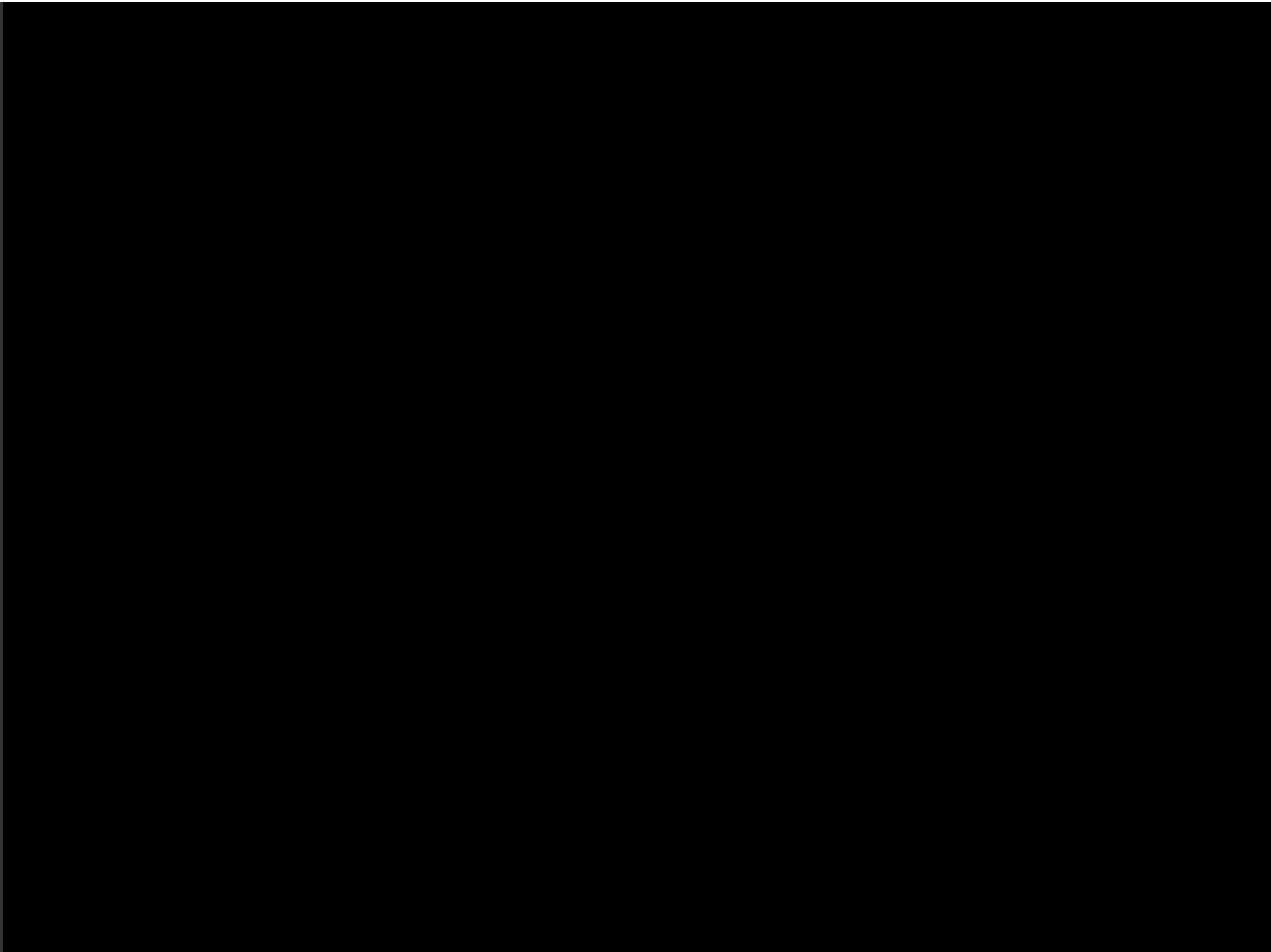
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				09.01.2018 20:24
<input checked="" type="checkbox"/> cmd.exe	Windows Command Proces...	Microsoft Corporation	c:\windows\system32\cmd.exe	23.01.1915 20:14
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				21.03.2018 13:34
<input checked="" type="checkbox"/> SecurityHealth	Windows Defender notifi...	Microsoft Corporation	c:\program files\windows defender\msascui.exe	26.09.1920 19:44
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				06.02.2018 13:10
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\admin\appdata\local\microsoft\onedrive\onedrive.exe	01.03.2018 07:07
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001				21.03.2018 18:53
<input checked="" type="checkbox"/> Line 1			c:\temp\test.exe	11.01.2018 12:41
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				09.01.2018 20:24
<input checked="" type="checkbox"/> Microsoft Wind...			File not found: C:\WINDOWS\inf\unregmp2.exe /ShowWMP.exe	
<input checked="" type="checkbox"/> n/a	Windows host process (Ru...	Microsoft Corporation	c:\windows\system32\rundll32.exe	02.04.2032 03:35
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				16.01.2018 12:40
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome\application\64.0.3282.186\installer\c...	22.02.2018 02:47
<input checked="" type="checkbox"/> n/a	Windows host process (Ru...	Microsoft Corporation	c:\windows\syswow64\rundll32.exe	24.02.1929 07:39

## Executing with Depend

The  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\000  
x\Depend  
registry key contains the .dll files and the .ocx files that should be kept in memory while section  
000  
xis running.





---

SHARE THIS:



---

PREVIOUS POST

NEXT POST

---

# 9 THOUGHTS ON “PERSISTENCE USING RUNONCEEX – HIDDEN FROM AUTORUNS.EXE”

wen





★ Oddvar Moe [MVP]



LEAVE A COMMENT

---



