
# 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
**x**section contain the commands that should be run for the section. The format is:

"
**DllFileName|**
**FunctionName|**
**CommandLineArguements**"

-or-

"||
**command parameters**"

For example:

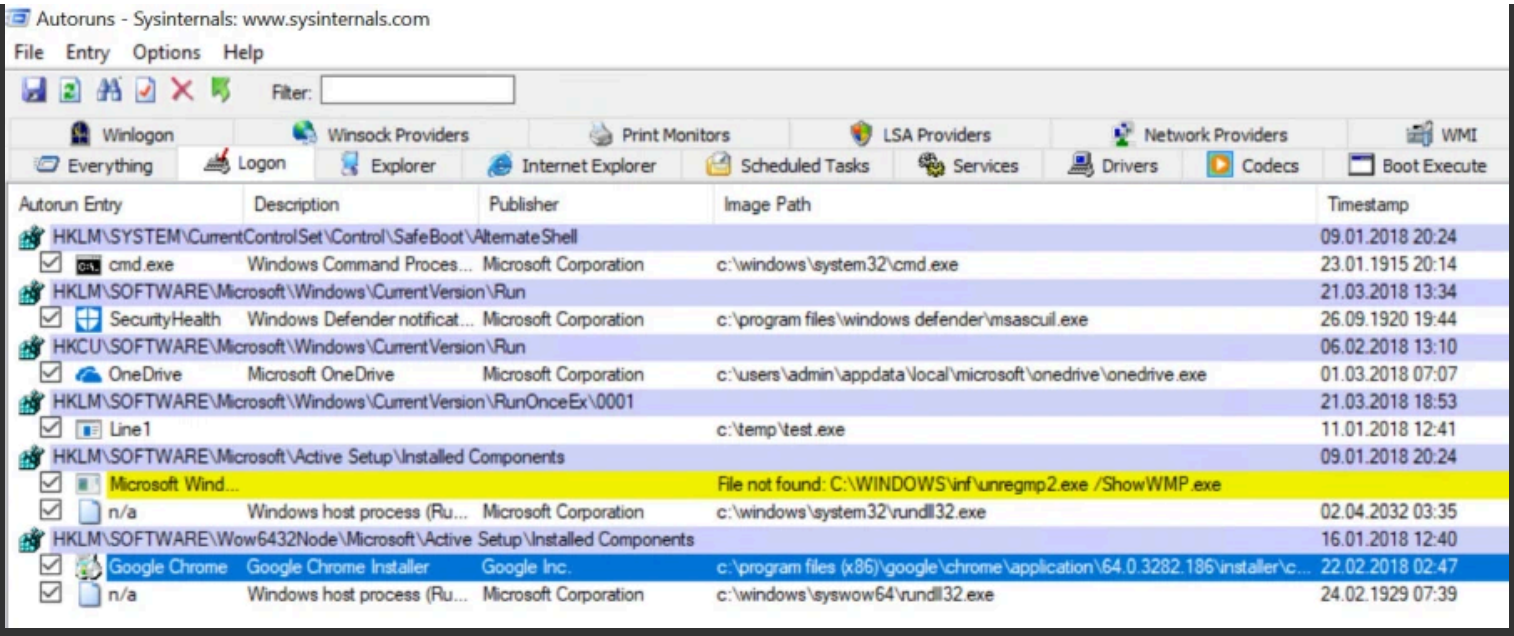
"Line1" = "||my.exe -quiet -url http://www.microsoft.com/"

"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.

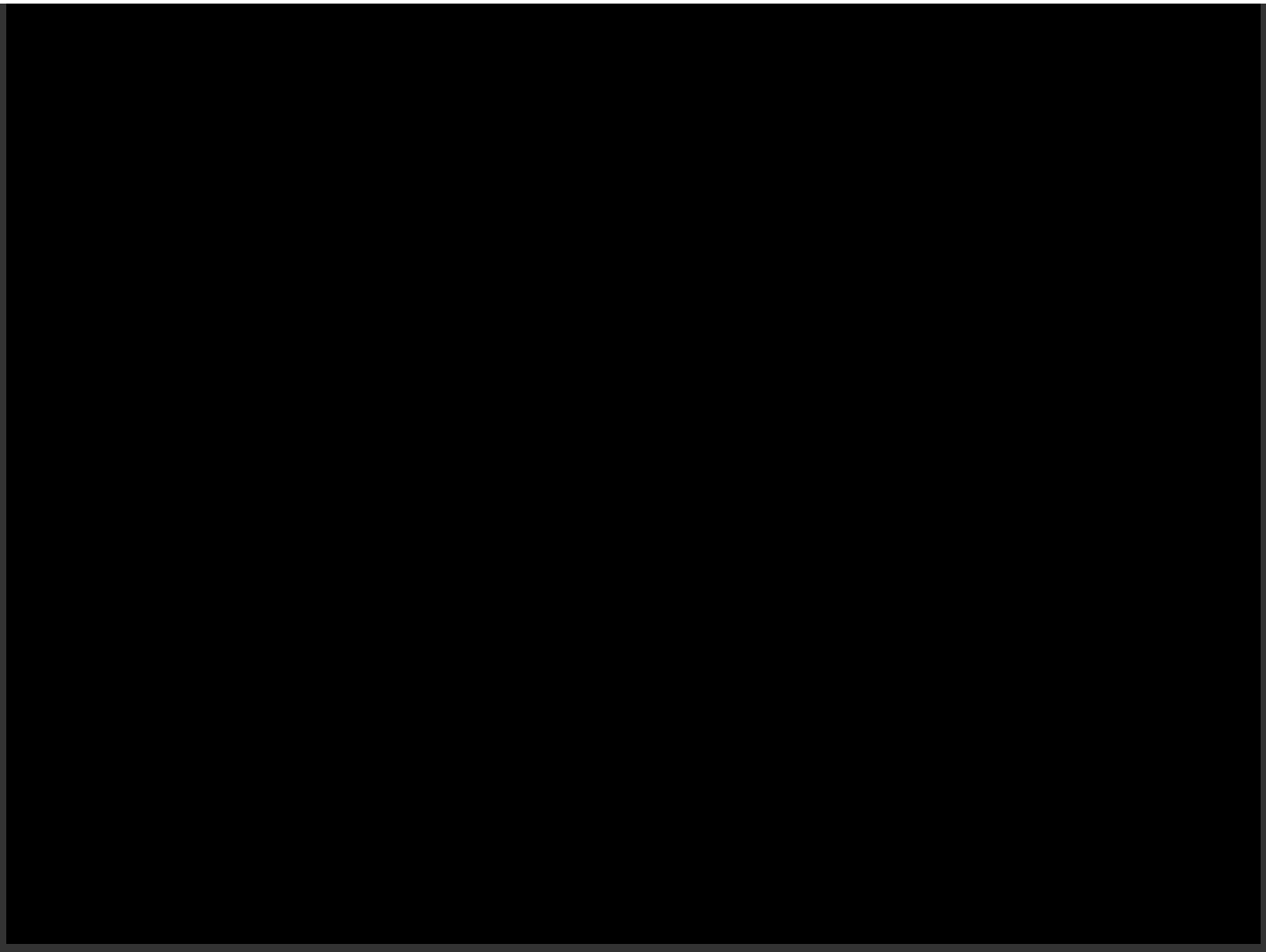
**RunOnceEx with ||Executable.exe**

**RunOnceEx with DLLFile|Function**




**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**x** is running.



SHARE THIS:

Twitter Facebook

PREVIOUS POST

NEXT POST

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

wen

★

★ Oddvar Moe [MVP]

★

## LEAVE A COMMENT