MENU

ODDVAR MOE'S BLOG

Notes from My adventures with Windows security

PERSISTENCE USING RUNONCEEX – HIDDEN FROM AUTORUNS.EXE

Posted on 21 Mar 2018

TL;DR

- Found a technique to execute DLL files without being detected by autoruns.exe at logon.
- Requires administrator rights and does not belong in userland.
- Run this to Exploit:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1
```

RunOnceEx

I finally had some time to do some unstructured research. With unstructured research I mean going after things you stumble upon and explore them. In this case I was looking into runonce.exe that lies in the system32 folder in Windows. I started out by running the command with /? and such, but did not give any results. I ended up Googling the file and stumbled upon this interesting article from Microsoft:

https://support.microsoft.com/en-us/help/310593/description-of-the-runonceex-registry-key

The thing that got my attention at first was these sentences here:

> Performance: The majority of the commands contained in the Run and RunOnce registry keys create separate processes, which is inefficient. The RunOnceEx registry key does not create a separate process. The RunOnceEx registry key also supports a dependency list of DLLs that remain loaded while either all the sections or some of the sections are being processed.

To me this meant that if I added these keys, the processes would probably execute directly in the parent process. It also meant that I could add a list of dependency DLL files that would be executed. That was very interesting and got me really curious.

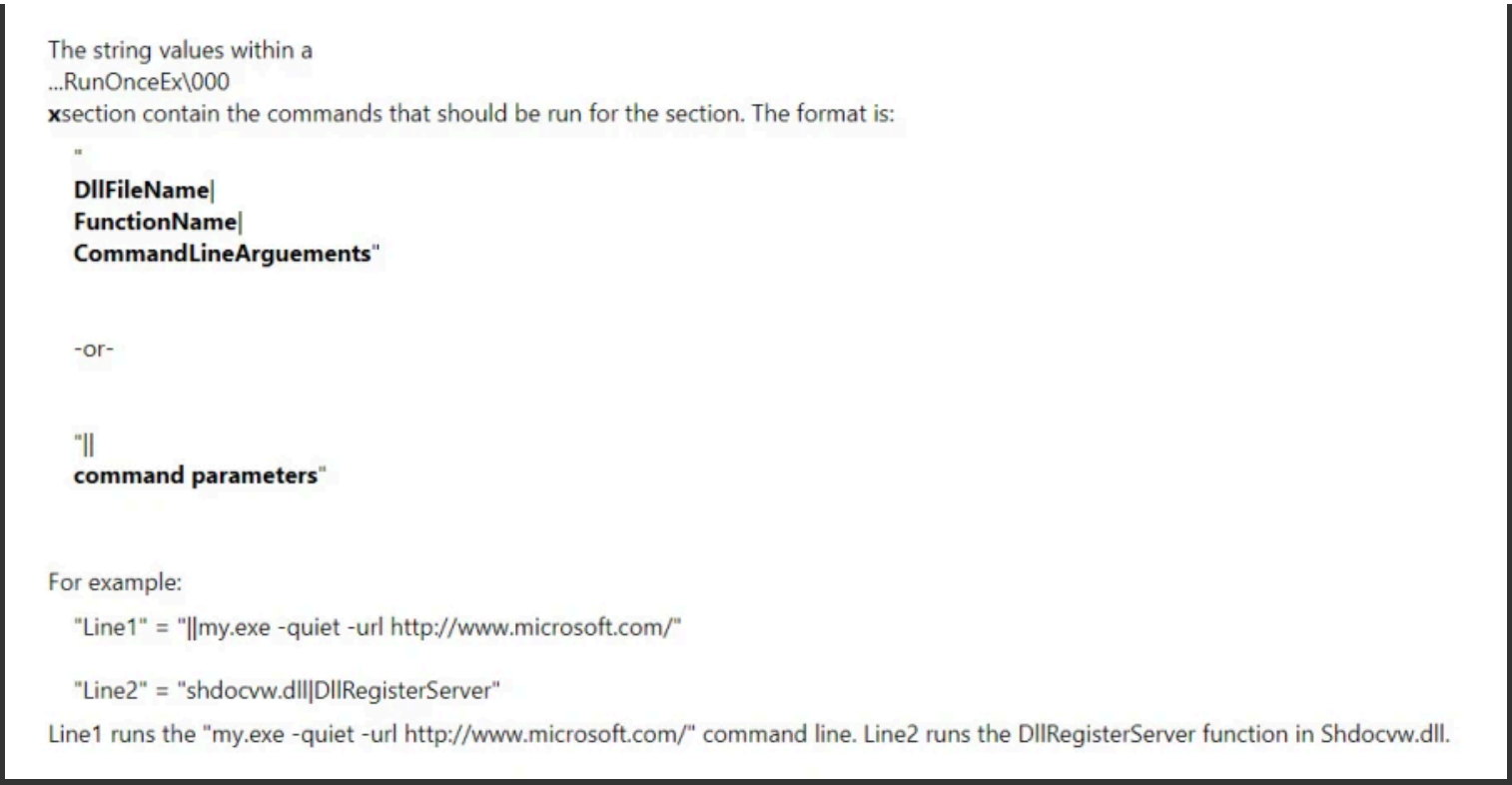
I then started to play around with the necessary registry keys. I first started in the HKEY_CURRENT_USER hive, but that did not provide any results at all. It turned out that after some Googling that the RunOnceEx only executes for administrators. This is explained in this KB from Microsoft:

https://support.microsoft.com/en-us/help/2021405/standard-user-runonce-and-runonceex-are-not-being-executed

It states that HKEY_CURRENT_USER RunOnceEx should execute for local admins, but this was not the case when I did the testing.

However I did get execution using the HKEY_LOCAL_MACHINE hive.

The documentation that I linked to at the top of this post also includes some examples.
Here is a screenshot of the most interesting part:



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

"
DllFileName|
FunctionName|
CommandLineArguements"

-or-

"||
command parameters"

For example:

"Line1" = "||my.exe -quet -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.

As you can see, it is possible to either specify an executable by using ||exename.exe or dll file by using DLLFilename|FunctionName|CommandLineArguements.

RunOnceEx with ||Executable.exe

In order to get execution of for example notepad.exe you must add the following registry keys (save them to .reg file and import them):

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001]
"Line1"="||c:\windows\system32\notepad.exe"
```

After adding these keys notepad.exe will launch at next logon. Or you can run this command to trigger the execution:

```
runonce /Explorer
```

I found that /Explorer parameter by running strings.exe against the runonce.exe binary.

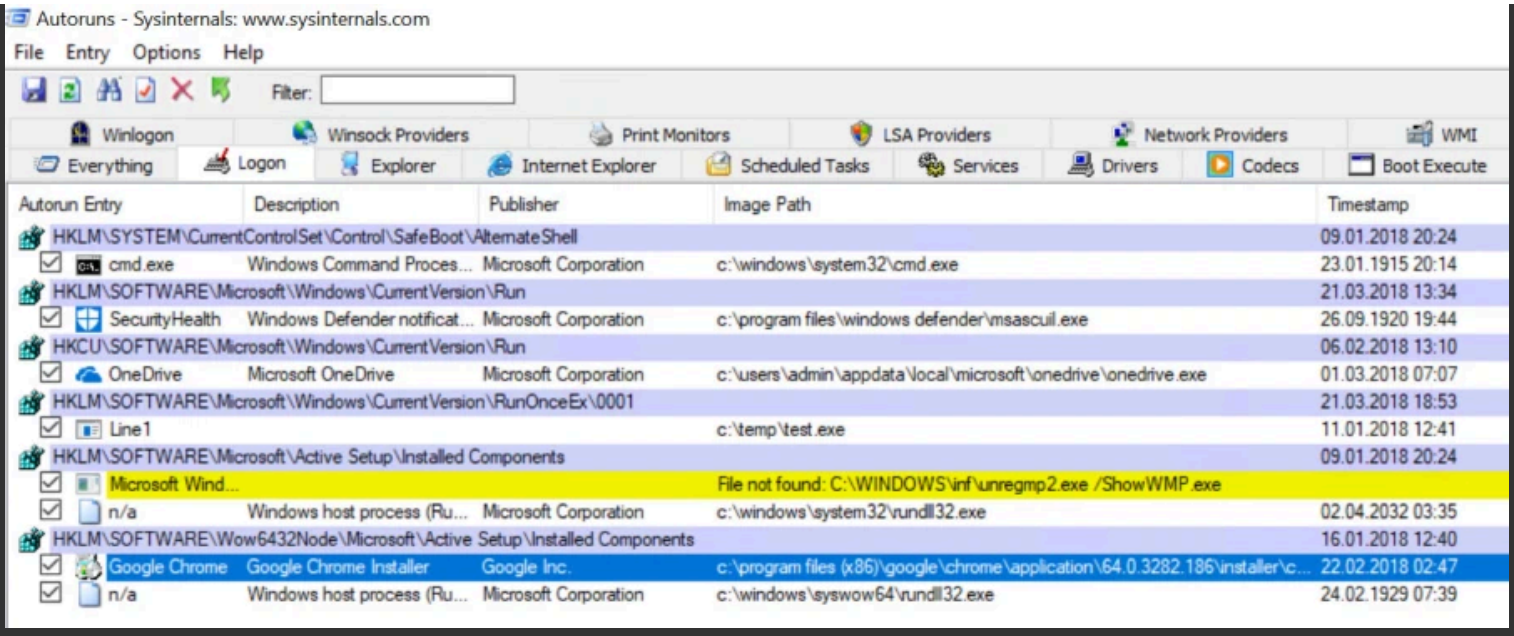
RunOnceEx with DLLFile|Function

Since I lacked creativity I just tried to open a URL using url.dll,OpenURL function (discovered by @bohops). In order to do that you must specify the registry keys like this:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001]
"Line1"="c:\windows\system32\url.dll|OpenURL|\"http://www.google.com\""
```

A thing I noticed when I was playing with this, was that the dll file must be registered. So it seems that you cannot just plant a dll file and execute it using this method.

The big problem with these approaches (from an offensive perspective) is that it will be pretty visible in the autoruns.exe application. In the screenshot below I am using a non signed binary just to show an example(Line1):



Executing with Depend

After I was done "playing" with this I decided that I would look into the part about dependent DLL files. And this is where the research became very interesting.

In the documentation (screenshot below) it gives an example using "depend", but it is unclear and I had to try and fail some times before I got it right.

> 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.

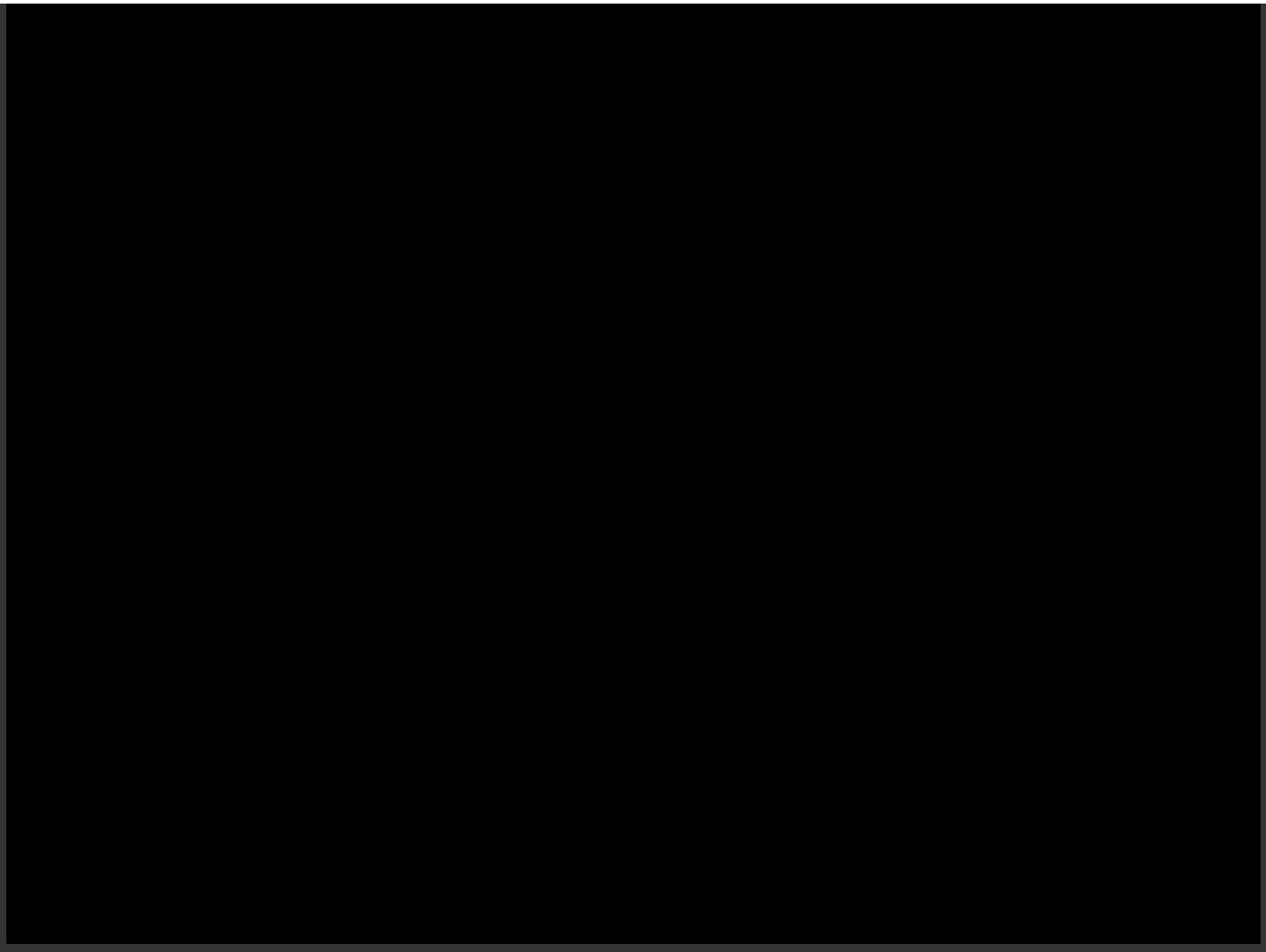
Just by adding this registry key, the dll file you specify will execute on next logon.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depe
"1"="c:\\temp\\MessageBox64.dll"
```

Or you can for example just execute this command:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1
```

The cool thing about this method is that it hides completely from autoruns.exe. Below is a video showing this technique.



I guess that this technique has already been used by other threat actors already. This is just another forgotten thing in Windows.
I know that this technique requires local administrator access, but still I find this interesting enough to blog about. Hope you liked it.

#Update – March 22 2018#
Mark Russinovich was thankful for the discovery and stated that this will be added in the next version of Autoruns.
https://twitter.com/markrussinovich/status/976856490941337600

#Update – December 16 2019#
Since this blog post is still linked to, just want to point out that this discover were added into autoruns 13.90 and newer:
https://blogs.technet.microsoft.com/sysinternals/2018/07/05/sysmon-v8-0-autoruns-v13-90/

RELATED

Research on CMSTP.exe
15 Aug 2017
In "Security"

AppLocker for admins – Does it work?
27 Jul 2018
In "Security"

Harden Windows with AppLocker – based on Case study part 1
13 Dec 2017
In "Security"

PREVIOUS POST
Windows Defender Attack Surface Reduction Rules bypass

NEXT POST
Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe

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

Pingback: Persistence using RunOnceEx – Hidden from Autoruns.exe – Information Security Outsider

wen says:
22 Mar 2018 at 11:42 am
i test in my windows server 2012 pc,when i add
“”Line1″=”||c:\windows\system32\notepad.exe”” ,autorun doesn’t detect it.

★ Like
Reply

★ **Oddvar Moe [MVP]** says:
22 Mar 2018 at 1:27 pm
Notepad.exe is a Windows binary. To detect it you have to unhide Windows entries from Autoruns.exe. or use a non ms signed binary.

★ Like
Reply

Pingback: Week 12 – 2018 – This Week In 4n6

Pingback: Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe – Oddvar Moe's Blog

Pingback: Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe – Information Security Outsider

Pingback: MOV AX, BX Code depilation salon: Articles, Code samples, Processor code documentation, Low-level programming, Working with debuggers List of Awesome Red Teaming Resources

Pingback: Persistence – Registry Run Keys | Penetration Testing Lab

Pingback: RED TEAMING_Final Att&ck – B4cKD00₹

LEAVE A COMMENT

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Search …

SEARCH