

RED TEAMER AND SECURITY ADDICT

ENIGMA0X3

« BYPASSING UAC ON WINDOWS 10 USING DISK CLEANUP

BYPASSING APPLICATION WHITELISTING BY USING DNX.EXE »

“FILELESS” UAC BYPASS USING EVENTVWR.EXE AND REGISTRY HIJACKING

August 15, 2016 by enigma0x3

After digging into Windows 10 and discovering a [rather interesting method for bypassing user account control](#), I decided to spend a little more time investigating other potential techniques for getting around UAC. Currently, there are a couple of public UAC bypass techniques, most of which require a privileged file copy using the IFileOperation COM object or WUSA extraction (Windows 7) to take advantage of a DLL hijack in a protected system location. All of these techniques require dropping a file to disk (for example, placing a DLL on disk to perform a DLL hijack). You can take a look at some of these public techniques [here](#) (by [@hfiref0x](#)). The technique covered in this post differs from the other public methods and provides a useful new technique that does not rely on a privileged file copy, code injection, or placing a traditional file on disk (such as a DLL). This technique has been tested on Windows 7 and Windows 10, but is expected to work on all versions of Windows that implement UAC.

As I mentioned in my last post on [bypassing UAC using Disk Cleanup](#), a common technique used to investigate loading behavior on Windows is to use [SysInternals Process Monitor](#) to analyze how a process behaves when executed. While digging into the Windows Event Log with ProcMon opened, I noticed that eventvwr.exe was executing some registry queries against the HKEY_CURRENT_USER hive as a high integrity process.

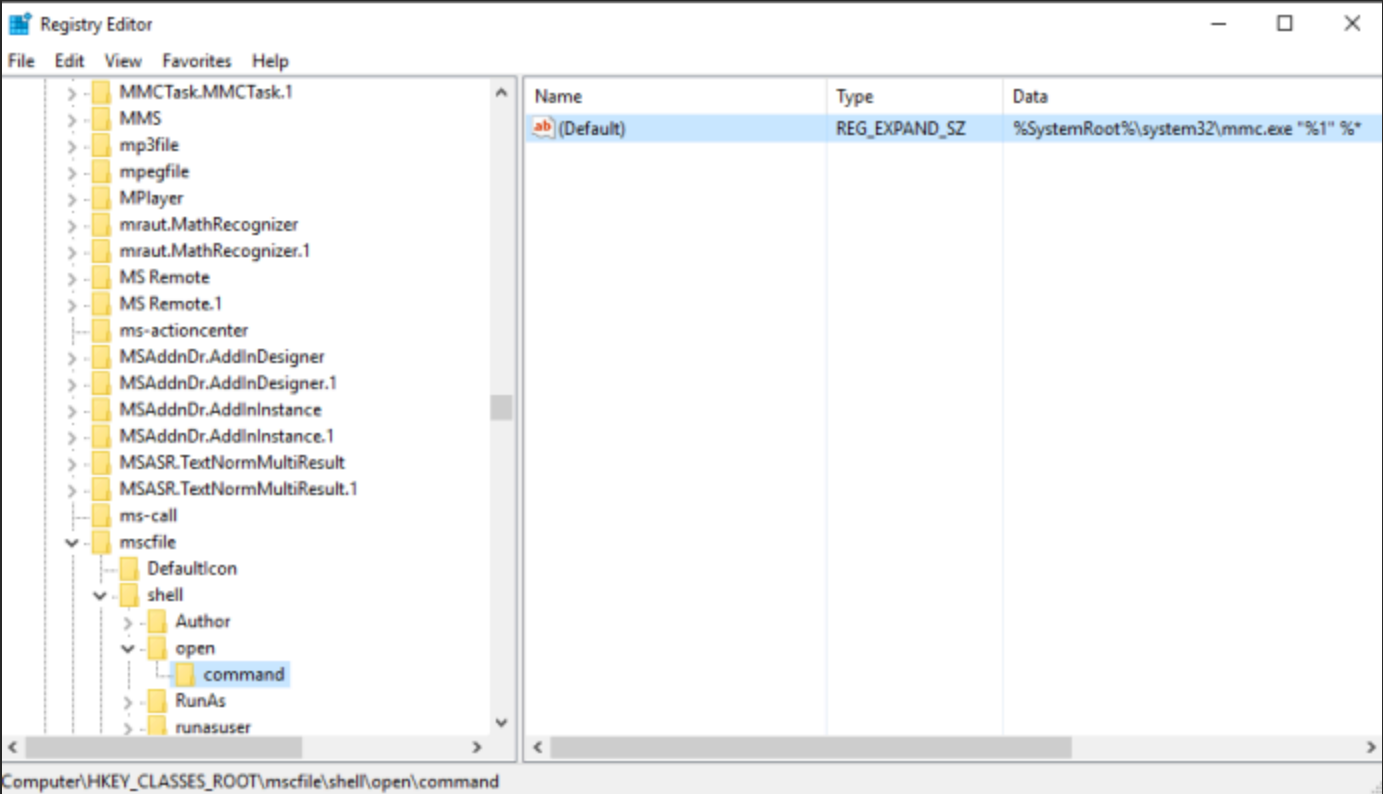
Before diving in too far, it is important to understand what the HKEY_CLASSES_ROOT (HKCR) and HKEY_CURRENT_USER (HKCU) registry hives are and how they interact. The HKCR hive is simply a combination of HKLM:\Software\Classes and HKCU:\Software\Classes. You can read more about HKCR and why the HKLM and HKCU hives are merged [here](#). Since these hives are merged, you can often hijack keys in HKCR:\ by creating them in HKCU:\Software\Classes. Since this relationship exists between these 2 hives, any elevated process that interacts with both HKCU and HKCR in succession are particularly interesting since you are able to tamper with values in HKCU. As a normal user, you have write access to keys in HKCU; if an elevated process interacts with keys you are able to manipulate, you can potentially interfere with actions a high-integrity process is attempting to perform.

Now, as some of you may know, there are some Microsoft signed binaries that auto-elevate due to their manifest. You can read more about these binaries and the manifests [here](#). By using the SysInternals tool “[sigcheck](#)”, I verified that “eventvwr.exe” auto-elevates due to its manifest:

```
<description>Event Viewer Snapin Launcher</description>

<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  <security>
    <requestedPrivileges>
      <requestedExecutionLevel
        level="highestAvailable"
        uiAccess="false"
      />
    </requestedPrivileges>
  </security>
</trustInfo>
<asmv3:application>
  <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
    <autoElevate>true</autoElevate>
  </asmv3:windowsSettings>
</asmv3:application>
</assembly>
```

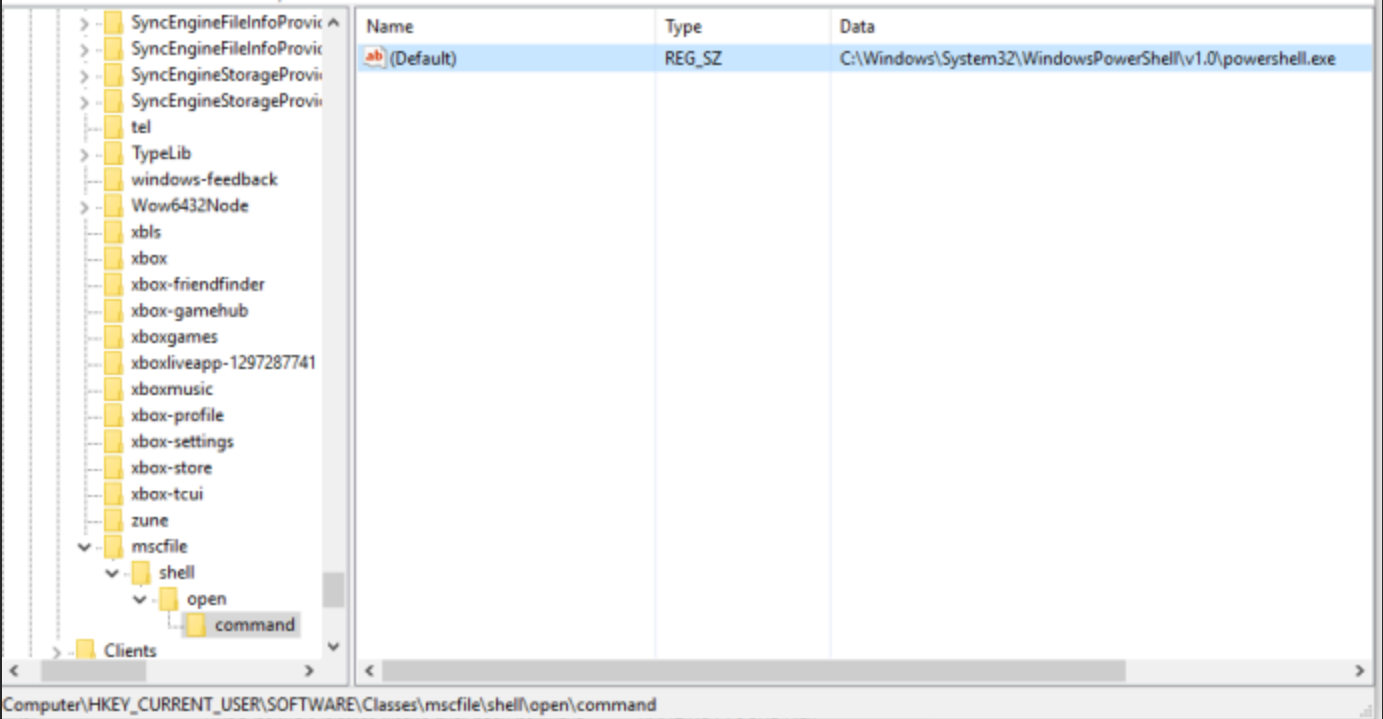
While digging deeper into the ProcMon output, I noticed that “eventvwr.exe” was interacting with **HKCU\Software\Classes\mscfile\shell\open\command**, which resulted in a “NAME NOT FOUND” result. Shortly after, eventvwr.exe was seen interacting with the key **HKCR\mscfile\shell\open\command**. Looking at **HKCR\mscfile\shell\open\command**, I noticed that the default value was set to call mmc.exe (Microsoft Management Console), the program responsible for loading Management Snap-Ins:



As mentioned above, calls to HKEY_CURRENT_USER (or HKCU) from a high integrity process are particularly interesting. This often means that an elevated process is somehow interacting with a registry location that a medium integrity process can tamper with. In this case, it was observed that “eventvwr.exe” was querying **HKCU\Software\Classes\mscfile\shell\open\command** before **HKCR\mscfile\shell\open\command**. Since the HKCU value returned with “NAME NOT FOUND”, the elevated process queried the HKCR location:

eventvwr.exe	3120	RegOpenKey	HKCU\Software\Classes\mscfile\shell\open\command	NAME NOT FOUND	High
eventvwr.exe	3120	RegQueryKey	HKCR\mscfile\shell\open	SUCCESS	High
eventvwr.exe	3120	RegOpenKey	HKCR\mscfile\shell\open\command	SUCCESS	High
eventvwr.exe	3120	RegQueryKey	HKCR\mscfile\shell\open\command	SUCCESS	High
eventvwr.exe	3120	RegQueryKey	HKCR\mscfile\shell\open\command	SUCCESS	High

From the output, it appears that “eventvwr.exe”, as a high integrity process, queries both HKCU and HKCR registry hives to start mmc.exe. After mmc.exe starts, it opens eventvwr.msc, which is a Microsoft Saved Console file, causing the Event Viewer to be displayed. This makes sense due to the fact that the Microsoft Management Console (mmc.exe) loads Microsoft Saved Console files (.msc). You can read more about the Microsoft Management Console and the corresponding Microsoft Saved Console files [here](#). With this information, I decided to create the registry structure needed for “eventvwr.exe” to successfully query the HKCU location instead of the HKCR location. Since the (Default) value located in **HKCR\mscfile\shell\open\command** contained an executable, I decided to simply replace the executable with powershell.exe:



When starting “eventvwr.exe”, I noticed that is successfully queried/opened **HKCU\Software\Classes\mscfile\shell\open\command**:

eventvwr.exe	4756	RegQueryKey	HKCU\Software\Classes\mscfile\shell\open	SUCCESS	High
eventvwr.exe	4756	RegQueryKey	HKCU\Software\Classes\mscfile\shell\open	SUCCESS	High
eventvwr.exe	4756	RegQueryKey	HKCU\Software\Classes\mscfile\shell\open	SUCCESS	High
eventvwr.exe	4756	RegOpenKey	HKCU\Software\Classes\mscfile\shell\open\command	SUCCESS	High
eventvwr.exe	4756	RegQueryKey	HKCU\Software\Classes\mscfile\shell\open\command	SUCCESS	High
eventvwr.exe	4756	RegQueryKey	HKCU\Software\Classes\mscfile\shell\open\command	SUCCESS	High

This action effectively replaced the expected “mmc.exe” value with our new value: “powershell.exe”. As the process continued, I observed that it ended up starting “powershell.exe” instead of “mmc.exe”:

eventvwr.exe	4756	Process Create	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	High
powershell.exe	820	Process Start		SUCCESS	High
powershell.exe	820	Thread Create		SUCCESS	High

Looking at Process Explorer, I was able to confirm that powershell.exe was indeed running as high integrity:

powershell.exe	0.02	56,436 K	63,552 K	820	Windows PowerShell	Microsoft Corporation	High
conhost.exe		4,340 K	9,268 K	348	Console Window Host	Microsoft Corporation	High

Due to the fact that I was able to hijack the process being started, it is possible to simply execute whatever malicious PowerShell script/command you wish. This means that code execution has been achieved in a high integrity process (bypassing UAC) without dropping a DLL or other file down to the file system. This significantly reduces the risk to the attacker because they aren’t placing a traditional file on the file system that can be caught by AV/HIPS or forensically identified later.

To demonstrate this attack, Matt Graeber (@[mattifestation](#)) and I constructed a PowerShell script that, when executed on a system, will create the required registry entry in the current user’s hive (**HKCU\Software\Classes\mscfile\shell\open\command**), set the default value to whatever you pass via the -Command parameter, run “eventvwr.exe” and then cleanup the registry entry.

You can find the script here: <https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-EventVwrBypass.ps1>

Within the script, we have provided an example command. This particular command uses PowerShell to write out “Is Elevated: True” to C:\UACBypassTest. This will demonstrate that the command has executed has a high integrity process due to the fact that “Is Elevated” equated to “True” and the text file it outputs is being written to a directory that a medium integrity process is not allowed to write to.

This technique differs from the other public techniques by having a few handy benefits:

1. This technique does not require dropping a traditional file to the file system. Most (if not all) public UAC bypasses currently require dropping a file (typically a DLL) to the file system. Doing so increases the risk of the attacker getting caught. Since this technique doesn’t drop a traditional file, that extra risk to the attacker is mitigated.
2. This technique does not require any process injection or evasion, meaning that the bypass isn’t flagged by security solutions that monitor for this type of behavior.

3. There is no privileged file copy required. Most UAC bypasses require some sort of privileged file copy in order to get a malicious DLL into a secure location to setup a DLL hijack. Since it is possible to replace what executable “eventvwr.exe” starts to load the required Snap-in, it is possible to simply use an existing, trusted Microsoft binary to execute code in memory instead.

This particular technique can be remediated or fixed by setting the UAC level to “Always Notify” or by removing the current user from the Local Administrators group. Further, if you would like to monitor for this attack, you could utilize methods/signatures to look for and alert on new registry entries in **HKCU\Software\Classes**.

SHARE THIS:

 Twitter

 Facebook

Loading...

RELATED

Bypassing UAC on Windows 10 using Disk Cleanup July 22, 2016 Liked by 1 person	Bypassing UAC using App Paths March 14, 2017 Liked by 2 people	“Fileless” UAC Bypass using sdclt.exe March 17, 2017
--	--	---

Bookmark the [permalink](#).

27 THOUGHTS ON ““FILELESS” UAC BYPASS USING EVENTVWR.EXE AND REGISTRY HIJACKING”

Pingback: [Latest Windows UAC Bypass Permits Code Execution | Threatpost | The first stop for security news](#)

- T says:

August 15, 2016 at 9:01 pm

Reply

Does this break event viewer? As in after modification of mmc.exe to our powershell script does event viewer still load?
- [enigma0x3](#) says:

August 15, 2016 at 9:32 pm

Reply

The PoC script will hijack the key, start eventvwr.exe (which starts powershell) and then once started, it deletes the created keys. Everything will work as expected afterwards.
- [SecGuy](#) says:

August 16, 2016 at 7:22 am

Reply

Hopefully security guys will catch up with your findings. What’s for sure, this will really help malware guys.

Apart from the above, nice work.
- [Phil Teale](#) says:

August 16, 2016 at 4:23 pm

Reply

There’s a typo in the final write.verbose line in your script – should read write.verbose rather than write.verboe
- [enigma0x3](#) says:

August 16, 2016 at 4:37 pm

Reply

Fixed. Thank you!

Pingback: [Windows Event Viewer Used for Malicious Code Execution – HOTforSecurity](#)

 Comment

 Reblog

 Subscribe



<div><div><div><div><div></div><div><u>jdorch</u></div><div>says:</div></div><div><div>August 17, 2016 at 11:45 pm</div><div>Reply</div></div></div></div></div>	<div>My UAC’s been sent to “Always Notify” since the feature debuted in Vista.</div>
<div><div><div><div><div></div><div><u>enigma0x3</u></div><div>says:</div></div><div><div>August 18, 2016 at 1:22 am</div><div>Reply</div></div></div></div></div>	<div>Awesome! Be aware that there are 2 public “Always Notify” UAC bypasses. Always recommended to not run as a local administrator.</div>
<div><div><div><div><div></div><div>Joe Brown</div><div>says:</div></div><div><div>August 19, 2016 at 8:55 pm</div><div></div></div></div></div></div>	<div>I also have my UAC set to always notify. I didn’t know there were any current bypasses for this setting. Can you direct me to some information that I can research this?</div>
<div><div><div><div><div></div><div><u>enigma0x3</u></div><div>says:</div></div><div><div>August 19, 2016 at 9:01 pm</div><div></div></div></div></div></div>	<div>1: https://enigma0x3.net/2016/07/22/bypassing-uac-on-windows-10-using-disk-cleanup/ 2: https://bugs.chromium.org/p/project-zero/issues/detail?id=156</div>
<div><div><div><div><div></div><div>Joe Brown</div><div>says:</div></div><div><div>August 29, 2016 at 6:26 pm</div><div></div></div></div></div></div>	<div>Thank you for the information!</div>
<div><div><div><div><div></div><div>Oliver</div><div>says:</div></div><div><div>September 16, 2016 at 8:39 pm</div><div></div></div></div></div></div>	<div>Does this fileless technique work with machines with the UAC ”Always Notify” level?</div>
<div><div><div><div><div></div><div><u>enigma0x3</u></div><div>says:</div></div><div><div>September 18, 2016 at 4:26 pm</div><div></div></div></div></div></div>	<div>This technique does not get around “always notify”. There are 2 public “Always Notify” bypasses. One for Windows 10 here: https://enigma0x3.net/2016/07/22/bypassing-uac-on-windows-10-using-disk-cleanup/ and one for 8.1 here: https://bugs.chromium.org/p/project-zero/issues/detail?id=156&can=1&q=uac</div>
<div><div><div><div><div></div><div><u>minxomat</u></div><div>says:</div></div><div><div>September 1, 2016 at 11:17 pm</div><div>Reply</div></div></div></div></div>	<div>Here’s a clean C implementation: https://github.com/minxomat/zero2hero</div>
<div><div><div><div><div></div><div><u>CS-Cart.com</u></div><div>says:</div></div><div><div>September 6, 2016 at 8:40 am</div><div>Reply</div></div></div></div></div>	<div>Many thanks for the suggestions, I will try to take advantage of it.</div>
<div><div><div><div><div></div><div>TH</div><div>says:</div></div><div><div>September 7, 2016 at 1:18 pm</div><div>Reply</div></div></div></div></div>	<div>Is there any requirements for the script to succeed in creating a file in C:\ folder. I’ve tried to run the Powershell script using a regular user account, but the file was not created.</div>
<div><div><div><div><div></div><div><u>enigma0x3</u></div><div>says:</div></div><div><div>September 18, 2016 at 4:27 pm</div><div>Reply</div></div></div></div></div>	<div>This is a UAC bypass, so you have to be running under the context of a local administrator with UAC on.</div>
<div><div><div><div><div></div><div><u>mjss</u></div><div>says:</div></div><div><div>December 30, 2016 at 9:55 pm</div><div>Reply</div></div></div></div></div>	<div>Does not work for Windows 10 (anymore). “eventvwr.exe” will not start if that “mscfile” path in the registry exists.</div>
<div><div><div><div><div></div><div><u>enigma0x3</u></div><div>says:</div></div><div><div>December 30, 2016 at 10:58 pm</div><div>Reply</div></div></div></div></div>	<div>What build? It works just fine on Version 1607 Build 14393.576</div>
<div><div><div><div><div></div><div><u>mjss</u></div><div>says:</div></div><div><div>December 31, 2016 at 12:48 pm</div><div></div></div></div></div></div>	<div>Sorry, I was wrong. Works fine, same build.</div>

Pingback: [Another example of maldoc string obfuscation, with extra bonus: UAC bypass, \(Sun, Mar 5th\) « CyberSafe NV](#)

Pingback: [Another example of maldoc string obfuscation, with extra bonus: UAC bypass, \(Sun, Mar 5th\) | Jeremy Murtishaw, Inc.](#)

Pingback: [Bypassing UAC using App Paths | enigma0x3](#)

Pingback: [NexusLogger: A New Cloud-based Keylogger Enters the Market - Palo Alto Networks Blog](#)

Pingback: [“Fileless” UAC Bypass using sdclt.exe | enigma0x3](#)

LEAVE A COMMENT

Search ...

Search

ARCHIVES

- [October 2023](#)
- [January 2020](#)
- [December 2019](#)
- [August 2019](#)
- [July 2019](#)
- [March 2019](#)
- [January 2019](#)
- [October 2018](#)
- [June 2018](#)
- [January 2018](#)
- [November 2017](#)
- [October 2017](#)
- [September 2017](#)
- [August 2017](#)
- [July 2017](#)
- [April 2017](#)
- [March 2017](#)
- [January 2017](#)
- [November 2016](#)
- [August 2016](#)
- [July 2016](#)
- [May 2016](#)
- [March 2016](#)
- [February 2016](#)
- [January 2016](#)
- [October 2015](#)
- [August 2015](#)
- [April 2015](#)
- [March 2015](#)
- [January 2015](#)
- [October 2014](#)
- [July 2014](#)
- [June 2014](#)
- [March 2014](#)
- [January 2014](#)

RECENT POSTS

- [CVE-2023-4632: Local Privilege Escalation in Lenovo System Updater](#)
- [Avira VPN Local Privilege Escalation via Insecure Update Location](#)
- [CVE-2019-19248: Local Privilege Escalation in EA's Origin Client](#)
- [Avira Optimizer Local Privilege Escalation](#)
- [CVE-2019-13382: Local Privilege Escalation in SnagIt](#)

CATEGORIES

- [Uncategorized](#)

RECENT COMMENTS

- Ron on [CVE-2019-13382: Local Privilege Escalation in SnagIt](#)

enigma0x3 on [CVE-2019-13382: Local Privilege Escalation in SnagIt](#)

Ron on [CVE-2019-13382: Local Privilege Escalation in SnagIt](#)

Soc on [Defeating Device Guard: A look at the possibilities](#)

“Fileless...” on [“Fileless” UAC Bypass using sdclt.exe](#)

META

- [Register](#)
- [Log in](#)
- [Entries feed](#)
- [Comments feed](#)
- [WordPress.com](#)