Posted on **2019-02-15**

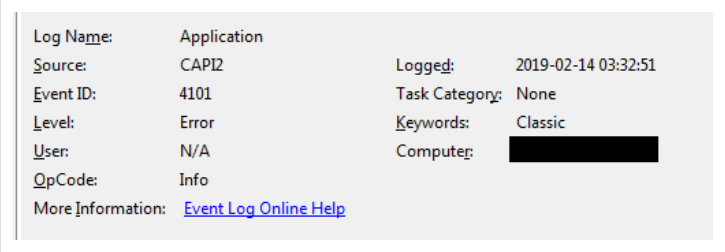
← Previous **Next →**

Beyond good ol' Run key, Part 103

This is yet another feature of Windows. This time it is a configuration settings for Event Viewer.

When you open the program via *eventvr.exe/msc* it will launch the *mmc.exe* which in turn will load an Event Viewer snap-in. The Event Viewer allows to view the system / application logs that we all should be familiar with.

As part of an user experience the Event Viewer offers a clickable *Event Log Online Help* link:



When the link is clicked, the *mmc.exe* will open a default help Microsoft link which will be rendered by the currently set up (default) browser.

It turns out that the default setting of this feature can be changed. It is very nicely described here, but the bottom line is that we can launch a program of our choice instead of the default browser; we just need to modify one, or more of the following registry entries:

```
HKLM\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Event Viewer\
```

- MicrosoftRedirectionURL=<url>
- MicrosoftRedirectionProgramCommandLineParameters=<args>
- MicrosoftRedirectionProgram=<program>

The *MicrosoftRedirectionURL* can be changed to e.g. *file://c:\windows\system32\notepad.exe*, or *MicrosoftRedirectionProgram* can point to the executable directly. One can also tinker with the command line parameters e.g. in a combo with a lolbin.

There is one gotcha moment while setting up this thing – there exist *Wow6432Node* equivalent for these entries, but they don't seem to be usable; even if entries under this key are changed, and the Event Viewer is launched from a *syswow64* directory (to enforce 32-bit version), the OS will still launch the proper 64-bit version anyway. Perhaps there is a way to enforce the 32-bit version to run, but I have not explored it

Also, we want to ensure the user is not asked for approval to send the data from the log to Microsoft (this dialog box shows up before the program is ran):

To do so, we just need to ensure this DWORD is changed to 0:

```
HKCU\Software\Microsoft\Windows NT\
CurrentVersion\Event Viewer\ConfirmUrl=0
```

And that's it. Plus, it's time for a small bonus.

While I was playing around with Event Viewer, I noticed that it uses Richedit control to render the data it shows. One of the features of this control is that it is automatically recognizing URLs embedded inside the data. As such, it highlights them and make them clickable.

A malicious user could inject a malicious link pointing to a full path on a disk into the logs (e.g. if sysmon is logging, or 4688+cmd line logging is enabled), and then make the richedit convert this path into a clickable link. When I posted this discovery on Twitter, it got immediately evilriched by Brent Muir, who asked if it could be used as a privilege escalation. This was confirmed by me and Csaba Fitzl in the same thread. Thanks to everyone who chipped in on that thread.

This entry was posted in **Anti-Forensics**, **Autostart (Persistence)** by **adam**. Bookmark the **permalink**.