Posted on **2018-08-31**

← Previous Next →

Beyond good ol' Run key, Part 85

This is a LOLbinish 2-stage persistence trick. One where we add startup items to point to OS binaries, and – while they will be ignored by many users and security solutions (at least at first glance) – they will be launching the second stage of the persistence mechanism for us…

Many people who use win7-win10 know that the Werfault.exe process is all over the place. It's a process 'repairer' or 'fixer' that handles crashes or other unpleasant activities of other processes. It turns out you can launch werfault.exe with a number of specific command line arguments. One of these modes is called 'reflective debugger' and is very interesting to us. To launch werfault in this mode we need to provide the following parameters:

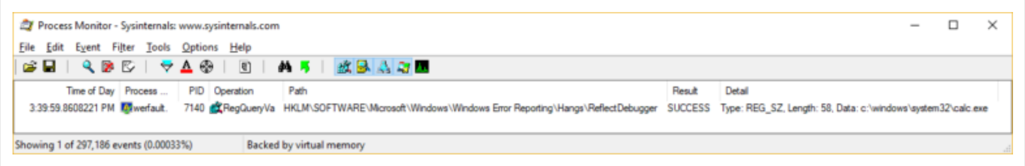
- werfault.exe -pr <somevalue>

And how does it load the debugger?

By reading:

- HKLM\Software\Microsoft\Windows\Windows Error Reporting\Hangs\ReflectDebugger=<path>

and… executing it.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
     Time of Day   Process ...  PID  Operation    Path                                                                       Result   Detail
3:39:59.8608221 PM werfault.   7140  RegQueryVa   HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs\ReflectDebugger  SUCCESS  Type: REG_SZ, Length: 58, Data: c:\windows\system32\calc.exe
Showing 1 of 297,186 events (0.00033%)        Backed by virtual memory
```

That’s it.

So if we add a Run key like this:

– it will in the end launch our program of choice when the user logs on.

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

Privacy Policy | **Proudly powered by WordPress**