Behavior Analysis and Detection of Bashware

Andrei Mermeze
email andrei.mermeze@gmail.com

Contents

1. State of the art

2. Used technologies

2.1 WDM

2.1.1 Legacy Filter Drivers

2.1.2 File System Legacy Filter and Minifilter Drivers

A Legacy Filter driver is a kernel-mode that could attach to a device's stack. In the context of file system filtering, these filter drivers could intercept file system I/O operations. Developing legacy filter drivers was quite troublesome and led to many incompatibilities between filter drivers. This is one of the reasons for which minifilter drivers were added.

Minifilters have the same abilities as file system legacy filter drivers, but they are easier to develop and are overall safer. Their load order no longer depends on the attach order, but on a predefined value named altitude. Minifilters are managed by FltMgr, which is a legacy filter driver implemented by microsoft.

2.2 C++ in Kernel Drivers

3. Architecture

3.1 High Level Overview

The system is composed of 4 main components

- wslflt.sys
- wslcore.dll
- wslsvc.exe
- wslam.exe

3.2 wslflt.sys

Wslflt.sys is minifilter driver that contains the requirued sensor for monitoring process' activity. It the components that filter disk I/O, process creation/termination and thread creation/termination.

It's key components are the process filter, file filter, event dispatcher, the communication framework and the detection heuristics.

3.3 wslcore.dll

This dll is an abstraction of the wslflt.sys driver. It contains the communication logic between kernel-mode and user-mode and exports multiple callbacks to an integrator. It's main purpose is to hide the filtering and detection logic and to provide an easy way to integrate the system in a complete security solution.

3.4 wslsvc.exe

Wslsvc.exe is Windows service that integrates the previously mentioned DLL.

3.5 wslam.exe

4. Implementation

4.1 Process Filter Implementation

```
            PsSetCreateProcessNotifyRoutineEx2(a, b);
```

5. Testing

6. Heuristics and Detection Algorithms

7. Performance impact analysis

8. Possible improvements

References

[1] https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/introduction-to-wdm/. [Online].

[2] Pavel Yosifovich et al. “Windows Internals, Part 1: System architecture, processes, threads, memory management, and more”. In: 2017.