A Behavioral Analysis Approach on Bashware Detection

Mermeze Andrei[1], Dragos Radu[2]

[1]) First affiliation
andrei.mermeze@gmail.com
[2]) Second affiliation
radu.dragos@cs.ubbcluj.ro

The release of Windows Subsystem for Linux (WSL) revealed a new attack surface, comprised of kernel drivers as well as user-mode components. The performed research is going to present how behavioral detection techniques can be applied for detecting potential threats that abuse WSL. This paper will provide an insight into the security issues created by this subsystem, while also explore Kernel-Mode based detection heuristics and techniques in order to identify and block this new type of malware.

The purpose of this work was to design and implement a reliable monitoring system and to come up with several detection algorithms in order to offer a defense mechanism against malicious WSL programs. This was achieved by implementing a kernel-mode driver that provided the monitoring and detection mechanisms and integrating it in a product that is deliverable to an end-user.

The thesis can be divided in four main parts. The first part consisting of chapter 2 will contain the current state of WSL and how it may be used to run malicious programs, how it can bypass monitoring tools and anti-malware solutions and explain some exploits that target WSL.

The second part, ranging from chapter 3 to chapter 7, presents the technologies and the reasons why they were used in order to develop the application as a whole, its architecture along with some implementation details and finally the testing process.

The third part consists of chapter 7 and will be dedicated to describing the detection algorithms logic and what steps I followed in creating them, as well as some implementation details and limitations.

Lastly, chapter 8 will show possible development directions for this project, how the current monitoring solution can be improved and how it could be extended to achieve more in-depth monitoring and more accurate detection.

This work is the result of my own activity. I have neither given nor received unauthorized assistance on this work.

MERMEZE Andrei