**The Threat**

We all leave our digital devices, laptops and smartphones, unattended sometimes. It might be at the office, at the library or at the local coffee shop. We believe they are protected by our passwords, PINs or fingerprints. Well, that is not completely true. Evil maid Attacks allow the attacker to bypass these protections easily, by using an exploitable vulnerability in the lock screen, overriding the need for password. These attacks allow the attackers to gain access to data on the device, impersonate the user and execute malicious code. And the worse part is – there is no solution today that can protect your device against these attacks.

**Project Goal**

Design and implement a system for Windows 10 that detects Evil Maid attacks and stops them in real-time.

**Our Results**

We defined and implemented a PoC of an innovative defense system whose purpose is to protect devices against this threat. The system is designed to stop both known and unknown attacks, based on heuristics. The system is based on a state-machine that escalates in response to different events in the device, and then triggers its different defense mechanisms fitting these events. Finally, we demonstrated our system’s capabilities in a real-time simulation of different attacks, all while distinguishing a malicious entity from a legitimate user.

When the design was tested against an unknown attack, our system fully detected, disrupted it, and alerted the user.

**Innovation**

• First system to defend against Evil Maid attacks in Windows 10.
• Embracing the EDR approach and applying it in a whole new domain – Detect malicious activity and not malicious files.
• The ability to detect unknown attacks and zero-day exploits.
• Special care to user experience – the Achilles heel of protective systems. Achieved by defining multiple alert levels with different reaction based on events analysis and utilizing a scoring system.