



# FSD – File System Defender

As part of project in ransomware, Spring 2018



Alexander Gurevich and Denys Svyschov

Assaf Rosenbaum

**FSD protects your PC against ransomware and guaranties zero file loss even in case of successful Ransomware attack.**

**FSD uses kernel module to filter filesystem activities and uses heuristics to detect Ransomware like behavior.**

**We protect your private files and backup them to Azure Cloud Storage.**

- Configure FSD using FSD Manager
- Set folder you want to protect
- FSD Manager backup your private files to Azure
- FSD Driver Module filters relevant IRPs (I/O request packet)
- FSD Manager receives IRPs information from Driver Module and analyzes them
- When FSD Manager detect a threat, it signals Kernel Module to kill malicious process and gives user a notification, that thread was detected, and instructions to backup saved files
- No files are lost during the attack thanks to backup

## Detection techniques:

- Measurement of writes entropy (Shannon's entropy)
- Comparison of file modifications ("distance" between initial and final file)
- File type changes
- Statistics of file access types

**Multiple indicators provide low false positive results and high accuracy**

