DAY 2

Common Windows APIs used by Malware

- Static Analysis of these APIs using IDA (Practical)
- Understanding Windows APIs
- Why are these specific APIs used by malware
- Dynamic Analysis of those APIs using WinDbg(Practical)

Understanding the PE file format

- Learning to use a Hex Editor
  - Practical walkthrough
  - Understanding & learning to use
- Anatomy of a PE file
  - DOS Header
  - DOS Stub
  - PE File Header
  - Image Optional Header
  - Section Table
  - Sections
  - Learning to use PEViewer
  - Looking into the Imports & Exports
  - Following the trail with IDA
- Packers vs. PE (malware specific)
  - Understanding UPX
  - Learning to use DIE
  - Understanding Morphine & Themida
  - Life of a unpacked binary (birth of the packer internals) (Practical)
  - Detecting Packers with PeiD

Getting started with the System Internals (Windows)

- Setting up WinDbg for Kernel Mode
- Execution Modes
- Privilege Rings
- Interrupts
- Paging
- Port I/O
- System Calls
- MSRs
- Registry
- Kernel Mode vS User Mode
- Key system components of Windows

Practicals

TBD