

# What do smart good folks do ...

- ➡ Analysis for IoC extraction, trend reports, detection engineering
- ➡ Static analysis
- ➡ Dynamic analysis
- ➡ Often a hybrid approach
- ➡ Operational Security (OPSEC) to protect analysis infrastructure
- ➡ Online repositories: VT, Anyrun, VXIntel etc

# Malware Anti-analysis