CyBOK

The Cyber Security
Body of Knowledge

Malware and Attack Technologies Knowledge
Tree

COPYRIGHT

malware taxonomy

dimensions
- standalone or host-program
- persistent or transient
- layers of system stack
- auto-spreading
- dynamically updatable
- coordinated

kinds
- viruses
- malicious browser extensions
- botnet malware
- memory-resident malware
- advanced persistent threats

potentially unwanted programs

malicious activities by malware

attacks on
- confidentiality
- integrity
- availability

cyber kill chain
- reconnaissance
- weaponisation
- delivery
- exploitation
- installation
- command and control
- actions on objectives

underground eco-system

malware analysis

analysis techniques
- static analysis
- dynamic analysis
- fuzzing
- symbolic execution
- concolic execution
  - offline concolic execution
  - online concolic execution
  - hybrid execution
  - path exploration

analysis environments
- environments
  - machine emulator
  - type 2 hypervisor
  - type 1 hypervisor
  - bare-metal machine
- safety and live-environment requirements
- virtualised network environments

anti-analysis and evasion techniques
- obfuscation
  - packing
  - code emulation
- basic blocks
- tracing
- fingerprinting
- multi-path analysis

indentifying the analysis environment
- red pill techniques
- mitigations

malware detection

identifying the presence of malware
- malware distribution methods
- malware infection sites
- runtime detection

evasion and countermeasures
- heuristics
- polymorphism
- update routines

attack detection
- network monitoring
  - host-based
  - network-based
  - spam detection
  - DDoS detection
  - ransomware detection
  - botnet detection
- machine learning-based security analytics
- limitations
  - machine learning countermeasures

malware response

disrupting malware operations
- DNS fast-flux
- domain-name generation algorithms
- command and control takedown
- P2P takedown

attribution
- historical signatures
- WHOIS