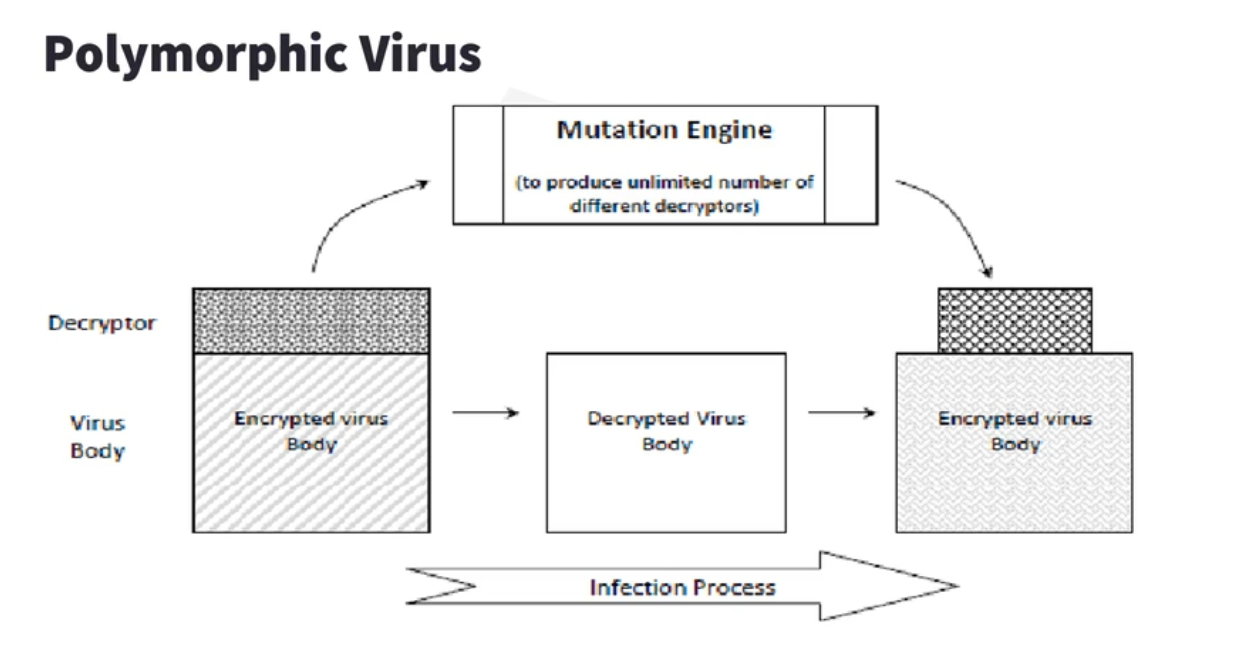
**Module 5 Malware**

**5.0 Malware Viruses**

**Malware**

1. Malicious program/code
2. Symptoms
   1. Comp slows down/crash/freeze
   2. Ad pop-ups
   3. System resources used high
   4. New toolbars/extensions in browser
   5. Antivirus disabled
3. How to get?
   1. Visit hacked websites
   2. Using game demos
   3. Download infected music files
   4. Open malicious email attachments
   5. Can also hide in seemingly legit apps

**Viruses**

1. Malicious program that can self-replicate
   1. Attach to another file & move from host to host
   2. Virus needs some kind of host program to propagate
2. Steps
   1. Design – develop virus code using programming languages/construction kits
   2. Replication – virus replicates for long period of time within target system & spreads itself
   3. Launch – activated with user performing actions like triggering/running infected program
   4. Detection – identified as threat
   5. Incorporation – antivirus assimilate defences against virus
   6. Elimination – users advised to install antivirus updates thus creating awareness
3. Types
   1. Boot sector
      1. Moves boot sector to another location on drive
      2. Causes virus code to be executed first
   2. Ransomware
      1. Locks you out of system resources & demands payment
      2. Eg. SamSam, WannaCash, Locky, CyptoLocker
   3. Shell
      1. Wraps itself around code of app, allowing it to run own code before app’s code everytime
   4. Cluster
      1. Modifies discovery table entries so system & user processes pointed to virus code itself
   5. Multipartite
      1. Attempts to infect boot sector & files at same time
      2. Virus with multiple infection vectors
   6. Macro
      1. Infects template files created by Microsoft Office (normally Word or Excel)
   7. Polymorphic code
      1. Mutates code (polymorphic engine) so signature constantly changes
      2. 
   8. Encryption
      1. Use encryption to evade antivirus detection
      2. Many viruses use this feature
   9. Metamorphic
      1. Rewrites itself everytime it infects new file
   10. Stealth
       1. Attempts to evade AV by intercepting AV’s request to OS
       2. Virus alters request to show its uninfected & sends request back to AV
       3. AKA tunnelling virus
   11. Cavity
       1. Overwrites portions (null content sections) of host fioes so it doesn’t increase size of files
   12. Sparse infector
       1. Only infects occasionally
       2. Eg. every 5th time or specific date
   13. File extension
       1. Changes file ext & take advantage of people that have file ext view turned off
       2. Eg. readme.txt.vbs show as readme.txt as file ext turned off