Malware Families

What is a malware family

Set of malicious samples that have mostly the same source code as a basis

Tips for malware family identification

- **MALPEDIA**
  library of malware families and article references
- **DETECTION NAMES**
  may give a hint to the family
- **BLOG ARTICLES**
  verify that your analysis matches description
- **BINARY DIFFING**
  verify code overlaps
- **STRING SEARCH**
  search unique strings you find in binary
- **LOOK FOR ALIASES**
  many families have several names