Malware analysis- to disarm malware sample add extension .malz with the sample name

STATIC ANALYSIS

1. Find hashes -> check in VT
2. Strings (floss)
3. Peview – virtual memory, size of raw data, file header (text, .rdata, data(IAT + EAT), .rsrc, .reloc)
4. Hex values in hexeditor
5. Windows API -> look at import address table for APIs (malapi[.]io)
6. To check whether malware is packed or not- UPX (can check in PEview -UPX 0, UPX 1)
7. PEstudio /Detectiteasy

DYNAMIC ANALYSIS- use REMNUX, and FlareVM

1. HOST – delete files, install persistence,
2. NETWORK – calls out to domain, downloads a file,
3. Use Remnux box as internet simulation by running INETSIM in that and listening instance of wireshark
4. Sysinternals suite – use procmon,