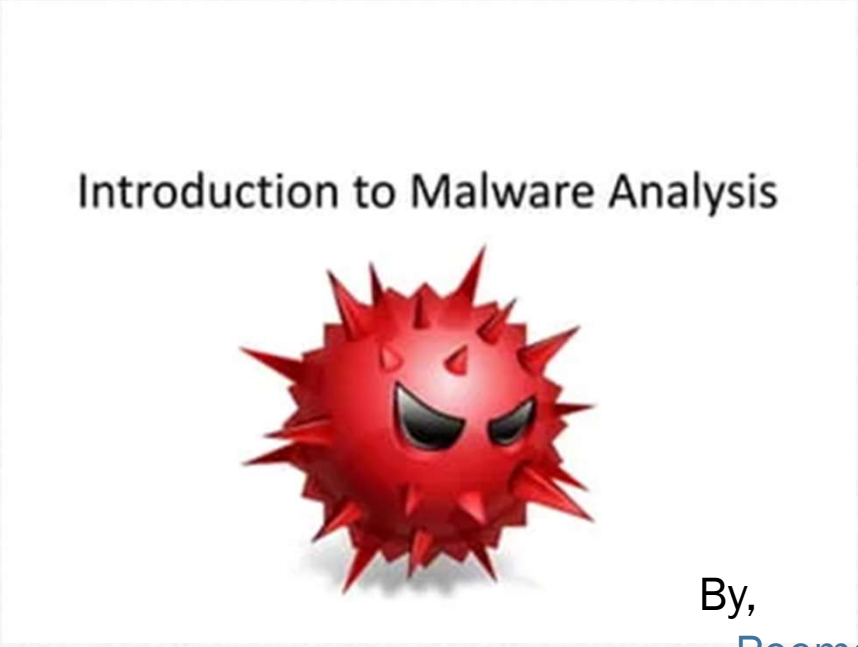
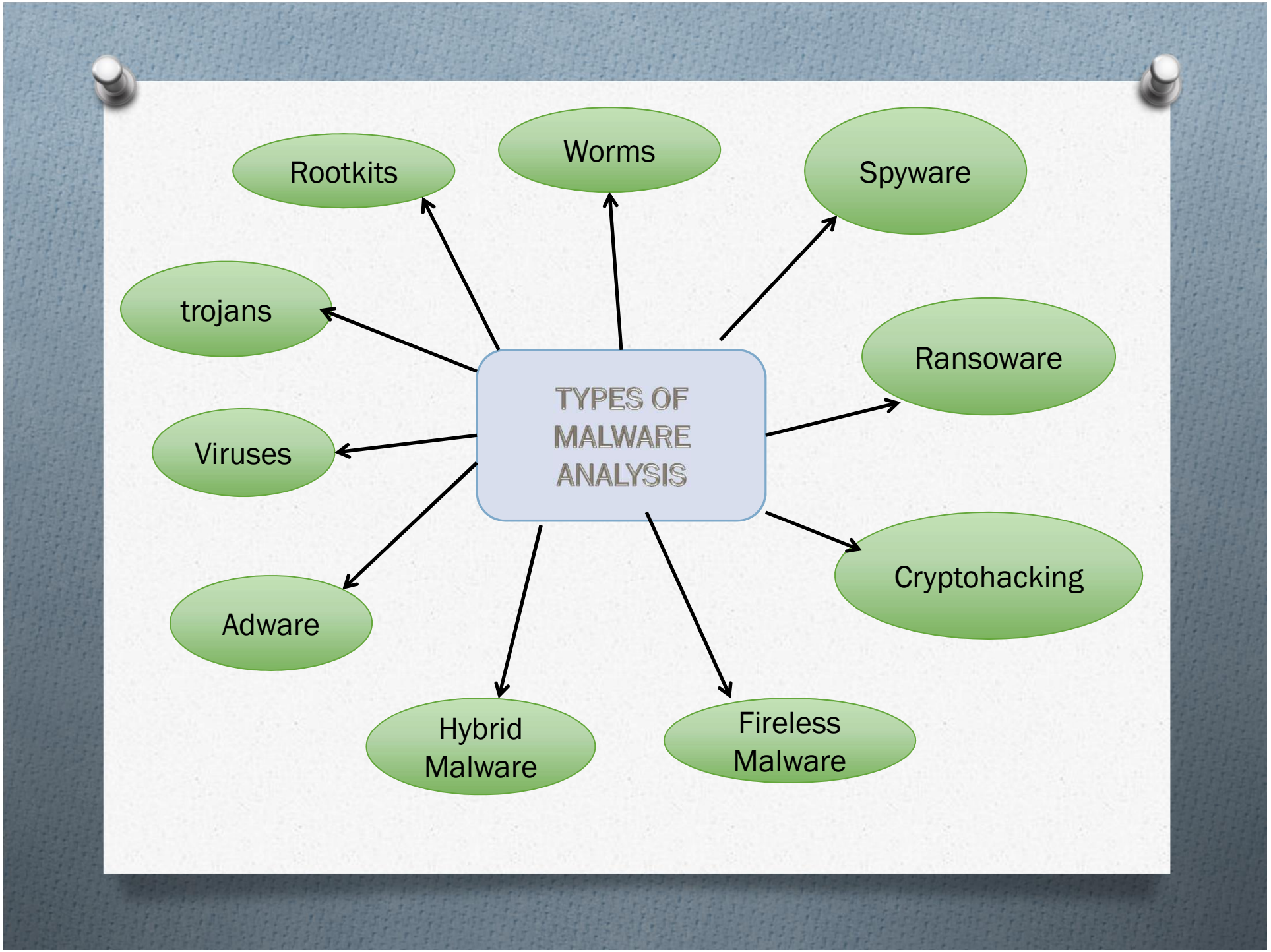
MALWARE ANALYSIS



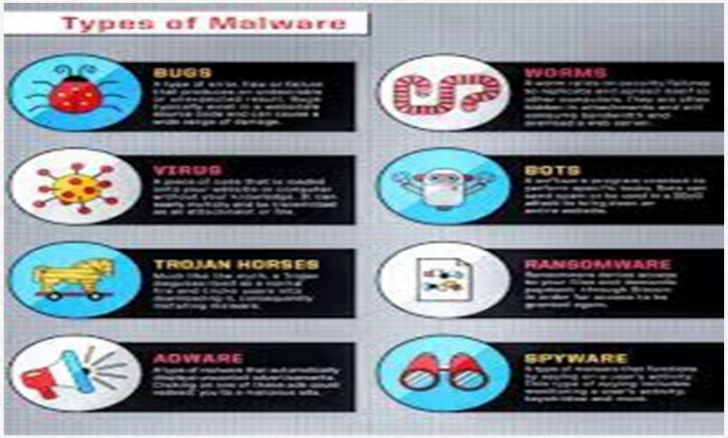
By,
Reema Taslim F
Monisha V
Ragavi M

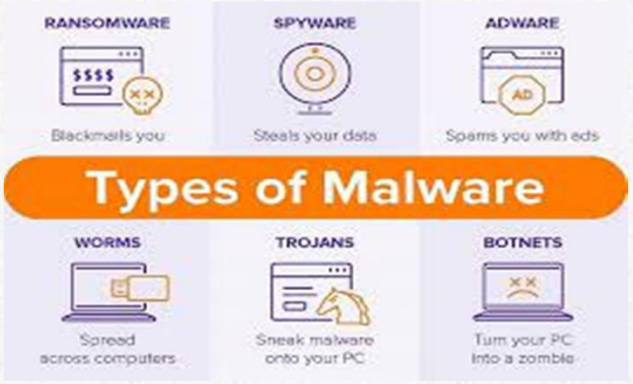
INTRODUCTION TO MALWARE ANALYSIS

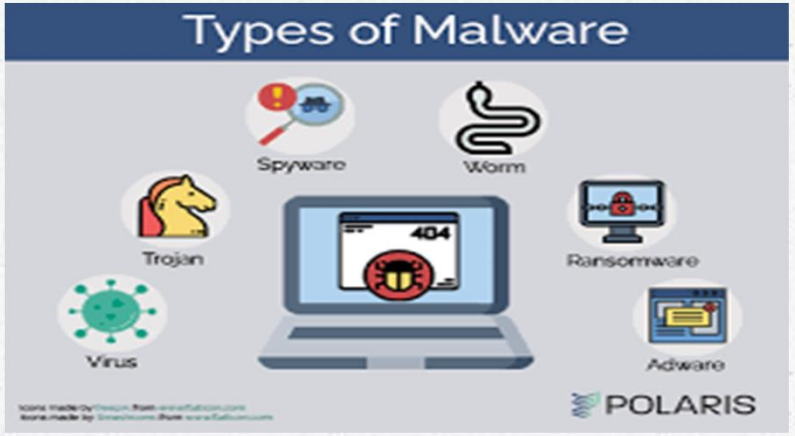
- Malware analysis is the study of the unique features, objectives, sources, and potential effects of harmful software and code, such as spyware, viruses, malvertising, and ransomware. It analyzes malware code to understand how it varies from other kinds.


TYPES OF MALWARE ANALYSIS
Rootkits
Worms
Spyware
trojans
Ransoware
Viruses
Adware
Cryptohacking
Hybrid Malware
Fireless Malware

MALWARE AND ITS TYPES







STATIC ANALYSIS VS DYNAMIC ANALYSIS

STATIC ANALYSIS

- It is a process of analyzing malware binary code without running code
- It uses signature based approach for malware analysis
- It involves Fingerprinting,virus,Scanning,analyzing memory & debugging
- It is ineffective against sophisticated malware analysis programs and codes

DYNAMIC ANALYSIS

- It requires programs to be executed in a closely monitored virtual environment
- It uses Behaviour based approach for malware detection and analysis
- It Involves API calls,Instruction Traces,Network,System calls,memory writes etc..
- It is effectiive against all types of malware because it analyzes the sample by executing it

MALWARE ANALYSIS TOOLS

GOALS OF MALWARE ANALYSIS

- ✓ The goal of malware analysis is to learn about how a cybersecurity threat works. This knowledge has various applications within an organization, Threat Detection: Malware analysis is commonly used to extract indicators of compromise (IoCs) for new malware variants.
- ✓ Malware Analysis is important because it helps security operations teams rapidly detect and prevent malicious objects from gaining persistence

THANK YOU..!!