GROUP - G20

Detecting Malware Infection on Infrastructure Hosted in IaaS Cloud using Cloud Visibility and Forensics

**Stakeholders**

1: Client cloud (customer) – Someone who stores his/her data on cloud.

2: Attacker – Tries to attack the cloud services in order to perform data breach.

3: Attack Analyzer - once attack is done on client cloud the attack analyzer will analyze the attack behavior pattern and perform cloud forensics and analysis etc.

**Ideas (How We Might…)**

Collecting performance counter data on malware and train a set of classifiers to detect malicious behavior.

In addition to data from malware programs, we can also collect data from non-malware programs. From there we can describe our program sets, provide details of our data collection infrastructure, describe our classifiers, and discuss types and granularity of malware detection.

Once malware is found on cloud then we can start doing cloud forensics. Basically, to check the malware’s behavior pattern.

Cloud Forensic techniques are used to collect and preserve evidence, reconstructing incidents, deciding how, where, and when an incident occurring and gives threat information.

Threat information includes Indicators of compromise that can be used to help an organization defend itself.

**Persona (Based on Project members)**

1. Cloud – managing and monitoring data uploaded on cloud and also using cloud forensics to analyze threat information.

2. Analytics – Implementing malware detection algorithm using machine learning for proper capture and analysis of data.

3. Cyber Security - Using SIEM based tools to detect malware and provide threat information.

**Journey Map of User**

