HTTP NETS - A NOVEL DETECTION MECHANISM OF HTTP - BASED MALWARES USING MALICIOUS NETWORK TRACES

PROJECT REFERENCE NO.: 39S_BE_1478
COLLEGE : JAWAHARLAL NEHRU NATIONAL COLLEGE OF ENGINEERING, SHIVAMOGGA
BRANCH : DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GUIDE : MR. CHETAN K.R
STUDENTS : MS. AISHWARYA PATEL
           MS. AMULYA D
           MS. ANKITAH .J
           MS. BHAGYASHREE N.G

INTRODUCTION:
The various hazards caused by different classes of malwares are:
1. Virus can range in severity from causing mildly annoying effects to damaging data or software and causing DoS conditions.
2. Trojan horses damages host by deleting files and stealing data. It can provide malicious party a remote access to an infected computer.
3. Worms works to “eat” the system operating files and data files until the drive is empty.
4. Adware displays ads on the computer and disables regular functioning of computer.
5. Spyware keeps track on the internet activities in the system in order to send advertising (adware) back to the system.
6. Ransomware demands the user to pay ransom to the operators of the malware to remove restriction.

Hence, in this project, we are motivated to develop a software that can detect malwares while browsing web pages. It allows an individual to be warned and get knowledge of malware websites accurately.

OBJECTIVES:
The following are the objectives of our project:
1. To develop a malware detector that finds a group of malware that interacts with the web in a similar way, learn a network behavior model for each group (or family) of malware and then use such models to detect the presence of malware.
2. To provide knowledge to the netizens about malware websites effectively.
3. To produce statistical reports of malware analysis.
4. To detect HTTP malwares over any type of network.
5. To reduce false positive and negative rates of malware detection.

METHODOLOGY:
The architecture of the HTTPNETS is as shown in Figure 1. Initially client browse some websites on web using HTTP protocol. Then these request is redirected to corresponding server. Server searches for the requested files and forward all responses to
malware detector. Malware detector on receiving the responses sniff all the packets then by extracting the statistical and structural features of samples it forms the clusters of malware samples. Later it performs merging of all clusters until all clusters become validated. Then reporter generates report and consult the administrator then suitable alert message is displayed on user terminal.

Figure 1: System Architecture

**CONCLUSION:**

The HTTPNETS is network-level behavioural malware clustering system that focuses on HTTP-based malware and clustered malware samples based on a notion of structural similarity between the malicious HTTP traffic they generate. Through statistical and structural analysis, this malware system is able to unveil similarities among malware samples that may not be captured by current system-level behavioural clustering systems. The result of this system substantiate successful detection of malware and non-malware websites accurately. The false positive and negative rates in detecting are found to be less than 5%. The output of our clustering system can be readily used as input for algorithms that automatically generate network signatures.

**FUTUREWORK:**

The application can be further developed by implementing signature generation module, which should be capable of generating signatures for all kinds of malwares, these signatures can then be deployed into an Intrusion Detection System at the edge of a network in order to detect malicious HTTP request.