Hard Drive Detection on Client Side

Pratik Sharma, Imran Tasgavkar, Tejas Watamwar

Dept. of Computer Science, Vivekanand Institute of Technology, Chembur

Email:pratik.sharma@ves.ac.in,imran.tasgavkar@ves.ac.in,tejas.watamwar@ves.ac.in

***Abstract*—A program is provided for detecting, unwanted hard-drive in a network environment. A host agent residing on a computing device in the network environment detects a new hard drive introduced to the computing device and sends the new hard drive to a network service for analysis. The network service is accessible to computing devices in the network environment i.e server side.**

Keywords-Hard Drive Detection

I. INTRODUCTION

As information technology has rapidly developed and as it has penetrated every aspect of human existence, the number of crimes aimed at breaching information security has grown.Cyber criminals have displayed great interest in the activity of state structures and commercial enterprises. They make attempts at theft and disclosure of confidential information, doing damage to business reputations, breaching business continuity, and consequently breach an organization's information resources. These acts can do extensive damage to assets, both tangible and intangible.

It is not big companies alone who are at risk. Individual users can also be attacked.Using various tools, criminals gain access to personal data (bank account and credit card numbers and passwords), cause your system to malfunction, or gain complete access to your computer. Then that computer can be used as part of a zombie network, a network of infected computers used by hackers to attack servers, send out spam, harvest confidential information, and spread new viruses and Trojans.In today's world, everyone acknowledges that information is a valuable asset and should be protected. At the same time, information must be accessible for a certain user group (for instance, employees, clients and partners of a business). This is why there is a need to create a comprehensive information security system.

Today, malicious programs propagate so quickly that antivirus companies have to release updates as quickly as possible to minimize the amount of time that users will potentially be at risk. Unfortunately, many antivirus companies are unable to do this - users often receive updates once they are already infected.USB flash drive is widely used for storing and transmitting information. It is also an important transmission route of threats.

When you use a USB disk that has malicious programs on it, you can damage data stored on your computer and spread the virus to your computer's other drives or other computers on the network

There are vast number of threats that could affect our computers today. They can be worms, viruses, trojans, spyware, riskware or rootkits.

The problem of detecting malicious and unwanted hard drive has become increasingly challenging. Antivirus software installed on end hosts in an organization is the de-facto tool used to prevent malicious and unwanted software, files, and data (henceforth referred to as 'unwanted files') from being installed through hard drive, opened, accessed, or executed. When a new hard-drive available from a network server or from another internal or external source, this information is passed along to a retrospective detector which in turn searches the file history data database for any previously stored count. If a match is not found, the retrospective detector can notify system administrators and users, remove the unwanted file from an infected host device.Briefly, the host agent is a host-based software component that acquires count of hard drive and forwards them to the network service for inspection. The host agent may further include a mechanism to block access to a file while it is being analyzed. A host agent resides on a host in the network environment, where a host is defined as a desktop, workstation, server, laptop, PDA, phone, mobile device, or other computing device or system through which a malicious file might traverse.

.

II. IMPLEMENTATION DETAIL

This program runs on a Client Server based system.External hardrive detection program detects any external harddrive connected to the client.This is an attack prevention system,where user identifies an attack before it happens.Once you connect the client to the server ,client continuously sents TCP packet to the server.

As soon as there is change in external harddrive count ,it gets detected on the serverThe count on the server side changes along with severel details that get displayed like :Time of connection, ip address of the client to which the external hdd is connected.

i.Procedure for Server side

Run Server side program firstCreate a server.

Type a server nameStart the server by pressing “Start Server”

It will show Client name, Address of client and the number of hard drives connected to that client

After pendrive is inserted the hard drive count is increased

ii.Procedure for Client side

Run Client side program after server side is run

Type name of client

Search for the server you want to connect

Name, address and port are shown to the client

Insert any hardrive at client side

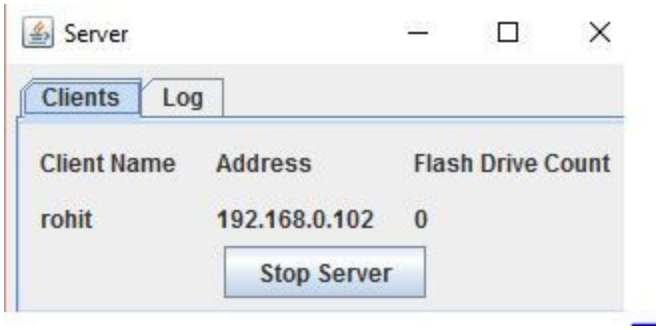
Once inserted the count at the server of hard drive is increased

III. RESULT

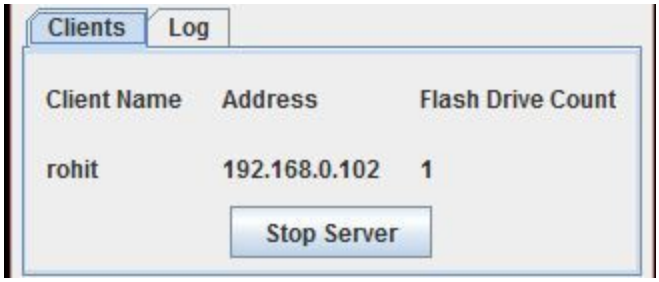
THUS IT CAN BE SEEN THAT IT IS POSSIBLE TO COMPROMISE ONE COMPUTER’S SECURITY (SERVER) BY CONNECTING AN EXTERNAL HARD DRIVE AT THE CLIENT SIDE THUS ENDANGERING THE WHOLE NETWORK. THE PROGRAM SHOWS THE COUNT ABOUT NUMBER OF EXTERNAL HARD DRIVES CONNECTED AND THUS IT ACTS AS AN ATTACK PREVENTION MECHANISM FOR THE SERVER.

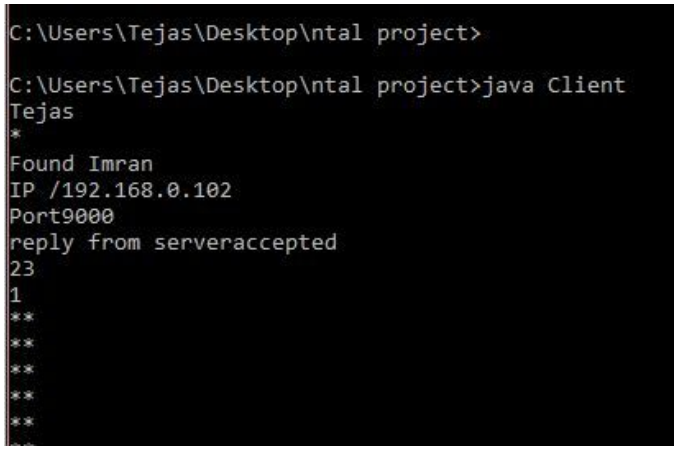
IV. SNAPSHOTS

Initial stage :



After external hard drive is inserted :





When the connection is established between client and server.

V. CONCLUSION

Thus the hard drive detection system has been implemented on java and we can detect any external hard drive on the Server.

VI. REFERENCES

1. Network service for the detection, analysis and quarantine of malicious and unwanted files.
https://www.google.co.in/patents/US8621610?dq=hard-drive+detector+on+network&hl=en&sa=X&ved=0ahUKEwjmkI3KnPbPAhVBy7wKHf7WDyYQ6AEIJDAB
2. Implementation and Implications of a Stealth Hard-Drive Backdoor
https://www.ibr.cs.tu-bs.de/users/kurmus/papers/acsac13.pdf
3. Server-Side Detection of Malware Infection
http://www.arijuels.com/wp-content/uploads/2013/09/JJ09.pd
4. Detection of spoofing of remote client system information
https://www.google.co.in/patents/US9137260?dq=hard-drive+detector+on+client&hl=en&sa=X&ved=0ahUKEwjkt5TVpfbPAhUEO7wKHX1kAQEQ6AEIHTAA