# BROWSER HIJACKING: REASONS AND SOLUTION

**Sarbjeet Singh**
Assistant Professor, Computer Science and Applications, Guru Nanak College, Panjab University, Punjab, India
Email – rakeshuppal44@gmail.com

***Abstract:*** *Hackers like to use most of their time to hack websites of various financial institutions like banks, Government's websites and military 's websites which contains highly top secret information. It is a type of Session Hijacking. The main purpose of this research paper is to give a concise Introduction to the browser hijacking on the application level. It is caused by unwanted guest on the browser.*

***Key Words:*** *Browser, Session Hijacking, Unwanted Guest, anti virus program.*

## 1. INTRODUCTION:

A browser hijacker is a type of malware program that alters any computer's browser settings so that user is redirected to those web sites that user does not want to visit and user had not any kind of intention to visit those web sites .Browser hijacking is also known as hijackware. Most of the browser hijackers alter the default home pages and search pages to those web sites and web pages where attacker want to generate traffic .Browser hijacker use browser hijacking so that they can make earnings by generating traffic of their desired web sites and web pages .Most of the browser hijacker are attached to advertising groups that pays them for making such type of attacks so that they can promote their products ,websites ,web pages etc .So ,browser hijacking includes hackers and advertisers that pay money to hijackers that performs browser hijacking attacks.

**2. OBJECTIVE:** The browser hijacker's objectives are-

- For setting the default page of user's home page of the browser by the web page that is set by the attacker.
- For generating a huge traffic on the websites, that's why browser hijacker attackers use this attack.
- It is a type of unwanted program that changes the browser's default settings without taking the permission of user.
- Used for making hits to a specific website forcefully for growing the advertising income.

## 3. WORKING:

Most of programs that are made for hijacking, alters the default configurations of the browsers and replaces the URL that is entered by the user with the URL and attacker want to open on the client's browser . Most of programs that are made for hijacking , alters the default configurations of the browsers and replaces the URL that is entered by the user with the URL and attacker want to open on the client's browser. Some Browser hijack attacks are so dangerous that take the browser's cookies data from the victim's computer for using the online accounts on which victim is logged in.

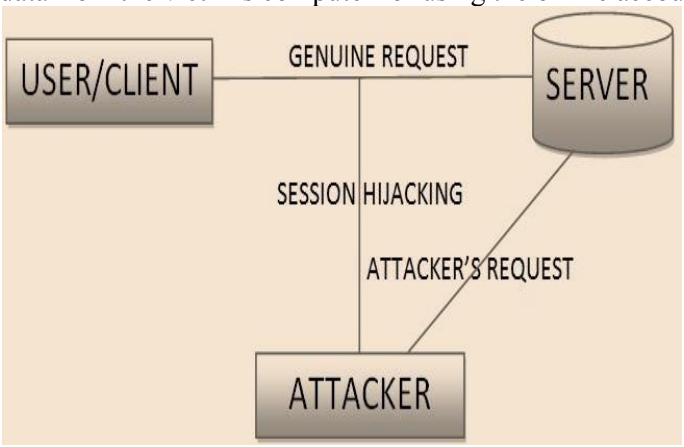


Fig. 1: Working of Browser Hijacking Attack

## 4. EXPERIMENAL RESULTS:

These are some software that It should be check that whether your system is infected with the browser's hijack attack. An infected system with the Browser Hijacker attack face many type of errors like instability of the browser and many other issues as well. Sometimes browser's default homepage is set by the unwanted guest on the browser to the adult websites due to such browser attacks .In such situations it become very difficult for the user to eliminate such kind of unwanted guests from the browser by using only various antivirus programs. It should be check that whether your system is infected with the browser's hijack attack. An infected system with the Browser Hijacker attack face many type of errors like instability of the browser and many other issues as well. Sometimes browser's default homepage is set by the unwanted guest on the browser to the adult websites due to such browser attacks .In such situations it become very difficult for the user to eliminate such kind of unwanted guests from the browser by using only various antivirus programs .These steps can be performed to get rid of from such kind of attacks-

- **Keep up-to-date with updates:** In order to eliminate various vulnerabilities, user should stay current with patches and use anti-malware updates for user's browsers, operating system, ,and other software.

- **Using anti-virus programs on regular basis:** For using anti virus program on daily basis auto scanning option can be used.

- **Try to avoid plug-ins from unknown sources**: User should try to avoid the installation of the plug-ins from unknown or sources that are not trusted.

- **Stay Informed**: When you are in doubt about a plug-in before installation, then internet can be used for help ,because many Social networking sites may contain various posts related to well known attacks which are caused by installing various plug ins , so you will stay informed in this way.

- **Using anti-spyware program:** well reputed and good anti-spyware programs exist in the market that can be used in case whenever your browser hijacked by any unwanted guest or attack.

## 5. ACKNOWLEDGEMENT:

During this research paper, I have put my best efforts for completing this research paper. I hope that this research paper will be helpful for the future authors who want to do further research related to browser Hijacking.

## 6. CONCLUSION:

In the upcoming two years the Browser hijacking infections will continue to grow as online marketing grows and attackers will increasingly use advertising as their major infection vector in future. Browser hijacking attacks increased over the past few days, and the procedures used to spread these infections have also increased at high rate. Browser hijackers are exploiting various trusted brands to cover up their malicious intentions. By using some basic tips like not installing plug ins from unknown sources, such kind of attacks can be avoided

## REFERENCES:

1. Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min;"Software vunerability Discovery Techniques : A Survey" IEEE Conference Publication, DOI : 10.1109/MINES.2012.202, Page(s) 152-156, 2012
2. Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI: 10.1147/sj.403.0769, Page(s): 769-780
3. Bradley, Rubin "Computer Security Education and Research: Handle with care" IEEE Conference Publication, DOI : 10.1109/MSP.2006.146, Page(s):56-59
4. Wilbanks "When Black Hats are really white" IEEE Conference Publication, DOI: 10.1109/MITP.2008.146, Page(s): 64
5. "Browser Hijacking Fix & Browser Hijacking Removal". Microsoft. Retrieved 23 October 2012.
6. Rudis Muiznieks. "Exploiting Android Users for Fun and Profit". The Code Word.
7. "PUA.Astromenda". symantec.com.
8. "How to Remove Astromenda Search From Your Browser". Lavasoft.
9. "Remove Astromenda, Buzzdock and Extended Update toolbar from your browser". norton.com.
10. Internet Crime Complaint Centre link:www.ic3.gov