# A Taxonomy of Browser Hijacking Malware

**Guided research**

Supervisors: Prof. Dr. Alexander Pretschner, Sebastian Banescu
Email: {alexander.pretschner, sebastian.banescu} @ in.tum.de
Phone: +49 89 289 – 17, 314
Starting date: immediately

Fakultät für Informatik
Lehrstuhl 22
Software Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3 85748
Garching bei München

Tel: +49 89 289 17885,
+49 89 289 17314

Web: http://www22.in.tum.de

## Context

Web-browsers are often targeted by so-called browser hijackers which affect browser behavior by manipulating its process memory, locally stored resources or the environment in which they are running. This change creates some form of financial gain for the vendor of such malware. At the same time it creates browser end-user dissatisfaction, due to: aggressively displaying pop-up advertisements in any web-page visited by the end-user, persistent modification of preferences (e.g. default search engine) and overall system slowdown.

Unfortunately, techniques employed by malware (e.g. code injection in the process memory of the browser, system call interposition) do not raise any alarms in anti-virus software, because they are also performed by non-malicious third party software including ant-virus software, accessibility and graphics driver tools.

## Goal

The goal of this project is to create taxonomy of browser hijackers based on a set of criteria, which will also be part of the contribution of this project. Such criteria may be related to: the social engineering attack vector used by vendors of the browser hijackers to infect victims, the effect of the hijacker on browser behavior, whether the hijacker is a browser extension that uses JavaScript or a malicious binary program, etc. Another useful outcome of this project may include a set of recommendations for browser end-users and/or reverse engineering descriptions of browser hijackers pointing out the technical means through which they operate.

## Work-plan

1. Collect a set of browser-hijacking malware to analyze. A list of such malware can be found using the following websites:
   a. http://malwaretips.com/blogs/category/hijackers/
   b. http://www.anti-spyware-101.com/threats/browser-hijackers
   c. http://www.shouldiremoveit.com/
2. Analyzing browser-hijacking malware:
   a. Setup of analysis environment based on Cuckoo Sandbox (http://www.cuckoosandbox.org/)
   b. Install and analyze browser-hijackers
   c. Develop set of criteria and classify different browser-hijackers
3. The final written document must contain:
   a. Description of the analysis environment
   b. Each criterion used for browser-hijacker classification and the reason why it makes sense to use this criterion
   c. Description of all the browser-hijackers tested / reversed and their classification according to the previous criteria
   d. Conclusions and future work.

## Deliverables

- A VM with the analysis environment used to test the browser-hijacking malware
- The VM should contain a README file with the instructions needed for performing the analysis using that environment and a folder with all the browser-hijackers analyzed (renamed according to the name used in the technical report)
- Final report written in conformance with TUM guidelines.

Fakultät für Informatik
Lehrstuhl 22
Software Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3 85748
Garching bei München

Tel: +49 89 289 17885,
+49 89 289 17314

Web: http://www22.in.tum.de