24 May 2017 Study · Web & Cloud

Analysis of Browser-Extensions

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/analysis-of-browser-extensions/

This study deals with dangers potentially posed from browser extensions.

Browser extensions can extend the functionality of modern web browsers almost arbitrarily. However, they are often used for malicious activities, due to their ability to easily access sensitive data (i.e. Cookies). Likewise, benign but faulty extensions can be used for targeted attacks by exploiting errors in the implementation. Usually, the security mechanisms of modern browsers only provide limited protection against such attacks.

We developed an analysis framework, which automatically analyses browser extensions for potential weaknesses. Using the example of Google Chrome, we analysed 1.000 extensions. The results show that many benign extensions show errors in the implementation which allow attackers, under some circumstances, to gain control over browser extensions. The analysis also shows that many deployed security mechanisms concentrate on protection against malware. Users often have hardly any control over used functionality.

Following responsive disclosure principles, we present the results statistically. This prevents to draw conclusions about weaknesses of concrete extensions. The present work is designed to help developers of browser extensions to avoid frequent errors and to support them in the implementation process.