University of Padova

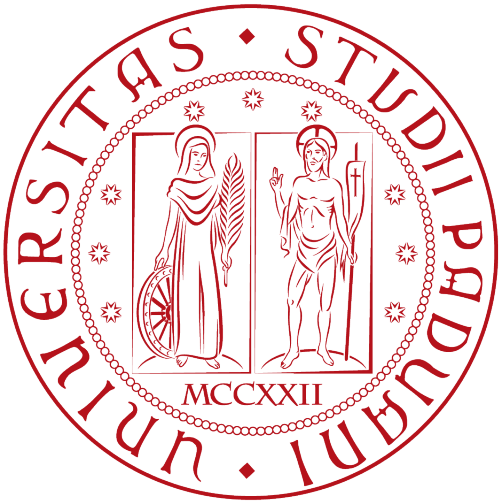
Computer and Network Security

insert-title-here

Students:
Davide Trevisan
Andrea Multineddu

Registration number:
1070686
MATRICOLA

Thursday 25 August 2016



Introduction

Nowadays the majority of browsers let users the possibility of customizing it in order to get a new feature o a new style of visualization to better match the taste of the single user. All of this is achievable through the existing extensions for modern browsers. But there is also the opposite situation in which a malicious user tries to get personal information using this extensions.

Abstract

Google Chrome browser is known for it huge ammount of extensions that let users do almost everything they want, but there also malicious extensions that aim to steal personal information about the life, bank accounts and every other single piece of information of the users. In this paper we presents 3 extensions: ChromeLogger[1], Stealth Screenshot e Activity Logger;

ChromeLogger is a keylogger and form grabber for Google Chrome that runs as an extension. ChromeLogger works by injecting javascript into all loaded web pages. The payload records keypresses using event listeners and saves them to Chrome's storage. Unlike other browser keyloggers, ChromeLogger runs natively in Chrome (on all OS's) without the need to install additional software. The form grabber works in a similar way. Javascript is injected and event listeners are added for all forms. When a form is submitted, its data is saved to ChromeLogger's storage. This allows form data transferred over SSL to be saved in plaintext. ChromeLogger's payload is written in pure JS and the log viewer is built using AngularJS.

Stealth Screenshot make screenshots of the active tab based on a timer and keep them until every opened tab is closed. Users can access with a combination of key to all screenshots taken during the session.

Activity Logger keep trace of all events related to extension and save them in Chrome storage. Users can check if there are installation, uninstallation, activation or deactivation of Chrome extension due to malicious code running in background.

How Chrome Extension works

Background

where to find an extension

The Chrome Web Store is the official way for users to find and install

extensions, where the developers can publish it. They can also push out updates without any action by the end-user. In addition to the Chrome Web Store, extensions can also be installed manually by a user or an external program. Extension that are not downloaded through the official channel are flagged by Chrome when it starts and the user is asked to disable them. However, the user can whitelist the extension through the console.

Manually install an extension

Once you have all the source code of an extension in a folder, go to CHROME://EXTENSIONS (or find it in the menu in more tools > extensions), then activate the developer mode on the top right of the page. To install the extension, you just have to indicate where is this folder on your computer clicking on load unpacked extention.

Permission

Chrome requires extensions to list the permissions needed to access the different parts of the extension API. The complete list of the permissions and their interaction can be found on google developer page.
Extensions must also specify a list of content scripts to indicate JavaScript files that will run inside of the web page, because this is a powerful feature that allows an extension to be indistinguishable to the webpage behaviour. Besides the content scripts that allow an extension to interact with a given page, Chrome also allows extensions to run scripts in a "background page" that often contain the logic and state an extension needs for the entirety of the browser session and do not have any visibility to the user.

Activity Logger Extension

Scope of the extension

The extension aims to keep traces about the activities of other extensions and let the user know about them through a dedicate page in which can check for every extension that are installed on the Chrome browser. This logger keep traces of logs even if some extensions are unistalled.
The extension makes use of the following permission in the manifest file:

- management
- storage
- unlimitedStorage

How the extenssion work

The extension at the browser start check the list of installed extension and updates the logs list with the one missing from it. After this first

check and update we create listener for the events related to extensions which are:

- chrome.management.onInstalled
- chrome.management.onUninstalled
- chrome.management.onEnabled
- chrome.management.onDisabled

Every time the user or some malicious code install, uninstall, enable or disable an extension a log of the triggered event is saved in the specific event log for the specific extension in the chrome storage. The computation time is defined by the computation time of the Chrome search in his storage.

Limitations

The main limitation to this extension can be reconducted to the limitation imposed by or absence of Chrome APIs. At the moment we can just check the events described early in the paper, every other event defined in Chrome APIs and the presence or absence of listener for a specific event. A better controll on browser activity could be achieved by adding APIs, for example that return the name of extension from which is running codes in response to a specific event.

Future work

The final aims of this extension are to log every single activity of installed extensions and jasvacript scripts inside web pages in response to every event happening inside Chrome itself (like a modification inside the chrome storafe area) or the web pages visited by the user (the pression of a button) and let the user check these logs in order to let users check some strange and unwanted activities caused by some malicious code. At this time, for what we have find out from our research on chrome API documentation we can just check if there is some code waiting a specific events that trigger it. But this is also a double-edged weapon that can led to problems for privacy maintenance because let every user, capable of writing chrome extension the possibility to check every activity, but from the other hands let malicious users the possibility on customizzable browsers to get knowledge about users routines, personal data and ad-hoc javascript code injection.

Stealth Screenshot Extension

The source code of the extension we developed is downloadable here

Scope of the extension

the scope of the stealth screenshot extension is to create a small prototype of an extension that catch screenshot

in a regular interval with the minimum possible user interaction and obviously giving it back.

Activation and screenshot collection

The extension uses the relatively new tab APIs given by chrome too take screenshot. The extension makes use of the "storage", "tabs", "all_urls;", "unlimitedStorage", "activeTab" permissions in his manifest file. The extension works in a simple way: it triggers on a browser event, in this case the click on the icon of the extension, but there are other possibilities: we tested that there are no simple ways to take screenshot without no interaction, because the security policy of the API doesn't allow to take a scrrenshot without some kind of events, presuming that the user should be aware of what is happening; not triggering any event returns only null. Once triggered, the extension schedule all the future screenshot through the Javascript setTimeout method: this allows to take screenshot for hours, with only the need for a click to start. The screenshot are stored in an array visible to all the extention methods.

Screenshot retrival

The screenshot can be collected in two ways in the wxtension we developed: through a combination of key for retriving all screenshots (we programmed it on Ctrl+Shift+Y) or writing "show" in the omnibox, pressing "tab" and writing in the omnibox the number of screenshot to show (starting from the last one).

Performance

We tested that the extension is able to take screenshot with a interval of 1 minute for more than 2 hours without losing any screenshot. The application occupy less of 50MB of RAM for an hour of screenshots taken every minute. The impact on the CPU is negligible. Screenshot retrival through the kay combo however can crash chrome, although it never happened in our PC because of the great performance (we had an Intel i5 6400, with 8GB of DDR4 memory and SSD), but it got freezed for some seconds.

Limitations

The major limitation of this extension is that the screenshot only lives until the extension is active: this implies that closing all the windows of chrome completely deletes the screenshot taken. This is a consequence of how the API and the chrome sandbox works. We at the moment found no way to get around it, but we are pretty confident that is possible to

save those screenshots, but for our lack of knowledge we are not able at the moment to demonstrate it.

Future work

Possible future works will focus on find a way to save those screenshot. The application should also be rewritten without the tab API, to avoid of the limitation of it. Javascript inject the code for the screenshot or use it for simulate the right events should do the work, but the time and the train needed to do it made impossible for us to test it for this paper.

conclusions

All the solution we have presented in thispaper makes use of the most used chrome permission, as already stated in the HULK paper[2]

Rank	Top 10 types of permissions	# ext.
1	tabs	16,787
2	notifications	12,011
3	unlimitedStorage	9,424
4	storage	5,725
5	contextMenus	4,774
6	cookies	2,872
7	webRequest	2,849
8	webRequestBlocking	2,102
9	webNavigation	1,623
10	management	1,533

Figure 1: The top 10 permissions found in the manifest files for all extensions we ran. Extensions can include more than one permission.

As shown in the screenshot extension, taking screenshot without user consensus should not be allowed to the API (just a popup should be enough)

References

[1] Eric Zhang,
ChromeLogger,
A keylogger and form grabber for Google Chrome that runs as an extension.
ChromeLogger
referring site

[2] *Hulk: Eliciting Malicious Behavior in Browser Extensions*
Alexandros Kapravelos, Chris Grier, Neha Chachra, Christopher Kruegel Giovanni Vigna, Vern Paxson, UC Santa Barbara, UC Berkeley, UC San Diego and International Computer Science Institute
23rd USENIX Security Symposium.
Paper