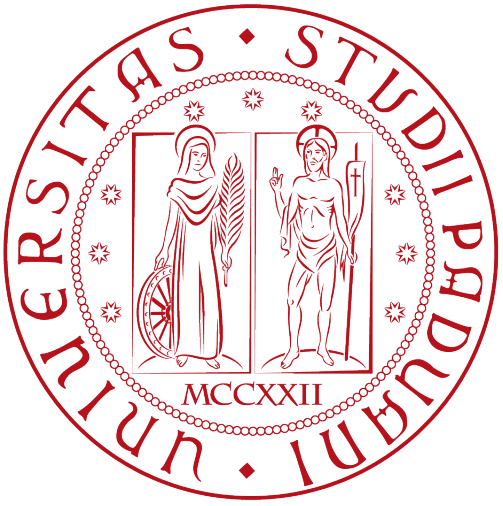
University of Padova

Computer and Network Security

insert-title-here

Students:	*Registration number:*
Davide Trevisan	1070686
Andrea Multineddu	1049261

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: [?], Stealth Screenshot e Activity Logger;

[?] is a keylogger and form grabber for Google Chrome that runs as an extension. [?] 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. [?]'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.