# Trends and Lessons from Three Years Fighting Malicious Extensions

Nav Jagpal Eric Dingle Jean-Philippe Gravel Panayiotis Mavrommatis
Niels Provos Moheeb Abu Rajab Kurt Thomas
Google
{nav, ericdingle, jpgravel, panayiotis, niels, moheeb, kurtthomasg}@google.com

## Abstract

In this work we expose wide-spread efforts by criminals to abuse the Chrome Web Store as a platform for distributing malicious extensions. A central component of our study is the design and implementation of WebEval, the first system that broadly identifies malicious extensions with a concrete, measurable detection rate of 96.5%. Over the last three years we detected 9,523 malicious extensions: nearly 10% of every extension submitted to the store. Despite a short window of operation—we removed 50% of malware within 25 minutes of creation— a handful of under 100 extensions escaped immediate detection and infected over 50 million Chrome users. Our results highlight that the extension abuse ecosystem is drastically different from malicious binaries: miscreants profit from web traffic and user tracking rather than email spam or banking theft.

## 1 Introduction

Browsers have evolved over recent years to mediate a wealth of user interactions with sensitive data. Part of this rich engagement includes extensions: add-ons that allow clients to customize their browsing experience by altering the core functionality of Chrome, Firefox, and Internet Explorer. Canonical examples include search toolbars, password managers, and ad blockers that once installed intercept webpage content through well-defined APIs to modify every page a user visits.

Criminals have responded in kind by developing malicious extensions that interpose on a victim's browsing sessions to steal information, forge authenticated requests, or otherwise tamper with page content for financial gain. Poignant malware strains include Facebook account hijackers, ad injectors, and password stealers that exist purely as man-in-the-browser attacks [21, 25, 37, 41]. While many of these threats have binary-based equivalents—for instance the Torpig banking trojan that injected rogue phishing forms into banking webpages or the ZeroAccess bot that tampered with page advertisements [27, 34]—extensions bridge the semantic gap between binaries and browsers, trivializing broad access to complex web interactions.

In this paper we expose wide-spread efforts by criminals to abuse the Chrome Web Store as a platform for distributing malicious extensions. Our evaluation covers roughly 100,000 unique extensions submitted to the Chrome Web Store over a three year span from January 2012–2015. Of these, we deem nearly one in ten to be malicious. This threat is part of a larger movement among malware authors to pollute official marketplaces provided by Chrome, Firefox, iOS, and Android with malware [7, 10, 42].

A central component of our study is the design and implementation of WebEval, the first system that broadly identifies malicious extensions with a concrete, measurable detection rate of 96.5%. We arrive at a verdict by classifying an extension's behaviors, code base, and developer reputation. In the process, we incorporate existing techniques that detect specific malware strains and suspicious extension behaviors and evaluate each of their effectiveness in comparison to our own [21, 37, 41]. WebEval also faces a unique challenge: live deployment protecting the Chrome Web Store where attackers have a strong incentive to adapt to our infrastructure. We explore the impact that evasive threats have on our overall accuracy throughout our deployment and the necessity of human experts to correct for model drift.

In total, we removed 9,523 malicious extensions from the Chrome Web Store. The most prominent threats included social network session hijackers that generated synthetic likes, friend requests, and fans; ad injectors that rewrote DOM content to laden pages with additional advertisements; and information stealers that injected rogue tracking pixels and covertly siphoned search keywords. Despite a short window of operation—we re-