

Hulk: Eliciting Malicious Behavior in Browser Extensions

Alexandros Kapravelos, Chris Grier, Neha Chachra, Christopher Kruegel, Giovanni Vigna, and Vern Paxson

USENIX Security 2014

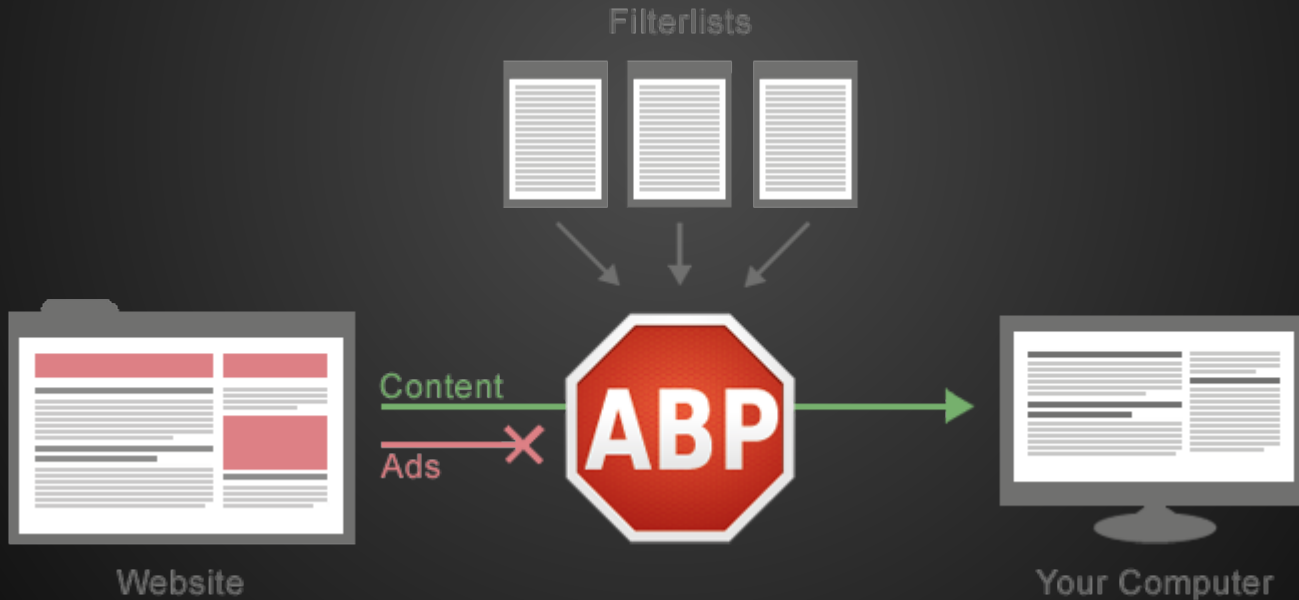
Browser extensions

- HTML + JavaScript
- Modify and enhance the functionality of the browser
- Have access to a privileged API



Adblock Plus

- Over 50 million users!





FB Color Changer

★★★★★ (4475)

[Social & Communication](#)

from fbcolorchanger.com

347,103 users

+ FREE



OVERVIEW

DETAILS

REVIEWS

RELATED

g+1

3.9k



facebook



facebook



facebook



facebook



facebook



facebook



facebook



facebook



facebook



Confirm New Extension

Add "FB Color Changer"?

It can:

- Access your data on all websites
- Access your tabs and browsing activity



Cancel

Add

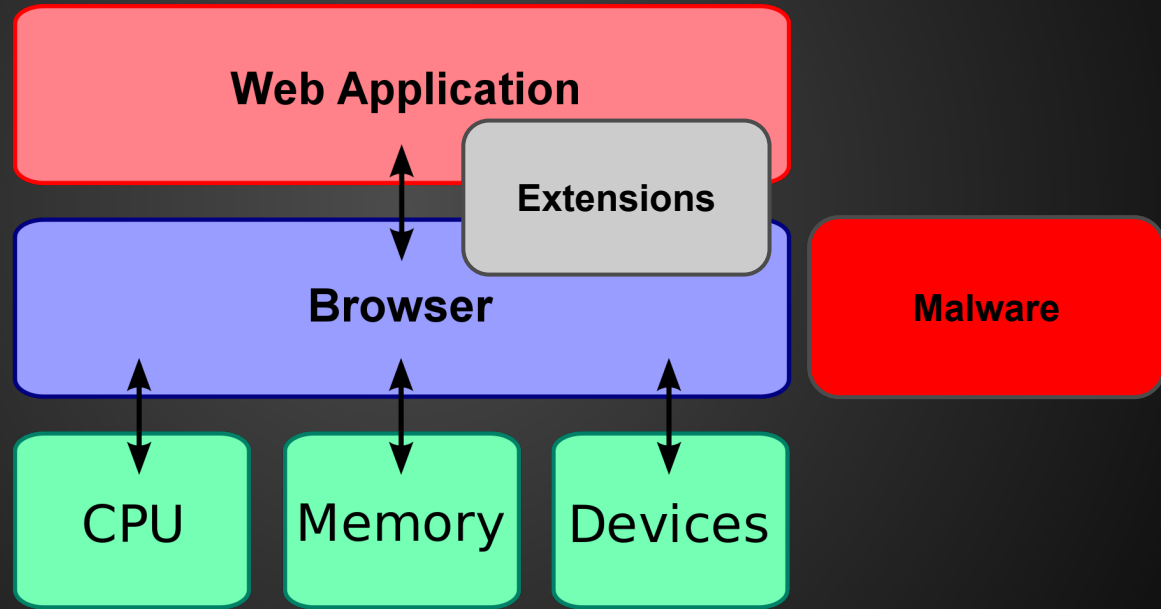
⚡ Runs Offline

Change the Facebook color scheme to anything you want.

Compromising the browser

- Drive-by downloads
- Browser extensions

Compromising the browser



Goal

- Understand malicious behavior in browser extensions
- Identify automatically malicious browser extensions



What can a malicious extension do?

- Inject advertisements
- Keylogger (only in the visited page)
- Affiliate fraud
- Steal credentials

Anything malicious that you can do with JavaScript having access to the visited page, the web requests, the browser's cookies

Approach

- Install extension in Chrome inside a VM
- Visit a few pages
- Monitor what the extension is doing
- Classify the extension

Challenges

- How to trigger malicious code?
 - What content should the pages contain?
 - Which pages should we visit?
- How to detect maliciousness?

Triggering malicious behavior

- Find the right content
 - HoneyPage
- Visit the right page
 - URL extraction
 - Event handler fuzzing



HoneyPage

```
<html>
```

```
  <div id="fb_newsfeed"></div>
```

```
</html>
```

```
document.getElementById("fb_newsfeed")
```

Event handler fuzzing

- Extensions can intercept network events
 - Triggering the event handlers is possible!
-
- Pretend to visit Alexa top 1 million domains
 - Point to a HoneyPage
 - Takes <10 sec on average

Detecting malicious behavior

- In JavaScript
 - Extension API
 - Interaction with visited pages
- In the network
- In injected code

Malicious behavior heuristics

- Prevents extension uninstall
- Steals email/password from form
- Contains keylogging functionality
- Manipulates security-related HTTP headers
- Uninstalls extensions

Suspicious behavior heuristics

- Injects dynamic JavaScript
- Evals with input >128 chars long
- Produces HTTP 4xx errors
- Performs requests to non-existent domains

Results

- 47,940 extensions from Chrome Web Store
- 392 extensions from Anubis

Analysis result	Count
Benign	43,490
Suspicious	4,712
Malicious	130

“SimilarSites Pro”



Similar Sites Pro

★★★★★ (47)

[Productivity](#)

[from SimilarGroup](#)

1,808,386 users



ad.yieldmanager.com/st?ad_type=iframe&ad_size=728x90§ion=4817275

7-ZIP

Try it free

Download



ad.yieldmanager.com/st?ad_type=iframe&ad_size=728x90§ion=4817275



You need to update your version of media player. [Update now.](#)

Alexandros Kapravelos

LATEST NEWS

May 9, 2013

Our paper got accepted at USENIX Security 2014!

November 4, 2013

I'm attending CCS'13 since I was awarded a travel grant

August 4, 2013

Our team Shellphish finished 7th at DEFCON CTF

Who am I?



My name is Alexandros Kapravelos and I'm a fourth year PhD candidate at the University of California, Santa Barbara. My advisors are [Giovanni Vigna](#) and [Christopher Kruegel](#). I'm a member of the [Computer Security Group](#) at [UCSB](#) and the [Epic Fail](#) and [Shellphish](#) hacking teams.

Tweets

Follow



Manos Antonakakis
@mAntonakakis

An open discussion about botnet takedowns tomorrow at usenix hotsec --- time to start figuring things out | usenix.org/conference/hotsec

Retweeted by AlexandrosKapravelos



Steve Carell
@SteveCarell

Robin Williams made the world a little bit better. RIP.

Retweeted by AlexandrosKapravelos



© KenRockwell.com

Canon 70D ([1.6x sensor](#) (nearly [APS-C](#))), 26.7 oz./756g with battery and card, about [\\$1,199](#)) and [Canon 50mm f/1.8 II](#), [enlarge](#). It comes as [body-only](#) ([\\$1,199](#)), kit with [18-55mm STM](#) ([\\$1,349](#)) or kit with [18-135mm STM](#) ([\\$1,549](#)).

I'd get it (with any of the lenses) at these links [directly to them at Adorama](#) or [directly to them at Amazon](#). This free website's biggest source of [support](#) is when you use those or any of [these links](#) when you get *anything*, regardless of the country in which you live — but I receive *nothing* for my efforts if you buy elsewhere. I'm not NPR; I get no government hand-outs and run no pledge drives to support my research, so please always use any of [these links](#) for the best prices and service whenever you get anything. Thanks for helping me help you! Ken.

Research Interests Last Blog Post

I'm currently focusing on **web security** and in particular finding new ways to detect if a web page is malicious or not. I'm the lead developer of [Wepawet's](#) development and improvement. My latest project is tracking the evolution of malicious JavaScript with [Revolver](#).

My last blog post is "[Attacking home routers via JavaScript](#)" where I explain an attack I found in the wild that targets the victim's local router via JavaScript.

[last blog post](#)

Recommendations

- Manipulating configuration pages e.g., `chrome://extensions`
- Uninstalling extensions
- Removing security-related HTTP headers
- Hooking keyboard events
- Local inclusion of static files instead of dynamic JavaScript inclusions

Limitations

- Dynamic analysis system
- Targeted attacks (location, time)
- Multistep queries of DOM elements in HoneyPages
- Evasions against HoneyPages

Conclusion

- Dynamic analysis system for browser extensions
- Detected malicious extensions affecting millions of users
- Proposed changes in Chrome browser ecosystem



Thank you!

@kapravel