AD INJECTION AT SCALE: ASSESSING DECEPTIVE ADVERTISEMENT MODIFICATIONS

Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal, Alexandros Kapravelos, Damon McCoy, Antonio Nappa, Vern Paxson, Paul Pearce, Niels Provos, Moheeb Abu Rajab
Browsers now analogous to the OS
Web injection threat

Malware, unwanted software now monetizes browser interactions
Rise of ad injection
Top Chrome user complaint

> 100,000 user complaints last year

No consent. Misattributed ads. No clear path to removal.
Our work

Exploring the structure of ad injection

- Prevalence of browser infection rates
- Delivery mechanisms: extensions & binaries
- Advertisers, ad networks affected

Identify bottlenecks in deceptive ad injection revenue
1 DETECTING AD INJECTION
Rogue DOM elements in Google sites
Rogue DOM elements in Google sites

1. Construct a whitelist of page scripts, iframes, urls
2. Client reports DOM elements that violate whitelist
Content integrity check

Hostile environment: OS, extensions, ISP

Duration: June 1, 2014 - Sept 30, 2014
Dataset: 102M pages
What changes caused by ad injection?

89% of tampered pages contain rogue scripts

Top 100 scripts account for 74% of tampered pages

Manually verify 65 of top 100 inject ads.
Ad injection infection rates

5% of clients exhibit ad injection

Tens of millions of users
# Top ad injection libraries

<table>
<thead>
<tr>
<th>Rank</th>
<th>Ad Injection Library</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>superfish.com</td>
<td>3.92%</td>
</tr>
<tr>
<td>2</td>
<td>api.jollywallet.com</td>
<td>2.40%</td>
</tr>
<tr>
<td>3</td>
<td>visadd.com</td>
<td>1.40%</td>
</tr>
<tr>
<td>4</td>
<td>intext.nav-links.com</td>
<td>1.29%</td>
</tr>
<tr>
<td>5</td>
<td>{crdrdpjs, rvzrjs, ...}.info</td>
<td>0.70%</td>
</tr>
</tbody>
</table>
Ad injection user base
Ad injection user base

Pages with ad injection:
Windows: 5.5%
Mac: 3.4%
2 DISTRIBUTION TECHNIQUES
Affiliate model

Users Browse, You Earn
SimilarProducts is a monetization platform that uses visual search technology to help users find and discover products visually. The technology instantly analyzes images on the web and presents identical and similar product offers.

Monetize your Userbase
Plug & Play JS Integration
20+ Supported GEOs

Get Code
1. Affiliate program gives *injection library*. Manages ad relationships.
3. Affiliates paid commission on clicks.
## Affiliate breakdown

<table>
<thead>
<tr>
<th>Ad Injection Library</th>
<th>Affiliates</th>
<th>Top Affiliate</th>
<th>Top Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>superfish.com</td>
<td>494</td>
<td>Crossrider</td>
<td>44%</td>
</tr>
<tr>
<td>api.jollywallet.com</td>
<td>114,486</td>
<td>Shopperpro</td>
<td>8%</td>
</tr>
<tr>
<td>visadd.com</td>
<td>885</td>
<td>Iwebar</td>
<td>7%</td>
</tr>
<tr>
<td>intext.nav-links.com</td>
<td>96</td>
<td>Crossrider</td>
<td>42%</td>
</tr>
<tr>
<td>{crdrdpjs, ...}.info</td>
<td>613</td>
<td>TornTV</td>
<td>7%</td>
</tr>
</tbody>
</table>

~1,000 affiliates fuel ecosystem
(Exception: Jollywallet)
Identifying ad injection software

Scan for injection behavior in extensions, binaries

Extensions: 1M  (50,870 inject ads)
Binaries: 25M  (34,407 inject ads)
### Ad Injection Library

<table>
<thead>
<tr>
<th>Ad Injection Library</th>
<th>Extensions</th>
<th>Binaries</th>
<th>First Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>superfish.com</td>
<td>49,127</td>
<td>33,486</td>
<td>Sep 2012</td>
</tr>
<tr>
<td>api.jollywallet.com</td>
<td>19,259</td>
<td>28,557</td>
<td>Jul 2013</td>
</tr>
<tr>
<td>visadd.com</td>
<td>11,843</td>
<td>13,763</td>
<td>Jan 2014</td>
</tr>
<tr>
<td>intext.nav-links.com</td>
<td>17,007</td>
<td>4,881</td>
<td>Jul 2013</td>
</tr>
<tr>
<td>{crdrdpjs, ...}.info</td>
<td>16,381</td>
<td>28,574</td>
<td>Mar 2013</td>
</tr>
</tbody>
</table>

**Total**

|                  | **50,870** | **34,407** |
### Binaries, extensions, ISPs

<table>
<thead>
<tr>
<th>Ad Injection Library</th>
<th>Extensions</th>
<th>Binaries</th>
<th>First Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>superfish.com</td>
<td>49,127</td>
<td>33,486</td>
<td>Sep 2012</td>
</tr>
<tr>
<td>api.jollywallet.com</td>
<td>19,259</td>
<td>28,557</td>
<td>Jul 2013</td>
</tr>
<tr>
<td>visadd.com</td>
<td>11,843</td>
<td>13,763</td>
<td>Jan 2014</td>
</tr>
<tr>
<td>intext.nav-links.com</td>
<td>17,007</td>
<td>4,881</td>
<td>Jul 2013</td>
</tr>
<tr>
<td>{crdrdpjs, ...}.info</td>
<td>16,381</td>
<td>28,574</td>
<td>Mar 2013</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>50,870</strong></td>
<td><strong>34,407</strong></td>
<td></td>
</tr>
</tbody>
</table>

35% more injected ads in HTTP traffic vs. HTTPS
Relationship to malware

Minimal control over affiliates

17% of ad injection binaries tied to malware
38% of ad injection extensions are malware

Other activities:
Search hijacking, facebook hijacking, user tracking
3 AD NETWORKS & ADVERTISERS
Ad enumeration platform

Install extensions, browse to Google, Amazon, Walmart.

Ad click chains: 114,999
Clickchain Example

Injection Logic
superfish.com/ws/sf_main.jsp

Impacted Page
google.com/webhp?sourceid=...
Clickchain Example

```
findByUrl.action?document=
```

```
cards: [{
  "merchantName": "Best Buy",
  "price": "$39.99",
  "title": ...
},
```

Injection Logic
superfish.com/ws/sf_main.jsp

Impacted Page
google.com/webhp?sourceid=

Injected Ad Url
superfish.com/ws/offerURL.action

Hop After Injector
windowshopper.pgpartner.com

www.pricegrabber.com/ut_sync

Hop Before Advertiser
windowshopper.pgpartner.com

Advertiser
bestbuy.com/site/boost-mobile-lg...
Bottleneck of ad networks

Three ad networks supply 77% of injected ads: DealTime, PriceGrabber, BizRate

Over 3,000 advertisers affected: Ebay, Sears, Walmart -- major brands
Putting it all together

- Tens of millions of infected users
- 100K binaries, extensions
- < 1K affiliates
- 25 affiliate programs
- 3 ad networks
Conclusion

Taking action against deceptive ad injection:

- Pulled 192 extensions: 14 million users cleaned up
- Google provides tool for users to clean up UwS
- Reached out to advertisers, ad networks affected

Ad networks can disincentivize entire practice.
THANKS!

kurtthomas@google.com
Ad injection infection rates
Are there legitimate ad injectors?

[Image of a Chrome Developer Program window showing policy details]

**Ads Context and Attribution:**
Ads must be presented in context or clearly state which app or extension they are bundled with. Ads must also be easily removable by either adjusting the settings or uninstalling the app or extension altogether. Ads may not simulate or impersonate system notifications or warnings.

**Ad Walls:**
Forcing the user to click on ads or submit personal information for advertising purposes in order to fully use an app or extension provides a poor user experience and is prohibited.

**Interfering with Third-party Ads and Websites:**
Ads associated with your app or extension may not interfere with any ads on a third-party website or application. You may show ads alongside a third-party website only if all of the following criteria are met:
Advertisers injecting own ads