All Your Clicks Belong to Me: Investigating Click Interception on the Web

Mingxue Zhang†, Wei Meng†, Sangho Lee‡, Byoungyoung Lee*, Xinyu Xing§

†Chinese University of Hong Kong
‡Microsoft Research
*Seoul National University
§Pennsylvania State University

BBC - Homepage

Theresa May's handling of Brex

Not Secure | theconversation.com/theresa-mays-handling-of-brexit-is-a-classic-case-of-bad-leadership-108646

THE CONVERSATION

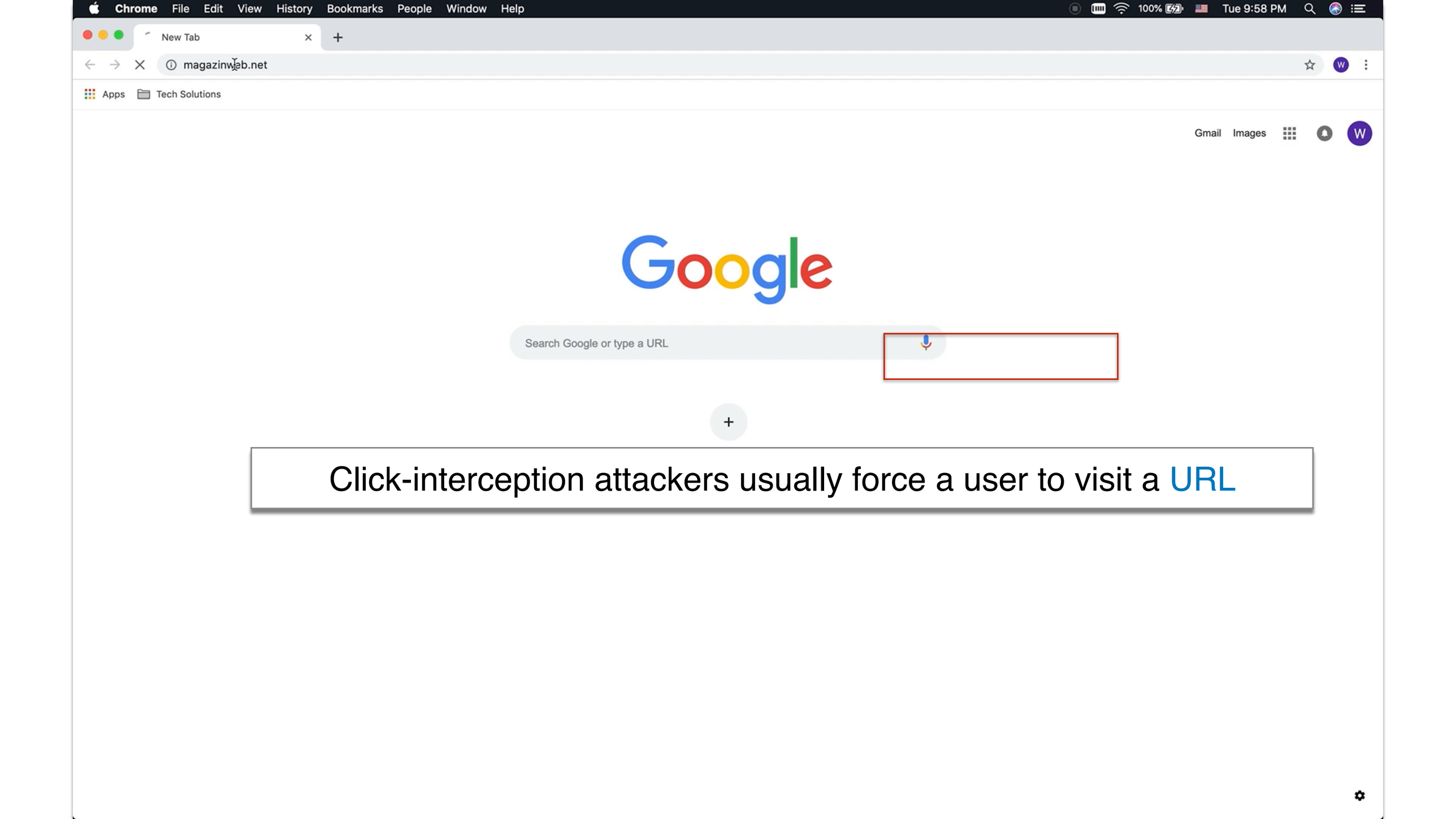
Academic rigour, journalistic flair

Search analysis, research, academics...

Arts + Culture | Business + Economy | Cities | Education | Environment + Energy | FactCheck | Health + Medicine | Politics + Society | Science + Technology

Theresa May's handling of Brexit is a classic case of bad leadership

December 12, 2018 9.35pm AEDT Updated December 13, 2018 8.47am AEDT


Chrome File Edit View History Bookmarks People Window Help
100% Tue 9:58 PM
New Tab
magazinweb.net
Apps
Tech Solutions
Gmail
Images
W
Google
Search Google or type a URL
Click-interception attackers usually force a user to visit a URL

Click Interception 101

- ***#1*: Hyperlinks**, i.e., <a> elements
  - Modifying *existing hyperlinks*

http://www.evil.com/

May offers MPs Brexit delay vote

```
<a id="head-1" href="http://www.evil.com/">ıews/uk-politics-47373996">
   <h2>May offers MPs Brexit delay vote</h2>
</a>
```

JavaScript

```
var a = document.getElementById("head-1");
var url = "http://www.evil.com/";
a.href = url;
```

Click Interception 101

- ***#1*: Hyperlinks**, i.e., <a> elements
  - Modifying *existing hyperlinks*
  - Creating *huge hyperlinks*

https://www.bbc.com/

<a href="http://www.evil.com/">

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

Vivamus eleifend felis nulla, in scelerisque orci vestibulum ut. Aenean augue sem, posuere sed finibus sit amet, accumsan quis elit. Nunc elementum tincidunt ante. Integer maximus nunc eget dolor pulvinar commodo. Vestibulum tincidunt libero sapien, vel egestas libero gravida et. Interdum et malesuada fames ac ante ipsum primis in faucibus.

JavaScript

```
var a = document.createElement("a");
var url = "http://www.evil.com/";
a.href = url;
a.innerText = "Lorem ipsum ...";
document.body.appendChild(a);
```

Click Interception 101

- ***#2*: EventListeners**

http://www.evil.com/

May offers MPs Brexit delay vote

```
<div class="container">
   <h2 id="head-1">May offers MPs Brexit delay vote</h2>
</div>
```

JavaScript

```
var h = document.getElementById("head-1");
var url = "http://www.evil.com/";
h.addEventListener("click", function() {
    window.location.href = url;
});
```

Click Interception 101

- ***#3: Visual Deception***
  - *Mimicry*

https://www.bbc.com/

Some Caption

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

Vivamus eleifend felis nulla, in scelerisque orci vestibulum ut. Aenean augue sem, posuere sed finibus sit amet, accumsan quis elit. Nunc elementum tincidunt ante. Integer maximus nunc eget dolor pulvinar commodo. Vestibulum tincidunt libero sapien, vel egestas libero gravida et. Interdum et malesuada fames ac ante ipsum primis in faucibus. Cras tempor eget ipsum non ullamcorper. Aliquam euismod lacus at elementum volutpat. Curabitur in fringilla quam, fermentum volutpat risus. Aenean eu sapien quam. Nulla sit amet sem pharetra, vestibulum nibh eu, dignissim diam. Vivamus condimentum in ipsum gravida feugiat.

Some Caption

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

Click Interception 101

- ***#3: Visual Deception***
  - *Mimicry*
  - *Transparent overlay*

http://www.evil.com/

Some Caption

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

Click me to visit http://www.evil.com/

Opacity: 50% 10% 1%

Threat Model

- First-party scripts are trustworthy (arguable)
- A third-party script may intercept click on any element
- Intercepting clicks on a script's own elements is allowed

http://www.a.com/

We focus on detecting third-party script click interception

First-party Scripts

```
<script src="assets/a.js">
<script src="http://static.a.com/b.js">
<script>alert("…");</script>
```

Third-party Scripts

```
<script src="https://doubleclick.net/ad.js">
<script src="https://lib.com/lib.js">
<script src="https://fb.com/like.js">
```

First-party elements

- Statically generated
- Dynamically generated

Third-party elements

- Dynamically generated
- Dynamically generated

A third-party script has the same privilege as a first-party script

Challenges of Detecting Click Interception

JavaScript code analysis

- JavaScript is a dynamic programming language
  - Static program analysis is difficult
- A script can insert an inline script, e.g., <script> ... </script>
  - Inline scripts do NOT have a src attribute
  - Determining the class of inline scripts is difficult

Element creation and mutation detection

- JavaScript is unable to determine the initiating script of an element
- A *MutationObserver* can observe mutation of attributes, childList, and subtree of a specific element
  - You have to create a MutationObserver for each element
  - It still does NOT know which script caused the change

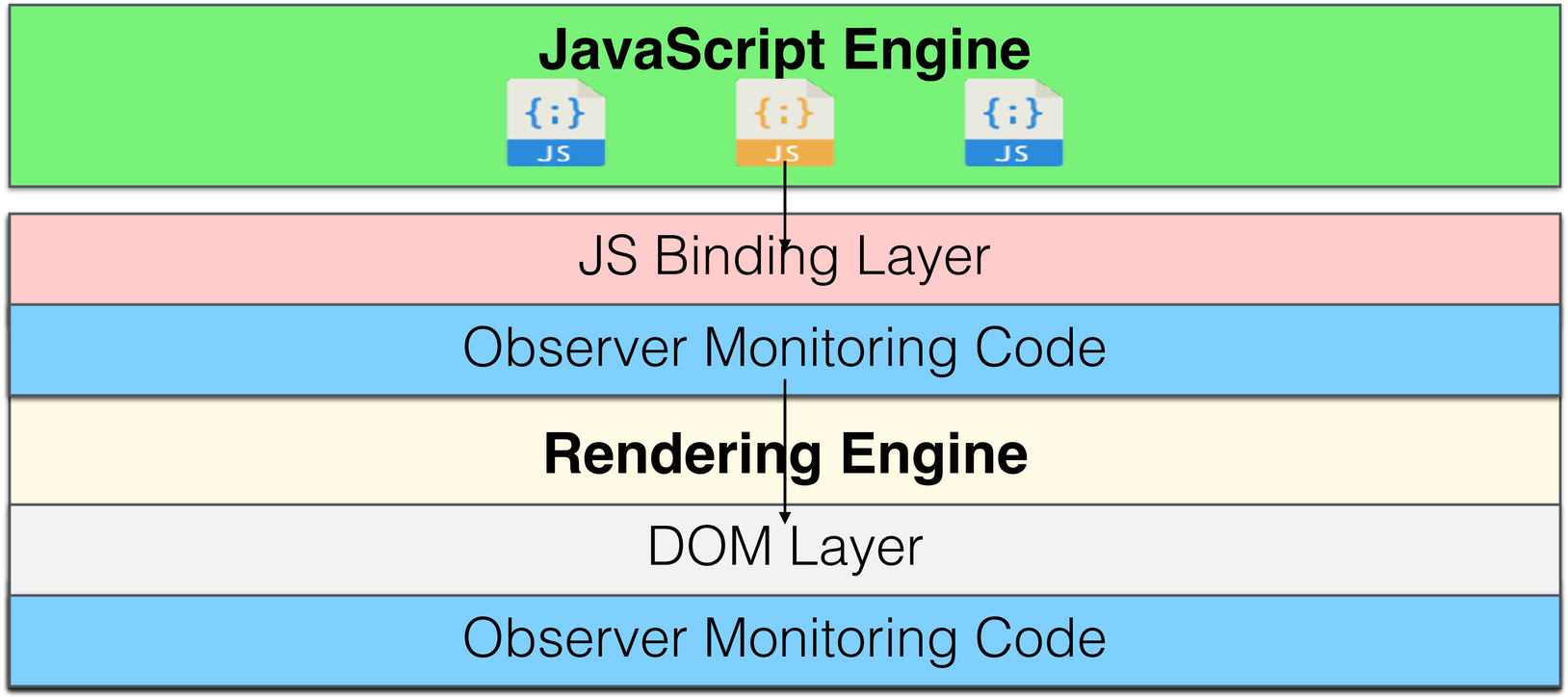
Would a browser extension help?

- No, browser extension is developed using JavaScript

Our Solution - Observer

A browser based analysis framework

- Detecting changes to hyperlinks
- Detecting dynamic hyperlink creations
- Detecting dynamic script insertions
- Detecting EventListener registrations



Detecting Changes to Hyperlinks

JavaScript Engine - V8

```
/* returns the scriptID of the bottom JS frame */
static int GetBottomScriptID();
```

JavaScript

```
var a = document.getElementById("head-1");
a.href = "http://www.evil.com/";
```

Rendering Engine

The Observer code is not exposed to JS

V8 Binding

```
static void HrefAttributeSetter(v8::Local ... alue,
  const v8::FunctionCallback ... nfo) {
 HTMLAnchorElem ... MLAnchorElement::ToImpl(info.Holder()
);

 ... ringOrTrustedURL cpp_value;
 V8USVStringOrTrustedURL::ToImpl(…, v8_value, cpp_value, …);
 impl->logChange(v8::GetBottomScriptID());
 impl->setHref(cpp_value, …);
}
```

DOM

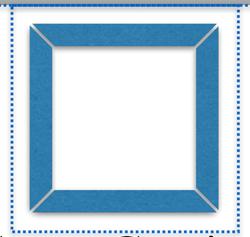
```
void HTMLAnchorElement::setHref(const USVStringOrTrustedURL& stringOrTrustedURL,
                                ExceptionState& exception_state) {
  setAttribute(kHrefAttr, stringOrTrustedURL, exception_state);
}
```

Observer Code

```
void HTMLAnchorElement::logChange(int scriptID) {
  this->changeLog->appendLog(scriptID, getAttribute(kHrefAttr));
}
```

Detecting Mimicry

https://www.bbc.com/

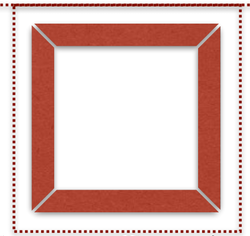


Some Caption

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

CSS class: para-medium, column-2
<img>: 1
size(container): 72K; ratio(<img>): 15%

Sibling element groups



Some Caption

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

CSS class: para-medium, column-2, xxx
<img>: 1
size(container): 70K; ratio(<img>): 16%

Detecting Transparent Overlay

https://www.bbc.com/

Some Caption

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas tempor dolor vel feugiat imperdiet. Vivamus maximus lectus ut pharetra consectetur. Duis in massa a lacus fringilla ullamcorper. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin aliquam lacinia nulla, a porttitor augue porta eu. Vivamus id vehicula quam. Phasellus tempor nibh ex, vitae fringilla elit maximus in. Vestibulum lacinia lobortis sem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla congue pulvinar ligula nec varius.

Opacity: 5% < threshold

Click me to visit http://www.evil.com/

Overlap: 10% 20% 100% > threshold

Implementation & Experiments

- Chromium 64.0.3282.186
  - ~1K lines of C++ code
- Browser automation using Selenium
  - Auto-clicking all elements
- Disabled page navigation in experiments to only log URLs

- Alexa top 250K websites
- Valid data from 228K websites (91.45%)
- 2M distinct third-party scripts
  - 1.2M distinct domains
- 2M unique *third-party* navigation URLs
  - 428K unique domains

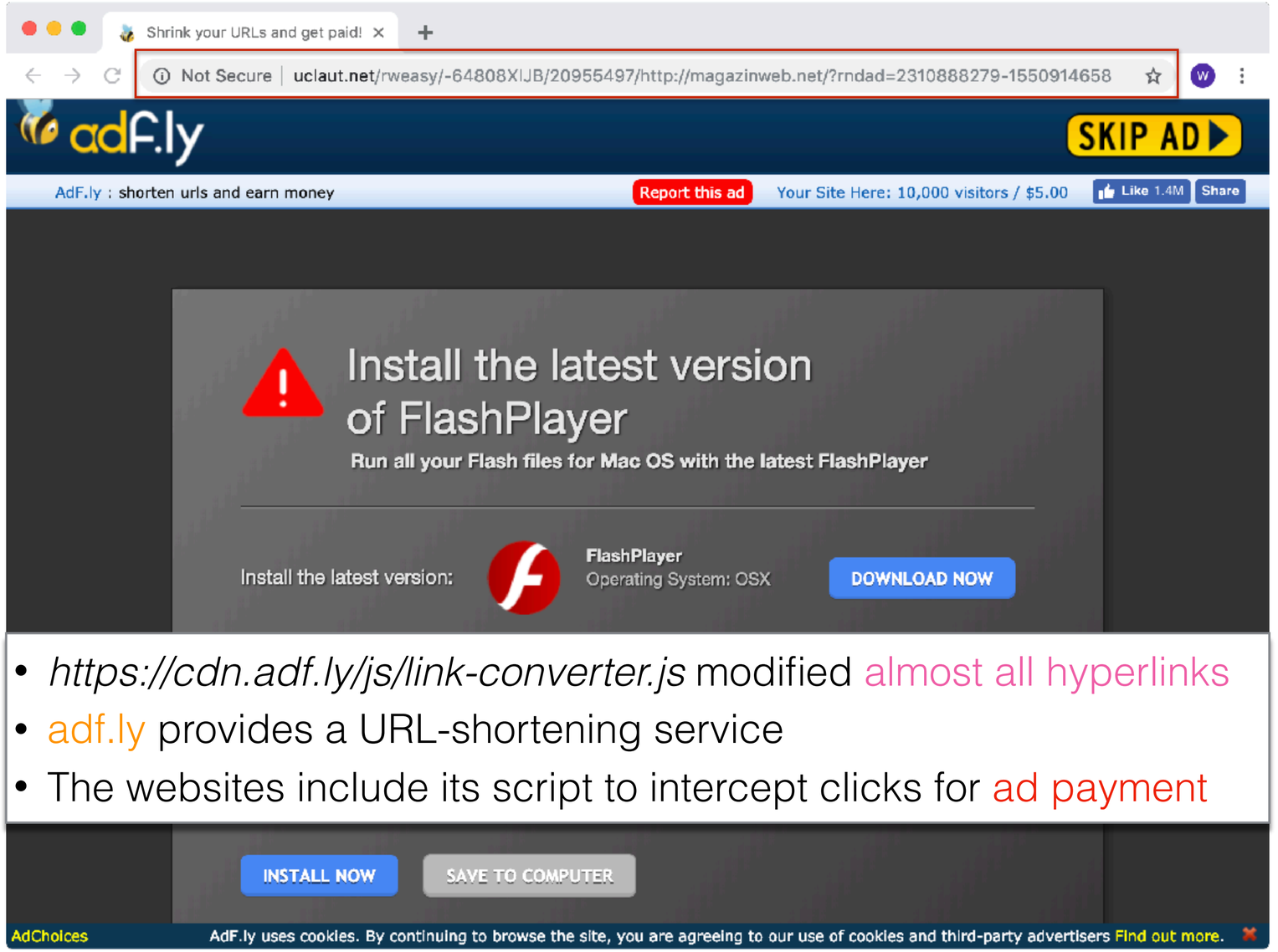
Results

437 scripts, 613 websites, 43 million combined daily visits

Technique	# Cases	# Websites	% Cases	# Daily Visits
Hyperlinks	4,178	221	89.52	12,686,591
Modifying 1st-party links	4,027	100	86.29	2,496,620
Modifying other 3rd-party links	31	2	0.66	638,247
Inserting huge 3rd-party links	120	119	2.57	9,551,724
Event Listeners	203	172	4.35	5,455,821
On 1st-party nodes	189	161	4.05	4,636,145
On other 3rd-party nodes	14	12	0.30	819,676
Visual Deceptions	286	231	6.13	25,269,314
Mimicry	140	87	3.00	16,604,258
Transparent Overlay	146	144	3.13	8,665,056

Case Study - Hyperlinks

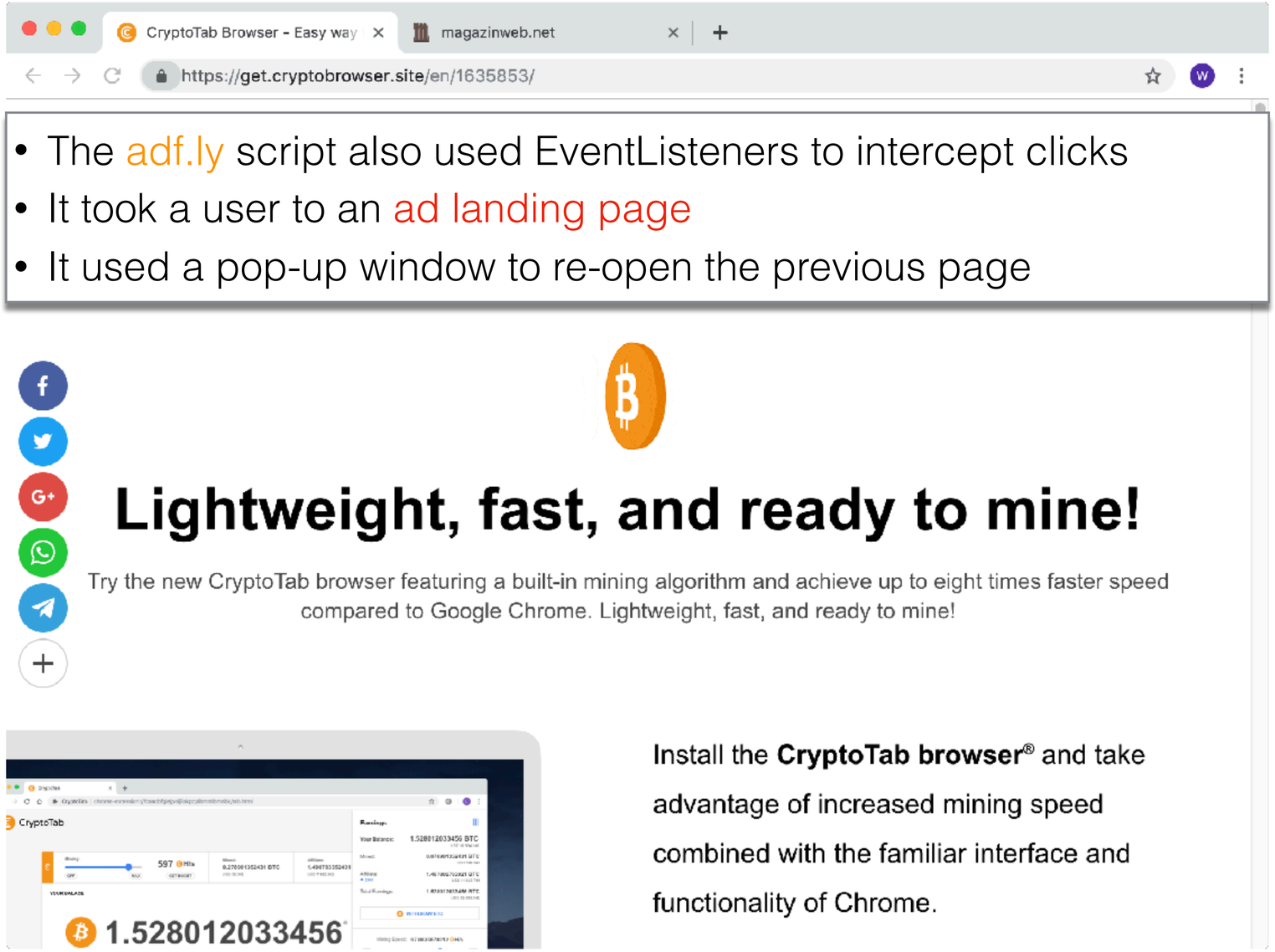
magazinweb.net



- *https://cdn.adf.ly/js/link-converter.js* modified almost all hyperlinks
- adf.ly provides a URL-shortening service
- The websites include its script to intercept clicks for ad payment

Case Study - EventHandlers

magazinweb.net



- The adf.ly script also used EventListeners to intercept clicks
- It took a user to an ad landing page
- It used a pop-up window to re-open the previous page

Case Study - Mimicry

bintag.com

TERKINI

Tessa Kaunang dan Sandy Tumiwa, Ketika Cerita Damai Bersenandung

4 hari lalu

Lirik Lagu Lauv, Bracelet

34 menit lalu

Ramai Fenomena Artis Bercadar, Ini Kata Alyssa Soebandono

49 menit lalu

Share Pengalaman #JagainKamu dan Menangkan Trip Sehat Kec...

Sponsored

Jelang Pernikahan Pria Ini

54 menit lalu

POPULER

Dikritik Netizen, Gaya Jessica Iskandar Dinilai Kurang Santu...

Nagita Slavina Selalu Dipuji Sabar, Raffi Ahmad Bongkar...

REKOMENDASI

10 Fashion Gagal yang Bikin Kamu Ingin Beliin Mereka Baju!

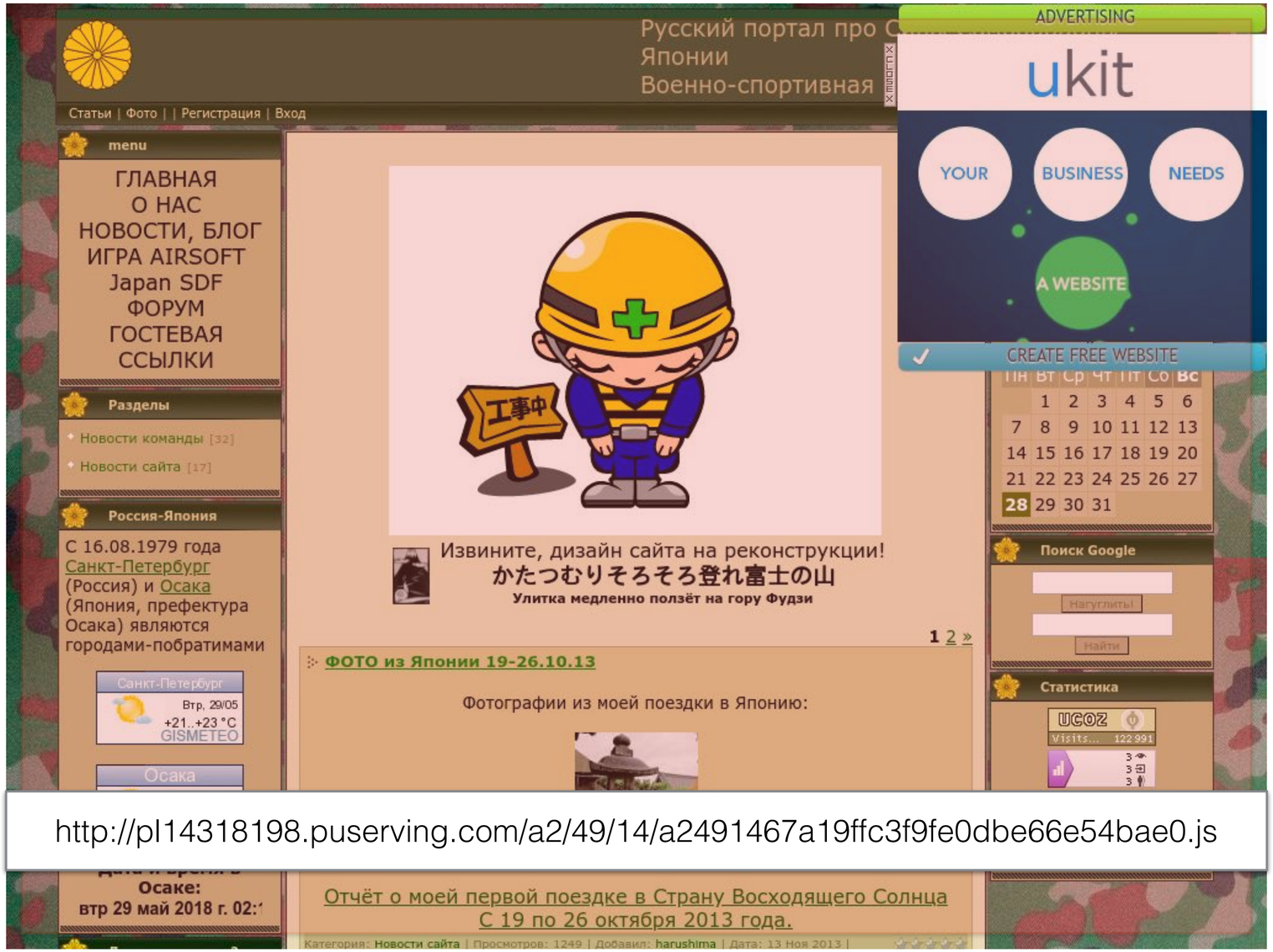
Ketika Nia Ramadhani Kena Getah Ucapannya Sendiri

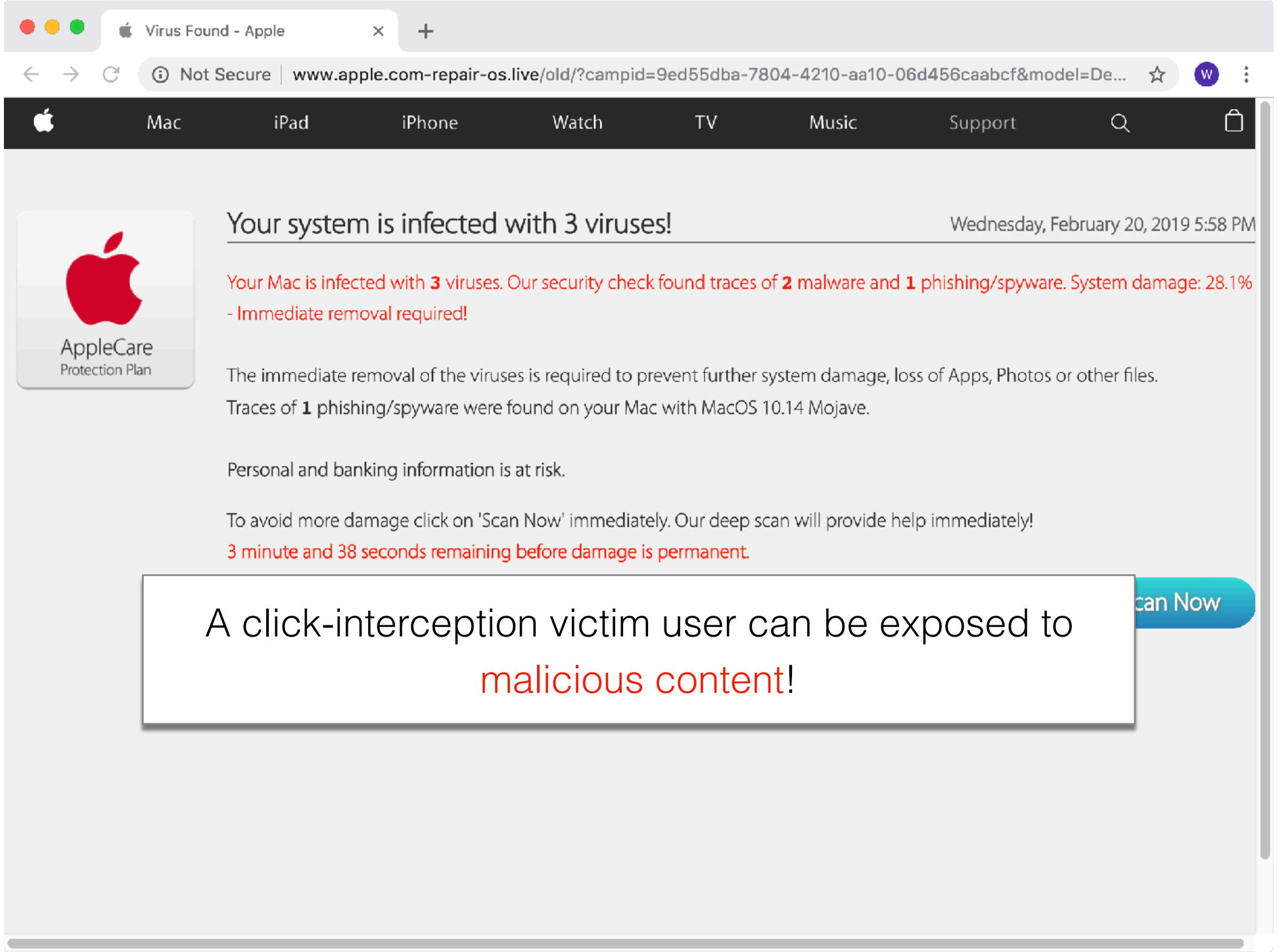
Pernah Populer, Nasib Pemain Boboho Sekarang Bikin Terkejut

https://securepubads.g.doubleclick.net/gpt/pubads_impl_207.js

Case Study - Transparent Overlay

jgsdf.ucoz.com




Virus Found - Apple
Not Secure
www.apple.com-repair-os.live/old/?campid=9ed55dba-7804-4210-aa10-06d456caabcf&model=De...
Mac
iPad
iPhone
Watch
TV
Music
Support
AppleCare
Protection Plan
Your system is infected with 3 viruses!
Wednesday, February 20, 2019 5:58 PM
Your Mac is infected with 3 viruses. Our security check found traces of 2 malware and 1 phishing/spyware. System damage: 28.1%
- Immediate removal required!
The immediate removal of the viruses is required to prevent further system damage, loss of Apps, Photos or other files.
Traces of 1 phishing/spyware were found on your Mac with MacOS 10.14 Mojave.
Personal and banking information is at risk.
To avoid more damage click on 'Scan Now' immediately. Our deep scan will provide help immediately!
3 minute and 38 seconds remaining before damage is permanent.
can Now
A click-interception victim user can be exposed to malicious content!

Conclusion

- A new class of privilege abuse by third-party JavaScript code
- Observer, a browser-based analysis framework
  - Hyperlinks, EventHandlers, Visual Deception
- 437 click-interception third-party scripts on 613 websites
- Click interception has become a new ad click fraud method
- Click interception can lead victim users to malicious contents
- Observer can be extended to stop click interception

Thank you!

Q & A