

Magecart Analizi

written by Mert SARICA | 4 April 2020

If you are looking for an English version of this article, please visit [here](#).

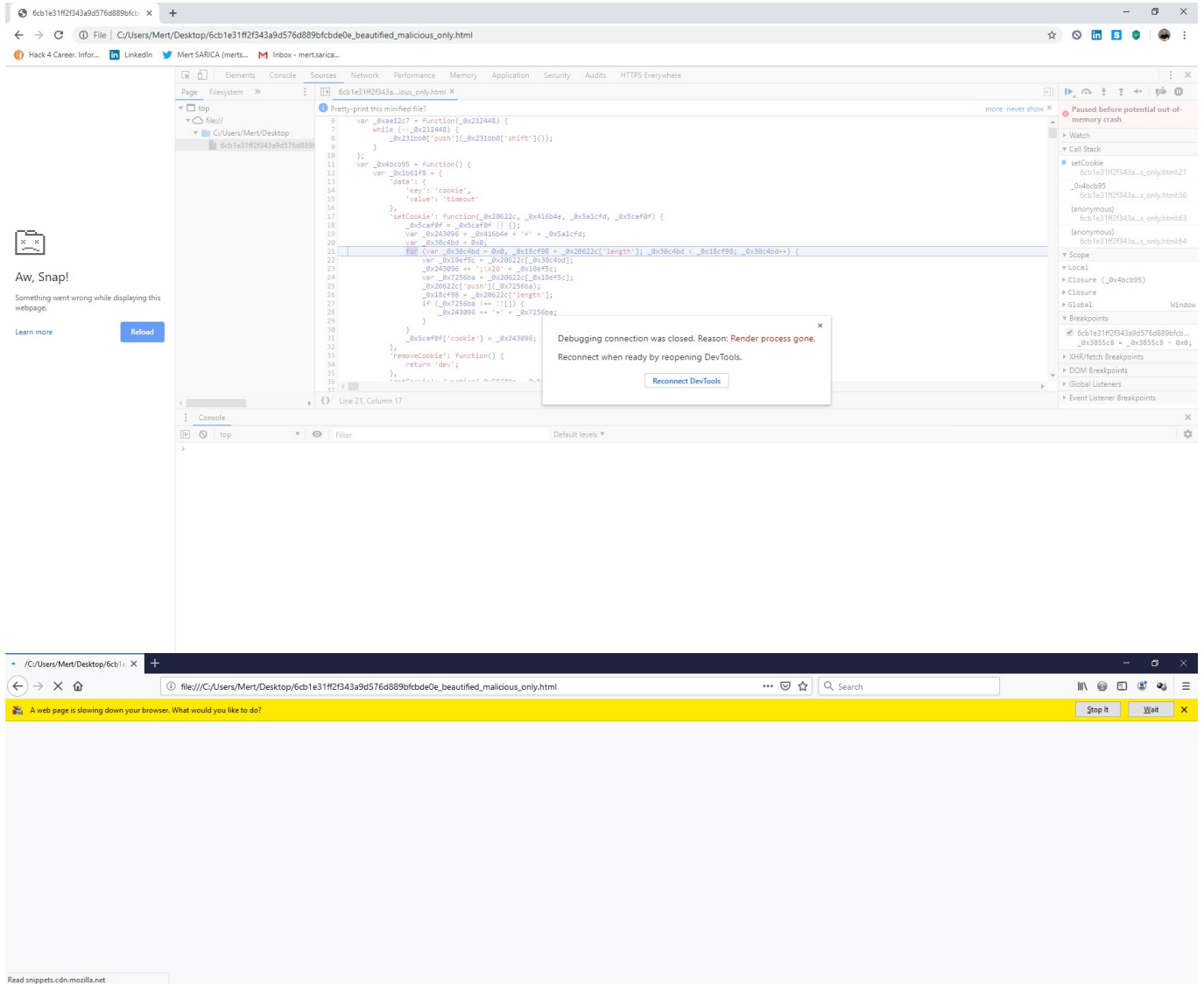
Hatırlarsanız Magecart ile Mücadele başlıklı blog yazımda zararlı JavaScript kodunun analizine başka bir yazımda yer vereceğimi belirtmiştim. Bu zamana dek çok defa zararlı javascript kodu analiz etmiş ve nasıl analiz edilebileceğine dair yaklaşık 3 yıl önce Zararlı JavaScript Analizi başlıklı bir blog yazısı da yazmıştım. Tabii yıllar geçtikçe tehdit aktörlerinin kullandığı yöntemler değişmeye ve siber güvenlik analistlerinin, araştırmacılarının işlerini git gide daha da zorlaştırmaya başladı.

Magecart grubunun geliştirdiği zararlı JavaScript kodu (6cble31ff2f343a9d576d889bfcdbde0e.js) ile ilk karşılaştığımda kodun kolay bir şekilde anlaşılamayacak kadar karmaşıklaştırılmış (obfuscated) olduğu JavaScript Obfuscator veya JavaScript Obfuscator Tool araçlarından biri kullanılmış olabilir.) hemen dikkatimi çekmişti. de4js ve IlluminateJs gibi araçların da varlığına güvenerek karmaşıklaştırılmış kodu kolay bir şekilde alt edeceğimi, en kötü dinamik kod analizi yaparak (debugging) mutlu sona ulaşabileceğimi düşünüyordum fakat evdeki hesap çarşıya uymadı. :)

```
"C:\Users\Mert\Desktop\YeniYazil\Magecart\6cble31ff2f343a9d576d889bfcdbde0e.js - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
6cble31ff2f343a9d576d889bfcdbde0e.js
1160 var childImgs=elem.querySelectorAll('img');for(var i=0;i<childImgs.length;i++){(var img=childImgs[i];this.addImage(img));
1161 if(typeof this.options.background=='string')(var children=elem.querySelectorAll(this.options.background);for(i=0;i<children.length;i++){var child=children[i];this.
addElementBackgroundImages(child);});var elementNodeTypes={1:true,9:true,11:true};ImagesLoaded.prototype.addElementBackgroundImages=function(elem)(var style=getComputedStyle(elem
);if(!style){return;
1162 var reURL=/url\(\s*(.*)?\s*\)/gi;var matches=reURL.exec(style.backgroundImage);while(matches!=null){var url=matches[2];if(url){this.addBackground(url,elem);}
1163 matches=reURL.exec(style.backgroundImage);});ImagesLoaded.prototype.addImage=function(img)(var loadingImage=new LoadingImage(img);this.images.push(loadingImage););ImagesLoaded.
prototype.addBackground=function(url,elem)(var background=new Background(url,elem);this.images.push(background););ImagesLoaded.prototype.check=function(){var _this=this;this.
progressedCount++;this.hasAnyBroken=false;setTimeout(function(){this.complete();return;
1164 function onProgress(image,elem,message){setInterval(function(){this.progress(image,elem,message);});
1165 this.images.forEach(function(loadingImage)(loadingImage.once('progress',onProgress);loadingImage.check();));ImagesLoaded.prototype.progress=function(image,elem,message)(this.
progressedCount++;this.hasAnyBroken=this.hasAnyBroken||!image.isLoaded;this.emitEvent('progress',[this,image,elem]);if(this.jqDeferred&&this.jqDeferred.notify)(this.jqDeferred.
notify(this,image));
1166 if(this.progressedCount===this.images.length){this.complete();}
1167 if(this.options.debug&&console){console.log('progress: '+message,image,elem);});ImagesLoaded.prototype.complete=function(){var eventName=this.hasAnyBroken?'fail':'done';this.
isComplete=true;this.emitEvent(eventName,[this]);this.emitEvent('always',[this]);if(this.jqDeferred){var jqMethod=this.hasAnyBroken?'reject':'resolve';this.jqDeferred[jqMethod](
this);};function LoadingImage(img){this.img=img;
1168 LoadingImage.prototype.create(EventEmitter.prototype.check=function(){var isComplete=this.getIsImageComplete();if(isComplete){this.confirm(this.img.
naturalWidth===0,'naturalWidth');return;
1169 this.proxyImage=new Image();this.proxyImage.addEventListener('load',this);this.proxyImage.addEventListener('error',this);this.img.addEventListener('load',this);this.img.
addEventListener('error',this);this.proxyImage.src=this.img.src;LoadingImage.prototype.getIsImageComplete=function(){return this.img.complete&&this.img.naturalWidth};
LoadingImage.prototype.confirm=function(isLoaded,message)(this.isLoaded=isLoaded;this.emitEvent('progress',[this,this.img,message]););LoadingImage.prototype.handleEvent=function(
event)(var method='on'+event.type;if(this[method]){this[method](event););LoadingImage.prototype.onload=function(){this.confirm(true,'onload');this.unbindEvents();};LoadingImage.
prototype.onerror=function(){this.confirm(false,'onerror');this.unbindEvents();};LoadingImage.prototype.unbindEvents=function(){this.proxyImage.removeEventListener('load',this);
this.proxyImage.removeEventListener('error',this);this.img.removeEventListener('load',this);this.img.removeEventListener('error',this);};function Background(url,element)(this.url=
url;this.element=element;this.img=new Image());
1170 $=jQuery;$=jQuery.extend(function(options,callback)(var instance=new ImagesLoaded(this,options,callback);return instance.jqDeferred.promise($($this));});ImagesLoaded.
makeQueryPlugin().return ImagesLoaded.});var _Ox4e75=['wzDlMOJw7ob','wqfDp2ndtww','wrfciABCQew','WMKypwNIX8OCCQ==','wprCoHPDjQ==','2CAmfA==','w0xw6fDnMKRwPmM','w7nDlMKRw6Y=','
FUTCjXCCoA==','wpbDmsOI','cV1w6M','wpjDlIHdnXbdq84=','2M04aMKlJQ==','wzDwqBlw5w','w5/Cq807wrcnF0=','wpXDvhrDp2g=','w4rCq8oAwpfCmw=','wzLdnOUsW47Ck2ABw75Pw5YFwUg=','
w0DhncLw4BBwqEKwrDp8kFR8Ew4E=','aMOXw6l2w5d0','wzHw7nDv8RTwpg=','2sOrdeKsMcK8wog2','w0l6wrcCmfcCn8K/QQ==','w5oVwocJw708Vh0=','
fjEzAMRTTMOqWELCtWbCpWdLwUwXDrGUpC02w5NFPcKfMM09FEXDKtZdrsRnoATDgWfDoGAlTaRBT3R9BUjw5rDpsOlwqfDw5HdhsKwAM0owpJcGEEfwQYAMKKIU/Dsg==','w5XCk8R7wqDnQ==','w68HDMoRtk=','
w4DtmIiw7Y=','L37dk3k9w==','wzDrs0rW6A4','w7PCncOPwQT','wonDkjnbokA=','w7EHAB0eSALCg8KsLMK4','QEDChB402zYN','w73DiYpDtcGw4LDjRV/w6DIw6Qxw8=','w5owQZTbSbCmQ==','
wzgxw6PdnCLmpUuwojDtcQjDvs0wqds','wzHhDjJdUDDlA==','wqjDgcOUw5Sw4HdxDCo8OeChXCVFs=','KlDCKATC0g8=','w77Ct148w8=','wohqpLcs3Xcm8K/QcKPw4Mdw6fciWc=','SMOpw54=','wpluworCg3w=','
H8Ktw4fdtUit=','w47Dv0bDn8Ka','wovcklTDqA==','QcKBA30v','w43cK8R6wzA=','wqk2CyCpCnw==','w5HDv0bDhg==','w6fCso06wpg5BB7CvcKw0/DksKRw0SAfEQXwooywQ==','wozHwbpCg20=','
eWw0pTtUQlfa80KwAoNajDkxw78T','tCkyypdUo8EArpPG2TCjsoHr7w0bLKM06JA==','2lYhw7vDuMKlUkM=','MDU5wpgvQ==','w0BpQxV6D3vDnyo=','w4RcQ804wHcnlA=','wzvcPgTDjD53NgQ5','
WMN0b15Nqocfsc0x','w5/DgTDnMKW4g=','os0uw57Dl==','w4cDf8ot','wqgDp3PrC0qBm0Q==','w7sXwpgUwzP','w4xeU8KYw4rDnQ==','wpcHmDgMKUvFTBwQ=','cizCgsOI','ecKywo1t','wpzDgcOw60=
','Ms0gw4vDbk8NssQJwQ=','wzuxwPcKlJCsK4YsKIw5Iz77Csw==','WDAqesK7BA==','w4bCo18rwr8u','w77DjYpDkg==','w5vDiMKRVw6ZDuso2','BrgLLA==','B3rDiXs=','H8KNw45n','wqjCk2/DJA==','
w0cDl3Xds80W==','WUUP','Es0qW4TDkMRaTA==','EhwRRCrW4zC12c=','w4OXD80uVCM=','w5fDhsKmw6k=','DW7DkHwsQA==','V8K078RX','FcK2w5dkwrPCmQ==','Pc0Zw7w=','wpDcGRVR','wzXDmsOlB==',
'EwZg','XiorfMR7BA==','w4wup85','wqCnXfDjCkFQ==','E8K0w52IwPcMq==','wzrDKM0taUFT','w0Fd180W70bW5DbmBacV8ODRCGLClFJc','Ys4Kw099W80TRhZTHGFCgsOfw4UI','QcOpbMK4',
w4RtKw4wzmq==','wKcGGA==','w6vCncK7wHDncR0w5vclMK8wpjJw7DnMoc','wq7woh','wzrDKM0taUFTB8KlqBwDvcO9w6AcwpU','w4DcuV4tw8u','IUTCiQM=','w4zc0Yo','w0LDi80ow60W',
wqzCgDblA==','bkDchXoR','w4zc0Ys','w1gUw8=','w4NDM04W==','wqbdJTDpQ==','w6vDu0vDmA==','w0nDqXTDv==','c8RkywoJc','NkDcXki=','w4rDmyTDmw==','w5DCL8Kj','CsKvMYtC',
bMKH0w7eq==','w7bDlCRAW6fDu0h','w6HduDTmg==','IMR8w6w=','wz7Dum8=','w4fCso06wP4ABTCvckQwondQ==','wph/wpAvf10=','w73DjYpDl==','w5PCmncDmsKSDg==','wpp7wo8zbY==','w4owupg9BwQ=
','ZyRywoB2w0E','w5XDU14=','dMRWtw==','Ej7Ck80Bw70c','WMow08=','M3cD20s','UcR0SMRTw6X','d8RwMKR2w0G','w68qwp8=','wqsCpYcnwq4=','
ZyRywoB2w0E','w5XDU14=','dMRWtw==','Ej7Ck80Bw70c','WMow08=','M3cD20s','UcR0SMRTw6X','d8RwMKR2w0G','w68qwp8=','wqsCpYcnwq4=','
length:1142,306 lines:1,171 Ln:1129 Col:1254 Sel:8:1 Unix (LF) UTF-8 INS
```

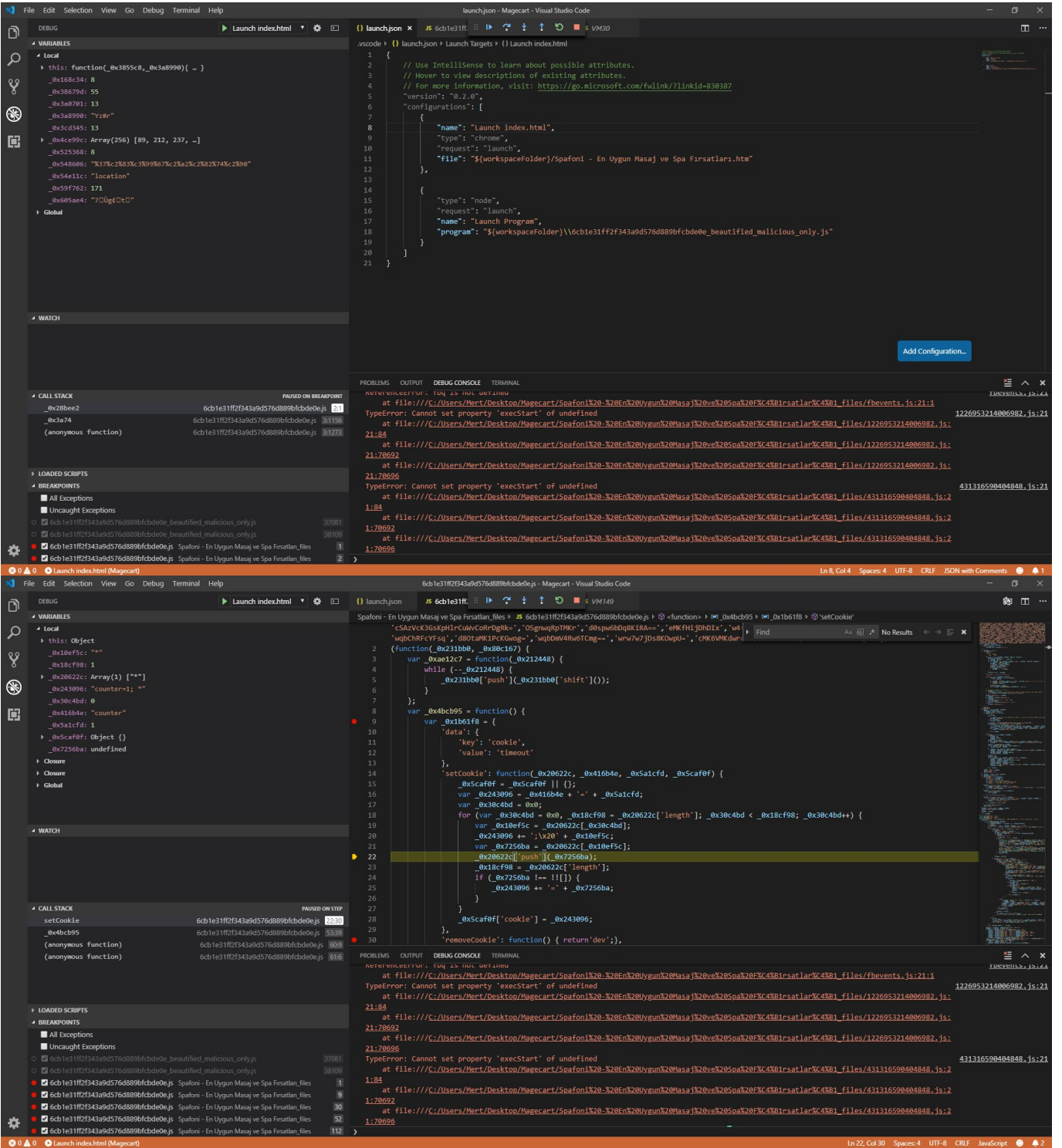
İlk iş olarak JavaScript Beautifier web sitesinden faydalanarak zararlı kod bloğunu okunaklı hale getirdim. Ardından kodu anlaşılır hale getirmek için

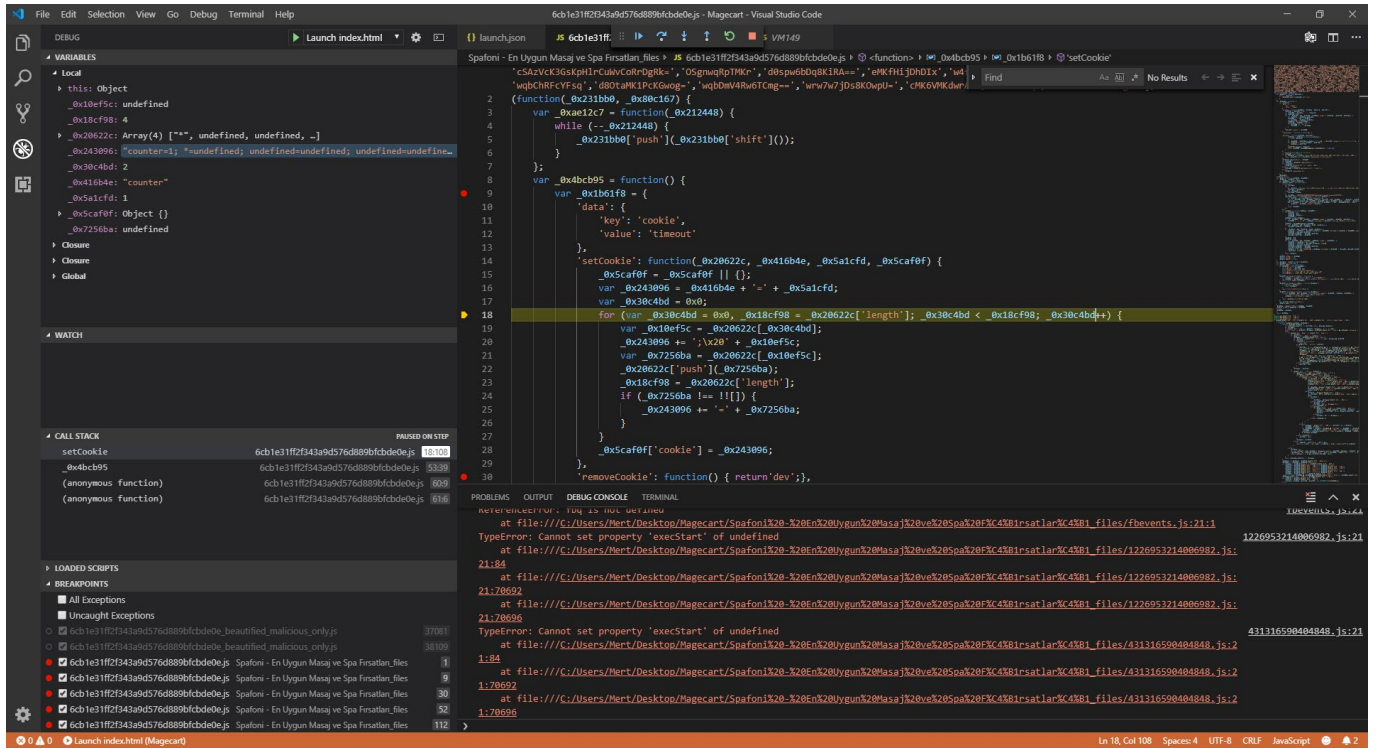
sırasıyla de4js ve IlluminateJs araçlarından faydalanmaya çalıştım ancak başarısız oldum. Chrome DevTools ile zararlı JavaScript kodunu hata ayıklaması (debugging) yaparak analiz etmeye başladım ve çok geçmeden bir zaman sonra işlerin yolunda gitmediğini farkettilim. Chrome'dan kaynaklanan bir problem olabileceğini düşünerek şansımı Firefox ile denemeye karar verdim fakat o da birşeylerin yolunda gitmediğine dair uyarı verdi.



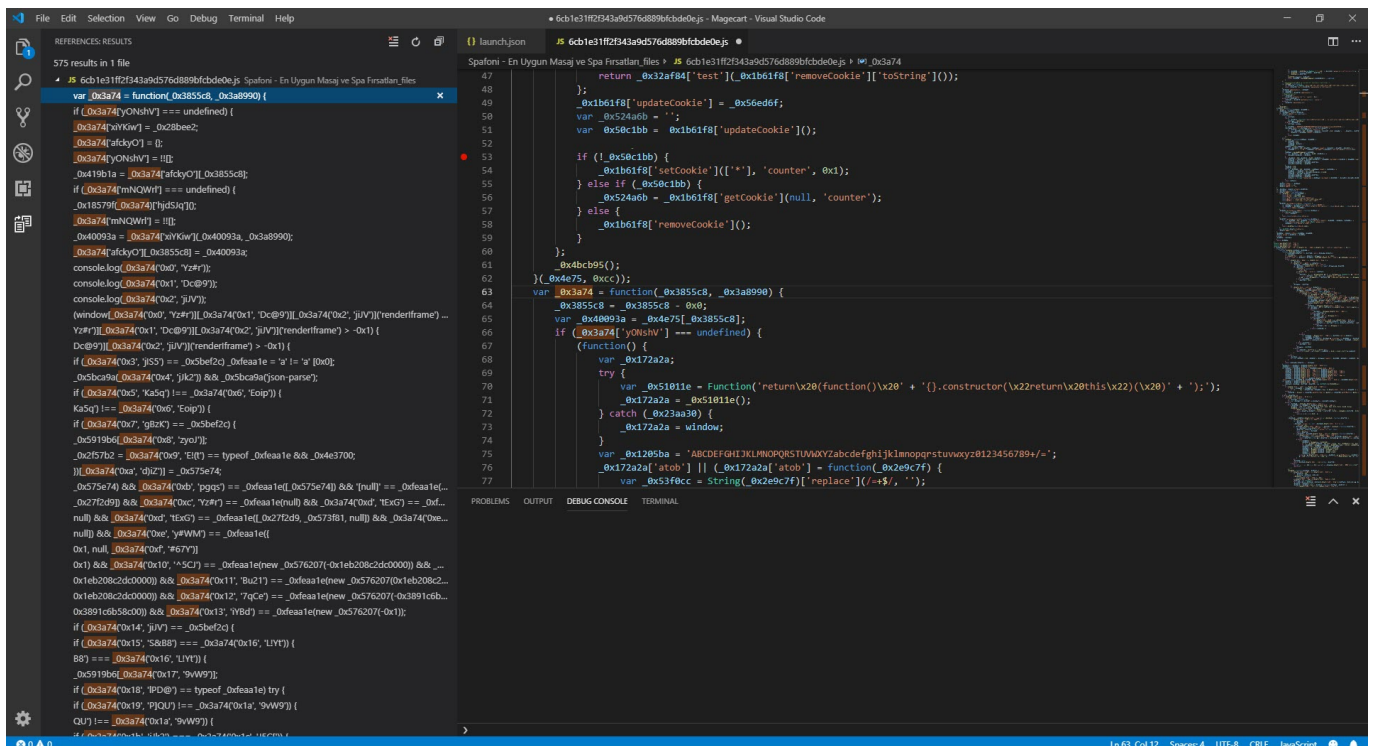
Ne yapabileceğime dair hindi gibi düşünüp dururken internet tarayıcısı yerine farklı bir araç ile hata ayıklaması yapabilmek için araştırma yapmaya

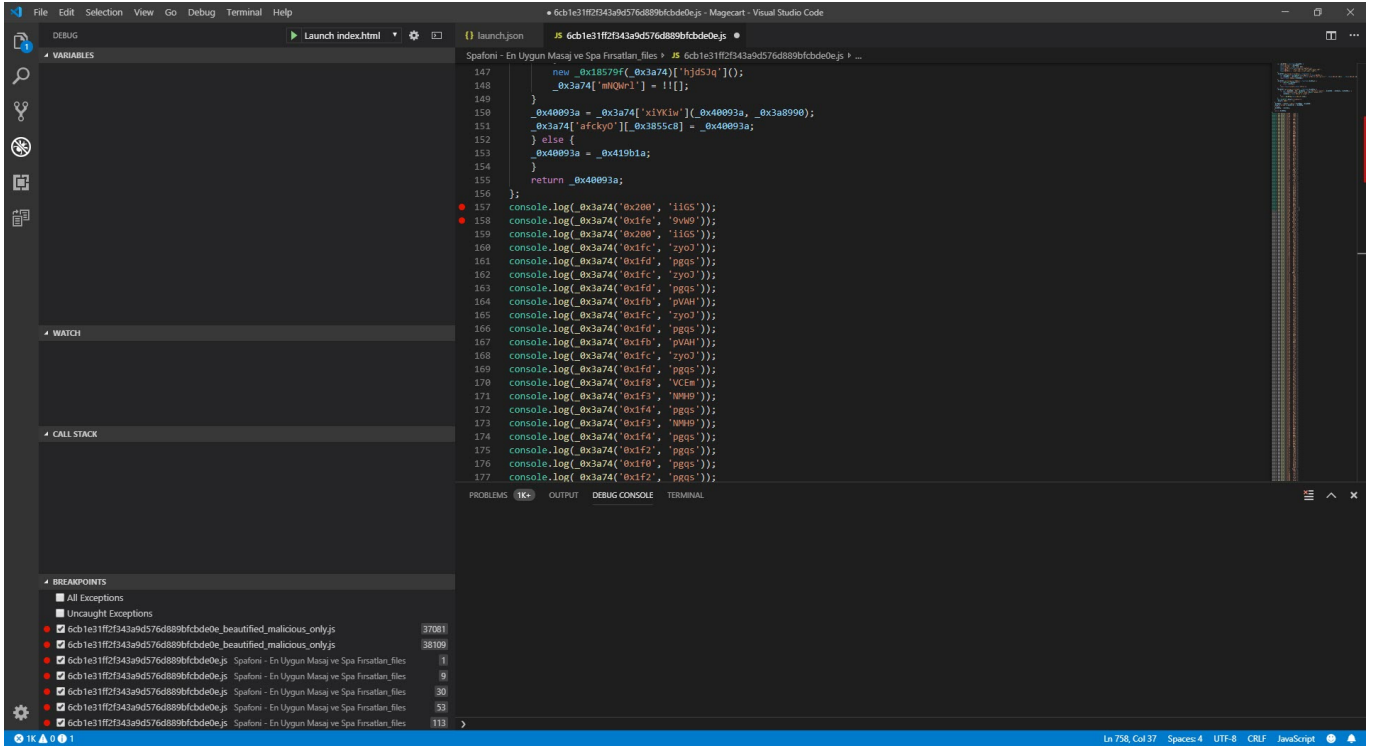
başladım ve Visual Studio Code isimli kaynak kodu editörü ile karşılaştım. Chrome hata ayıklama eklentisi sayesinde arka planda HTML, JavaScript kodu analiz etmeye imkan tanıyan ve çok sayıda eklentiye sahip olan bu editör ile hata ayıklaması yapmaya başladığımda, SetCookie ile ilişkili fonksiyonun çok sayıda dizi (Array) oluşturarak bellekteki kullanılabilecek alanları tüketerek hata ayıklamasını etkisiz hale getirdiğini (self defending) gördüm.



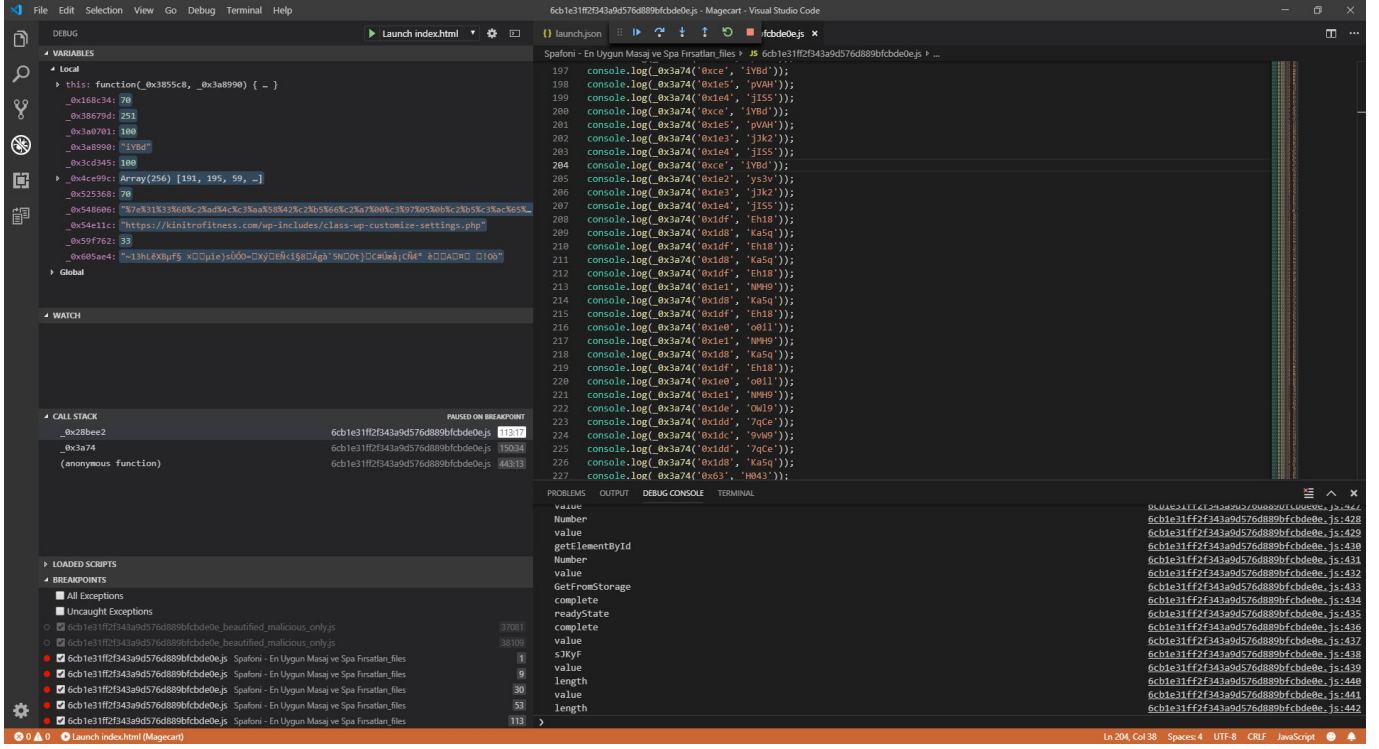


Art niyetli kişilerin amaçları doğrultusunda bu kodun internet tarayıcısında sorunsuz bir şekilde çalışması gerektiği için koda hata ayıklamasına yönelik kontroller olduğunu düşünerek her bir fonksiyonu adım adım analiz etmeye başladım. Nihai hedefim kodu baştan sonra dinamik olarak analiz etmek olmayıp çalınan bilgilerin hangi web sitesine iletilildiğini ve gizlenmiş karakter dizilerini (strings) çözmek olduğu için gizlenmiş dizilerin çözülmesi amacıyla kullanılan `_0x3a74` fonksiyonundan yola çıkarak ilerledim.





Analiz ederken bir yerde Regex ile removeCookie değerinde { işareti ile return kelimesi arasında boşluk kontrolü yapıldığını farkettim. Boşluk karakterinin tespit edilmesi durumunda kodun akışı yukarıda bahsettiğim çok sayıda dizi oluşturup probleme yol açan fonksiyona ilerliyordu. Peki art niyetli geliştirici neden böyle bir kontrol koymuştu ? Bu gibi karmaşılaştırılmış, okunaklı olmayan kodlarla karşılaşan analistlerin ilk yaptığı iş, kodu araçlar (JavaScript Beautifier gibi) yardımıyla okunaklı, formata uygun bir hale getirmek olduğu için bu araçlar otomatik olarak araya boşluk koyuyorlardı ve bu da kodun analiz edildiğine dair art niyetli kişilere güzel bir tespit mekanizması oluşturmaya imkan tanıyordu.



Ülke olarak COVID-19 salgınını geride bırakacağımız sağlıklı günlerde yeni bir yazı ile tekrar görüşmek dileğiyle herkese sağlıklı ve güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediyem Var #17 oyununun çözüm yolunu da içermektedir.