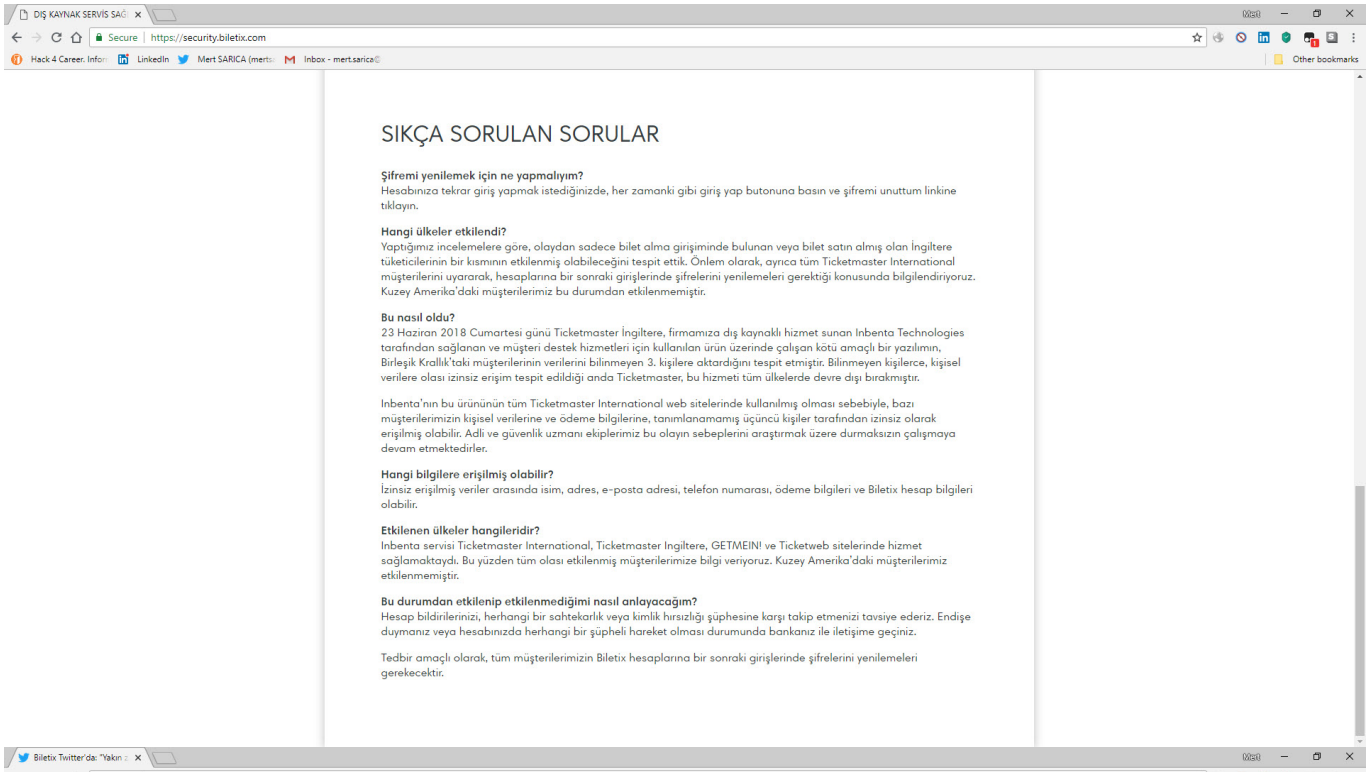
Biletix Vakası

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.



SIKÇA SORULAN SORULAR

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

Hangi ülkeler etkilendi?
Yaptığımız incelemelere göre, olaydan sadece bilet alma girişiminde bulunan veya bilet satın almış olan İngiltere tüketicilerinin bir kısmının etkilenmiş olabileceğini 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 etkilenmemiştir.

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 verilere olası izinsiz erişim tespit edildiği anda Ticketmaster, bu hizmeti tüm ülkelerde devre dışı bırakmıştır.

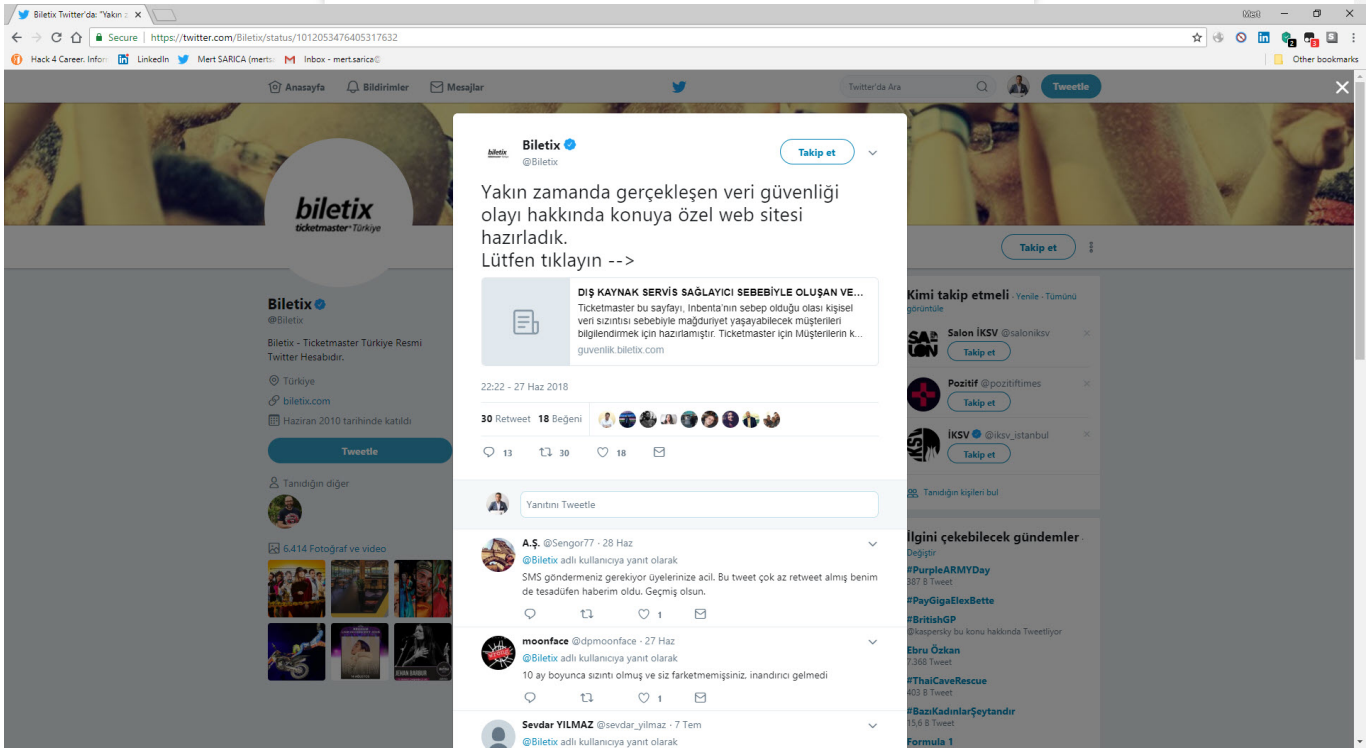
Inbenta'nın bu ürününün tüm Ticketmaster International web sitelerinde kullanılmış olması sebebiyle, bazı müşterilerimizin kişisel verilerine ve ödeme bilgilerine, tanımlanamamış üçüncü kişiler tarafından izinsiz olarak erişilmiş olabilir. Adli ve güvenlik uzmanı ekiplerimiz bu olayın sebeplerini araştırmak 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 sağlamaktaydı. Bu yüzden tüm olası etkilenmiş müşterilerimize bilgi veriyoruz. Kuzey Amerika'daki müşterilerimiz etkilenmemiştir.

Bu durumdan etkilenip etkilenmediğimi nasıl anlayacağım?
Hesap bildirilerinizi, 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.



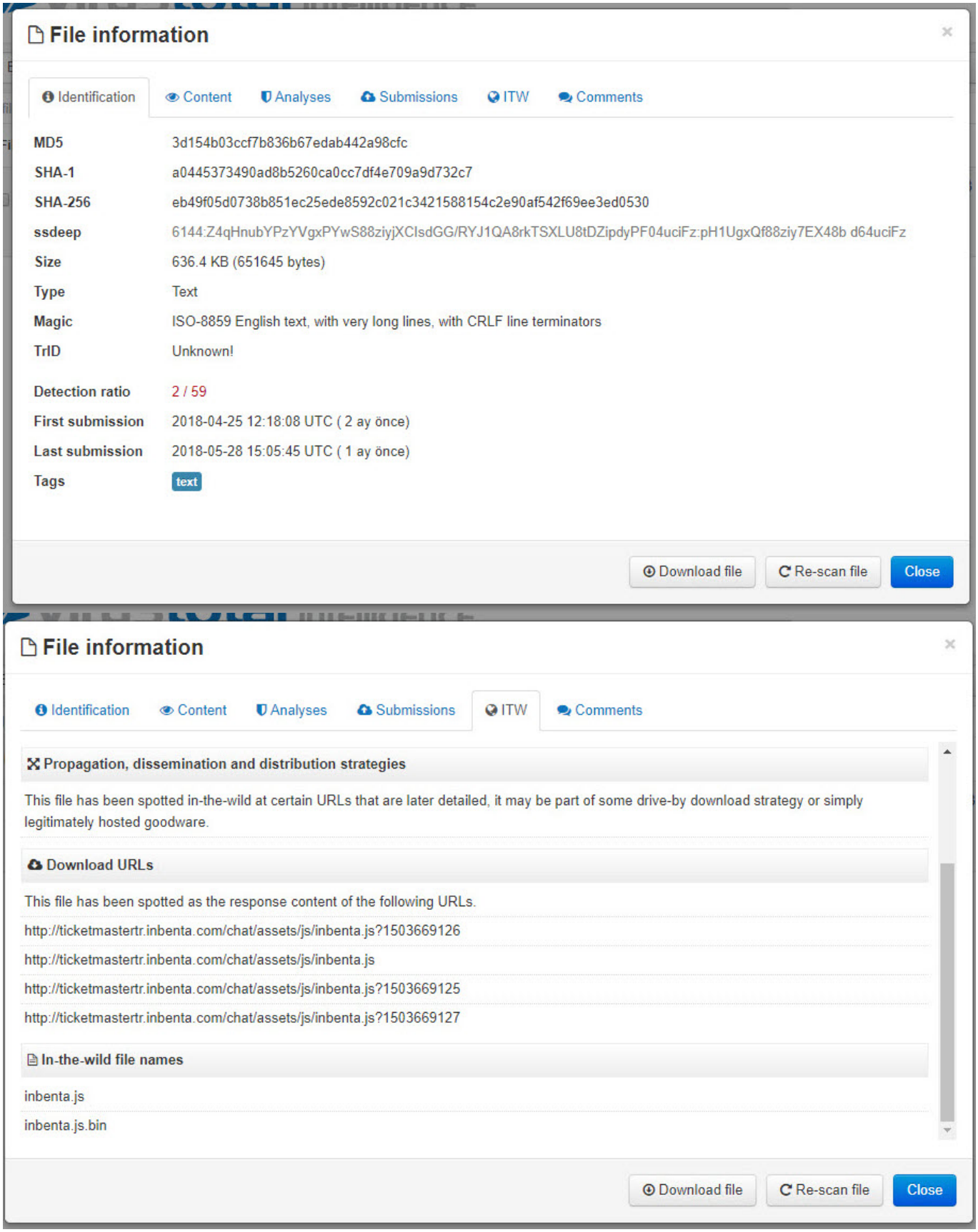
Aktif olarak bünyelerinde izleme ve müdahale yapan analistlerden oluşan bir Siber Güvenlik Merkezi'ne sahip olan kurumlar, Biletix'te doğru gitmeyen birşeyler olduğunu Nisan ayı gibi kullandıkları güvenlik teknolojilerinin ürettiği alarmları sayesinde öğrendiler. ;) Mayıs ayı itibariyle antivirüs yazılımlarına 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.

virustotal

SHA256:	eb49f05d0738b851ec25ede8592c021c3421588154c2e90af542f69ee3ed0530
Tespit edilme orani	2 / 59
Analiz tarihi:	2018-06-21 10:20:15 UTC (2 hafta, 3 gün önce) En sonuncusunu görüntüle

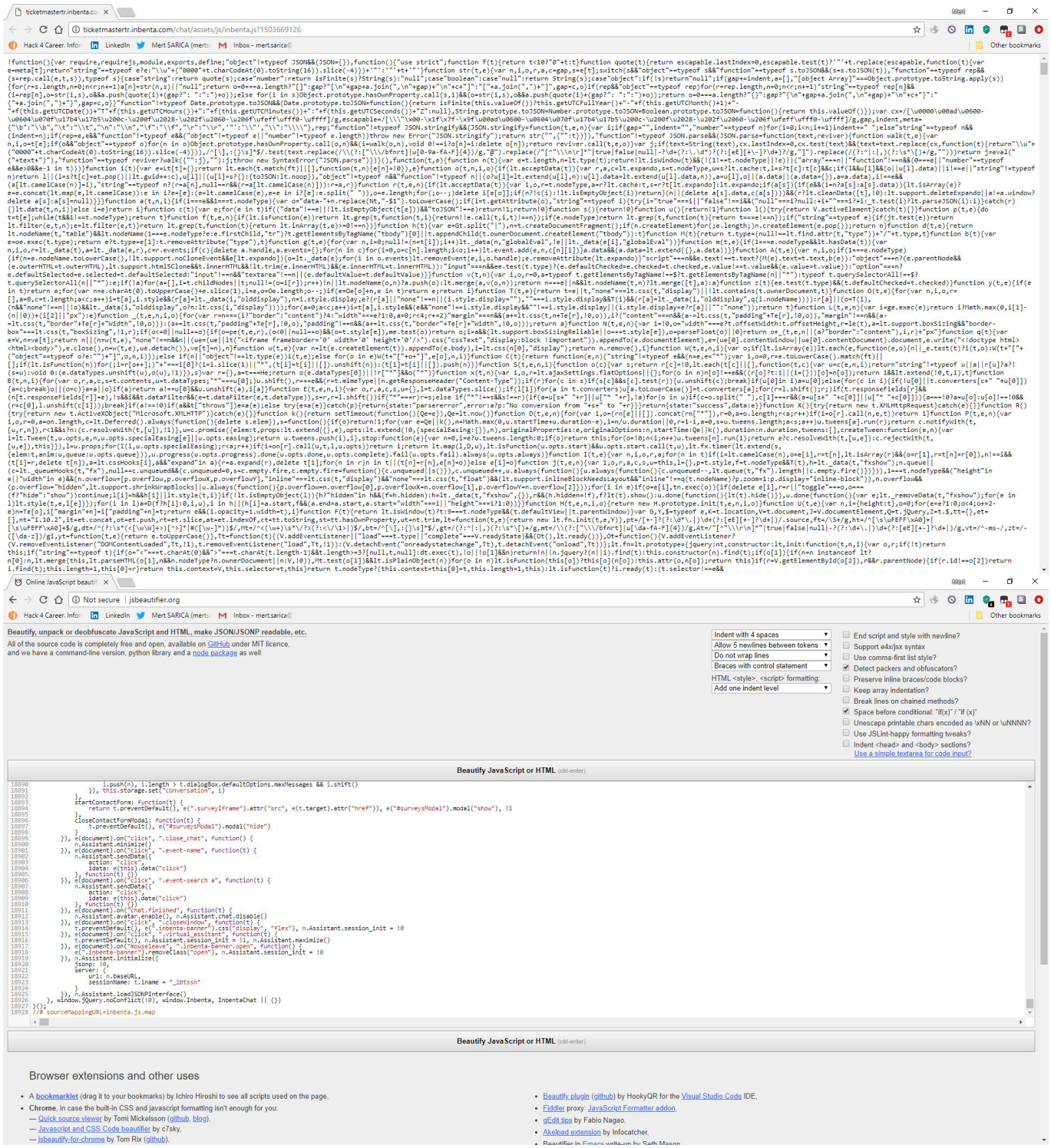
Analizler. Ek bilgi. Yorumlar. 1 Oylar

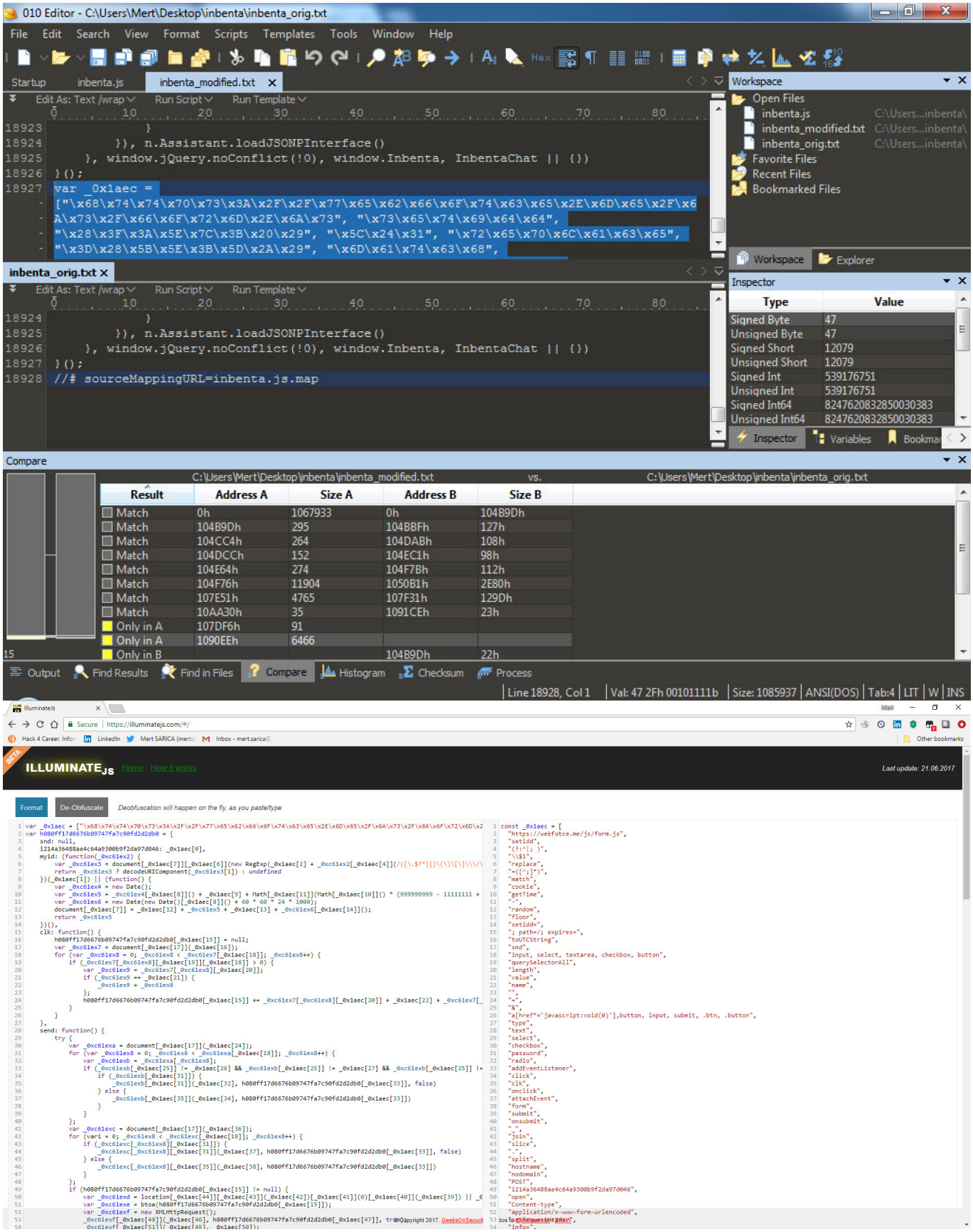
Antivirus	Sonuç	Güncelle
Symantec	Infostealer	20180621
TrendMicro-HouseCall	Suspicious_GEN.F47V0516	20180621
Ad-Aware	✓	20180621
AegisLab	✓	20180621
AhnLab-V3	✓	20180621
Alibaba		20180621
ALYac	✓	20180621
Antiy-AVL	✓	20180621
Arcabit	✓	20180621
Avast	✓	20180621
Avast-Mobile	✓	20180621
AVG	✓	20180621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



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





Javascript kodunu okunaklı, anlaşılır hale getirdikten sonra 2. satırda yer alan hxxps://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 orani	16 / 58
Analiz tarihi:	2018-07-07 00:16:17 UTC (7 saat, 1 dakika önce)

Analizler. | Ek bilgi. | Yorumlar. 1 | 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

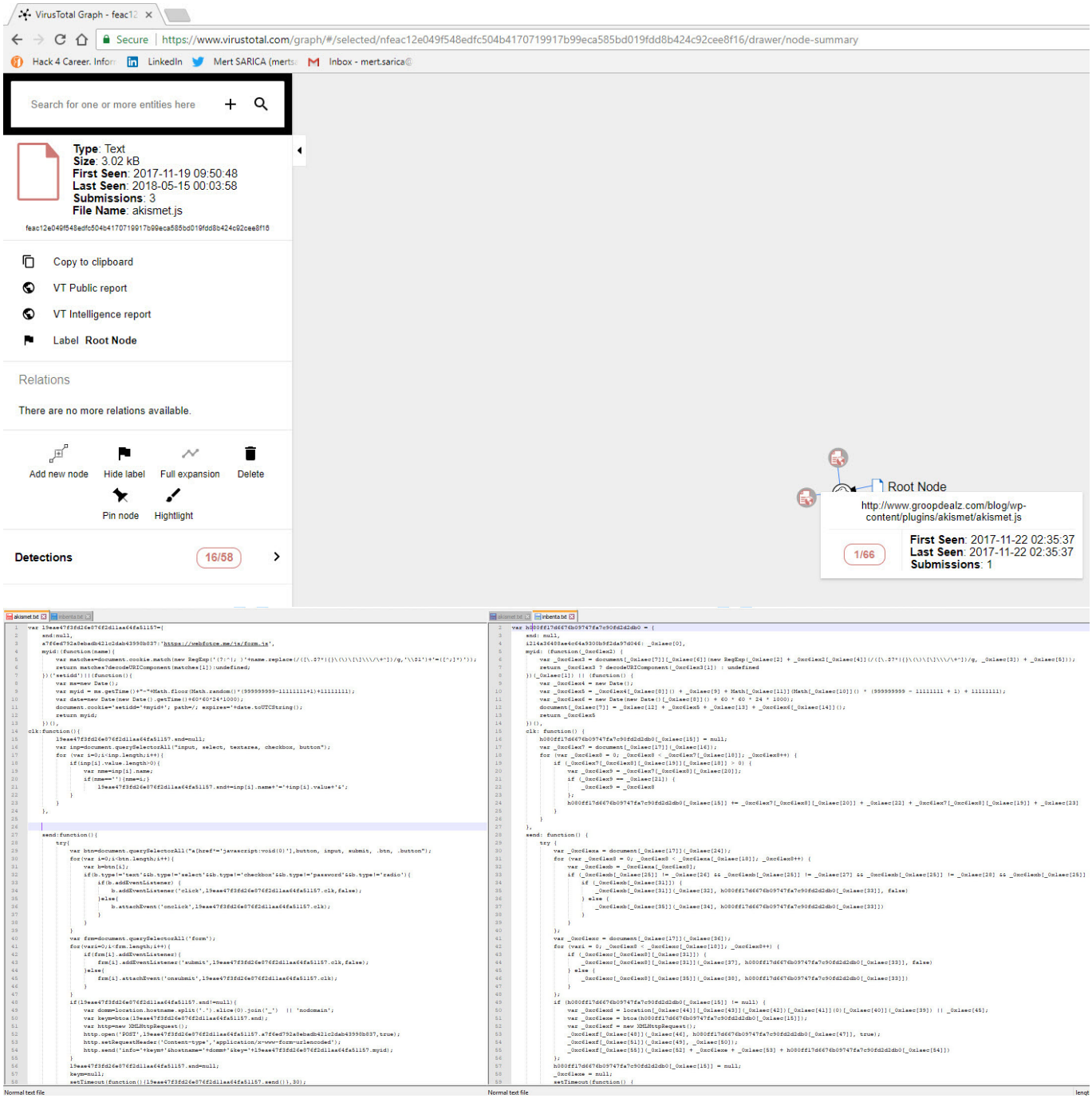
First submission	2017-11-19 09:50:48 UTC (7 ay, 2 hafta önce)
Last submission	2018-05-15 00:03:58 UTC (1 ay, 3 hafta önce)
Dosya isimleri	VirusShare_b63188547f7504194e171a0438a44746 akismet.js

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

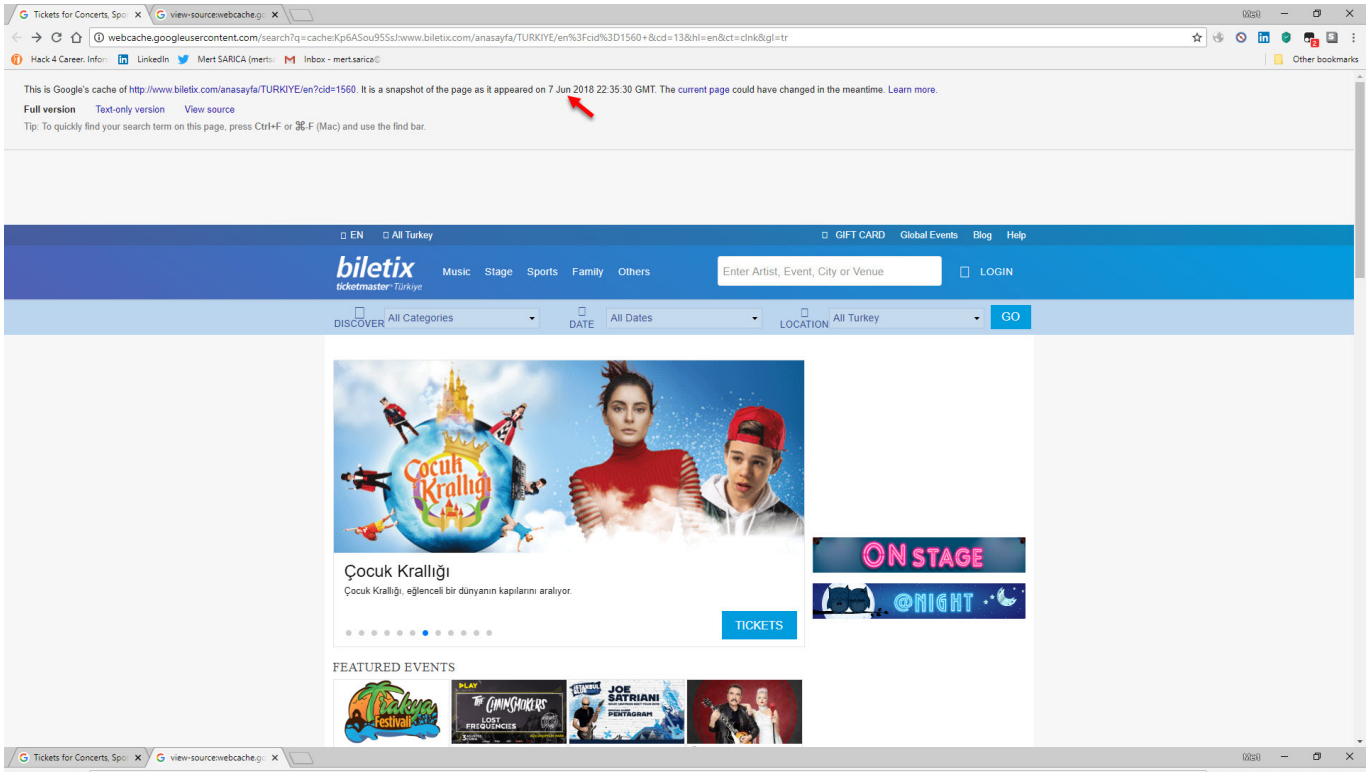
Analizler. | Ek bilgi. | Yorumlar. 1 | Oylar

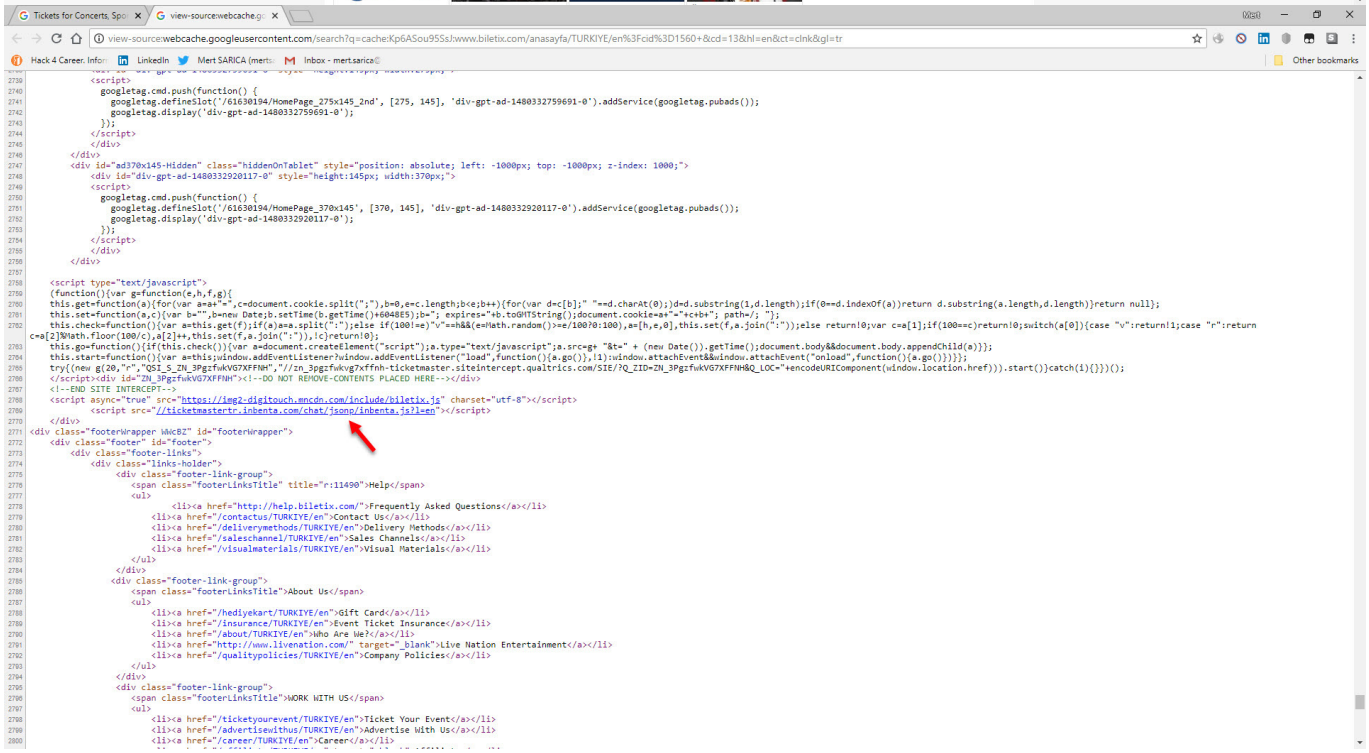
submitname:"feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16.js.bin"
falcon-threatscore:82/100
memurl:"Pattern match: https://webfotce.me/js/form.js"
source:https://www.hybrid-analysis.com/sample/feac12e049f548edfc504b4170719917b99eca585bd019fdd8b424c92cee8f16?environmentId=100

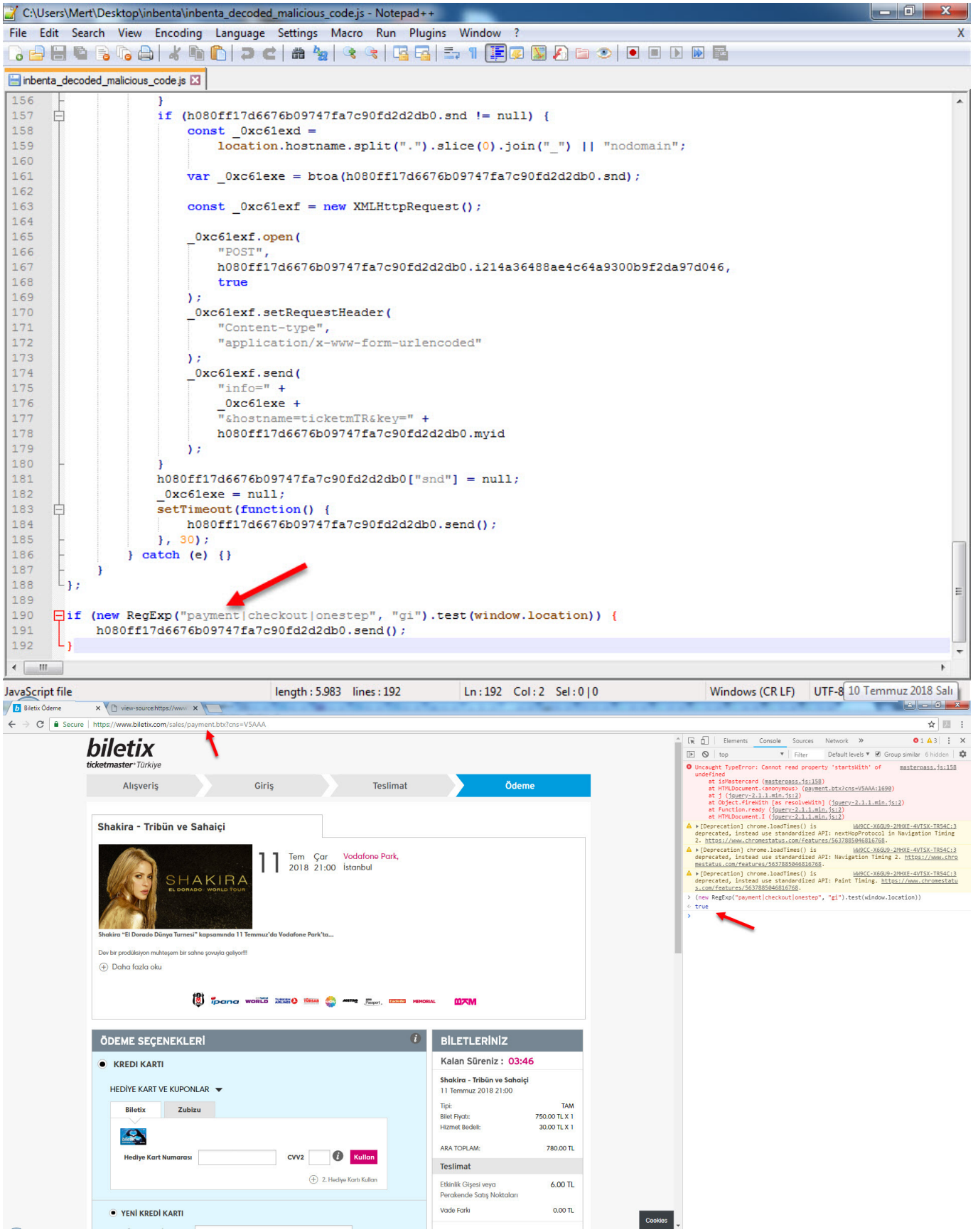
PayloadSecurity tarafından 5 ay, 1 hafta önce gönderildi Kullanışlı (0) Kullanışlı değil. (0) Kötüye kullanım (0)



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.

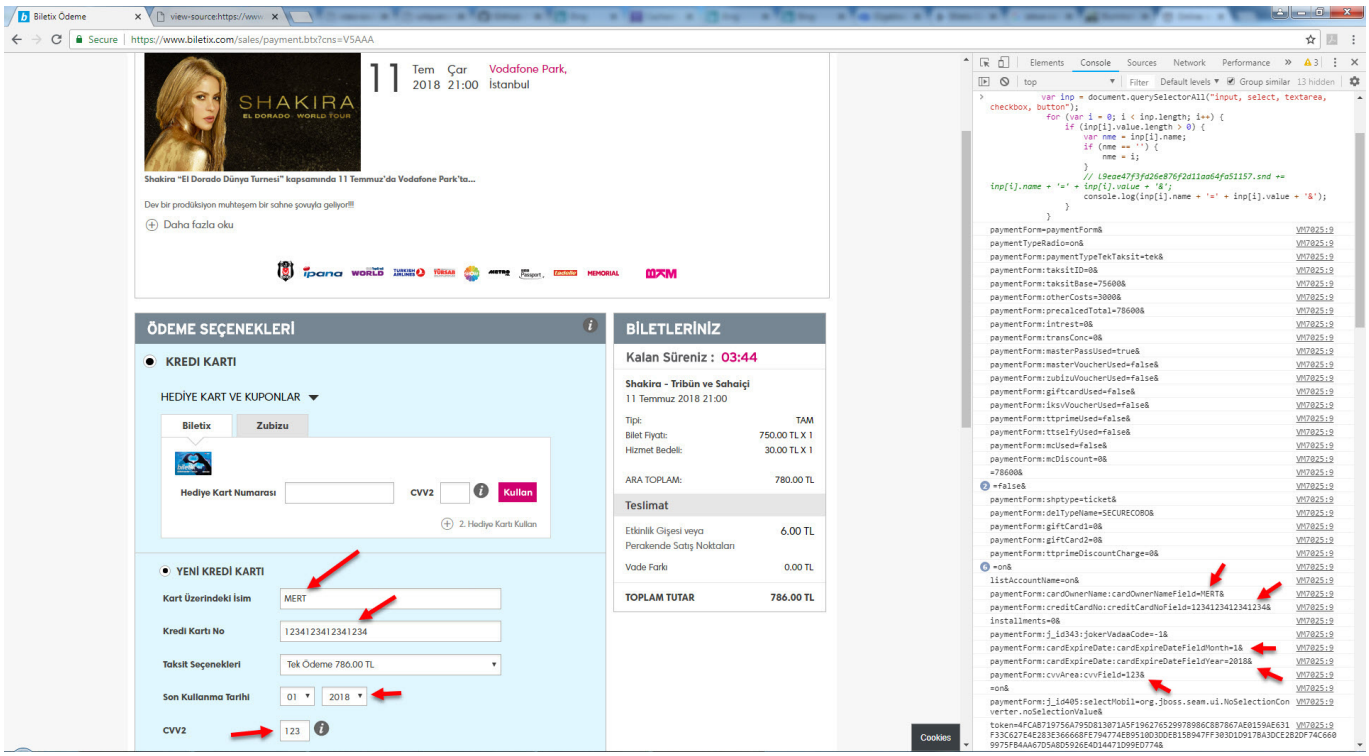

webcache.googleusercontent.com/search?q=cache:Kp6ASou95SsJ:www.biletix.com/anasayfa/TURKIYE/en%3Fcid%3D1560+&cd=13&hl=en&ct=clnk&gl=tr
This is Google's cache of http://www.biletix.com/anasayfa/TURKIYE/en?cid=1560. It is a snapshot of the page as it appeared on 7 Jun 2018 22:35:30 GMT. The current page 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 arıyor.
TICKETS
ON STAGE
@NIGHT
FEATURED EVENTS

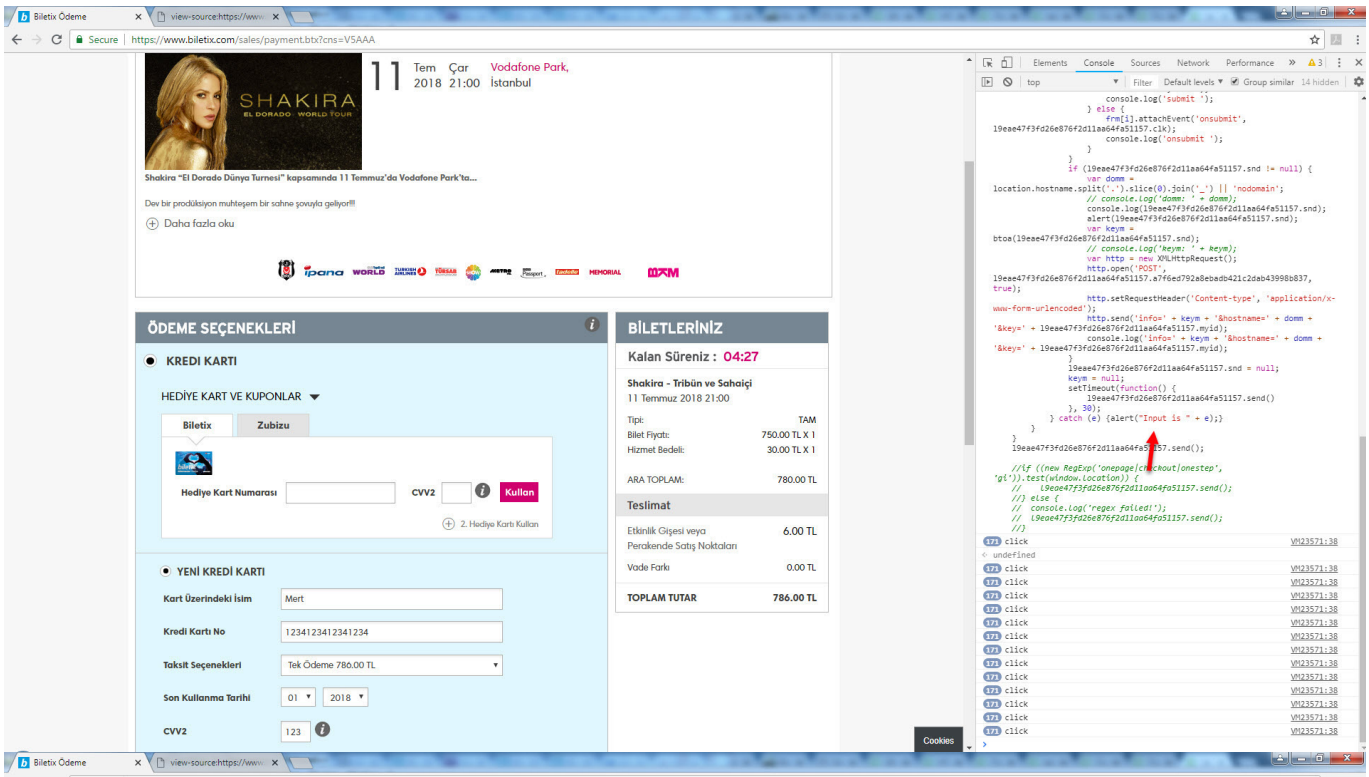

view-source:webcache.googleusercontent.com/search?q=cache:Kp6ASou95SsJ:www.biletix.com/anasayfa/TURKIYE/en%3Fcid%3D1560+&cd=13&hl=en&ct=clnk&gl=tr
googletag.cmd.push(function() {
googletag.defineSlot('/61630194/HomePage_275x145_2nd', [275, 145], 'div-gpt-ad-1480332759691-0').addService(googletag.pubads());
googletag.display('div-gpt-ad-1480332759691-0');
});
googletag.defineSlot('/61630194/HomePage_370x145', [370, 145], 'div-gpt-ad-1480332920117-0').addService(googletag.pubads());
googletag.display('div-gpt-ad-1480332920117-0');
<!--DO NOT REMOVE-CONTENTS PLACED HERE-->
<!--END SITE INTERCEPT-->
https://img2-digitouch.mncdn.com/include/biletix.js
//ticketmastertr.inbenta.com/chat/jsonp/inbenta.js?lang=en
Help
Frequently Asked Questions
Contact Us
Delivery Methods
Sales Channels
Visual Materials
About Us
Gift Card
Event Ticket Insurance
Who Are We?
Live Nation Entertainment
Company Policies
WORK WITH US
Ticket Your Event
Advertise With Us
Career

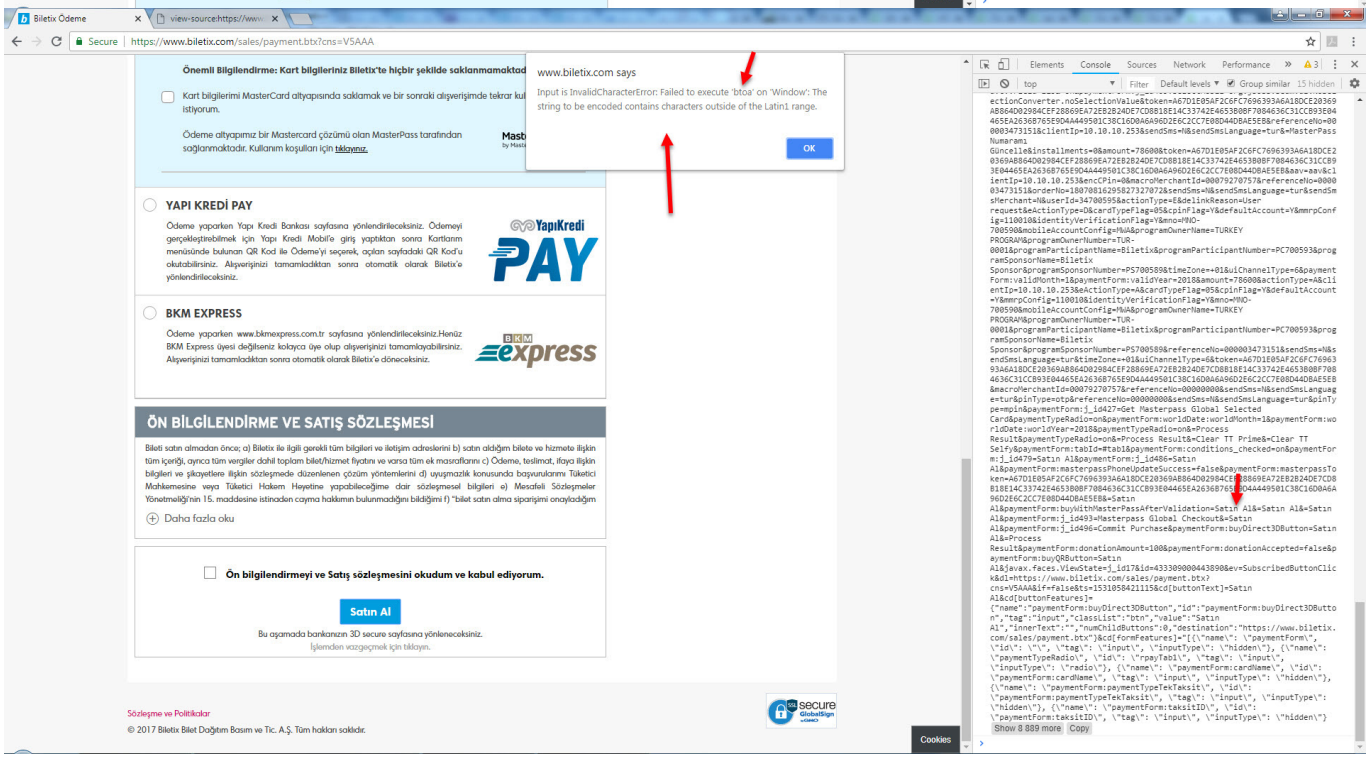


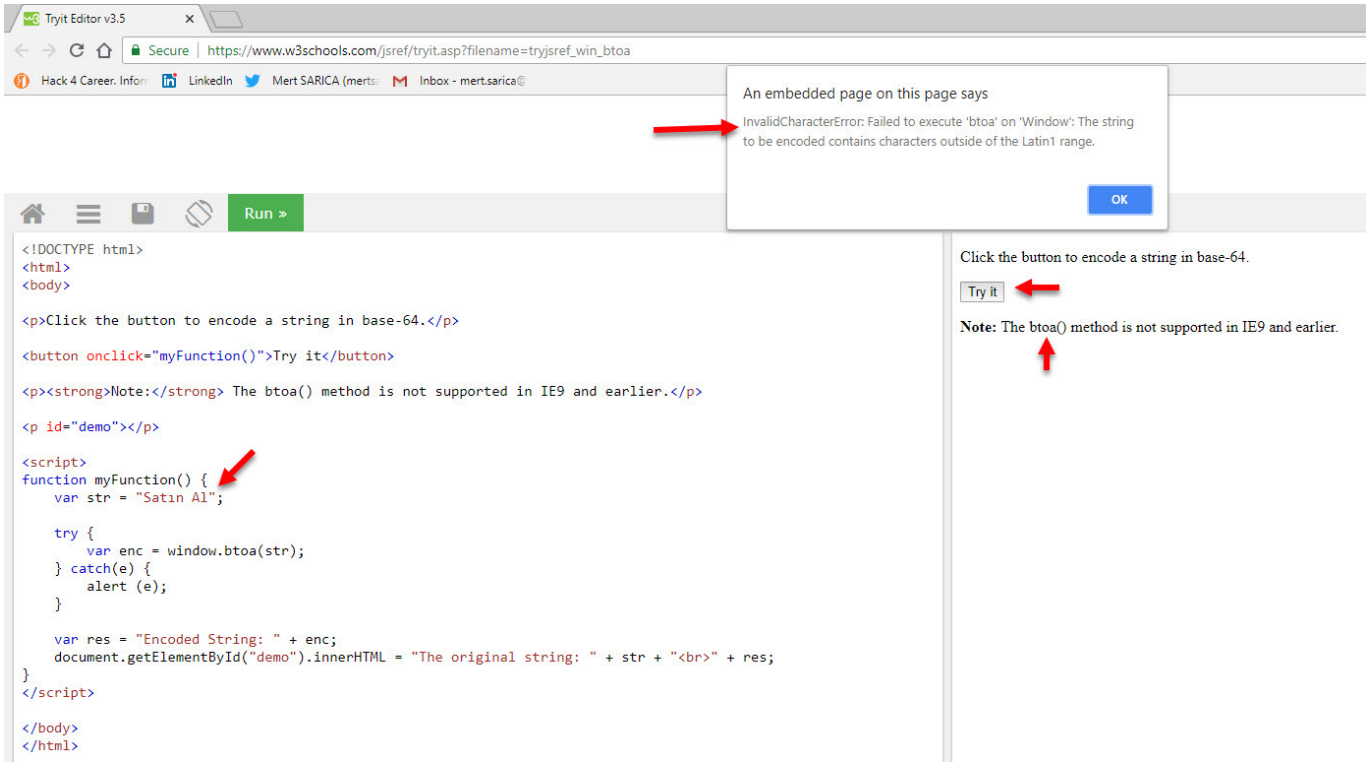
Zararlı javascript kodunu peyderpey analiz ettikçe, zararlı kodun ödeme sayfasındaki forma girilen tüm kredi kartı bilgilerini, sayfada yer alan diğer bilgilerle birlikte Satın Al butonuna bastıktan sonra hxxps://webfotce.me/js/form.js adresine gönderecek şekilde tasarlandığını

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. :)




Biletix Ödeme
view-source:https://www
Secure
https://www.biletix.com/sales/payment.btx?cns=V5AAA
SHAKIRA
EL DORADO WORLD TOUR
11 Tem Çar 2018 21:00
Vodafone Park, İstanbul
Shakira "El Dorado Dünya Turnesi" kapsamında 11 Temmuz'da Vodafone Park'ta...
Dev bir prodüksiyon muhteşem bir sahne şovuyla geliyor!!!
Daha fazla oku
ÖDEME SEÇENEKLERİ
KREDI KARTI
HEDİYE KART VE KUPONLAR
Biletix
Zubizu
Hediye Kart Numarası
CVV2
Kullan
2. Hediye Kartı Kullan
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 Gişesi veya Perakende Satış Noktaları 6.00 TL
Vade Farkı 0.00 TL
TOPLAM TUTAR 786.00 TL
Elements
Console
Sources
Network
Performance
Filter
Default levels
Group similar
14 hidden
undefined
click
Cookies


Biletix Ödeme
Secure
https://www.biletix.com/sales/payment.btx?cns=V5AAA
Önemli Bilgilendirme: Kart bilgileriniz Biletix'te hiçbir şekilde saklanmamaktad
Kart bilgilerimi MasterCard altyapısında saklamak ve bir sonraki alışverişimde tekrar kul
istiyorum.
Ödeme altyapımız bir Mastercard çözümü olan MasterPass tarafından sağlanmaktadır. Kullanım koşulları için tıklayınız.
YAPI KREDİ PAY
Ödeme yaparken Yapı Kredi Bankası sayfasına yönlendirileceksiniz. Ödemeyi gerçekleştirebilmek için Yapı Kredi Mobil'e giriş yaptıktan sonra Kartlarım menüsünde bulunan QR Kod ile Ödeme'yi seçerek, açılan sayfadaki QR Kod'u okutabilirsiniz. Alışverişiniz tamamlandıktan sonra otomatik olarak Biletix'e yönlendirileceksiniz.
BKM EXPRESS
Ödeme yaparken www.bkmexpress.com.tr sayfasına yönlendirileceksiniz.Henüz BKM Express üyesi değilseniz kolayca üye olup alışverişinizi tamamlayabilirsiniz. Alışverişiniz tamamlandıktan sonra otomatik olarak Biletix'e döneceksiniz.
ÖN BİLGİLENDİRME VE SATIŞ SÖZLEŞMESİ
Bileti satın almadan önce; a) Biletix ile ilgili gerekli tüm bilgileri ve iletişim adreslerini b) satın aldığım bilete ve hizmete ilişkin tüm içeriği, ayrıca tüm vergiler dahil toplam bilet/hizmet fiyatını ve varsa tüm ek masraflarını c) Ödeme, teslimat, iltiaya ilişkin bilgileri ve şikayetlere ilişkin sözleşmede düzenlenen çözüm yöntemlerini d) uyuşmazlık konusunda başvurulanını Tüketici Mahkemesine veya Tüketici Hakem Heyetine yapabileceğime dair sözleşmesel bilgileri e) Mesafeli Sözleşmeler Yönetmeliği'nin 15. maddesine istinaden cayma hakkımın bulunmadığını bildiğimi f) "bilet satın alma siparişimi onaylad
Daha fazla oku
Ön bilgilendirmeyi ve Satış sözleşmesini okudum ve kabul ediyorum.
Satın Al
Bu aşamada bankanızın 3D secure sayfasına yönlenceksiniz.
İşlemden vazgeçmek için tıklayın.
Sözleşme ve Politikalar
© 2017 Biletix Bilet Dağıtım Basım ve Tic. A.Ş. Tüm hakları saklıdır.
www.biletix.com says
Input is InvalidCharacterError: Failed to execute 'btoa' on 'Window': The string to be encoded contains characters outside of the Latin1 range.
OK
Elements
Console
Sources
Network
Performance
Filter
Default levels
Group similar
15 hidden
Show 8 889 more
Copy
Cookies



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 çalınamamış 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.