Tehdit Avı

written by Mert SARICA | 1 August 2017
If you are looking for an English version of this article, please visit here.

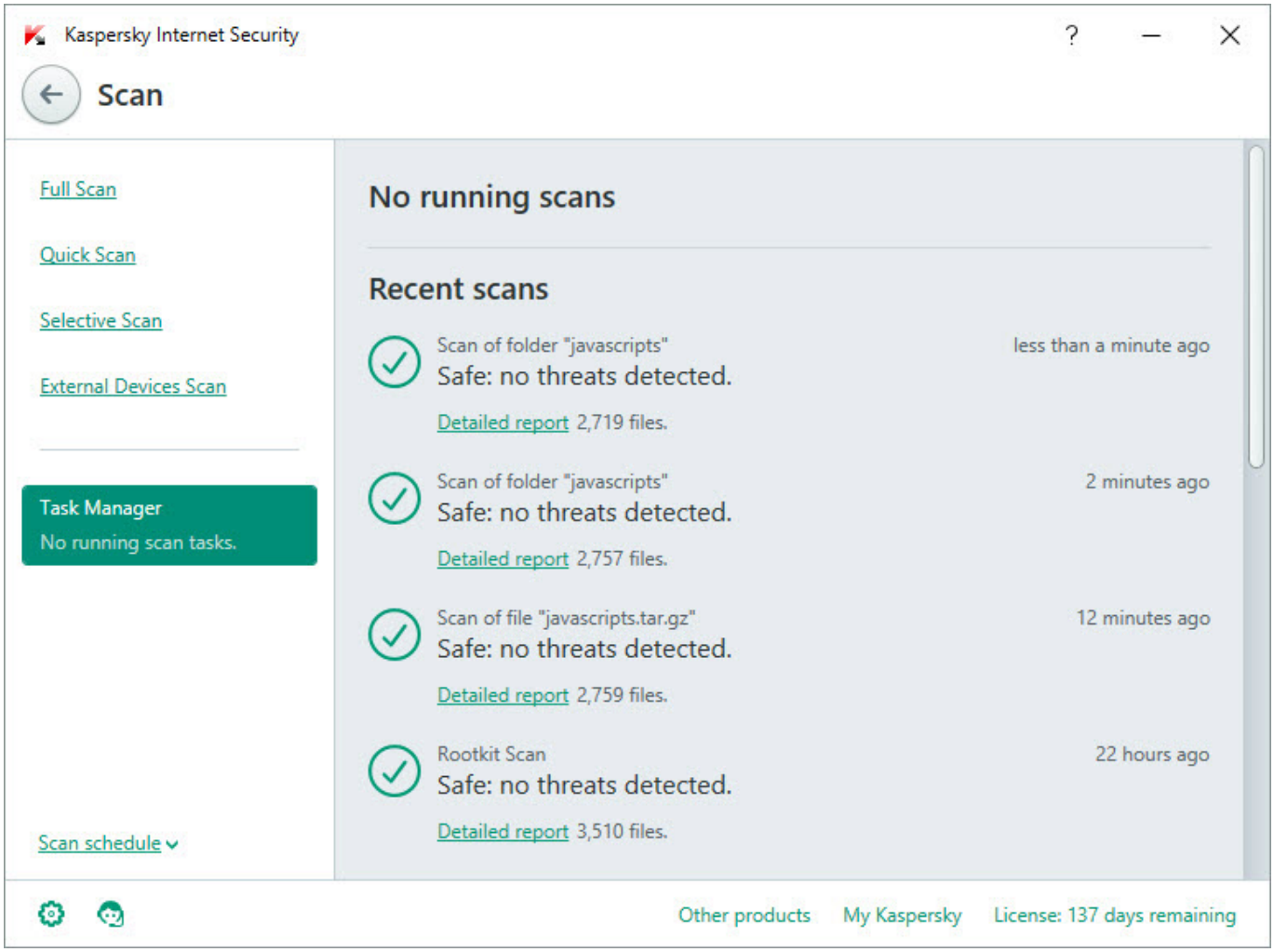
Bazen bir zararlı yazılımı konu alan blog yazısı yazdıktan sonra “Peki sen olsan bunu nasıl tespit edebilirdin ?” diye kendi kendime soruyorum ve arka planda aklımı kurcalayan, yanıtlanmayı bekleyen bu soru ile ilgili bir süreç istemsiz olarak başlamış oluyor. Bu süreç tamamlandığında, soru yanıtlandığında ise şekil 1-A’da görüleceği üzere ortaya yeni bir blog yazısı çıkıvermiş oluyor. Okumakta olduğunuz bu yazıda da yine benzer şekilde Aralık 2016’nın blog yazısı olan They PWN Houses! yazısını yazdıktan sonra “Peki bu art niyetli kişiler devlet sitelerini hedef alıyorlar ve sayfaya zararlı JavaScript kodu enjekte ediyorlar ise bunu tespit etmek pratikte ne kadar zor olabilir ?” sorusuna yanıt aradım.

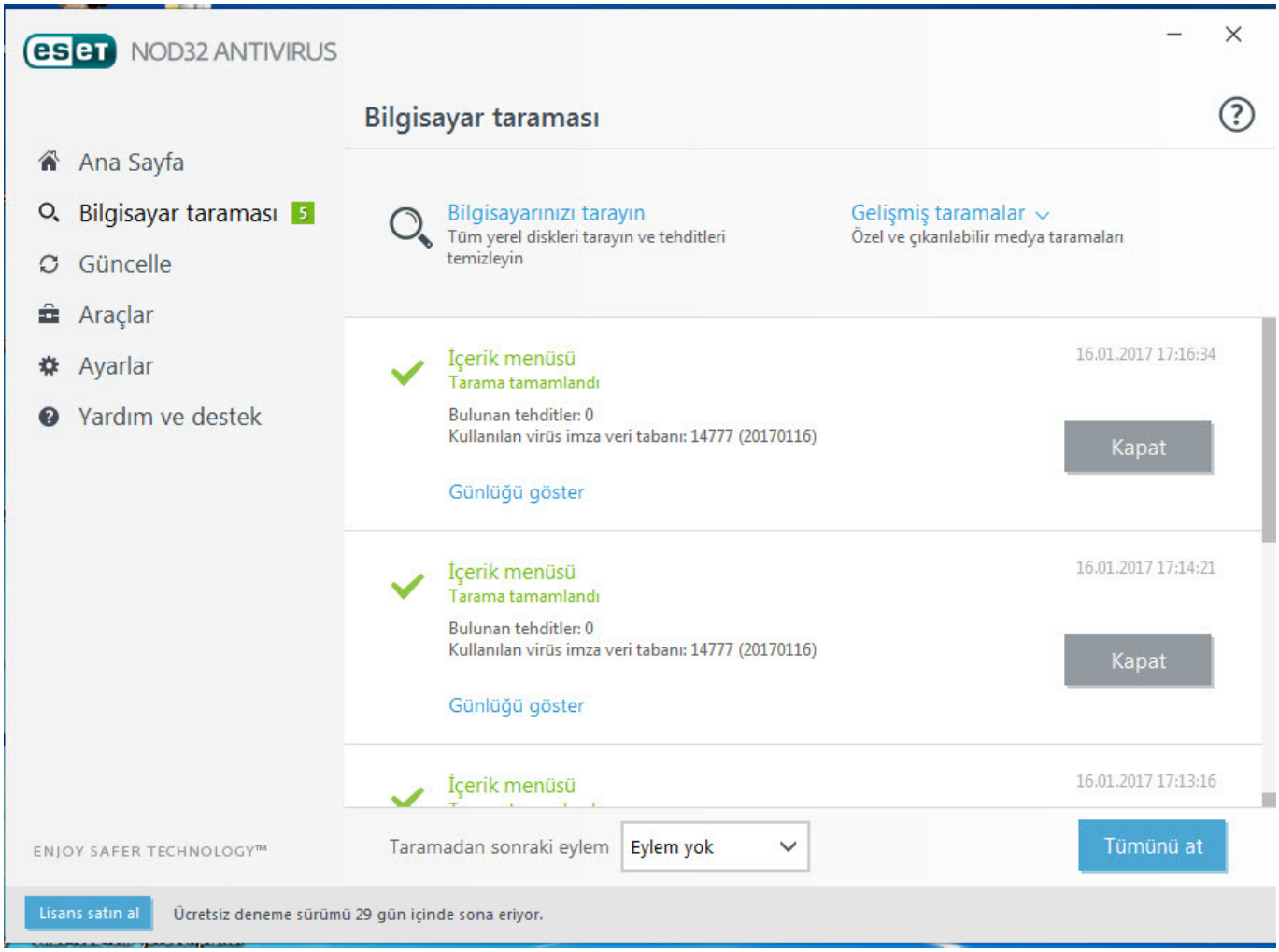
İlk iş olarak Google, Bing gibi arama motorlarından faydalanarak devlet sitelerimizin (.gov.tr uzantılı) alan adlarına arama motorlarının APIleri üzerinden ulaşmaya çalışsam da, mevcut kısıtlarından dolayı başarılı olamadım. Keşke elimin altında OpenDNS servisine yapılan DNS istekleri olsaydı da oradan listeyi çıkarabilirdim diye çaresizce hayal kurarken aklıma OpenDNS’in muadili olan Roksit geldi ve kendileri ile iletişime geçerek yapmış olduğum güvenlik araştırması ile ilgili olarak bu konuda destek istemeye karar verdim. Sağolsunlar niyetimin iyi olduğunu anladıktan sonra her ne kadar tamamı olmasa da aklımdaki fikri pratiğe dökebileceğim kadar gov.tr uzantılı alan adlarının listesini (~8000 tane) benimle paylaştılar.

Listeyi temin ettikten sonra vakit kaybetmeden Python ile tüm web sitelerini gezip, ana sayfaya mevcut site üzerinden veya herhangi bir web adresi üzerinden enjekte edilen (import) JavaScript kodlarını tespit eden ve web adresleri ile birlikte diske kayıt eden JavaScript Crawler adında oldukça basit bir araç tasarladım. Bu aracı çalıştırdıktan kısa bir süre sonra tespit edilen tüm JavaScript dosyalarını ilgili adreslerinden indiren (download) bir betik dosyası hazırladım. JavaScript dosyalarını indirdikten sonra ClamAV, ESET NOD32 ve Kaspersky Internet Security Suite güvenlik yazılımları ile tüm bu dosyaları tarattığımda herhangi bir zararlı dosyaya rastlamadım.

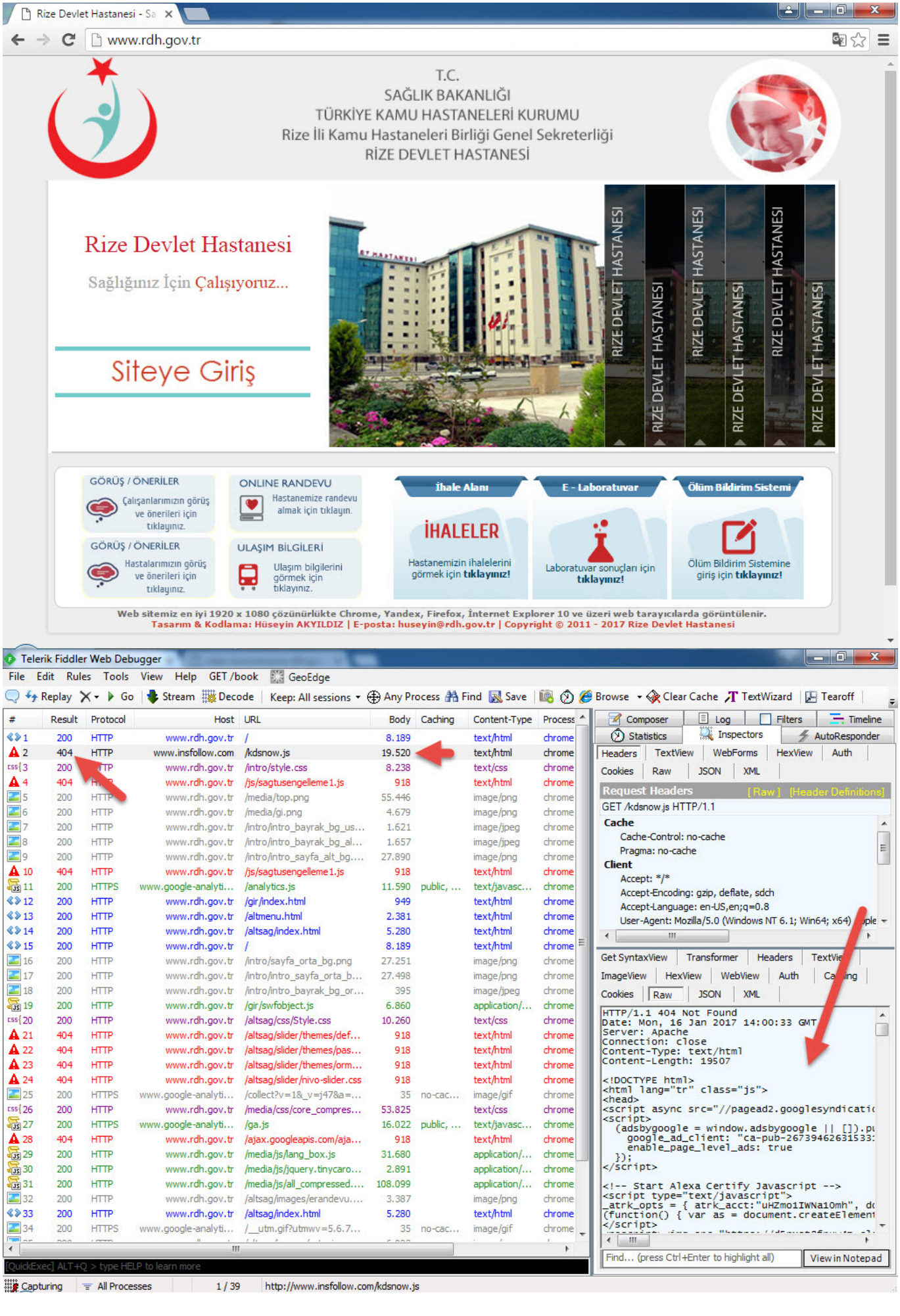
```
================================================
JavaScript Crawler v1.0 [https://www.mertsarica.com]
================================================
[+] Crawling...
[*] Connecting to: http://atam.gov.tr
[+] 1. Script tag: http://ajax.googleapis.com/ajax/libs/jquery/1/jquery.min.js
[+] 1. Script tag: http://www.atam.gov.tr/wp-content/themes/v1/js/slider.js
[+] 1. Script tag: http://code.jquery.com/ui/1.10.3/jquery-ui.js
[+] 1. Script tag: http://www.atam.gov.tr/wp-includes/js/jquery/jquery.js?ver=1.7.2
[+] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/media-element-html5-video-and-audio-player/mediaelement/mediaelement-and-player.min.js?ver=2.1.3
[+] 1. Script tag: http://www.atam.gov.tr/wp-includes/js/tw-sack.js?ver=1.6.1
[+] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/contact-form-7/includes/js/jquery.form.js?ver=3.09
[+] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.2
[+] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/lightbox-plus/js/jquery.colorbox.1.3.32.js?ver=1.3.32
[*] Connecting to: http://atasehir.gov.tr
[*] Connecting to: http://atasehirtarim.gov.tr
[*] Connection error: <urlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://atatm.gov.tr
[*] Connection error: <urlopen error [Errno -2] Name or service not known>
[*] Connecting to: http://ataturkcocukyuvasi-shcek.gov.tr
[*] Connection error: <urlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://ataturkhavalimani.gov.tr
[+] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/contentslider.js
[+] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/css3-multi-column.js
[+] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/config.js
[+] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/jquery.jcarousel.min.js?v=14480
[+] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/jssor.slider.min.js
[+] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/slideItFeatured.js
[*] Connecting to: http://ataturkyuksekkurum.gov.tr
[*] Connection error: <urlopen error [Errno -5] No address associated with hostname>
[*] Connecting to: http://atb.gov.tr
[*] Connection error: <urlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://athgm.gov.tr
[*] Connection error: <urlopen error timed out>
[*] Connecting to: http://atk.gov.tr
[*] Connection error: <urlopen error timed out>
[*] Connecting to: http://atkaracalar.gov.tr
```

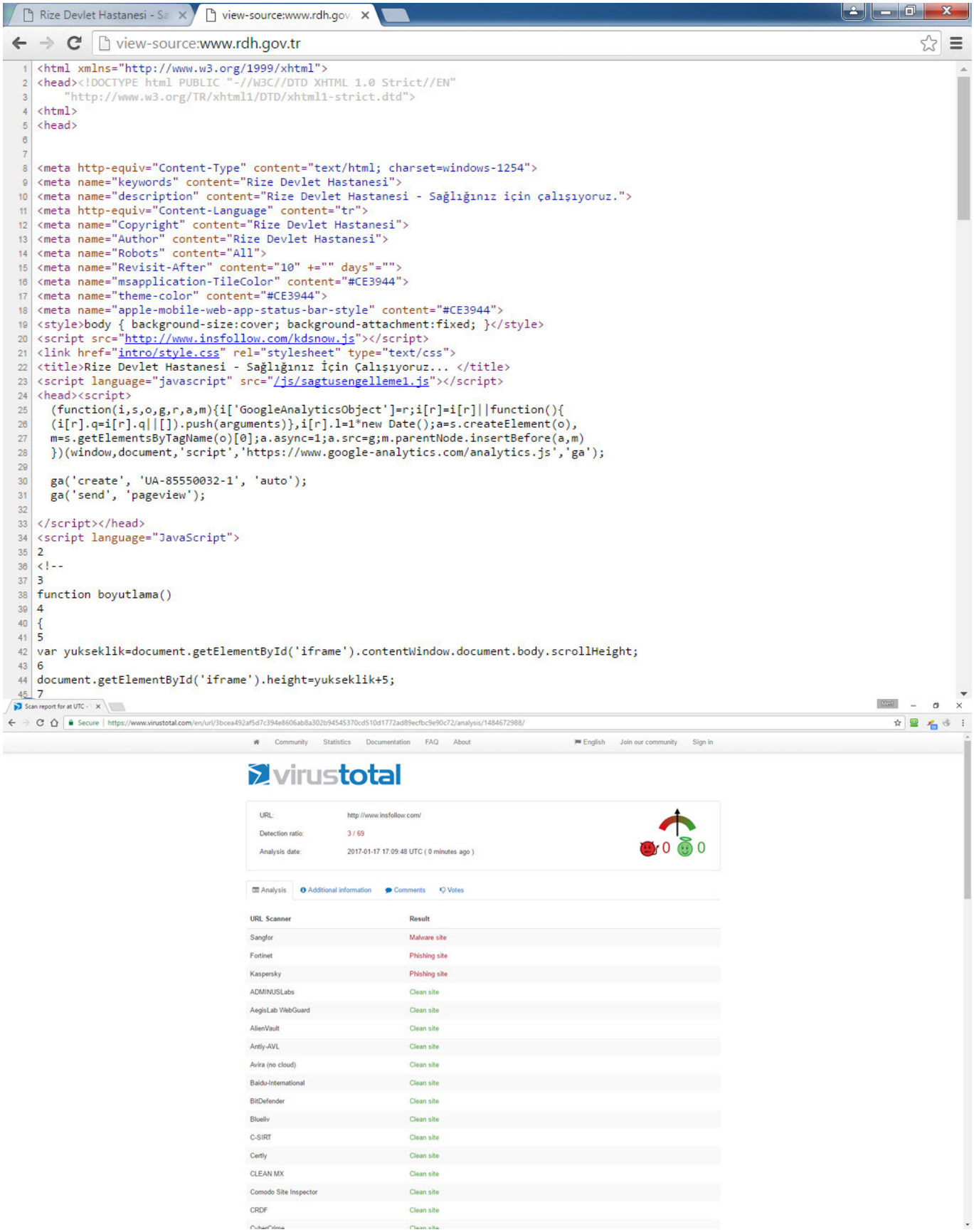
```
/root/javascripts/jquery.quicksand.js.2: OK
/root/javascripts/easing.1.3.min.js: OK
/root/javascripts/sliderjquery.flexslider-min.js: OK
/root/javascripts/jquery.fancybox.js.1: OK
/root/javascripts/interstitial.js: OK
/root/javascripts/jquery.simplemodal.1.4.1.min.js: OK
/root/javascripts/js_XjZh1hVfCgvAIxhmmB6Go8TUMPOipra-2vkC-oWXARQ.js.1: OK
/root/javascripts/TouchScrollExtender.js: OK
/root/javascripts/jquery.touchSwipe.min.js.7: OK
/root/javascripts/jquery.js.40: OK
/root/javascripts/cta-javascript.js.1: OK
/root/javascripts/jquery.min.js.1: OK
/root/javascripts/highslide-with-gallery.js.9: OK
/root/javascripts/jquery-1.8.3.min.js.1: OK
/root/javascripts/MyriadPro-Regular.font.js: OK
/root/javascripts/jquery.placeholder.min.js.1: OK
/root/javascripts/flowplayer.min.js: OK
/root/javascripts/jquery.js.20: OK
/root/javascripts/bootstrap-hover-dropdown.js.2: OK
/root/javascripts/scripts.js: OK
/root/javascripts/jquery.fancybox.pack.js.3: OK
/root/javascripts/jquery.js.35: OK
/root/javascripts/script.js.14: OK
/root/javascripts/js.8: OK
/root/javascripts/jssor.slider.mini.js: OK
/root/javascripts/mootools-core.js: OK
/root/javascripts/respond.min.js.12: OK
/root/javascripts/jquery.easing.1.2.js.3: OK
/root/javascripts/selectBox.js.1: OK
/root/javascripts/jquery.nivo.slider.pack.js.8: OK
/root/javascripts/lightbox.js.5: OK
/root/javascripts/sangarResponsiveClass.js: OK
/root/javascripts/html5.js.5: OK
/root/javascripts/easing.js: OK
/root/javascripts/jquery.formatCurrency-1.4.0.min.js: OK
/root/javascripts/sangarSlider.js: OK
/root/javascripts/pgt_rssscroller.js: OK
/root/javascripts/bootstrap.min.js.53: OK
/root/javascripts/owl.carousel.min.js.3: OK
/root/javascripts/R8Y5xHryEeS1SQoORWfmyA.js: OK
/root/javascripts/download.sh: OK
/root/javascripts/jquery.min.js.25: OK
/root/javascripts/all.js: OK
/root/javascripts/engine.mootools.js.4: OK
/root/javascripts/TouchScrollExtender.js.1: OK
/root/javascripts/jquery.themepunch.plugins.min.js.1: OK
/root/javascripts/mergen-core.min.js: OK
/root/javascripts/rp.js.2: OK
/root/javascripts/plugins-extra.js: OK
/root/javascripts/atrk.js: OK
/root/javascripts/yui_combo.php?rollup%2F3.17.2%2Fyui-moodlesimple.js&amp;rollup%2F1455265854%2Fmcore-debug.js: OK
/root/javascripts/jquery.jplayer.min.js: OK
/root/javascripts/jquery.jcarousel.min.js: OK
/root/javascripts/snowstorm.js: OK
/root/javascripts/swfobject.js.5: OK
/root/javascripts/jquery.easing.1.2.js: OK
/root/javascripts/touchSlider.plugin.js: OK
/root/javascripts/jquery.mcustomscrollbar.js: OK
/root/javascripts/jquery.validate.js.1: OK
/root/javascripts/html5.min.js.2: OK

----------- SCAN SUMMARY -----------
Known viruses: 5403271
Engine version: 0.99.2
Scanned directories: 1
Scanned files: 2761
Infected files: 0
Data scanned: 200.23 MB
Data read: 104.07 MB (ratio 1.92:1)
Time: 146.844 sec (2 m 26 s)
root@ubuntu:~/javascripts#
```


Kaspersky Internet Security
Scan
Full Scan
Quick Scan
Selective Scan
External Devices Scan
Task Manager
No running scan tasks.
Scan schedule
No running scans
Recent scans
Scan of folder "javascripts"
less than a minute ago
Safe: no threats detected.
Detailed report 2,719 files.
Scan of folder "javascripts"
2 minutes ago
Safe: no threats detected.
Detailed report 2,757 files.
Scan of file "javascripts.tar.gz"
12 minutes ago
Safe: no threats detected.
Detailed report 2,759 files.
Rootkit Scan
22 hours ago
Safe: no threats detected.
Detailed report 3,510 files.
Other products
My Kaspersky
License: 137 days remaining



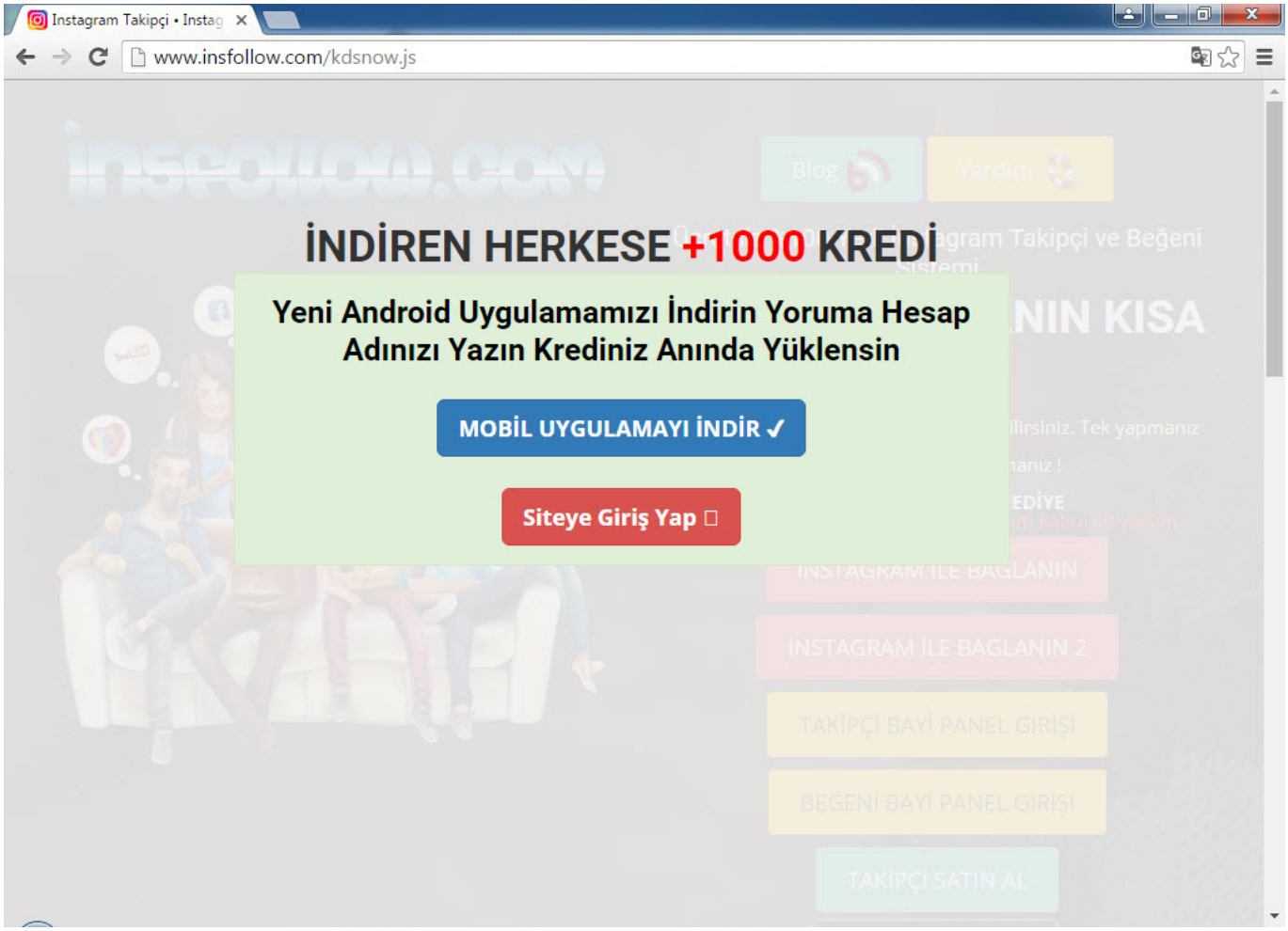
Ardından kayıt dosyasında yer alan JavaScript dosyalarının web adreslerini sort aracı ile sıralayıp ajax.googleapis.com gibi bilinen adresleri ayıkladıktan sonra insfollow.com alan adı dikkatimi çekti. Bu alan adının hangi gov.tr uzantılı devlet sitesi üzerinde tespit edildiğini kontrol ettiğimde ise Rize Devlet Hastanesi'nin web sitesi olduğunu gördüm. Web sitesini ziyaret edip kaynak koduna baktığımda insfollow.com alan adını ve enjekte edilen JavaScript dosyasını kolaylıkla tespit edebildim. VirusTotal sitesi üzerinde insfollow.com adresini arttığımda ise 3 güvenlik yazılımının bunu oltalama (phishing) sitesi olarak tespit ettiğini gördüm.

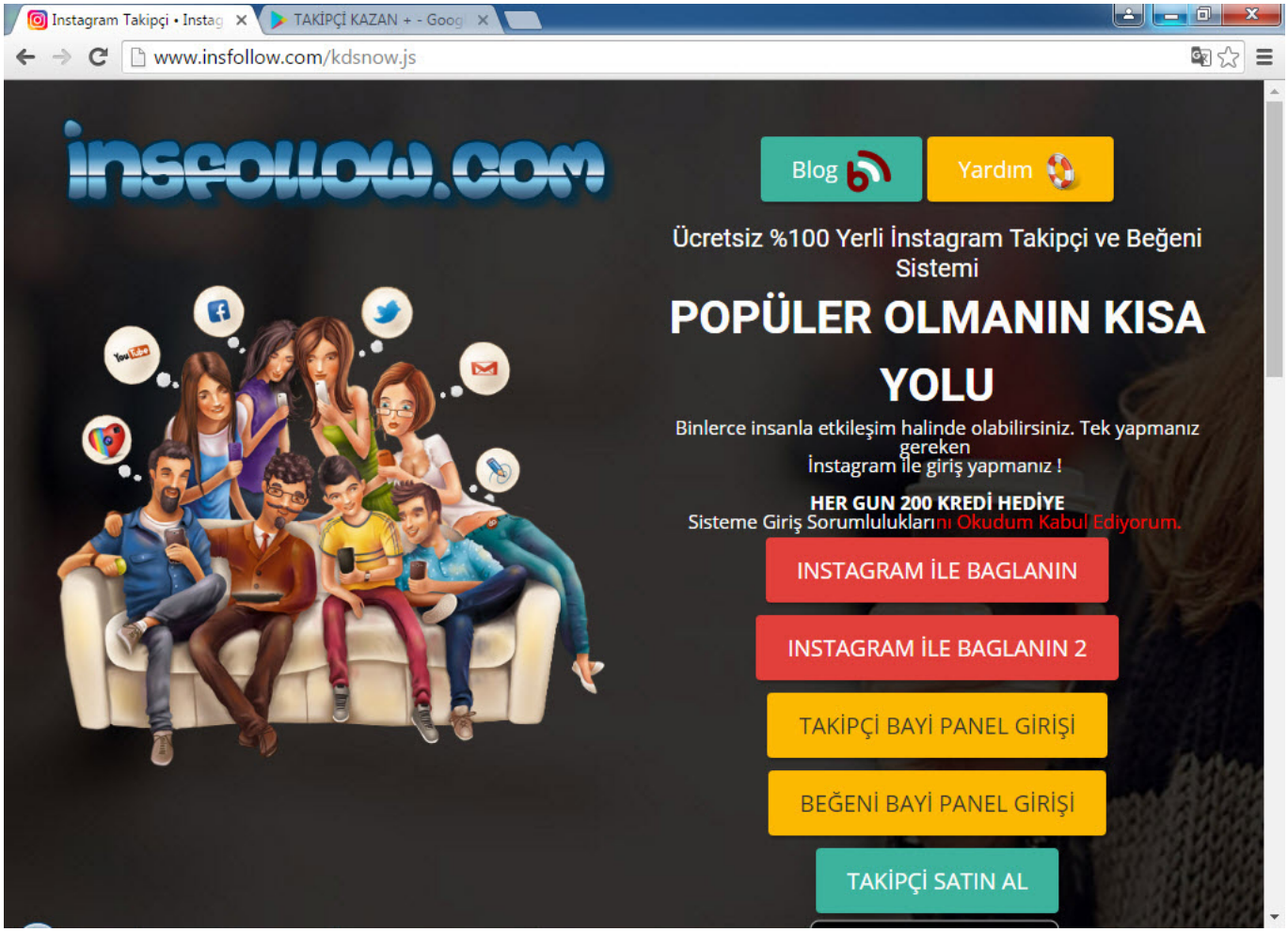

Rize Devlet Hastanesi - Sa
www.rdh.gov.tr
T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
Rize İli Kamu Hastaneleri Birliği Genel Sekreterliği
RİZE DEVLET HASTANESİ
Rize Devlet Hastanesi
Sağlığınız İçin Çalışıyoruz...
Siteye Giriş
RIZE DEVLET HASTANESI
GÖRÜŞ / ÖNERİLER
Çalışanlarımızın görüş ve önerileri için tıklayınız.
ONLINE RANDEVU
Hastanemize randevu almak için tıklayın.
GÖRÜŞ / ÖNERİLER
Hastalarımızın görüş ve önerileri için tıklayınız.
ULAŞIM BİLGİLERİ
Ulaşım bilgilerini görmek için tıklayınız.
İhale Alanı
İHALELER
Hastanemizin ihalelerini görmek için tıklayınız!
E - Laboratuvar
Laboratuvar sonuçları için tıklayınız!
Ölüm Bildirim Sistemi
Ölüm Bildirim Sistemine giriş için tıklayınız!
Web sitemiz en iyi 1920 x 1080 çözünürlükte Chrome, Yandex, Firefox, İnternet Explorer 10 ve üzeri web tarayıcılarda görüntülenir.
Tasarım & Kodlama: Hüseyin AKYILDIZ | E-posta: huseyin@rdh.gov.tr | Copyright © 2011 - 2017 Rize Devlet Hastanesi
Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
Result Protocol Host URL Body Caching Content-Type Process
1 200 HTTP www.rdh.gov.tr / 8.189 text/html chrome
2 404 HTTP www.insfollow.com /kdsnow.js 19.520 text/html chrome
3 200 HTTP www.rdh.gov.tr /intro/style.css 8.238 text/css chrome
4 404 HTTP www.rdh.gov.tr /js/sagtusengelleme1.js 918 text/html chrome
5 200 HTTP www.rdh.gov.tr /media/top.png 55.446 image/png chrome
6 200 HTTP www.rdh.gov.tr /media/gi.png 4.679 image/png chrome
7 200 HTTP www.rdh.gov.tr /intro/intro_bayrak_bg_us... 1.621 image/jpeg chrome
8 200 HTTP www.rdh.gov.tr /intro/intro_bayrak_bg_al... 1.657 image/jpeg chrome
9 200 HTTP www.rdh.gov.tr /intro/intro_sayfa_alt_bg.... 27.890 image/png chrome
10 404 HTTP www.rdh.gov.tr /js/sagtusengelleme1.js 918 text/html chrome
11 200 HTTPS www.google-analyti... /analytics.js 11.590 public, ... text/javasc... chrome
12 200 HTTP www.rdh.gov.tr /gir/index.html 949 text/html chrome
13 200 HTTP www.rdh.gov.tr /altmenu.html 2.381 text/html chrome
14 200 HTTP www.rdh.gov.tr /altsag/index.html 5.280 text/html chrome
15 200 HTTP www.rdh.gov.tr / 8.189 text/html chrome
16 200 HTTP www.rdh.gov.tr /intro/sayfa_orta_bg.png 27.251 image/png chrome
17 200 HTTP www.rdh.gov.tr /intro/intro_sayfa_orta_b... 27.498 image/png chrome
18 200 HTTP www.rdh.gov.tr /intro/intro_bayrak_bg_or... 395 image/jpeg chrome
19 200 HTTP www.rdh.gov.tr /gir/swfobject.js 6.860 application/... chrome
20 200 HTTP www.rdh.gov.tr /altsag/css/Style.css 10.260 text/css chrome
21 404 HTTP www.rdh.gov.tr /altsag/slider/themes/def... 918 text/html chrome
22 404 HTTP www.rdh.gov.tr /altsag/slider/themes/pas... 918 text/html chrome
23 404 HTTP www.rdh.gov.tr /altsag/slider/themes/orm... 918 text/html chrome
24 404 HTTP www.rdh.gov.tr /altsag/slider/nivo-slider.css 918 text/html chrome
25 200 HTTPS www.google-analyti... /collect?v=1&_v=j47&a=... 35 no-cac... image/gif chrome
26 200 HTTP www.rdh.gov.tr /media/css/core_compres... 53.825 text/css chrome
27 200 HTTPS www.google-analyti... /ga.js 16.022 public, ... text/javasc... chrome
28 404 HTTP www.rdh.gov.tr /ajax.googleapis.com/aja... 918 text/html chrome
29 200 HTTP www.rdh.gov.tr /media/js/lang_box.js 31.680 application/... chrome
30 200 HTTP www.rdh.gov.tr /media/js/jquery.tinycaro... 2.891 application/... chrome
31 200 HTTP www.rdh.gov.tr /media/js/all_compressed.... 108.099 application/... chrome
32 200 HTTP www.rdh.gov.tr /altsag/images/erandevu.... 3.387 image/png chrome
33 200 HTTP www.rdh.gov.tr /altsag/index.html 5.280 text/html chrome
34 200 HTTPS www.google-analyti... /__utm.gif?utmwv=5.6.7... 35 no-cac... image/gif chrome
Composer Log Filters Timeline
Statistics Inspectors AutoResponder
Headers TextView WebForms HexView Auth
Cookies Raw JSON XML
Request Headers [Raw] [Header Definitions]
GET /kdsnow.js HTTP/1.1
Cache
Cache-Control: no-cache
Pragma: no-cache
Client
Accept: */*
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
Get SyntaxView Transformer Headers TextVie
ImageView HexView WebView Auth Ca ing
Cookies Raw JSON XML
HTTP/1.1 404 Not Found
Date: Mon, 16 Jan 2017 14:00:33 GMT
Server: Apache
Connection: close
Content-Type: text/html
Content-Length: 19507
<!DOCTYPE html>
<html lang="tr" class="js">
<head>
<script async src="//pagead2.googlesyndicati
<script>
(adsbygoogle = window.adsbygoogle || []).pu
google_ad_client: "ca-pub-26739462631533
enable_page_level_ads: true
});
</script>
<!-- Start Alexa Certify Javascript -->
<script type="text/javascript">
_atrk_opts = { atrk_acct:"uHZmo1IWNa10mh", d
(function() { var as = document.createElement
</script>
Find... (press Ctrl+Enter to highlight all) View in Notepad
[QuickExec] ALT+Q > type HELP to learn more
Capturing All Processes 1 / 39 http://www.insfollow.com/kdsnow.js



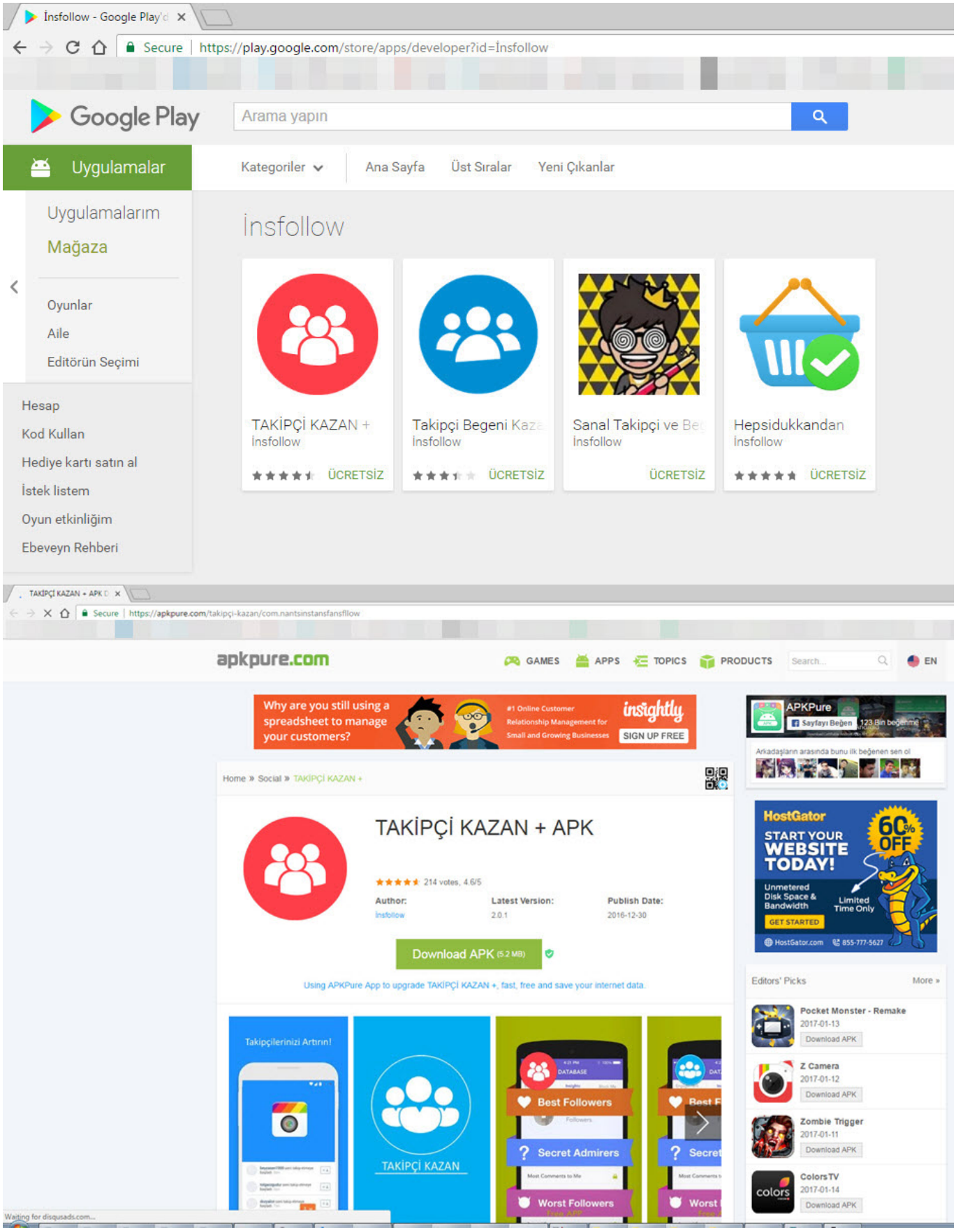
http://www.insfollow.com web sitesini ziyaret ettiğimde ise bu sitenin Instagram sosyal medya platformu için takipçi satmak amacıyla oluşturulmuş bir web sitesi olduğunu gördüm. Bu kılıf altında oluşturulup, kullanıcıların sosyal medya ve ağ parolalarını çalan zararlı siteleri ve zararlı JavaScript

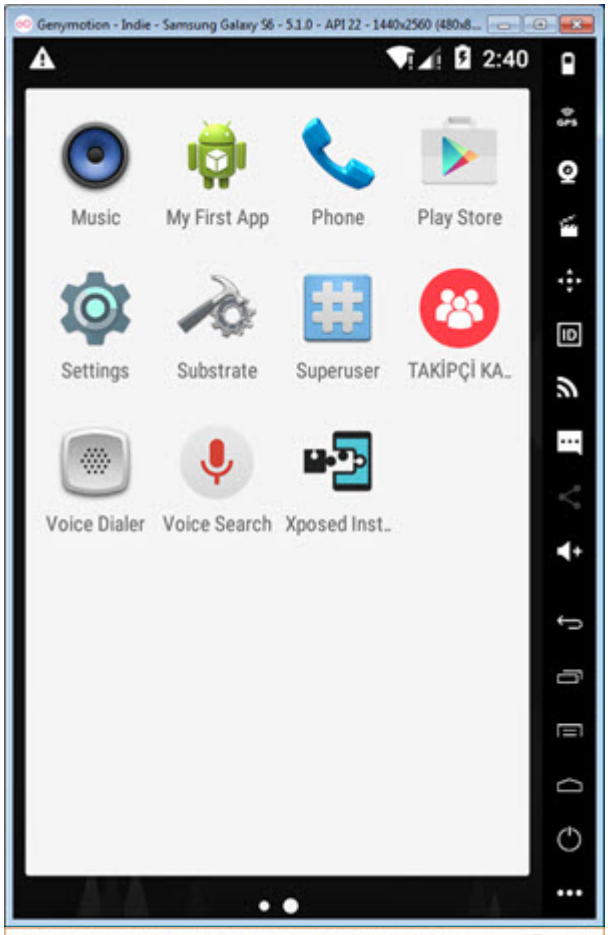
kodlarını daha önce analiz ettiğim (Jeton Hırsızları , Sosyal Ağ Hırsızları) için araştırmaya devam etmeye karar verdim.

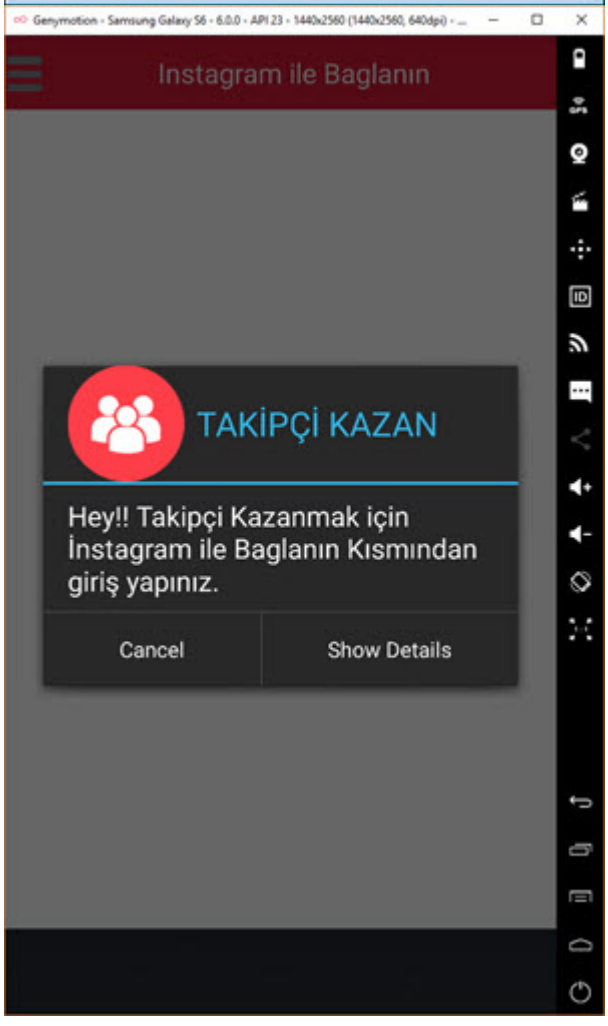




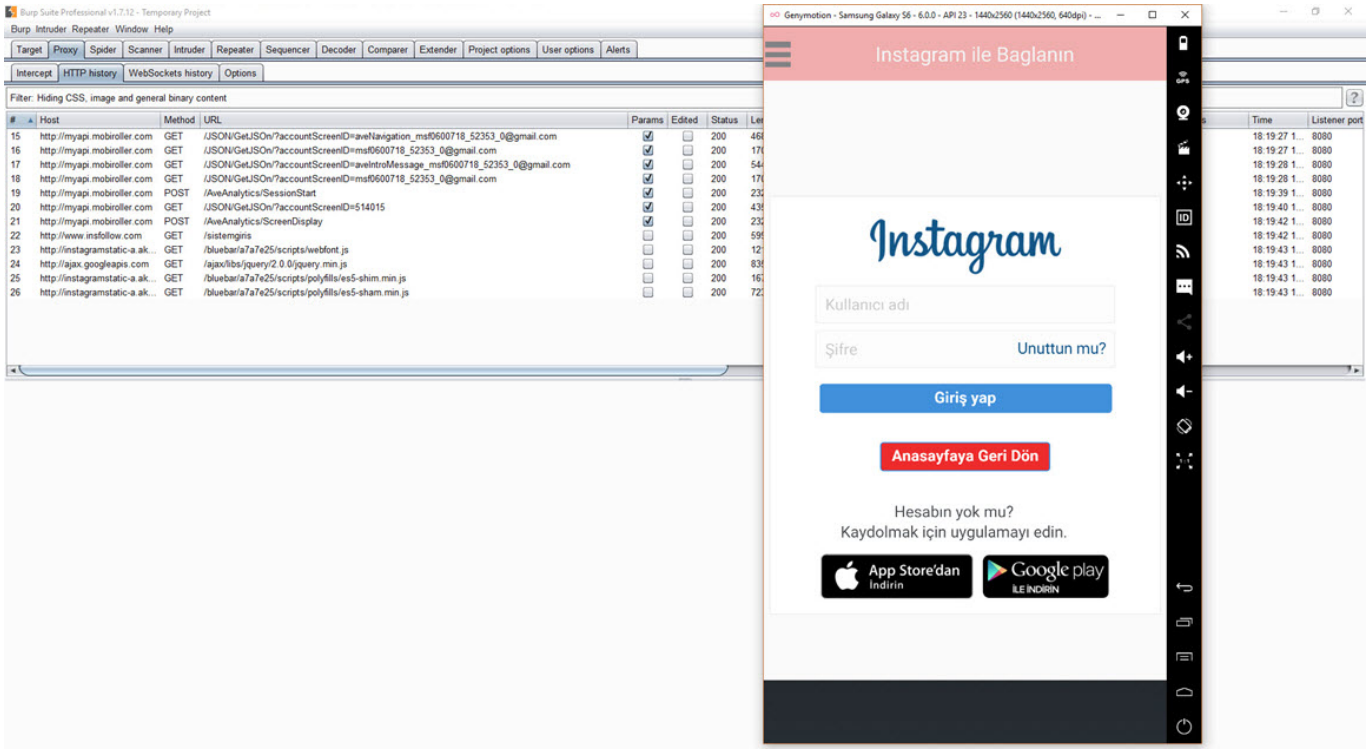
İlk olarak sitede reklamı yapılan Takipçi Kazan mobil uygulamasını indirip Genymotion öykünücüsü (emulator) üzerinde çalıştırdım. Açılan mesaj penceresinde, uygulamaya Instagram hesabı ile giriş yapılması gerektiği söyleniyordu. Ben de bunun üzerine kendime parolasını gönül rahatlığıyla çaldırabileceğim bir Instagram hesabı açtım.


İnsfollow - Google Play'
Secure | https://play.google.com/store/apps/developer?id=İnsfollow
Google Play
Arama yapın
Uygulamalar
Kategoriler
Ana Sayfa
Üst Sıralar
Yeni Çıkanlar
Uygulamalarım
Mağaza
Oyunlar
Aile
Editörün Seçimi
Hesap
Kod Kullan
Hediye kartı satın al
İstek listem
Oyun etkinliğim
Ebeveyn Rehberi
İnsfollow
TAKİPÇİ KAZAN +
İnsfollow
ÜCRETSİZ
Takipçi Begeni Kaz
İnsfollow
ÜCRETSİZ
Sanal Takipçi ve Be
İnsfollow
ÜCRETSİZ
Hepsidukkandan
İnsfollow
ÜCRETSİZ
TAKİPÇİ KAZAN + APK
Secure | https://apkpure.com/takipçi-kazan/com.nantsinstansfansfllow
apkpure.com
GAMES
APPS
TOPICS
PRODUCTS
Search...
EN
Why are you still using a spreadsheet to manage your customers?
insightly
SIGN UP FREE
Home » Social » TAKİPÇİ KAZAN +
TAKİPÇİ KAZAN + APK
214 votes, 4.6/5
Author:
İnsfollow
Latest Version:
2.0.1
Publish Date:
2016-12-30
Download APK (5.2 MB)
Using APKPure App to upgrade TAKİPÇİ KAZAN +, fast, free and save your internet data.
Takipçilerinizi Artırın!
TAKİPÇİ KAZAN
Best Followers
Secret Admirers
Worst Followers
APKPure
Sayfayı Beğen 123 Bin beğenmiş
Arkadaşların arasında bunu ilk beğenen sen ol
HostGator
START YOUR WEBSITE TODAY!
60% OFF
Unmetered Disk Space & Bandwidth
Limited Time Only
GET STARTED
HostGator.com 855-777-5627
Editors' Picks
More »
Pocket Monster - Remake
2017-01-13
Download APK
Z Camera
2017-01-12
Download APK
Zombie Trigger
2017-01-11
Download APK
ColorsTV
2017-01-14
Download APK
Waiting for disqusads.com...


Genymotion - Indie - Samsung Galaxy S6 - 5.1.0 - API 22 - 1440x2560
2:40
Music
My First App
Phone
Play Store
Settings
Substrate
Superuser
TAKİPÇİ KA..
Voice Dialer
Voice Search
Xposed Inst..

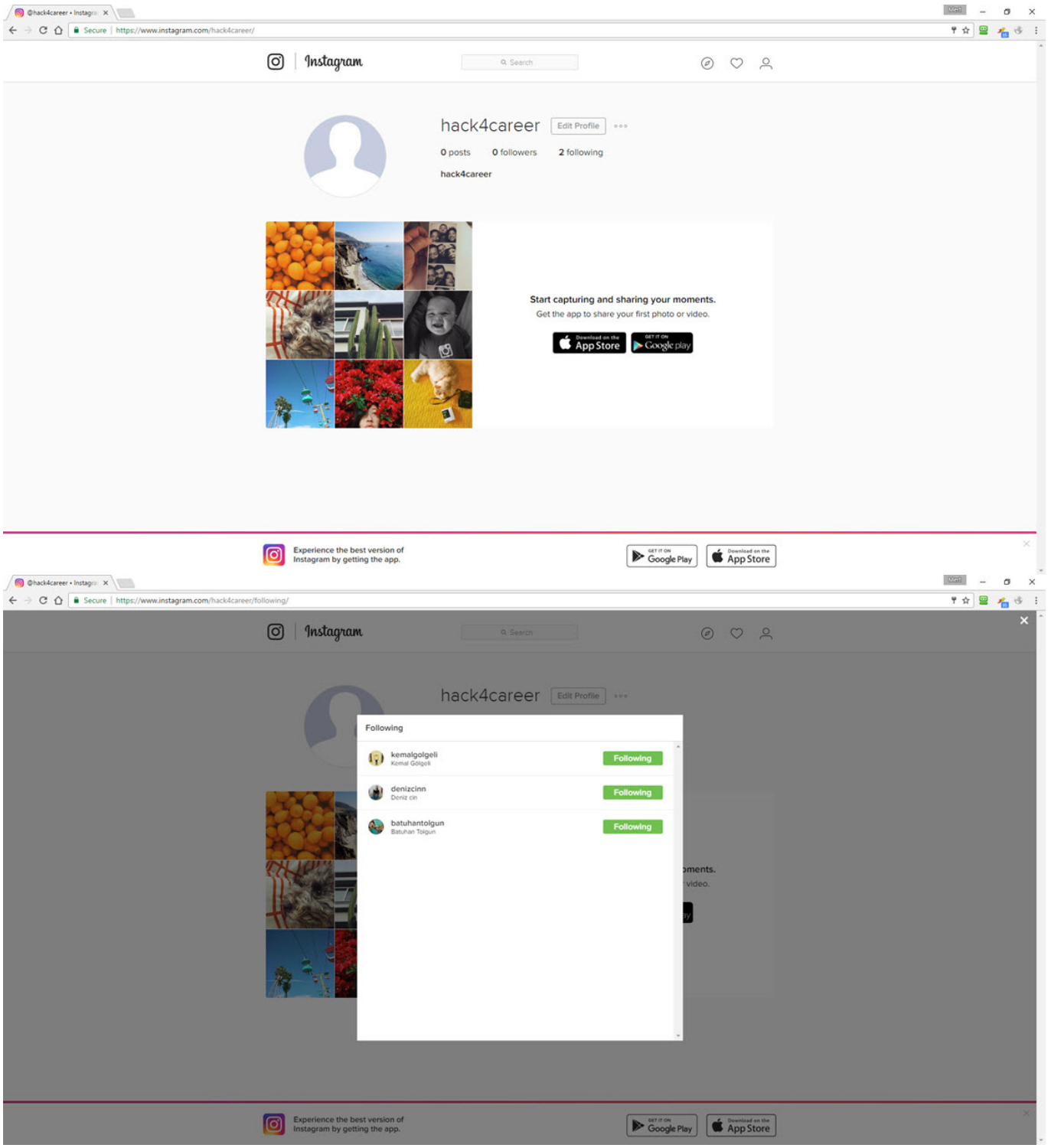

Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560
Instagram ile Baglanın
TAKİPÇİ KAZAN
Hey!! Takipçi Kazanmak için İnstagram ile Baglanın Kısmından giriş yapınız.
Cancel
Show Details

Uygulamayı çalıştırdığımda arka planda http://myapi.mobiroller.com web adresine yapılan isteklerden bu uygulamanın Mobiroller ile geliştirildiğini öğrendim. Giden isteklere daha detaylı baktığımda da, uygulama geliştiricine ait olan e-posta adresleri rahatlıkla görülebiliyordu.



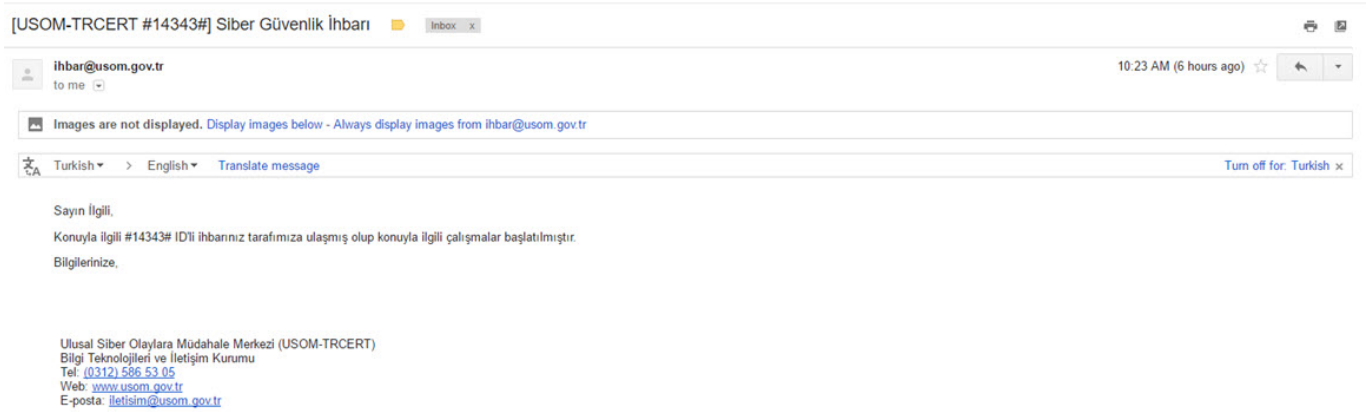
Takipçi Kazan uygulamasının davranışını anlamak için ilk olarak uygulamaya hatalı Instagram parolamı girdim. “Kullanıcı adı veya şifre yanlış!!!” mesajından uygulamanın aldığı kullanıcı adı ve parola bilgisini anlık olarak Instagram üzerinde kullandığı açıkça anlaşılıyordu. Doğru parola girdikten sonra ise uygulamanın beni bilgilendirme ve ödeme sayfasına yönlendirdiğini gördüm. Daha sonra Instagram hesabıma giriş yaptığımda ise takip ettiğim kişilerin hızla arttığını gördüm. Çok geçmeden Instagram hesabıma giriş yapamaz oldum ve kısa bir süre sonra hesabım Instagram tarafından donduruldu.


Burp Suite Professional v1.7.12 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Request Response
Raw Params Headers Hex
POST /login.php HTTP/1.1
Host: www.insfollow.com
Content-Length: 86
Cache-Control: max-age=0
Origin: http://www.insfollow.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.insfollow.com/sistemgiris
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.nantsinstansfansfllow
Connection: close
csrfmiddlewaretoken=80626eeff59ee387f9c4b7afd3659fdf67&username=mert&password=dg36rg327g
Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 (1440x2560, 640dpi) - ...
Instagram ile Baglanın
Instagram
Kullanıcı adı
Şifre
Unuttun mu?
Giriş yap
Kullanıcı adı veya şifre yanlış !!!
E-posta Adresinizi veya Hesabınızı Kontrol ediniz Tekrar Deneyiniz !!!
Anasayfaya Geri Dön
Hesabın yok mu?
Kaydolmak için uygulamayı edin.
App Store'dan İndirin
Google play İLE İNDİRİN
Type a search term
0 matches
Filter: Showing all items
GET /home HTTP/1.1
Host: www.insfollow.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://www.insfollow.com/sistemgiris?error=hata
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: PHPSESSID=6b3q24nkotuftvbjbpq0ifst6
X-Requested-With: com.nantsinstansfansfllow
Connection: close
İNSFOLLOW.COM - BİLGİLENDİRME
Hoşgeldin Hemen Vip Üyelik alarak istediğiniz kullanıcıya Takipçi ve Beğeni atabilirsiniz. Vip kullanıcılar günlük 500 kredi kazanırlar.
0553
Aktif Kullanıcı Sayısı : 5865
500 Türk Takipçi + Son 3 fotografınıza 200 Begeni 10 TL Hemen al Arkadaşlarını Şaşırt
Kredi Kartı ile Ödeme
9 Fotografınıza 1000 Begeni 49,99 TL
Hemen al Arkadaşlarını Şaşırt
Kredi Kartı ile Ödeme



Bu çalışmanın sonucunda, devlet sitelerimizin They PWN Houses! yazısına konu olan organize gruplar haricinde takipçi kılıfı altında siteler oluşturan sosyal ağ ve medya hırsızları tarafından da hedef alındığını öğrenmiş oldum. Yaptığım bu bireysel çalışmanın devlet sitelerinin güvenliğini sağlayan yetkili kurumlara ışık tutmasını temenni eder, takipçi kazan, beğeni kazan gibi web sitelerine, mobil uygulamalara karşı sosyal ağ ve medya kullanıcılarının dikkatli olmasını önerir, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Yapmış olduğum bildirime istinaden çalışma başlatan USOM‘a, sorumlu bir vatandaş olarak teşekkür ederim.


[USOM-TRCERT #14343#] Siber Güvenlik İhbarı

Inbox x

ihbar@usom.gov.tr
to me

10:23 AM (6 hours ago)

Images are not displayed. Display images below - Always display images from ihbar@usom.gov.tr

Turkish > English Translate message

Turn off for: Turkish

Sayın İlgili,

Konuyla ilgili #14343# ID'li ihbarınız tarafımıza ulaşmış olup konuyla ilgili çalışmalar başlatılmıştır.

Bilgilerinize,

Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: iletisim@usom.gov.tr

Not: Araştırmayı yaptığım zaman ile blog yazısını yazmam ve yayımlamam arasında geçen süre zarfında yazıya konu olan hastanenin web sayfasından ilgili zararlı kodun kaldırıldığı görülmüştür.