

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 çıkmış 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://atasehiratim.gov.tr
[*] Connection error: <urlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://atam.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://ataturkhalimani.gov.tr
[*] 1. Script tag: http://ataturkhalimani.gov.tr/wp-content/themes/airportthememobile/js/contentslider.js
[*] 1. Script tag: http://ataturkhalimani.gov.tr/wp-content/themes/airportthememobile/js/css3-multi-column.js
[*] 1. Script tag: http://ataturkhalimani.gov.tr/wp-content/themes/airportthememobile/js/config.js
[*] 1. Script tag: http://ataturkhalimani.gov.tr/wp-content/themes/airportthememobile/js/jquery.jcarousel.min.js?v=14480
[*] 1. Script tag: http://ataturkhalimani.gov.tr/wp-content/themes/airportthememobile/js/jssor.slider.min.js
[*] 1. Script tag: http://ataturkhalimani.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/.javascrpts/jquery.quicksand.js.2: OK
/root/.javascrpts/easing.1.3.min.js: OK
/root/.javascrpts/slider/jquery.flexslider-min.js: OK
/root/.javascrpts/jquery.fancybox.js.1: OK
/root/.javascrpts/interstitial.js: OK
/root/.javascrpts/jquery.simplemodal.1.4.1.min.js: OK
/root/.javascrpts/js_xjzhnhvCgVAlxHmMB6Go8TUMPOiprA-2vkc-owxARQ.js.1: OK
/root/.javascrpts/touchScrollExtender.js: OK
/root/.javascrpts/jquery.touchSwipe.min.js.7: OK
/root/.javascrpts/jquery.js.40: OK
/root/.javascrpts/cta-javascript.js.1: OK
/root/.javascrpts/jquery.min.js.1: OK
/root/.javascrpts/highslide-with-gallery.js.9: OK
/root/.javascrpts/jquery-1.8.3.min.js: OK
/root/.javascrpts/MyriadPro-Regular.font.js: OK
/root/.javascrpts/jquery.placeholder.min.js.1: OK
/root/.javascrpts/flopplayer.min.js: OK
/root/.javascrpts/jquery.js.20: OK
/root/.javascrpts/bootstrap-hover-dropdown.js.2: OK
/root/.javascrpts/scripts.js: OK
/root/.javascrpts/jquery.fancybox.pack.js.3: OK
/root/.javascrpts/jquery.js.33: OK
/root/.javascrpts/script.js.14: OK
/root/.javascrpts/js.8: OK
/root/.javascrpts/jssor.slider.mini.js: OK
/root/.javascrpts/mootools-core.js: OK
/root/.javascrpts/respond.min.js.12: OK
/root/.javascrpts/jquery.easing.1.2.js.3: OK
/root/.javascrpts/selectBox.js.1: OK
/root/.javascrpts/jquery.nivo.slider.pack.js.8: OK
/root/.javascrpts/lightbox.js.5: OK
/root/.javascrpts/sangarResponsiveClass.js: OK
/root/.javascrpts/html5.js.5: OK
/root/.javascrpts/easing.js: OK
/root/.javascrpts/jquery.Formatcurrency-1.4.0.min.js: OK
/root/.javascrpts/sangarSlider.js: OK
/root/.javascrpts/pgt_rsscroll.js: OK
/root/.javascrpts/bootstrap.min.js.53: OK
/root/.javascrpts/owl.carousel.min.js.3: OK
/root/.javascrpts/8V5xnyJes15Qo0RfmyA.js: OK
/root/.javascrpts/download.sh: OK
/root/.javascrpts/jquery.min.js.25: OK
/root/.javascrpts/all.js: OK
/root/.javascrpts/engine.mootools.js.4: OK
/root/.javascrpts/touchScrollExtender.js.1: OK
/root/.javascrpts/jquery.themepunch.plugins.min.js.1: OK
/root/.javascrpts/mergen-core.min.js: OK
/root/.javascrpts/rp.js.2: OK
/root/.javascrpts/plugins-extra.js: OK
/root/.javascrpts/atrK.js: OK
/root/.javascrpts/yui_combo.php?rollup%2F3.17.2%2Fyui-moodlesimple.js&rollup%2F1455265854%2Fmcore-debug.js: OK
/root/.javascrpts/jquery.jplayer.min.js: OK
/root/.javascrpts/jquery.jcarousel.min.js: OK
/root/.javascrpts/snowstorm.js: OK
/root/.javascrpts/swfobject.js.5: OK
/root/.javascrpts/jquery.easing.1.2.js: OK
/root/.javascrpts/touchSlider.plugin.js: OK
/root/.javascrpts/jquery.ncustomscrollbar.js: OK
/root/.javascrpts/jquery.validate.js.1: OK
/root/.javascrpts/html5.min.js.2: OK
```

```
----- SCAN SUMMARY -----
Known viruses: 540321
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:~/javascrpts#
```

 Scan[Full Scan](#)[Quick Scan](#)[Selective Scan](#)[External Devices Scan](#)

Task Manager

No running scan tasks.

[Scan schedule](#) ▼

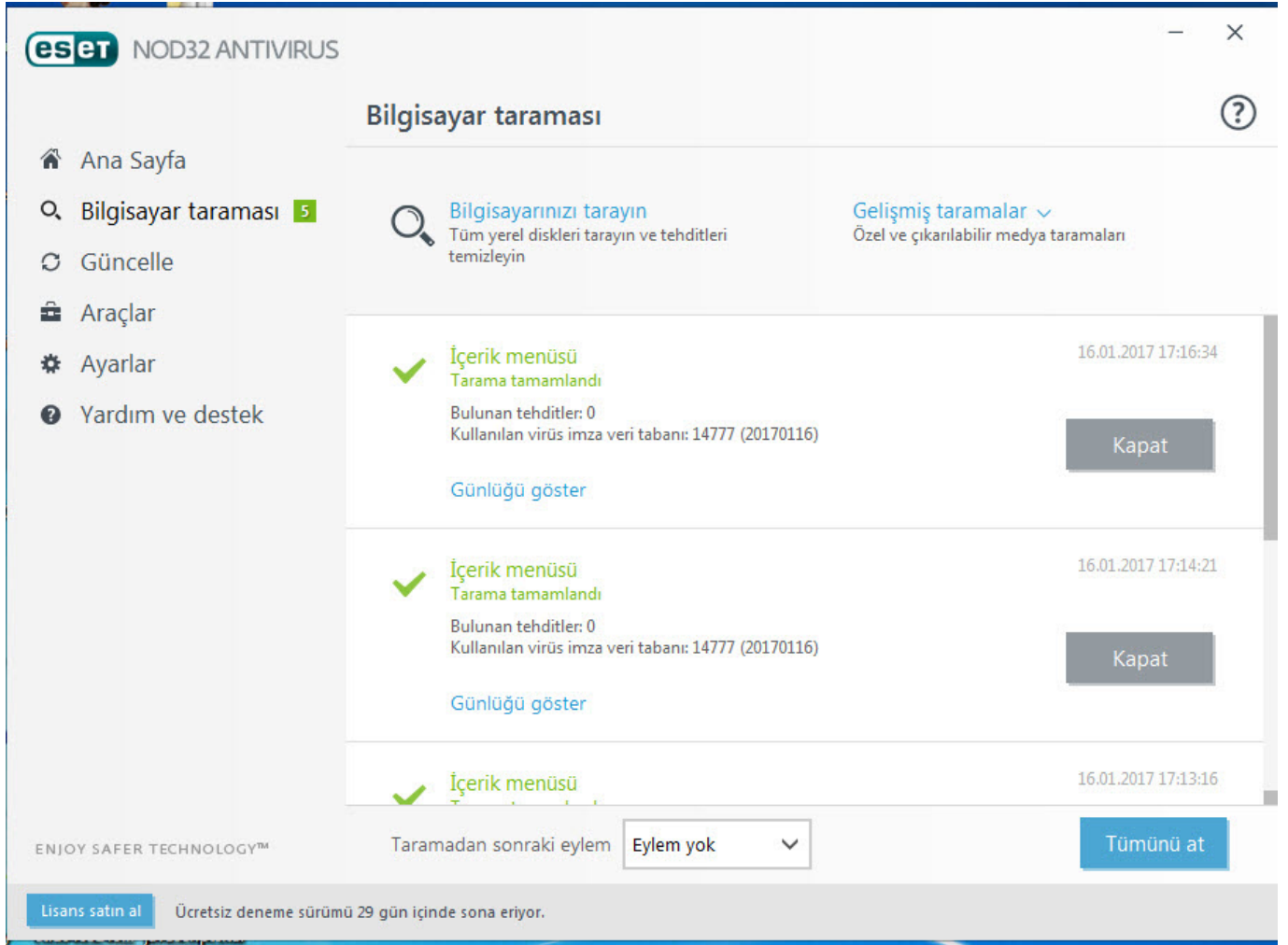
No running scans

Recent scans

- | | | |
|---|---|------------------------|
|  | Scan of folder "javascripts"
Safe: no threats detected.
Detailed report 2,719 files. | less than a minute ago |
|  | Scan of folder "javascripts"
Safe: no threats detected.
Detailed report 2,757 files. | 2 minutes ago |
|  | Scan of file "javascripts.tar.gz"
Safe: no threats detected.
Detailed report 2,759 files. | 12 minutes ago |
|  | Rootkit Scan
Safe: no threats detected.
Detailed report 3,510 files. | 22 hours ago |

[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 x

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

GÖRÜŞ / ÖNERİLER
Çalışanlarımızın görüş ve önerileri için tıklayınız.

ONLINE RANDEVU
Hastanemize randevu almak için tıklayın.

İHALE ALANI
Hastanemizin ihalelerini görmek için tıklayınız!

E - Laboratuvar
Laboratuvar sonuçları için tıklayınız!

Ölüm Bildirim Sistemi
Ölüm Bildirim Sistemine giriş için tıklayınız!

GÖRÜŞ / ÖNERİLER
Hastaların görüş ve önerileri için tıklayınız.

ULAŞIM BİLGİLERİ
Ulaşım bilgilerini görmek 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 X 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=j478a=...	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.tinycar...	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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36

Get SyntaxView Transformer Headers TextView

ImageView HexView WebView Auth Caching

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.googlesyndication.com/pagead/js/adsbygoogle.js"></script>

(adsbygoogle = window.adsbygoogle || []).push({

google_ad_client: "ca-pub-2673946263153333",

enable_page_level_ads: true

});

</script>

<!-- Start Alexa Certify Javascript -->

<script type="text/javascript">

_atrk_opts = { atrk_acct: "uH2m01IWNai0mh", 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

view-source:www.rdh.gov.tr

```
1 <html xmlns="http://www.w3.org/1999/xhtml">
2 <head><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
3 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
4 <html>
5 <head>
6
7
8 <meta http-equiv="Content-Type" content="text/html; charset=windows-1254">
9 <meta name="keywords" content="Rize Devlet Hastanesi">
10 <meta name="description" content="Rize Devlet Hastanesi - Sağlığınız için çalışıyoruz.">
11 <meta http-equiv="Content-Language" content="tr">
12 <meta name="Copyright" content="Rize Devlet Hastanesi">
13 <meta name="Author" content="Rize Devlet Hastanesi">
14 <meta name="Robots" content="All">
15 <meta name="Revisit-After" content="10" +="" days="">
16 <meta name="msapplication-TileColor" content="#CE3944">
17 <meta name="theme-color" content="#CE3944">
18 <meta name="apple-mobile-web-app-status-bar-style" content="#CE3944">
19 <style>body { background-size:cover; background-attachment:fixed; }</style>
20 <script src="http://www.insfollow.com/kdsnow.js"></script>
21 <link href="intro/style.css" rel="stylesheet" type="text/css">
22 <title>Rize Devlet Hastanesi - Sağlığınız İçin Çalışıyoruz... </title>
23 <script language="javascript" src="/js/sagtusengelleme1.js"></script>
24 <head><script>
25 (function(i,s,o,g,r,a,m){if('GoogleAnalyticsObject'==r;i[r]=i[r]||function(){
26 (i[r].q=i[r].q||[]).push(arguments)};i[r].l=1*new Date();a=s.createElement(o),
27 m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
28 })(window,document,'script','https://www.google-analytics.com/analytics.js','ga');
29
30 ga('create', 'UA-85550032-1', 'auto');
31 ga('send', 'pageview');
32
33 </script></head>
34 <script language="JavaScript">
35 2
36 <!--
37 3
38 function boyutlama()
39 4
40 {
41 5
42 var yukseklik=document.getElementById('iframe').contentWindow.document.body.scrollHeight;
43 6
44 document.getElementById('iframe').height=yukseklik+5;
45 7
46 }
```

Scan report for at UTC - X

Secure | https://www.virustotal.com/en/url/3bcea492af5d7c394e8606abba302b94545370cd510d1772ad89ecfbc9e90c72/analysis/1484672988/

Community Statistics Documentation FAQ About English Join our community Sign in

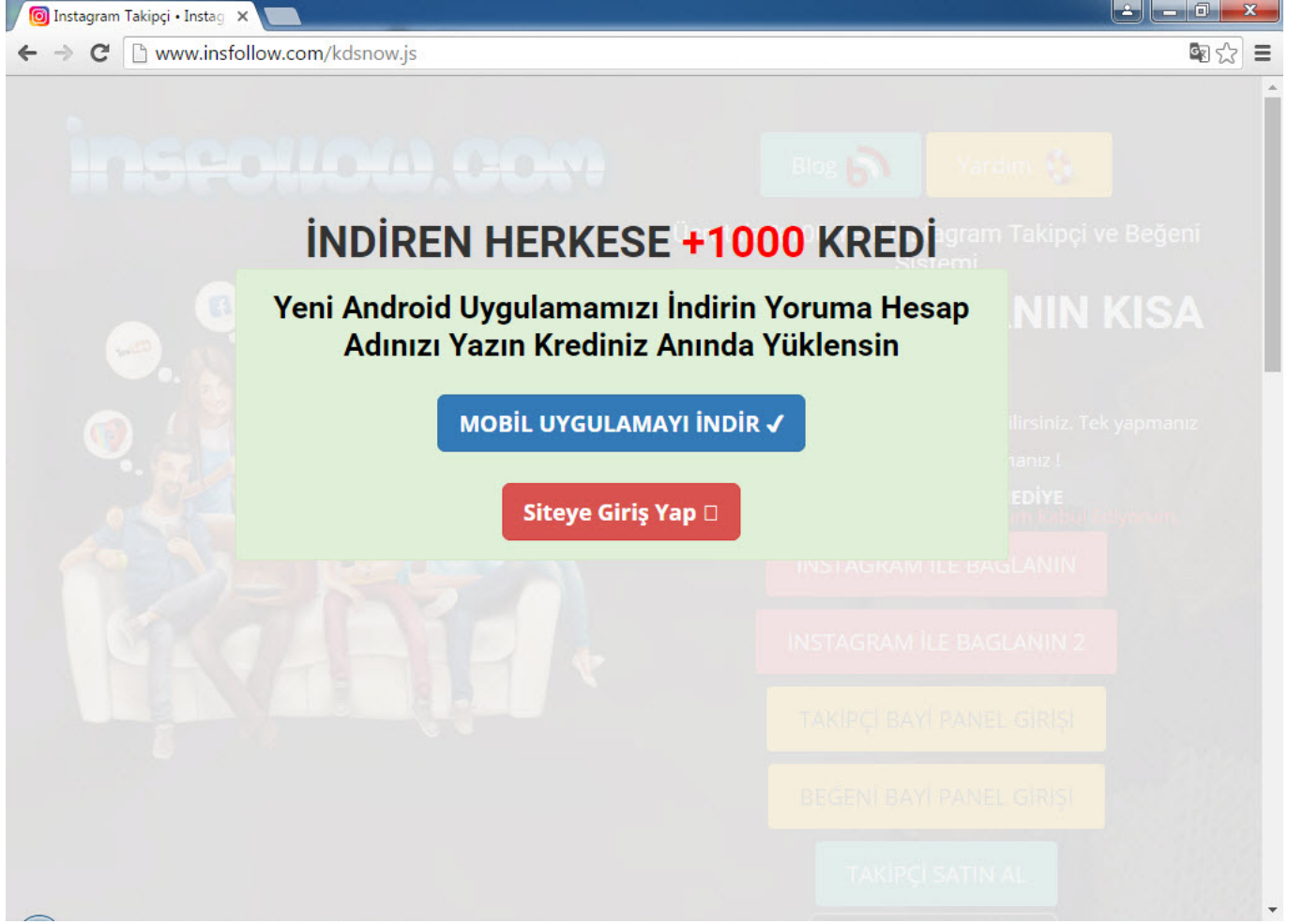


URL:	http://www.insfollow.com/
Detection ratio:	3 / 69
Analysis date:	2017-01-17 17:09:48 UTC (0 minutes ago)

Analysis	Additional information	Comments	Votes
URL Scanner	Result		
Sangfor	Malware site		
Fortinet	Phishing site		
Kaspersky	Phishing site		
ADMINUSLabs	Clean site		
AegisLab WebGuard	Clean site		
AllenVault	Clean site		
Antiy-AVL	Clean site		
Avira (no cloud)	Clean site		
Baidu-International	Clean site		
BitDefender	Clean site		
Blueliv	Clean site		
C-SIRT	Clean site		
Certly	Clean site		
CLEAN MX	Clean site		
Comodo Site Inspector	Clean site		
CRDF	Clean site		
Cybereason	Clean site		

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 Kazan
İnsfollow

★★★★★ ÜCRETSİZ

Sanal Takipçi ve Begeni
İnsfollow

ÜCRETSİZ

Hepsidukkandan
İnsfollow

★★★★★ ÜCRETSİZ

TAKİPÇİ KAZAN + APK

Secure | https://apkpure.com/takipci-kazan/com.nantsinstansinsfollow

apkpure.com

GAMES APPS TOPICS PRODUCTS

Search...

EN

Why are you still using a spreadsheet to manage your customers?

#1 Online Customer Relationship Management for Small and Growing Businesses

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

HostGator

START YOUR WEBSITE TODAY!

60% OFF

Unmetered Disk Space & Bandwidth

Limited Time Only

GET STARTED

HostGator.com 855-777-5627

Editors' Picks

Pocket Monster - Remake

2017-01-13

Download APK

Z Camera

2017-01-12

Download APK

Zombie Trigger

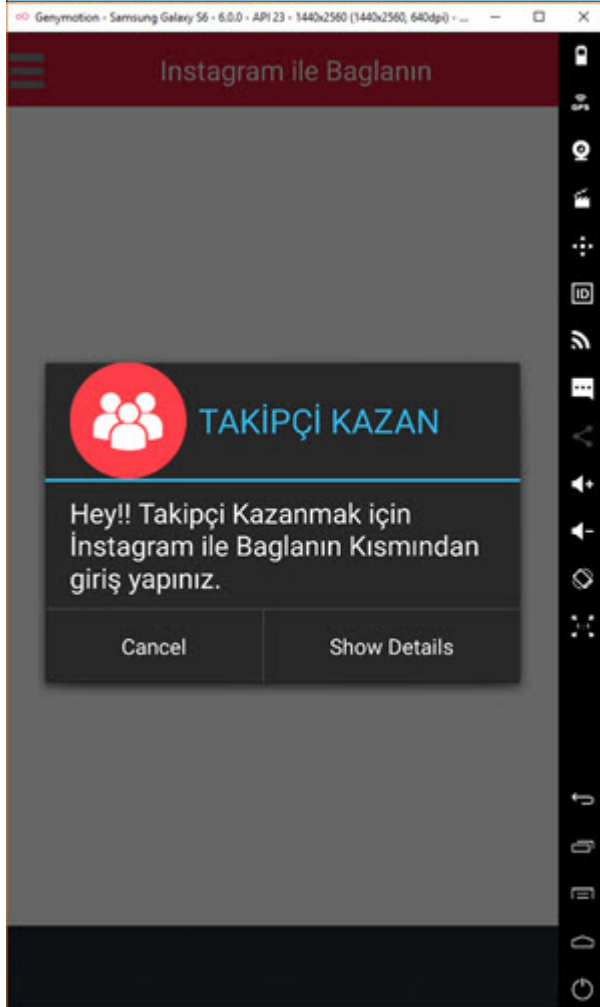
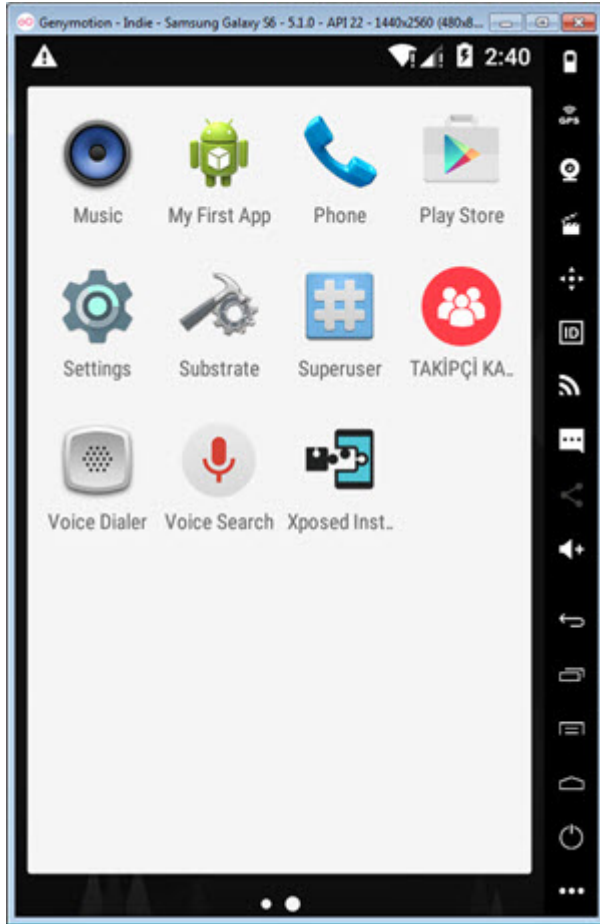
2017-01-11

Download APK

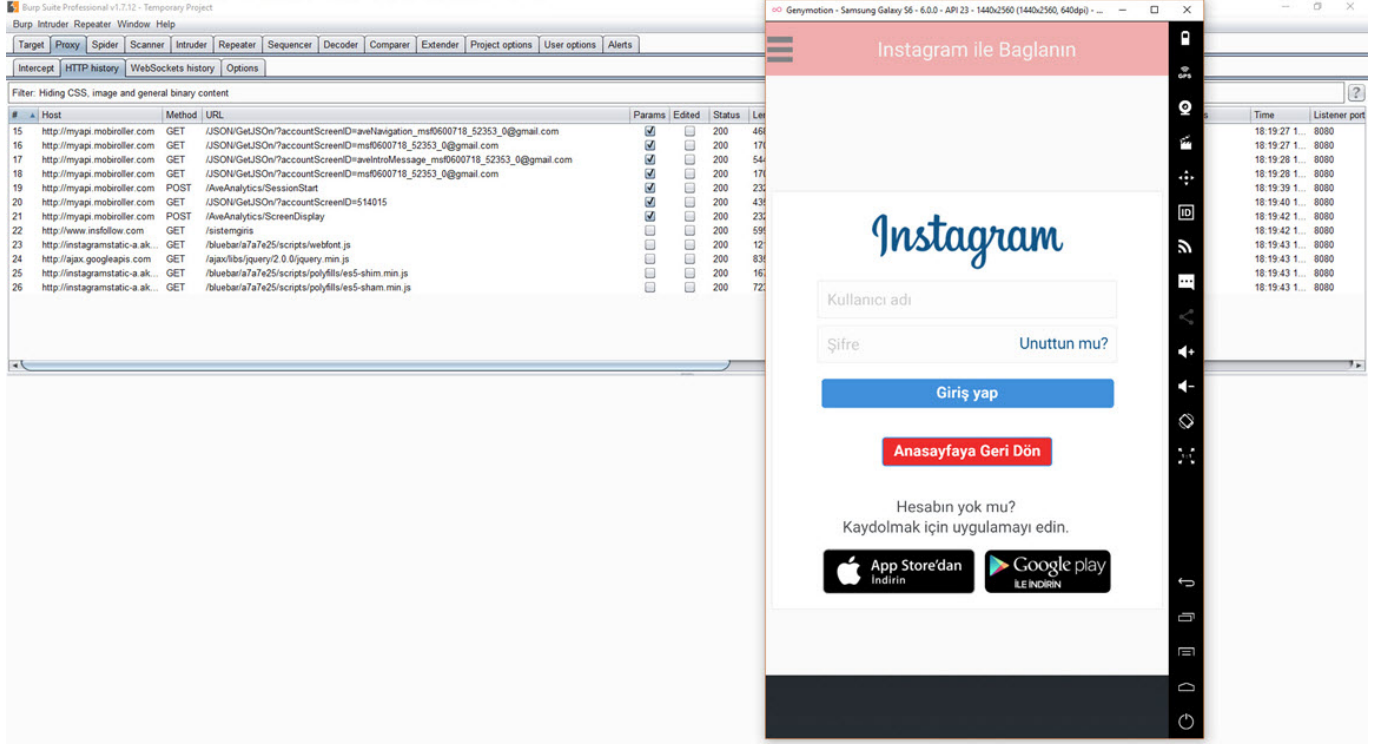
ColorsTV

2017-01-14

Download APK



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.

Wireshark - Burp Suite Professional v1.7.12 - Temporary Project

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

#	Host	Method	URL	Params	Edited	Status	Length	MIME t.	Extension	Title
15	http://myapi.mobileroller.com	GET	/JSON/GetJSON?accountScreenID=aveNavigation_ms0600718_52353_0@gmail.com			200	461			
16	http://myapi.mobileroller.com	GET	/JSON/GetJSON?accountScreenID=ms0600718_52353_0@gmail.com			200	171			
17	http://myapi.mobileroller.com	GET	/JSON/GetJSON?accountScreenID=aveIntroMessage_ms0600718_52353_0@gmail.com			200	54			
18	http://myapi.mobileroller.com	GET	/JSON/GetJSON?accountScreenID=ms0600718_52353_0@gmail.com			200	171			
19	http://myapi.mobileroller.com	POST	/AwAnalytics/SessionStart			200	23			
20	http://myapi.mobileroller.com	GET	/JSON/GetJSON?accountScreenID=514015			200	43			
21	http://myapi.mobileroller.com	POST	/AwAnalytics/ScreenDisplay			200	25			
22	http://www.insfollow.com	GET	/sistemgrisi			200	59			
23	http://instagramstatic-a.akamai.net	GET	/bluebar/a7a7e25/scripts/webfont.js			200	12			
24	http://ajax.googleapis.com	GET	/ajax/libs/jquery/2.0.0/jquery.min.js			200	83			
25	http://instagramstatic-a.akamai.net	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js			200	16			
26	http://instagramstatic-a.akamai.net	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js			200	72			
30	http://www.insfollow.com	POST	/login.php			302	37			
31	http://www.insfollow.com	GET	/sistemgrisi?error=hata			200	60			

Request Response

Raw Params Headers Hex

POST /login.php HTTP/1.1
Host: www.insfollow.com
Content-Length: 86
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://www.insfollow.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 Build/MPA50E; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://www.insfollow.com/sistemgrisi?error=hata
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.nantinstanfianfollow
Connection: close

csrfmiddlewacToken=8062ceff59ee3875c4b7a6d365d667&username=metc&password=dg36rg27g

Instagram ile Bağlanın

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 İNDİRİN

Wireshark - Burp Suite Professional v1.7.12 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status	Length	MIME t.	Extension	Title
32	http://www.insfollow.com	POST	/login.php			302	37			
33	http://www.insfollow.com	GET	/home			200	38517	HTML	php	m339
34	http://www.insfollow.com	GET	/bootstrap/css/bootstrap.min.css			200	109725	CSS	css	
35	http://www.insfollow.com	GET	/style/font-awesome.min.css			200	20972	CSS	css	
36	http://www.insfollow.com	GET	/style/pace.css			200	2474	CSS	css	
37	http://s7.addthis.com	GET	/js/300/addthis_widget.js			200	345149	script	js	
38	http://www.insfollow.com	GET	/style/endskin.min.css			200	139472	CSS	css	
39	http://www.insfollow.com	GET	/css/sly.css			200	196509	CSS	css	
40	http://www.insfollow.com	GET	/css/sly-responsive.css			200	5818	CSS	css	
41	http://bc.vc	GET	/js/bc_v.js			200	1846	script	js	
42	http://code.ionicframework.com	GET	/ionicons/2.0.0/css/ionicons.min.css			200	51844	CSS	css	
43	http://www.insfollow.com	GET	/style/endskin.min.css			200	21285	CSS	css	
44	http://www.insfollow.com	GET	/js/jquery-1.10.2.min.js			200	93283	script	js	
45	http://www.insfollow.com	GET	/bootstrap/js/bootstrap.min.js			200	32039	script	js	
46	http://www.insfollow.com	GET	/js/modernizr.min.js			200	2465	script	js	
47	http://fonts.googleapis.com	GET	/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic			200	24346	CSS	css	
48	http://www.insfollow.com	GET	/js/pace.min.js			200	12277	script	js	

Request Response

Raw Params Headers Hex

GET /home HTTP/1.1
Host: www.insfollow.com
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 Build/MPA50E; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Mobile Safari/537.36
Referer: http://www.insfollow.com/sistemgrisi?error=hata
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: PHPSESSID=6b3c4akotufitvb3p9q1st6
X-Requested-With: com.nantinstanfianfollow
Connection: close

Instagram ile Bağlanın

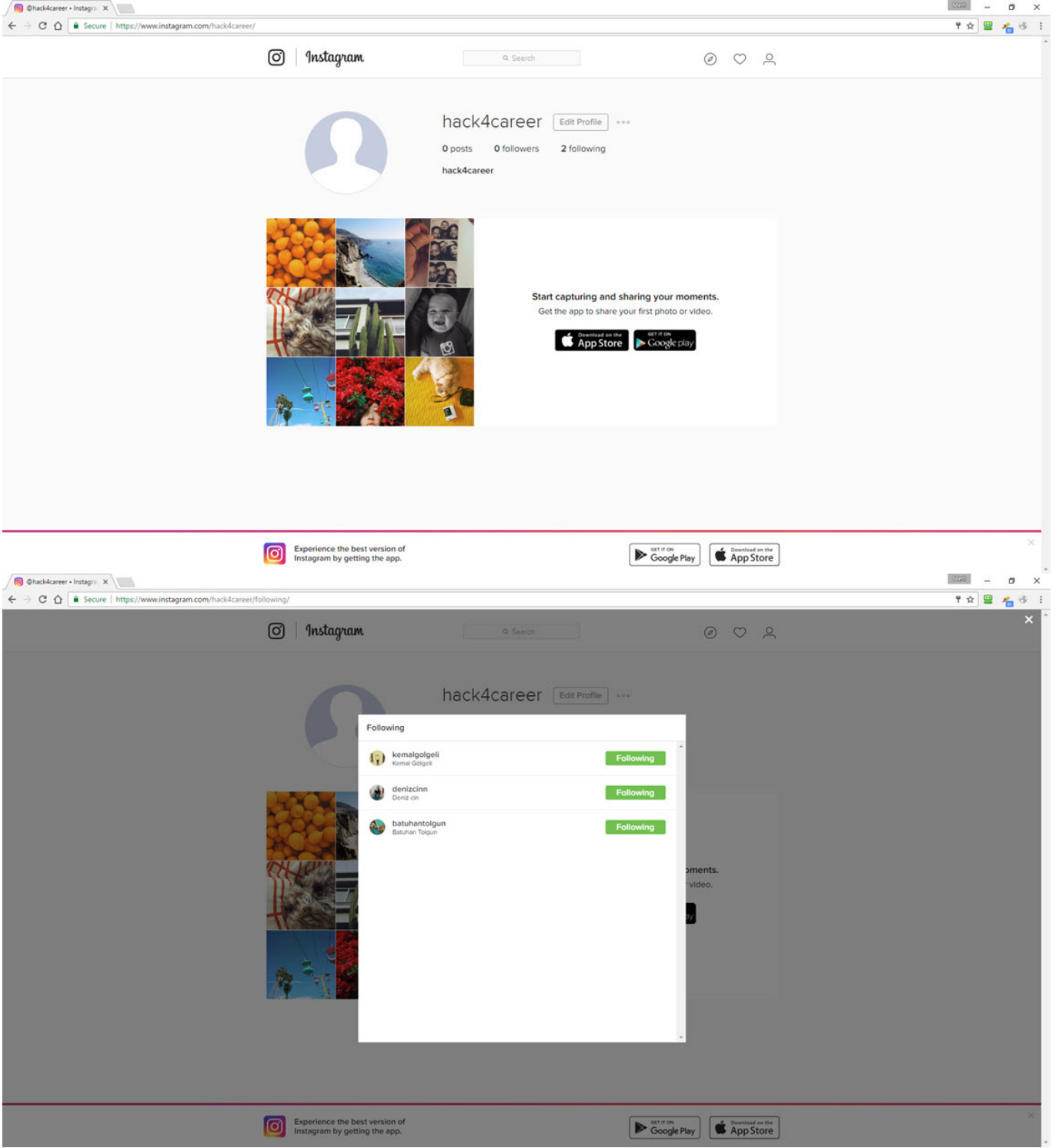
İNSFOLLOW.COM - BİLGİLENDİRME

Hoşgeldin Hemen Vip Üyelik alarak İstedığınız kullanıcıya Takipçi ve Beğeni atabilirsiniz. Vip kullanıcılar günlük 500 kredi kazanırlar.

0553 Aktif Kullanıcı Sayısı : 5865

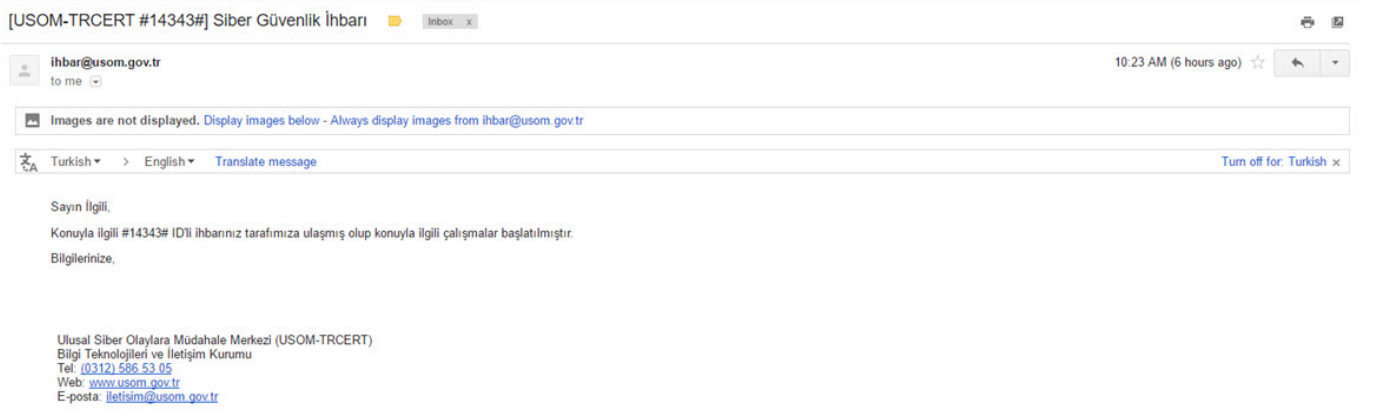
500 Türk Takipçi + Son 3 fotoğrafınıza 200 Beğeni 10 TL Hemen al Arkadaşlarınızı Şaşırt Kredi Kartı ile Ödeme

9 Fotoğrafınıza 1000 Beğeni 49.99 TL Hemen al Arkadaşlarınızı 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 olduđum bildirime istinaden alıřma bařlatan USOM'a, sorumlu bir vatandař olarak teřekkür ederim.



Not: Arařtırmayı yaptığım zaman ile blog yazısını yazmam ve yayımlamam arasında geen sre zarfında yazıya konu olan hastanenin web sayfasından ilgili zararlı kodun kaldırıldıđı grlmřtr.