Threat Hunting

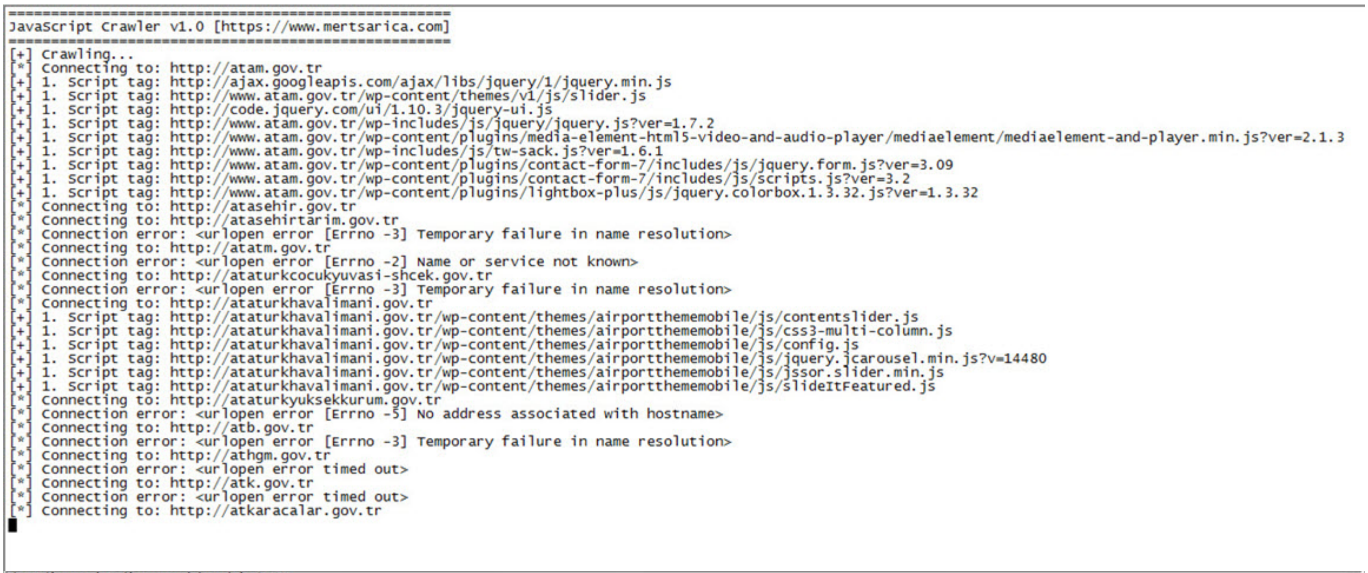
written by Mert SARICA | 1 August 2017

Sometimes, after writing a blog post about a malware, I find myself asking, “How would I detect this if I were in that situation?” and unintentionally a process begins in the background, with this question lingering and waiting to be answered. Once this process is completed and the question is answered, a new blog post emerges, as seen in Figure 1-A. In this current article you are reading, I also sought an answer to the question, “If these malicious individuals are targeting government websites and injecting malicious JavaScript code into the pages, how difficult can it be to detect this in practice?”, following the December 2016 blog post titled “They PWN Houses!”

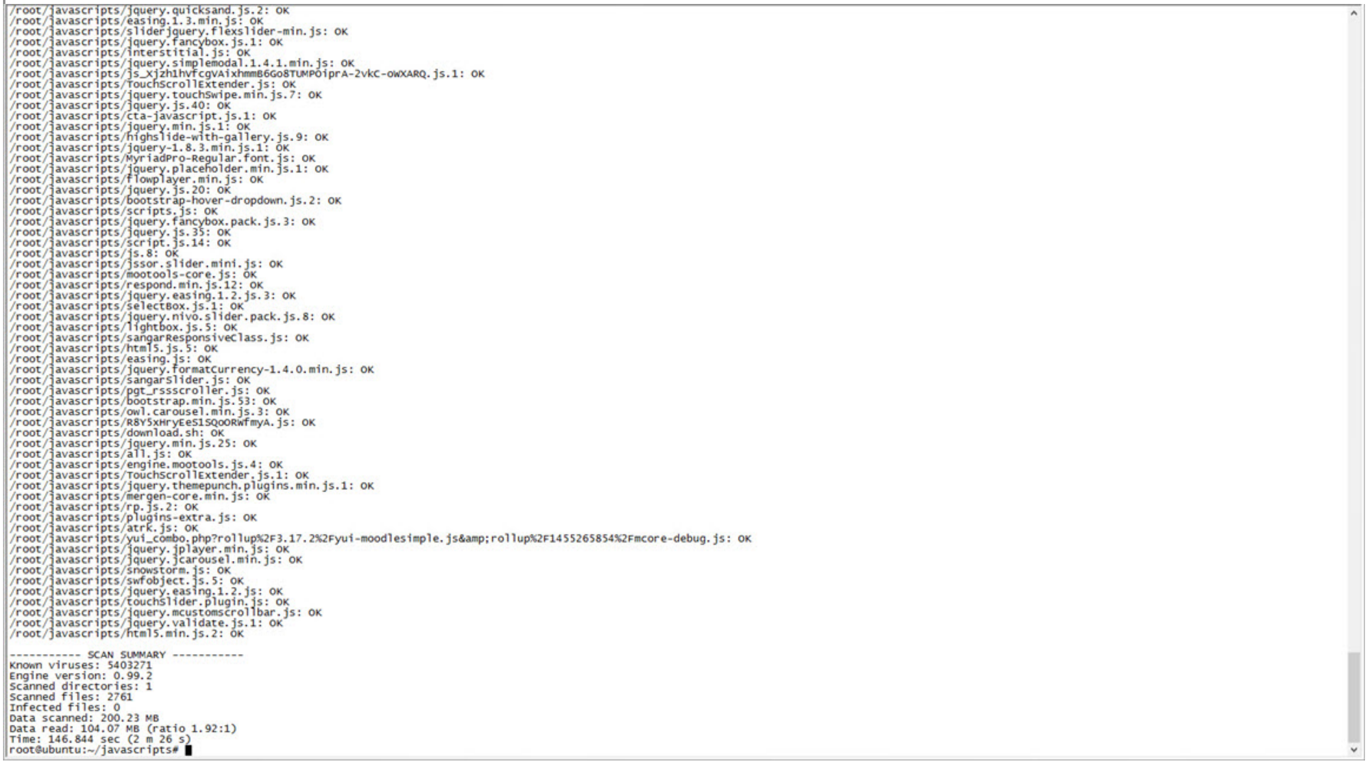
As a first step, I tried to access the domain names of our government websites (with the .gov.tr extension) through search engine APIs such as Google and Bing, but I was unsuccessful due to their existing limitations. While desperately daydreaming about having access to DNS requests made to the OpenDNS service, so that I could extract the list from there, the idea of Roksit, the counterpart of OpenDNS, came to mind. I decided to contact them and ask for support regarding my security research on this matter. Thankfully, once they understood my good intentions, they shared with me a list of government domain names (~8000 in total), although not complete, which I could practically implement the idea in my mind.

After obtaining the list, without wasting any time, I quickly developed a simple tool called JavaScript Crawler using Python, which crawls through all the websites and detects JavaScript code injected (imported) into the homepage via the current site or any other web address. It saves the detected JavaScript code along with the corresponding web addresses to the disk. Shortly after running this tool, I created a script that downloads all the identified JavaScript files from their respective addresses.

Once the JavaScript files were downloaded, I scanned them using security software such as ClamAV, ESET NOD32, and Kaspersky Internet Security Suite. Fortunately, I did not come across any malicious files during the scanning process.

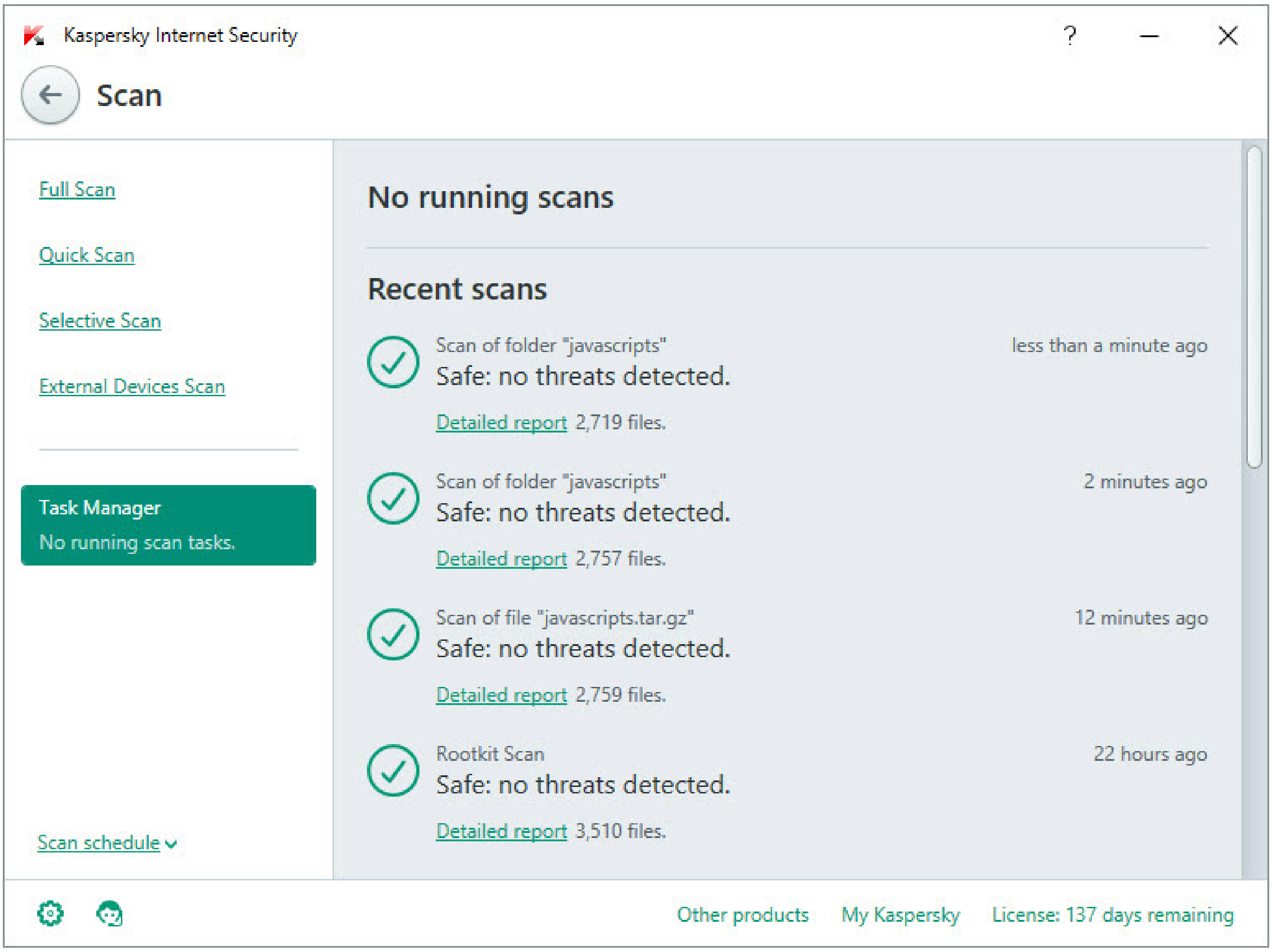


```
======================================================
JavaScript Crawler v1.0 [https://www.mertsarica.com]
======================================================
[+] Crawling...
[*] Connecting to: http://atam.gov.tr
[+] 1. Script tag: http://ajax.googleapis.com/ajax/libs/jquery/1/jquery.min.js
[+] 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# █
```



No running scans

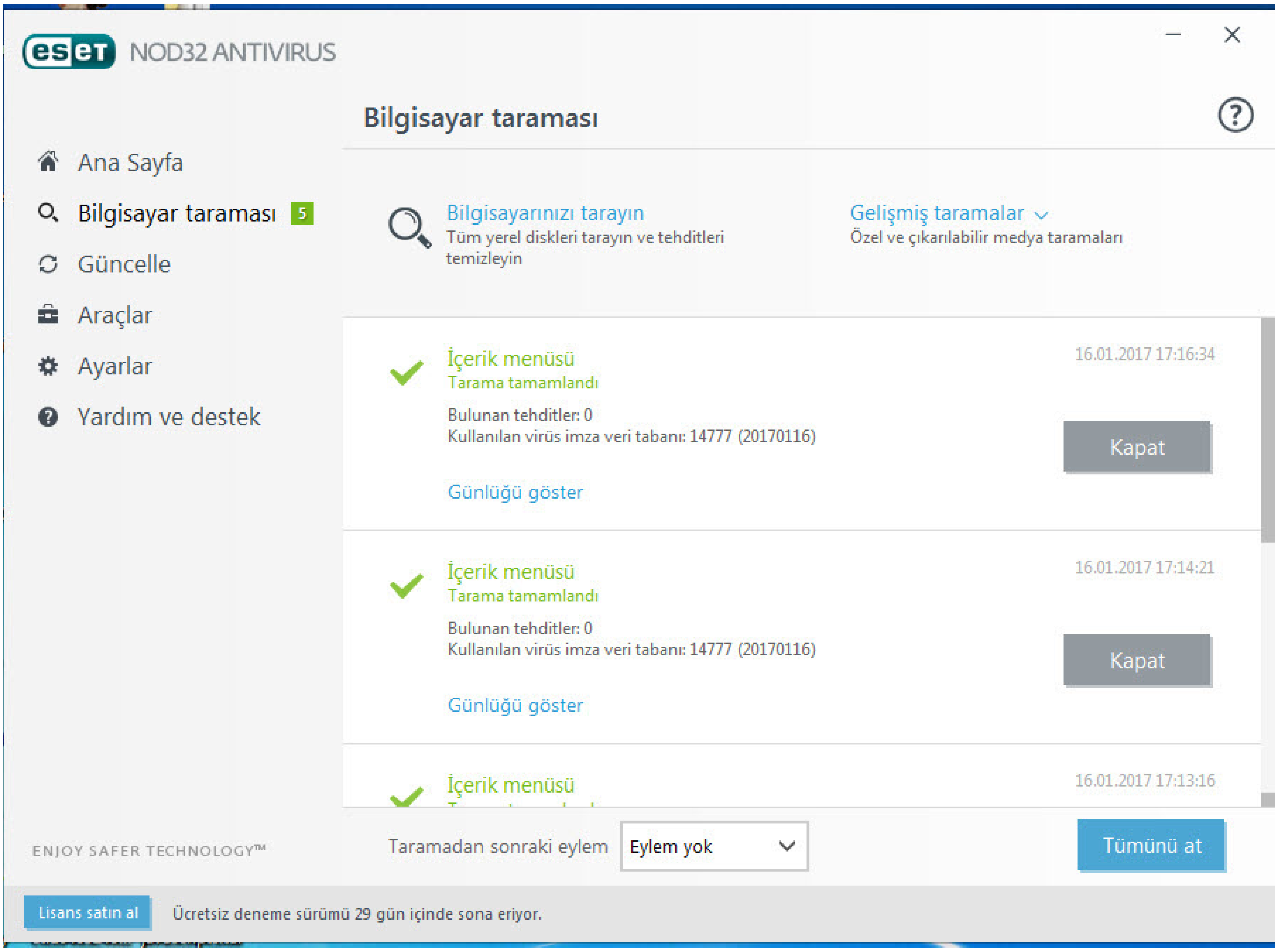
Recent scans

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.



Bilgisayar taraması

Bilgisayarınızı tarayın
Tüm yerel diskleri tarayın ve tehditleri temizleyin

Gelişmiş taramalar
Özel ve çıkarılabilir medya taramaları

İçerik menüsü
Tarama tamamlandı
16.01.2017 17:16:34
Bulunan tehditler: 0
Kullanılan virüs imza veri tabanı: 14777 (20170116)
Günlüğü göster

İçerik menüsü
Tarama tamamlandı
16.01.2017 17:14:21
Bulunan tehditler: 0
Kullanılan virüs imza veri tabanı: 14777 (20170116)
Günlüğü göster

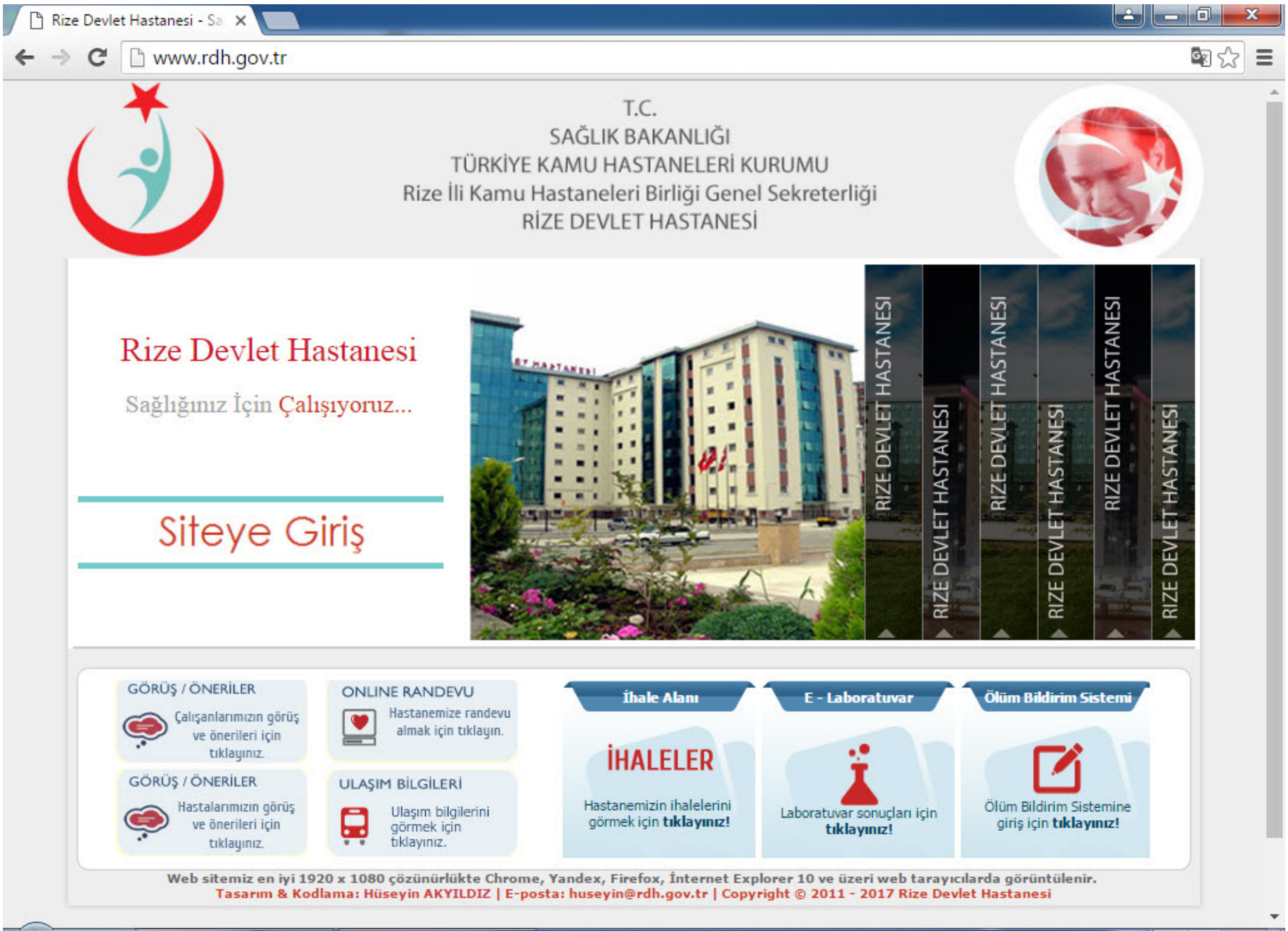
İçerik menüsü
16.01.2017 17:13:16

Taramadan sonraki eylem: Eylem yok

Ücretsiz deneme sürümü 29 gün içinde sona eriyor.

Then, I used the sort tool to arrange the web addresses of the JavaScript files listed in the log file, and filtered out well-known addresses like ajax.googleapis.com. Among the remaining addresses, one domain caught my attention: insfollow.com. When I checked which government website this domain was detected on, I found that it belonged to Rize State Hospital. I visited the website and examined its source code, where I easily identified the insfollow.com domain and the injected JavaScript file.

To gather more information, I submitted the insfollow.com address to VirusTotal, and it revealed that three security software detected it as a phishing site.



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.

GÖRÜŞ / ÖNERİLER
Hastalarımızın görüş ve önerileri için tıklayınız.

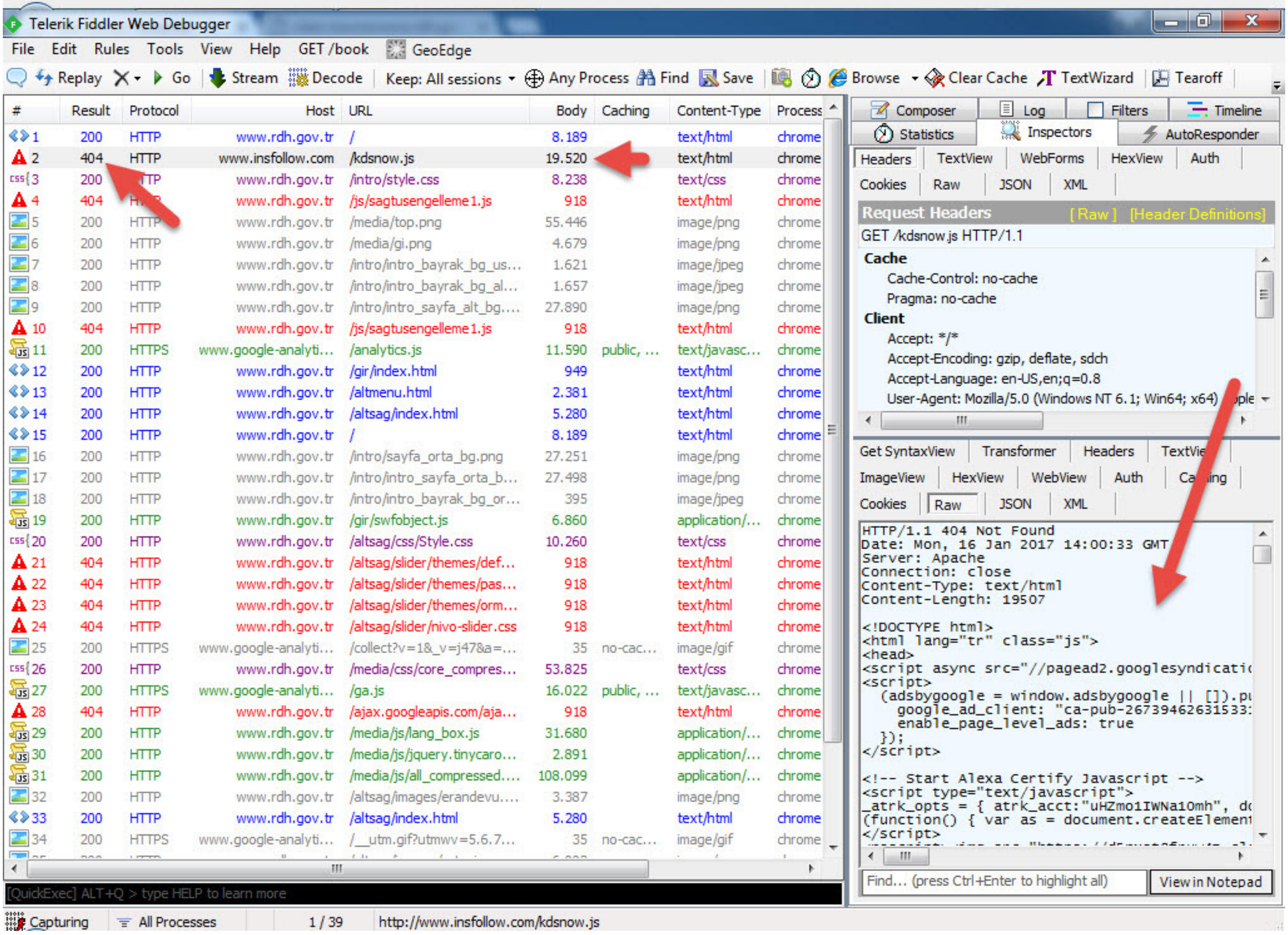
ULAŞIM BİLGİLERİ
Ulaşım bilgilerini görmek için tıklayınız.

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



#	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

```
[QuickExec] ALT+Q > type HELP to learn more
```

1 / 39   http://www.insfollow.com/kdsnow.js

Request Headers [Raw] [Header Definitions]

GET /kdsnow.js HTTP/1.1

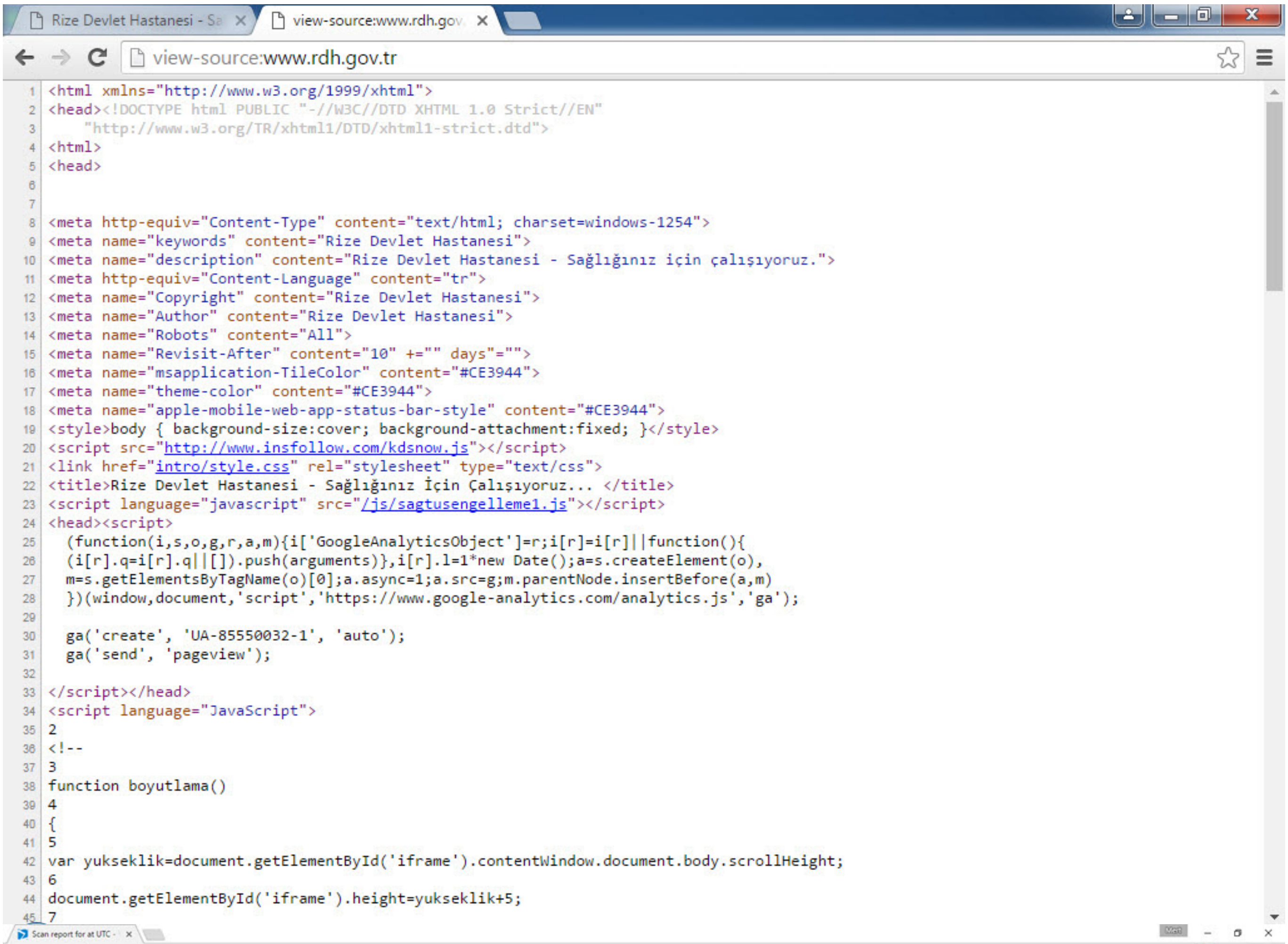
Cache
Cache-Control: no-cache
Pragma: no-cache

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) ple

```
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", do
(function() { var as = document.createElement
</script>
```

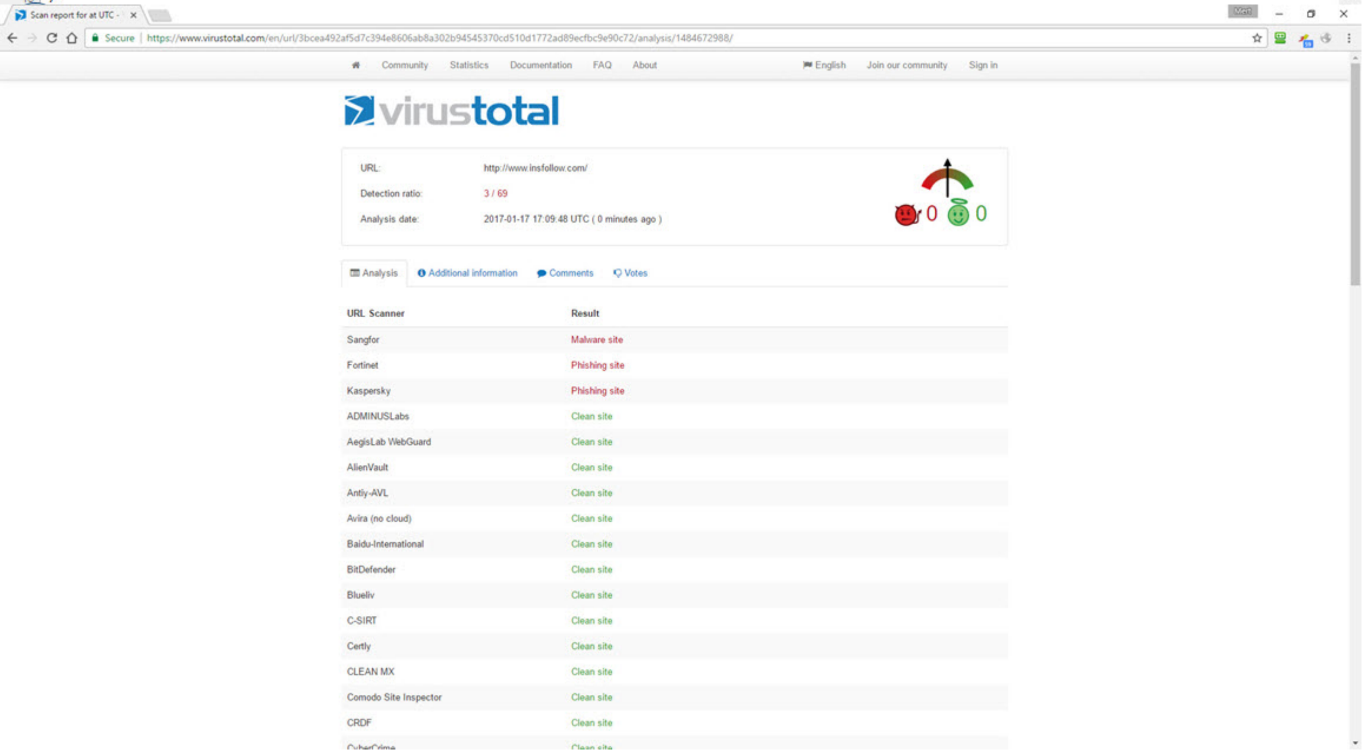


```
<html xmlns="http://www.w3.org/1999/xhtml">
<head><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>


<meta http-equiv="Content-Type" content="text/html; charset=windows-1254">
<meta name="keywords" content="Rize Devlet Hastanesi">
<meta name="description" content="Rize Devlet Hastanesi - Sağlığınız için çalışıyoruz.">
<meta http-equiv="Content-Language" content="tr">
<meta name="Copyright" content="Rize Devlet Hastanesi">
<meta name="Author" content="Rize Devlet Hastanesi">
<meta name="Robots" content="All">
<meta name="Revisit-After" content="10" +="" days"="">
<meta name="msapplication-TileColor" content="#CE3944">
<meta name="theme-color" content="#CE3944">
<meta name="apple-mobile-web-app-status-bar-style" content="#CE3944">
<style>body { background-size:cover; background-attachment:fixed; }</style>
<script src="http://www.insfollow.com/kdsnow.js"></script>
<link href="intro/style.css" rel="stylesheet" type="text/css">
<title>Rize Devlet Hastanesi - Sağlığınız İçin Çalışıyoruz... </title>
<script language="javascript" src="/js/sagtusengelleme1.js"></script>
<head><script>
  (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
  (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
  m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
  })(window,document,'script','https://www.google-analytics.com/analytics.js','ga');

  ga('create', 'UA-85550032-1', 'auto');
  ga('send', 'pageview');

</script></head>
<script language="JavaScript">
2
<!--
3
function boyutlama()
4
{
5
var yukseklik=document.getElementById('iframe').contentWindow.document.body.scrollHeight;
6
document.getElementById('iframe').height=yukseklik+5;
7
```



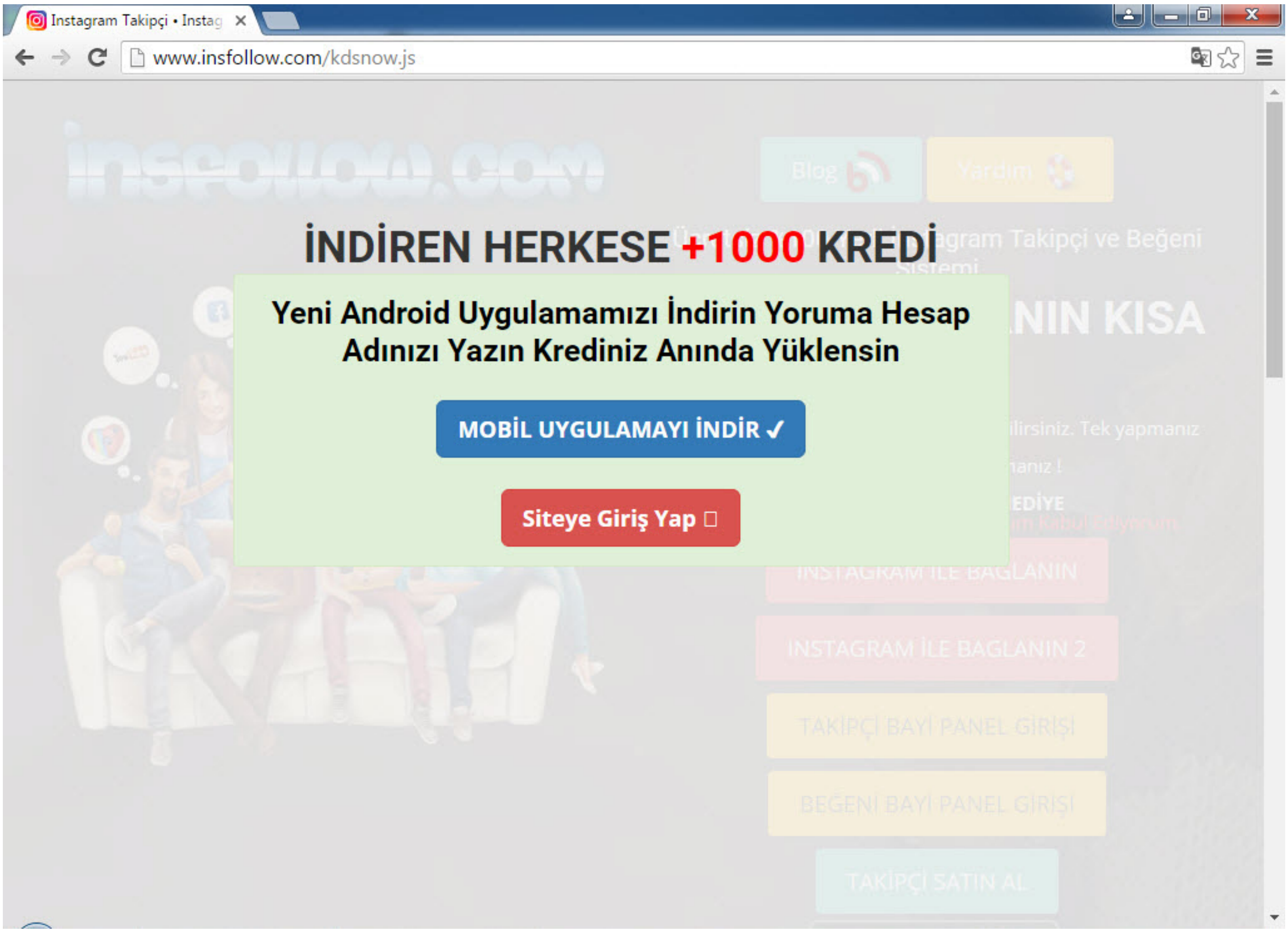
URL: http://www.insfollow.com/

Detection ratio: 3 / 69

Analysis date: 2017-01-17 17:09:48 UTC (0 minutes ago)

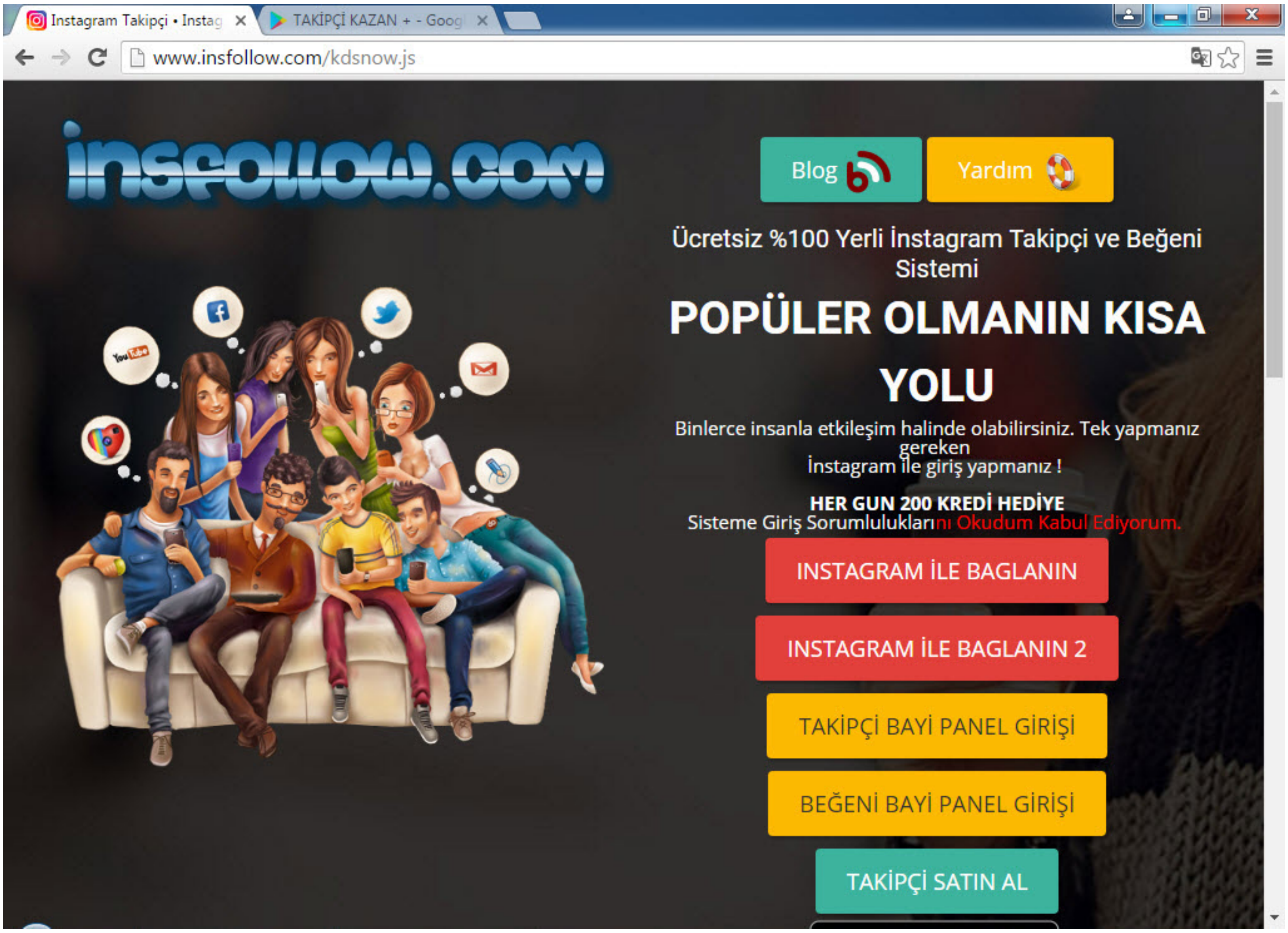
URL Scanner	Result
Sangfor	Malware site
Fortinet	Phishing site
Kaspersky	Phishing site
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira (no cloud)	Clean site
Baidu-International	Clean site
BitDefender	Clean site
Blueliv	Clean site
C-SIRT	Clean site
Certly	Clean site
CLEAN MX	Clean site
Comodo Site Inspector	Clean site
CRDF	Clean site
CyberCrime	Clean site

When I visited http://www.insfollow.com, I discovered that it was a website created with the purpose of selling Instagram followers, indicating that it operated under the guise of providing such services. However, based on my previous analysis of malicious websites and JavaScript codes involved in stealing social media and network passwords (such as Token Thieves and Social Network Thieves), I decided to continue my research.



İNDİREN HERKESE +1000 KREDİ

Yeni Android Uygulamamızı İndirin Yoruma Hesap Adınızı Yazın Krediniz Anında Yüklensin



Ücretsiz %100 Yerli İnstagram Takipçi ve Beğeni Sistemi

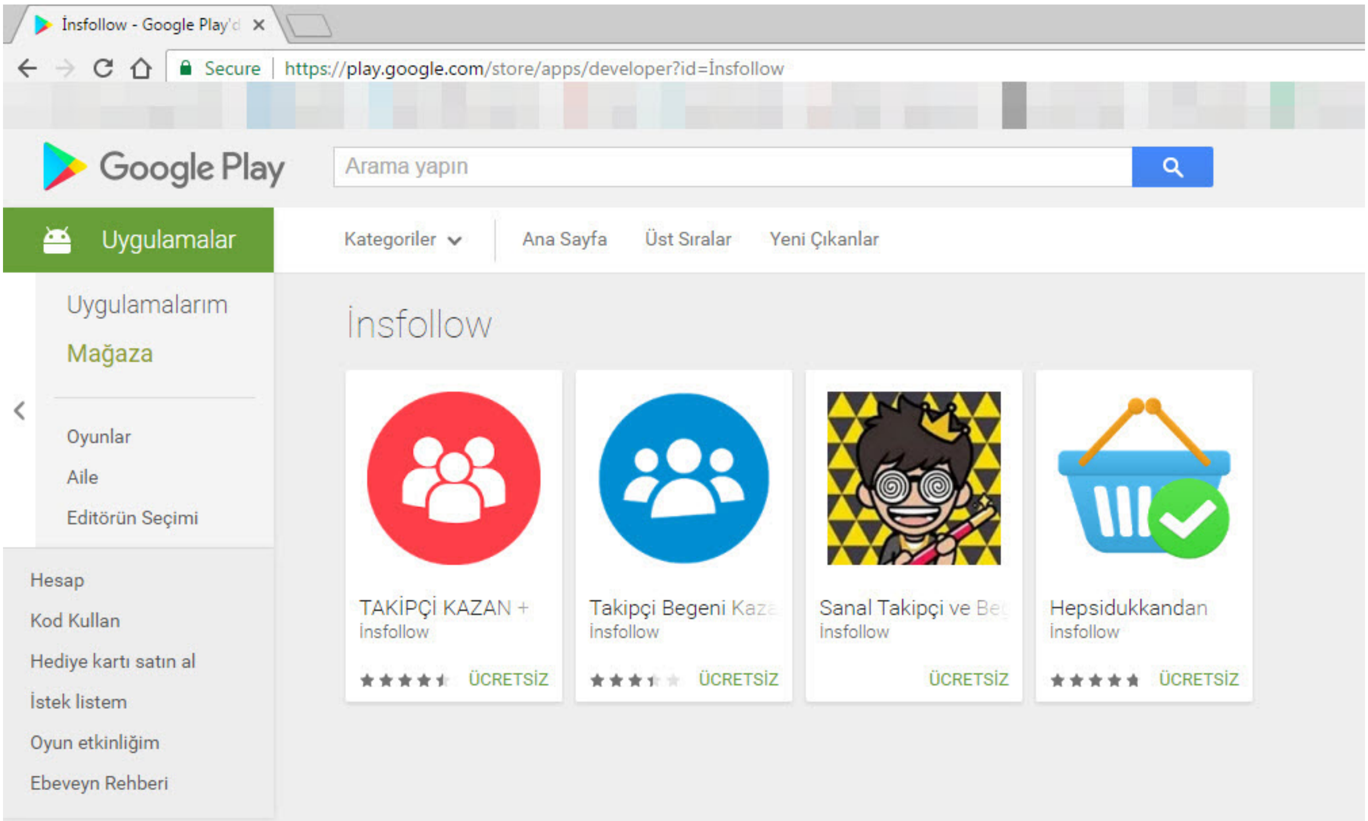
POPÜLER OLMANIN KISA YOLU

Binlerce insanla etkileşim halinde olabilirsiniz. Tek yapmanız gereken İnstagram ile giriş yapmanız !

HER GUN 200 KREDİ HEDİYE

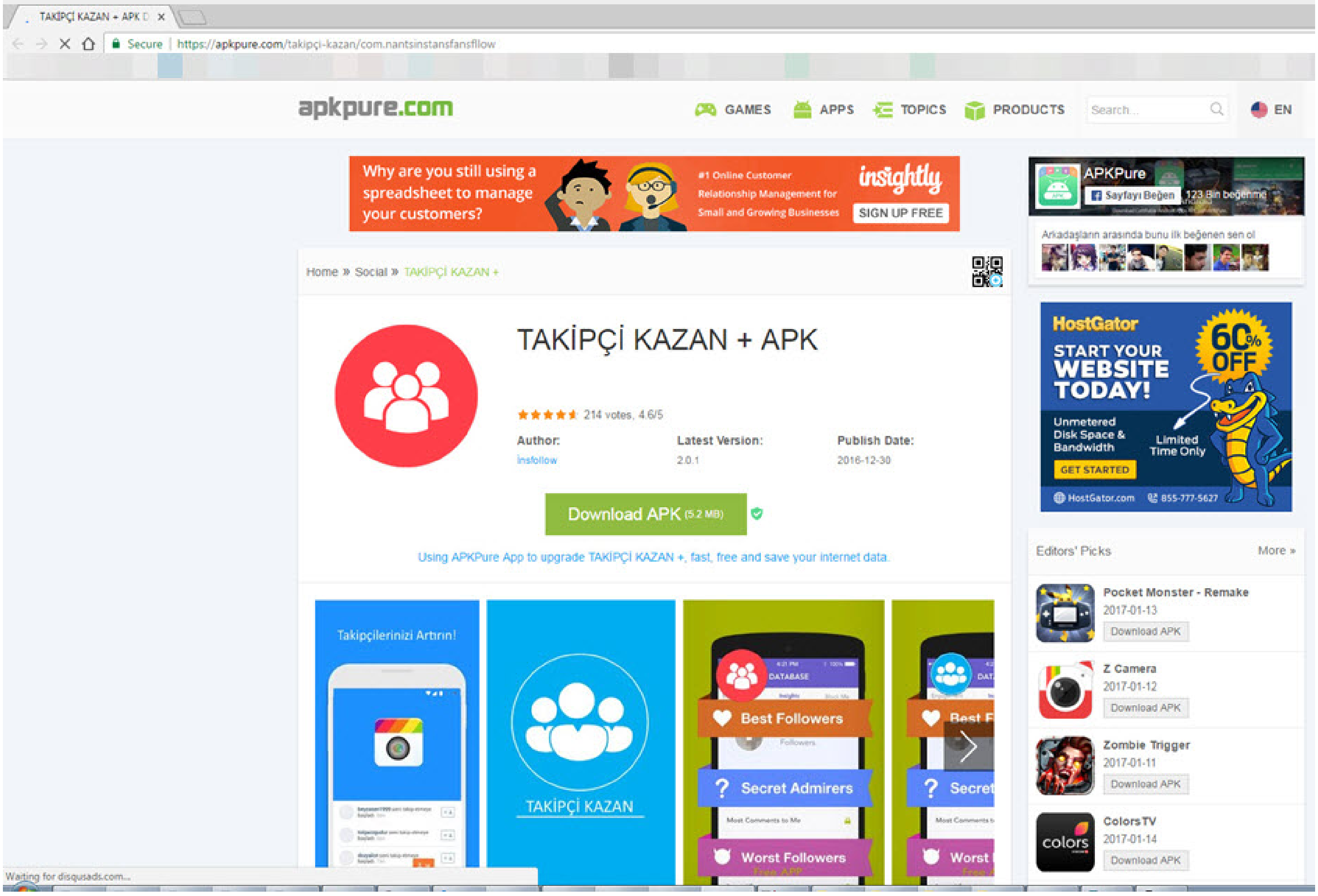
Sisteme Giriş Sorumluluklarını Okudum Kabul Ediyorum.

First, I downloaded the advertised “Takipçi Kazan” mobile application from the website and ran it on the Genymotion emulator. In the pop-up message window, it instructed me to log in to the application with an Instagram account. Therefore, I created a new Instagram account specifically for this purpose, knowing that I could safely expose its password.



İnsfollow

TAKİPÇİ KAZAN +	İnsfollow	ÜCRETSİZ
Takipçi Begeni Kaza	İnsfollow	ÜCRETSİZ
Sanal Takipçi ve Be	İnsfollow	ÜCRETSİZ
Hepsidukkandan	İnsfollow	ÜCRETSİZ



TAKİPÇİ KAZAN + APK D ×
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?
#1 Online Customer Relationship Management for Small and Growing Businesses
insightly
SIGN UP FREE
APKPure
Sayfayı Beğen
123 Bin beğenme
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
Takipçilerinizi Artırın!
TAKİPÇİ KAZAN
Best Followers
Secret Admirers
Worst Followers
Waiting for disqusads.com...

Home » Social » TAKİPÇİ KAZAN +

TAKİPÇİ KAZAN + APK

★★★★★ 214 votes, 4.6/5

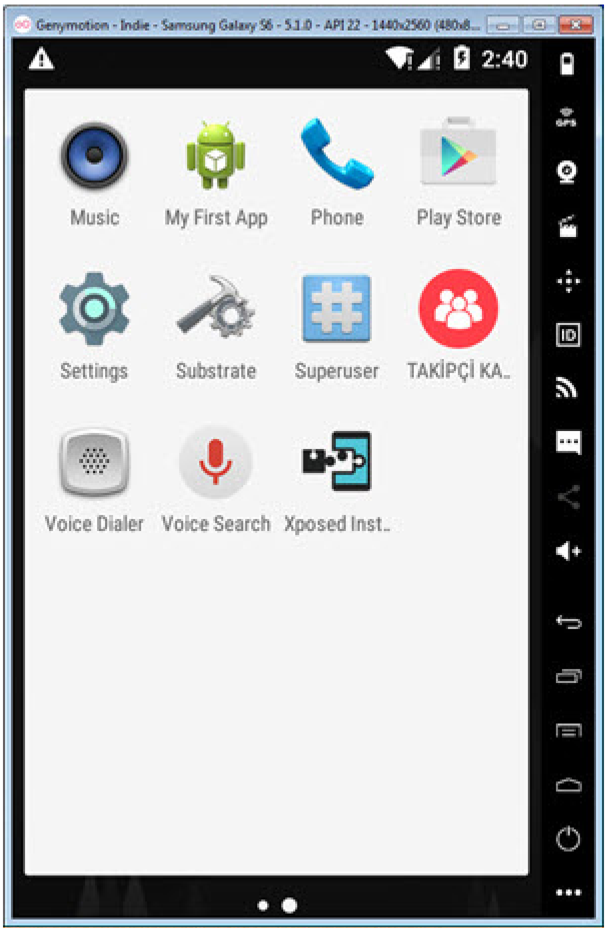
Author:	Latest Version:	Publish Date:
İnsfollow	2.0.1	2016-12-30

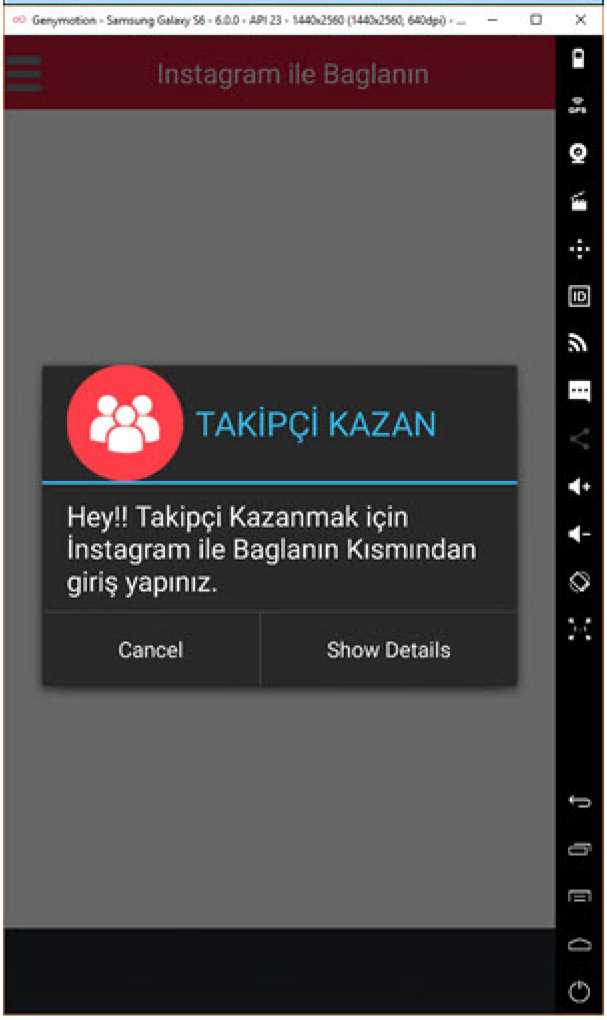
Download APK (5.2 MB)

Using APKPure App to upgrade TAKİPÇİ KAZAN +, fast, free and save your internet data.

Editors' Picks More »

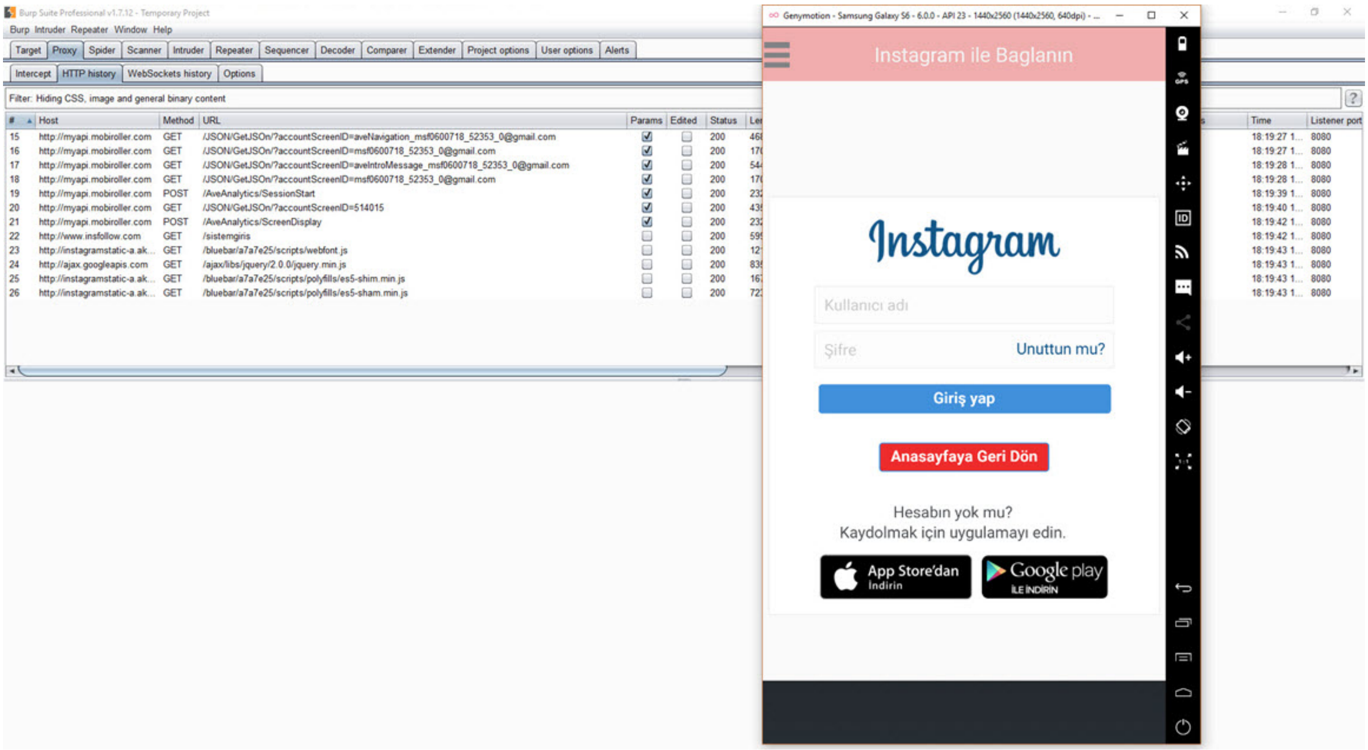
Pocket Monster - Remake	2017-01-13	Download APK
Z Camera	2017-01-12	Download APK
Zombie Trigger	2017-01-11	Download APK
Colors TV	2017-01-14	Download APK




Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 (1440x2560, 640dpi) - ...
Instagram ile Baglanın
TAKİPÇİ KAZAN

Hey!! Takipçi Kazanmak için İnstagram ile Baglanın Kısmından giriş yapınız.

When I ran the application, I discovered that it was developed using Mobiroller, as there were requests being made to the URL http://myapi.mobiroller.com in the background. Upon further inspection of the outgoing requests, I was able to easily see the email addresses of the application developer.



Burp Suite Professional v1.7.12 - Temporary Project

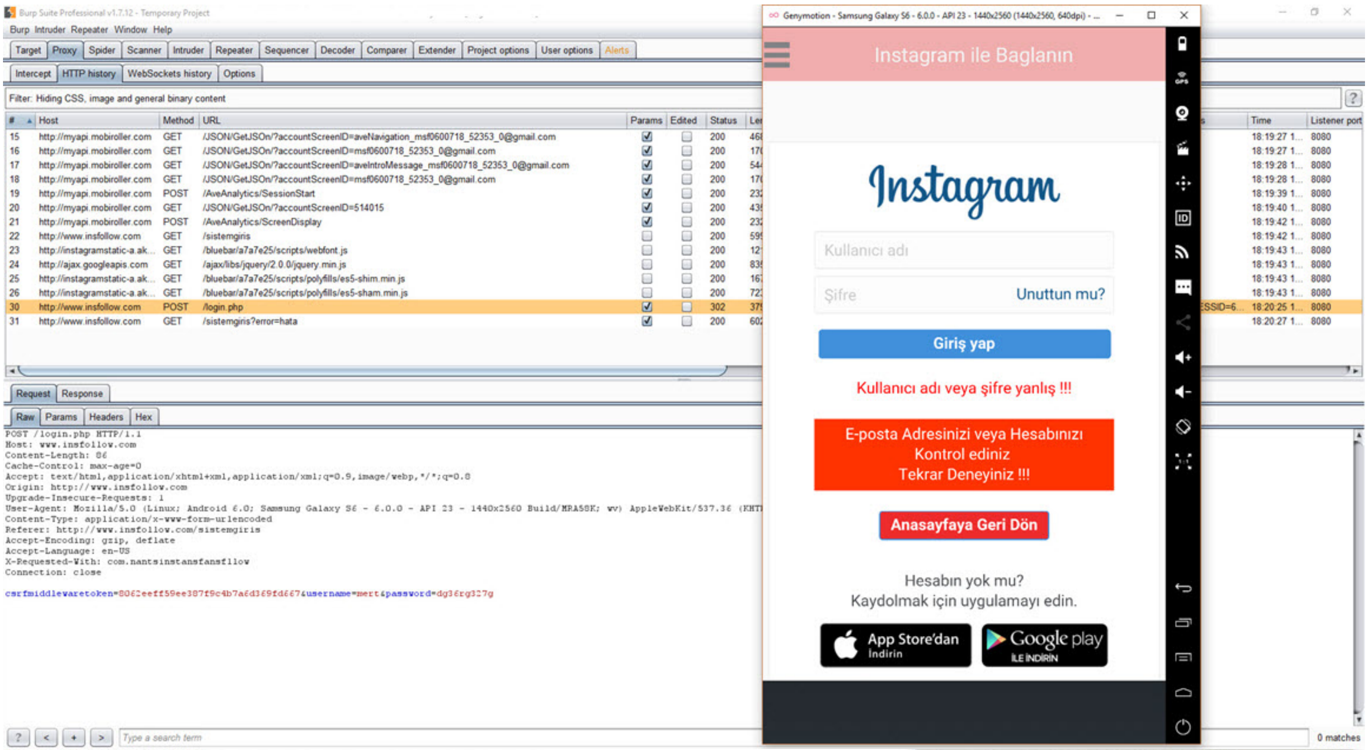
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Le	Time	Listener port
15	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=aveNavigation_msf0600718_52353_0@gmail.com	☑	□	200	46	18:19:27 1...	8080
16	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=msf0600718_52353_0@gmail.com	☑	□	200	17	18:19:27 1...	8080
17	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=aveIntroMessage_msf0600718_52353_0@gmail.com	☑	□	200	54	18:19:28 1...	8080
18	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=msf0600718_52353_0@gmail.com	☑	□	200	17	18:19:28 1...	8080
19	http://myapi.mobiroller.com	POST	/AveAnalytics/SessionStart	☑	□	200	23	18:19:39 1...	8080
20	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=514015	☑	□	200	43	18:19:40 1...	8080
21	http://myapi.mobiroller.com	POST	/AveAnalytics/ScreenDisplay	☑	□	200	23	18:19:42 1...	8080
22	http://www.insfollow.com	GET	/sistemgiris	□	□	200	59	18:19:42 1...	8080
23	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/webfont.js	□	□	200	12	18:19:43 1...	8080
24	http://ajax.googleapis.com	GET	/ajax/libs/jquery/2.0.0/jquery.min.js	□	□	200	83	18:19:43 1...	8080
25	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js	□	□	200	16	18:19:43 1...	8080
26	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-sham.min.js	□	□	200	72	18:19:43 1...	8080

Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 (1440x2560, 640dpi) - ...

Hesabın yok mu?
Kaydolmak için uygulamayı edin.

To understand the behavior of the “Takipçi Kazan” application, I first entered my incorrect Instagram password. From the error message “Username or password is incorrect!!!” it was clear that the application was capturing and instantly using the entered username and password on Instagram. After entering the correct password, the application redirected me to its information and payment page. When I logged into my Instagram account afterwards, I noticed a rapid increase in the number of accounts I was following. However, it wasn’t long before I was unable to log into my Instagram account, and shortly thereafter, my account was suspended by Instagram.



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

#	Host	Method	URL	Params	Edited	Status	Le		Time	Listener port
15	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=aveNavigation_msf0600718_52353_0@gmail.com	☑	□	200	46		18:19:27 1...	8080
16	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=msf0600718_52353_0@gmail.com	☑	□	200	17		18:19:27 1...	8080
17	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=aveIntroMessage_msf0600718_52353_0@gmail.com	☑	□	200	54		18:19:28 1...	8080
18	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=msf0600718_52353_0@gmail.com	☑	□	200	17		18:19:28 1...	8080
19	http://myapi.mobiroller.com	POST	/AveAnalytics/SessionStart	☑	□	200	23		18:19:39 1...	8080
20	http://myapi.mobiroller.com	GET	/JSON/GetJSOn/?accountScreenID=514015	☑	□	200	43		18:19:40 1...	8080
21	http://myapi.mobiroller.com	POST	/AveAnalytics/ScreenDisplay	☑	□	200	23		18:19:42 1...	8080
22	http://www.insfollow.com	GET	/sistemgiris	□	□	200	59		18:19:42 1...	8080
23	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/webfont.js	□	□	200	12		18:19:43 1...	8080
24	http://ajax.googleapis.com	GET	/ajax/libs/jquery/2.0.0/jquery.min.js	□	□	200	83		18:19:43 1...	8080
25	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js	□	□	200	16		18:19:43 1...	8080
26	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-sham.min.js	□	□	200	72		18:19:43 1...	8080
30	http://www.insfollow.com	POST	/login.php	☑	□	302	37	ESSID=6...	18:20:25 1...	8080
31	http://www.insfollow.com	GET	/sistemgiris?error=hata	☑	□	200	60		18:20:27 1...	8080

```
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/MRA58K; wv) AppleWebKit/537.36 (KHT
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=8062eeff59ee387f9c4b7a6d369fd667&username=mert&password=dg36rg327g
```

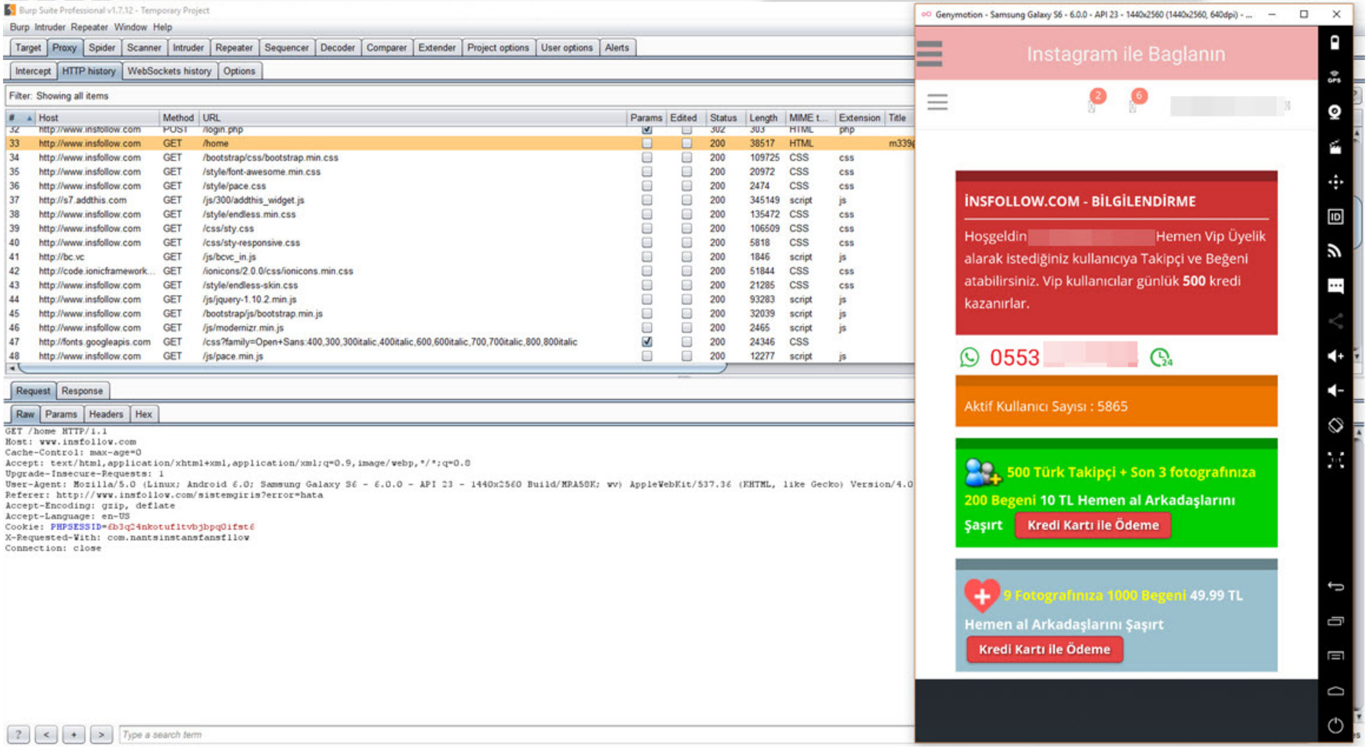
? < + > Type a search term
0 matches
Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 (1440x2560, 640dpi) - ...
Instagram ile Baglanın
Instagram
Kullanıcı adı
Şifre
Unuttun mu?
Giriş yap

Kullanıcı adı veya şifre yanlış !!!

E-posta Adresinizi veya Hesabınızı
Kontrol ediniz
Tekrar Deneyiniz !!!

Hesabın yok mu?
Kaydolmak için uygulamayı edin.

App Store'dan İndirin
Google play İLE İNDİRİN



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: Showing all items

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title
32	http://www.insfollow.com	POST	/login.php	☑	□	302	303	HTML	php	
33	http://www.insfollow.com	GET	/home	□	□	200	38517	HTML		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/endless.min.css	□	□	200	135472	CSS	css	
39	http://www.insfollow.com	GET	/css/sty.css	□	□	200	106509	CSS	css	
40	http://www.insfollow.com	GET	/css/sty-responsive.css	□	□	200	5818	CSS	css	
41	http://bc.vc	GET	/js/bcvc_in.js	□	□	200	1846	script	js	
42	http://code.ionicframework...	GET	/ionicons/2.0.0/css/ionicons.min.css	□	□	200	51844	CSS	css	
43	http://www.insfollow.com	GET	/style/endless-skin.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		
48	http://www.insfollow.com	GET	/js/pace.min.js	□	□	200	12277	script	js	

```
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/MRA58K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Referer: http://www.insfollow.com/sistemgiris?error=hata
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: PHPSESSID=6b3q24nkotufltvbjbpq0ifst6
X-Requested-With: com.nantsinstansfansfllow
Connection: close
```

? < + > Type a search term
Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 (1440x2560, 640dpi) - ...
Instagram ile Baglanın
2
6

[redacted]

İNSFOLLOW.COM - BİLGİLENDİRME

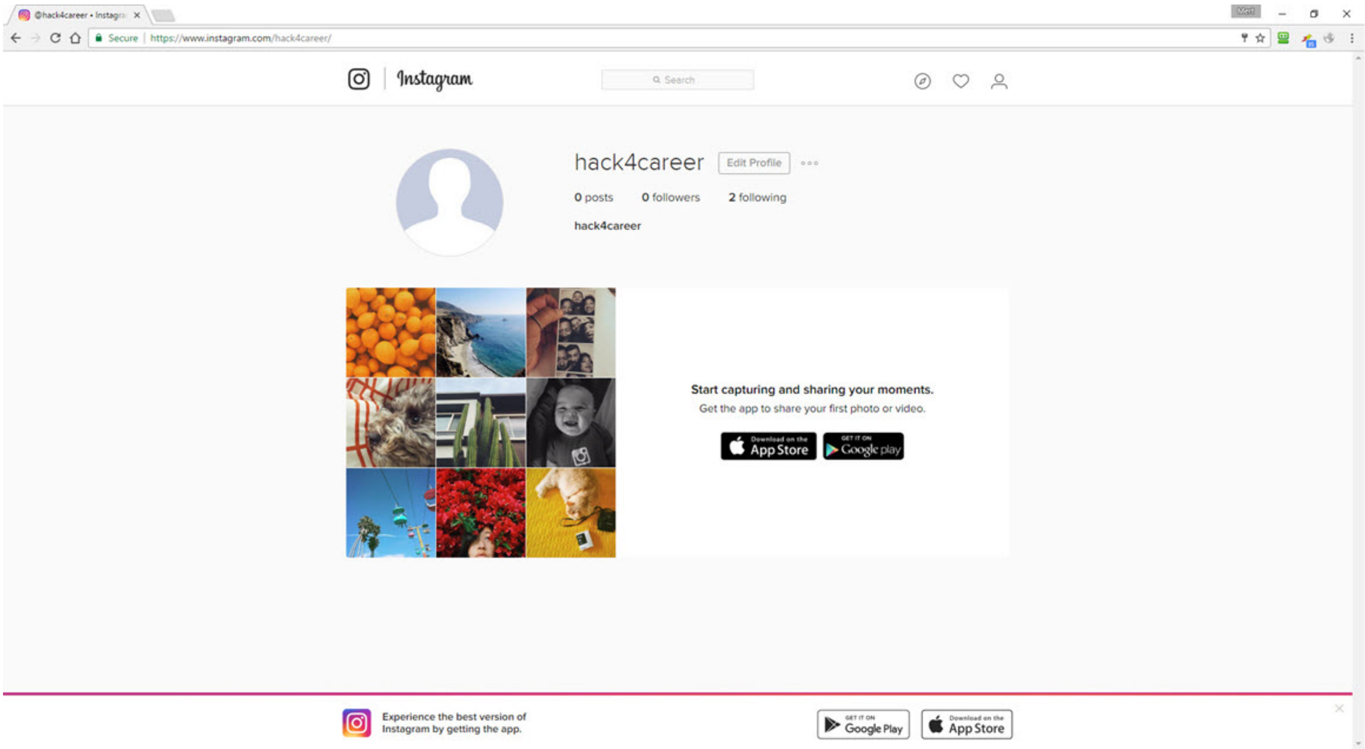
Hoşgeldin [redacted] Hemen Vip Üyelik alarak istediğiniz kullanıcıya Takipçi ve Beğeni atabilirsiniz. Vip kullanıcılar günlük **500** kredi kazanırlar.

0553 [redacted]

Aktif Kullanıcı Sayısı : 5865

500 Türk Takipçi + Son 3 fotografınıza 200 Begeni 10 TL Hemen al Arkadaşlarını Şaşırt

9 Fotografınıza 1000 Begeni 49.99 TL Hemen al Arkadaşlarını Şaşırt



https://www.instagram.com/hack4career/

hack4career

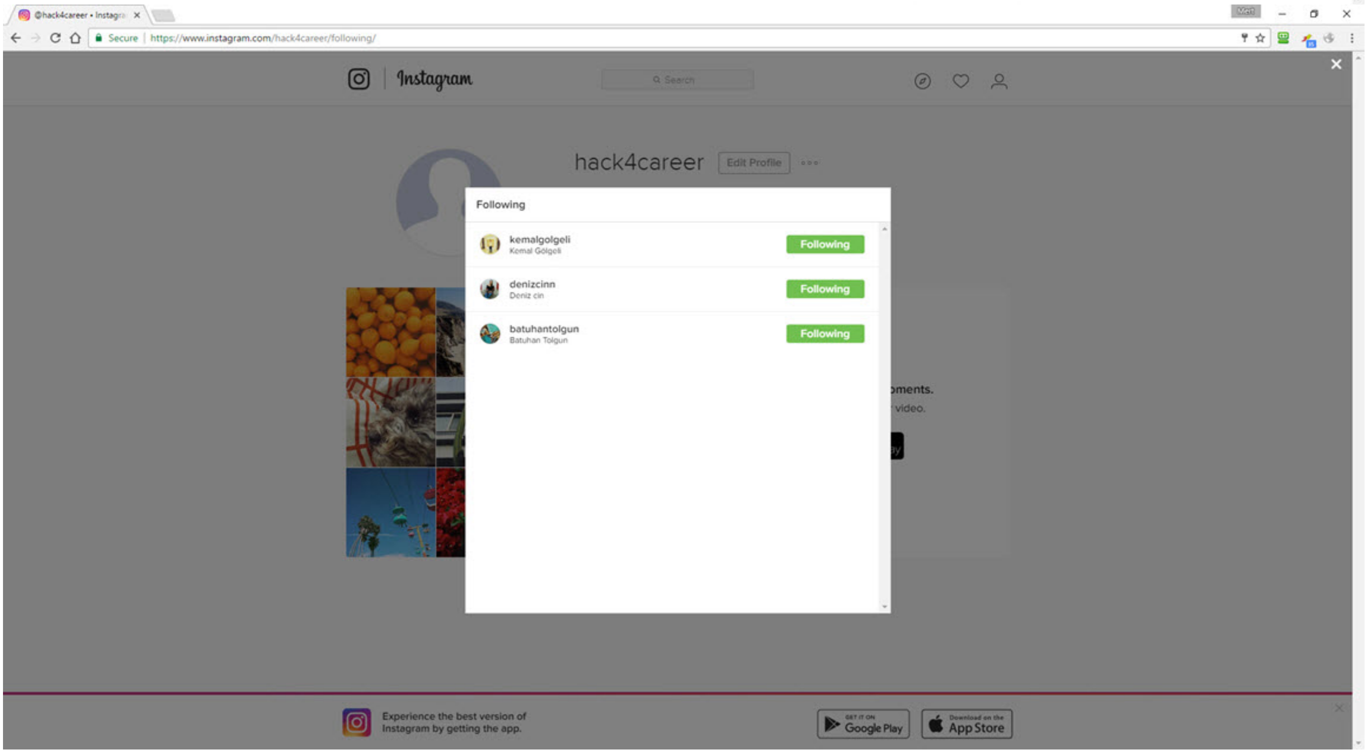
0 posts 0 followers 2 following

hack4career

Start capturing and sharing your moments.

Get the app to share your first photo or video.

Experience the best version of Instagram by getting the app.



https://www.instagram.com/hack4career/following/

Following

kemalgolgeli
Kemal Gölgeli

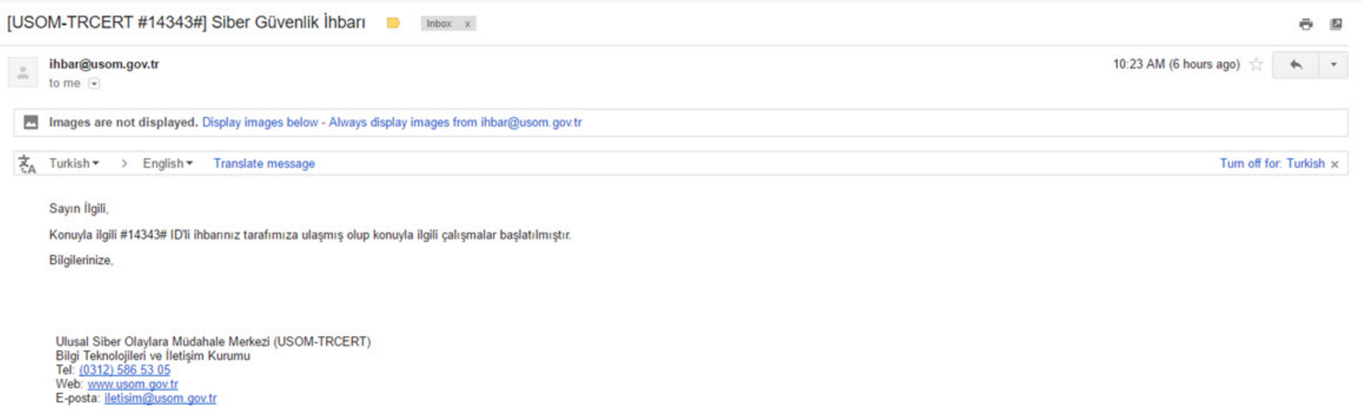
denizcinn
Deniz cin

batuhantolgun
Batuhan Tolgun

As a result of this research, I have learned that in addition to the organized groups mentioned in the “They PWN Houses!” article, social media and network thieves who create websites under the guise of follower services also target our government websites. I hope that this individual effort sheds light on the authorized institutions responsible for the security of government websites. I would like to remind social media users to be cautious when using websites and mobile applications that promise followers or likes.

Hope to see you in the following articles.

Note: I would like to express my gratitude to USOM (National Cybersecurity Intervention Center) for initiating an investigation based on my report as a responsible citizen.



[USOM-TRCERT #14343#] Siber Güvenlik İhbarı

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

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

Note: It has been observed that the malicious code mentioned in the blog post was removed from the website of the hospital during the time between my research and writing/publishing the blog post.