

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://atasehirim.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://aturkocukyuvasi-shcek.gov.tr
[*] Connection error: <urlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://aturkhavalimani.gov.tr
[*] 1. Script tag: http://aturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/contentslider.js
[*] 1. Script tag: http://aturkhavalimani.gov.tr/wp-content/themes/airportthememobile/css3-multi-column.js
[*] 1. Script tag: http://aturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/config.js
[*] 1. Script tag: http://aturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/jquery.jcarousel.min.js?v=14480
[*] 1. Script tag: http://aturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/jssor.slider.min.js
[*] 1. Script tag: http://aturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/slidedetFeatured.js
[*] Connecting to: http://aturkyuksekkurum.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/sliderjquery.flexslider-min.js: OK
/root/.javascrpts/jquery.fancybox.js.1: OK
/root/.javascrpts/js.js: OK
/root/.javascrpts/jquery.simplemodal.1.4.1.min.js: OK
/root/.javascrpts/js_xjzhlvCgVAIXhmmB6G0TUMPOlprA-2vkc-0wXARQ.js.1: 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/flowlayer.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.35: OK
/root/.javascrpts/scripts.js.14: OK
/root/.javascrpts/js.8: OK
/root/.javascrpts/jssor.slider.min.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/sangarResponsiveClass.js: OK
/root/.javascrpts/html5.js.5: OK
/root/.javascrpts/jquery.Formatcurrency-1.4.0.min.js: OK
/root/.javascrpts/sangarSlider.js: OK
/root/.javascrpts/gtt_rssscroller.js: OK
/root/.javascrpts/bootstrap.min.js.53: OK
/root/.javascrpts/owl.carousel.min.js.3: OK
/root/.javascrpts/8v5heryeS15Q00wFmYA.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/rg.js.2: OK
/root/.javascrpts/plugins-extra.js: OK
/root/.javascrpts/atrk.js: OK
/root/.javascrpts/yul_combo.php?rollup%2F3.17.2%2Fyui-moodlesimple.js&rollup%2F1455265854%2Fmcore-debug.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.ecstasyscrollbar.js: OK
/root/.javascrpts/jquery.validate.js.1: OK
/root/.javascrpts/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:~/javascrpts#
```

← Scan

[Full Scan](#)

[Quick Scan](#)

[Selective Scan](#)

[External Devices Scan](#)





Task Manager

No running scan tasks.

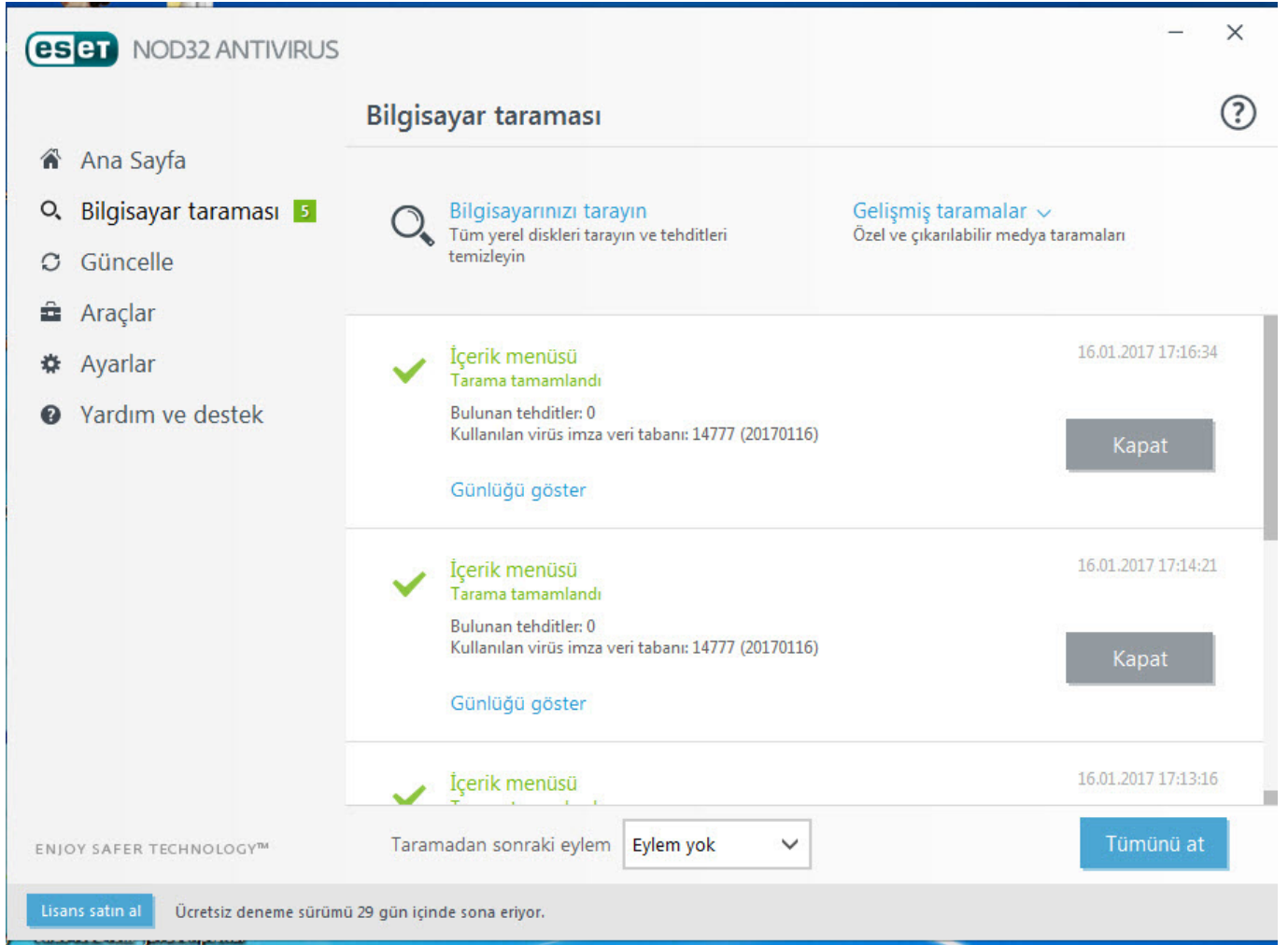
[Scan schedule](#) ▾

No running scans

Recent scans

-  Scan of folder "javascripsts" less than a minute ago
Safe: no threats detected.
[Detailed report](#) 2,719 files.
-  Scan of folder "javascripsts" 2 minutes ago
Safe: no threats detected.
[Detailed report](#) 2,757 files.
-  Scan of file "javascripsts.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.





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.

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 tıklayınız.

İhale Alanı
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 bilgilerinizi 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/sagtusengelleme.1.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/sagtusengelleme.1.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/form...	918		text/html	chrome
24	404	HTTP	www.rdh.gov.tr	/altsag/slider/nivo-slides.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 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.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: "uHZm01IWNa10mh", d...
(function() { var as = document.createElement...
</script>
Find... (press Ctrl+Enter to highlight all) View in Notepad

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 - Sađlđınız iin alıřıyoruz.">
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 - Sađlđınız iin alıřıyoruz... </title>
23 <script language="javascript" src="/js/sagtusengelleme1.js"></script>
24 <head><script>
25 (function(i,s,o,g,r,a,m){i['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
```

Scan report for at UTC - X

Secure | https://www.virustotal.com/en/url/3bcea492af5d7c394e806ab8a302b94545370cd510d1772ad89ectbc9v90c72/analysis/1484672988/

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

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
GRDF	Clean site
Trustwave	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.

Instagram Takipçi • Instag X

www.insfollow.com/kdsnow.js

insfollow.com

Blog Yardım

İNDİREN HERKESE +1000 KREDİ Instagram Takipçi ve Beğeni Sistemi

Yeni Android Uygulamamızı İndirin Yoruma Hesap Adınızı Yazın Krediniz Anında Yüklensin

MOBİL UYGULAMAYI İNDİR ✓

Siteye Giriş Yap

İNİN KISA

İlirsiniz. Tek yapmanız

tanız!

EDİYE

Kabul Ediyorum

INSTAGRAM İLE BAĞLANIN

INSTAGRAM İLE BAĞLANIN 2

TAKİPÇİ BAYİ PANEL GİRİŞİ

BEĞENİ BAYİ PANEL GİRİŞİ

TAKİPÇİ SATIN AL

Instagram Takipçi • Instag x TAKİPÇİ KAZAN + - Goog x

www.insfollow.com/kdsnow.js

insfollow.com

Blog Yardım

Ücretsiz %100 Yerli Instagram Takipçi ve Beğeni Sistemi

POPÜLER OLMANIN KISA YOLU

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

HER GÜN 200 KREDİ HEDİYE
Sisteme Giriş Sorumluluklarını Okudum Kabul Ediyorum.

INSTAGRAM İLE BAĞLANIN

INSTAGRAM İLE BAĞLANIN 2

TAKİPÇİ BAYİ PANEL GİRİŞİ

BEĞENİ BAYİ PANEL GİRİŞİ

TAKİPÇİ SATIN AL

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 - Google Play'de

Secure | https://play.google.com/store/apps/developer?id=İnsfollow

Google Play

Arama yapın

Uygulamalar

Kategoriler v 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 Beğeni Kazan
İnsfollow

★★★★★ ÜCRETSİZ

Sanal Takipçi ve Beğeni
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

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

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

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!

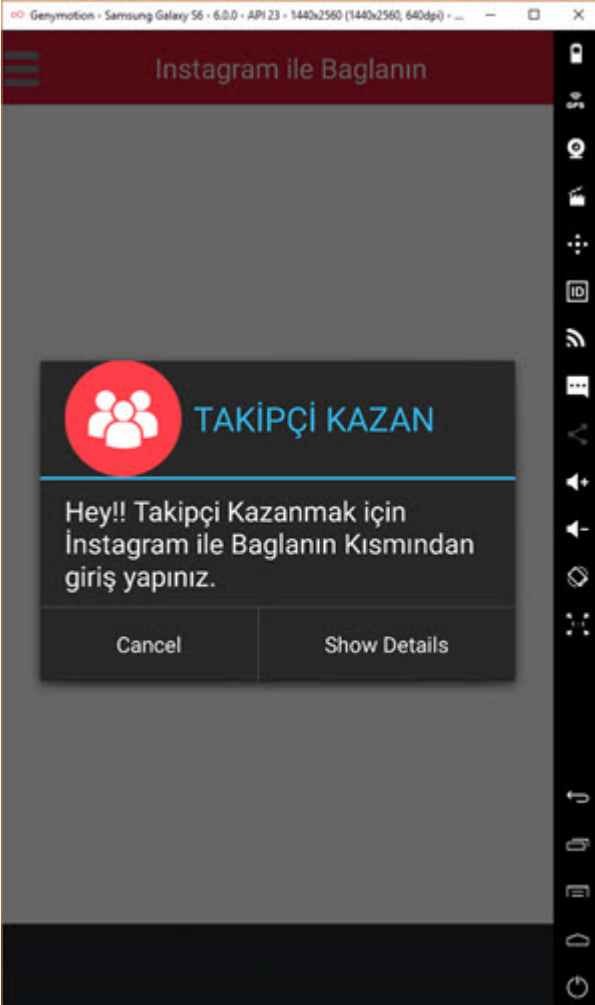
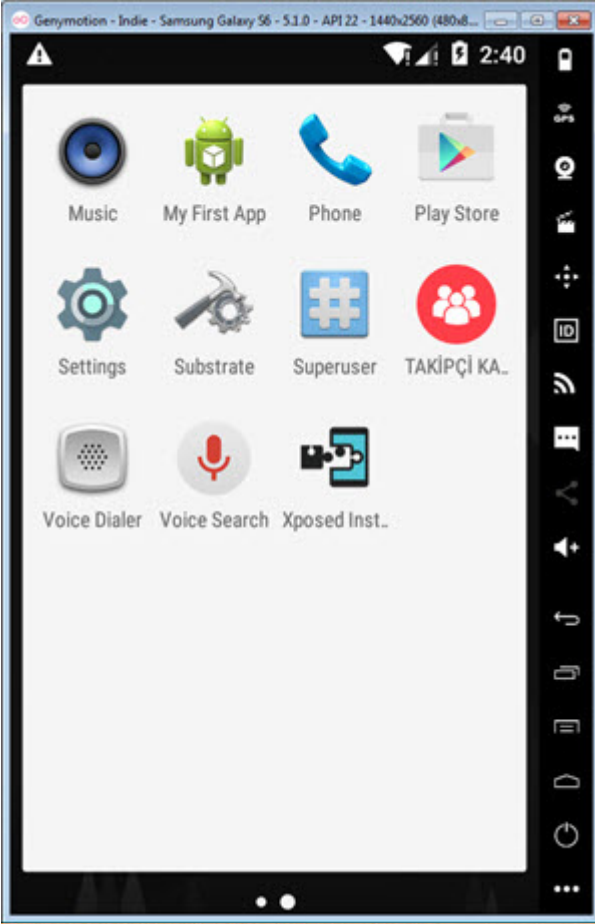
TAKİPÇİ KAZAN

Best Followers

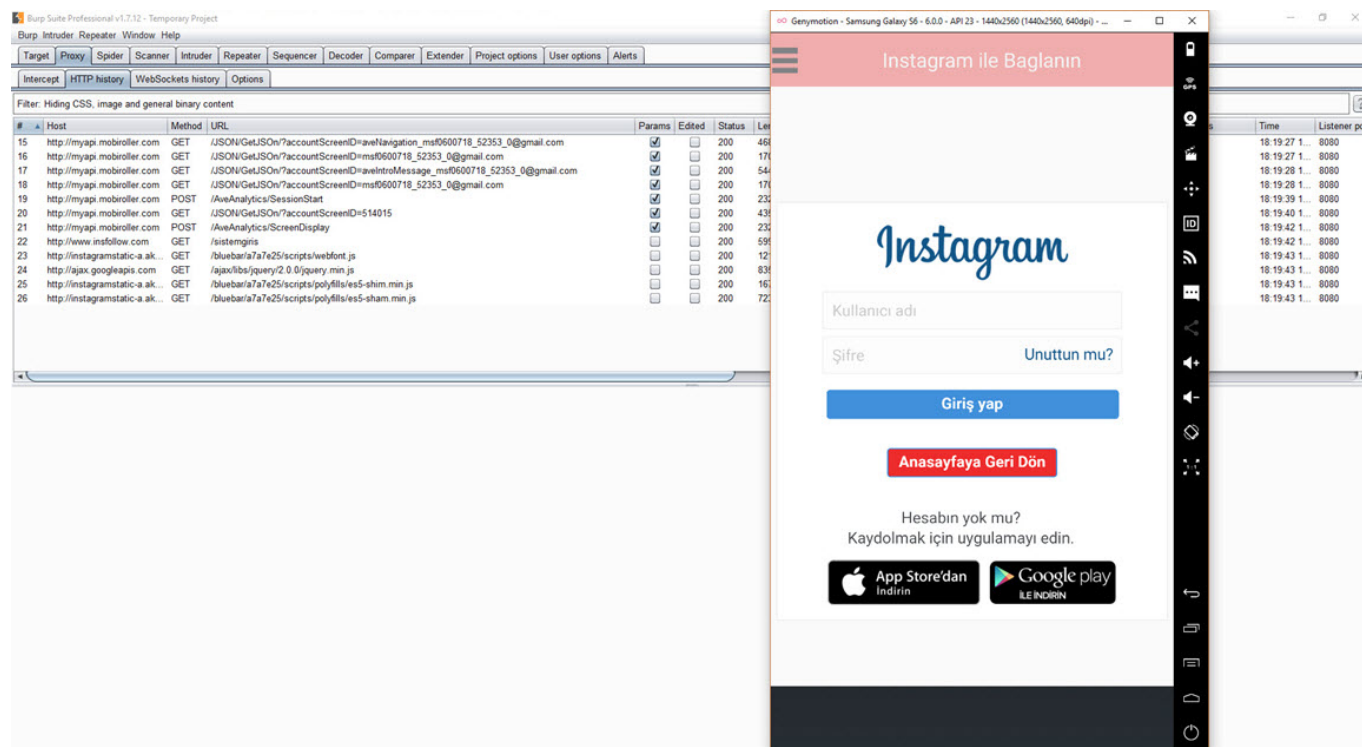
Secret Admirers

Worst Followers

Waiting for disqusads.com...



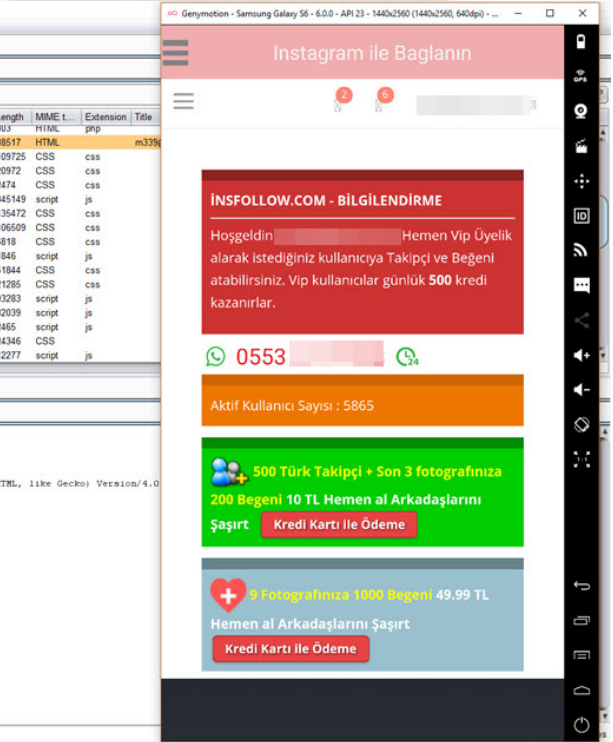
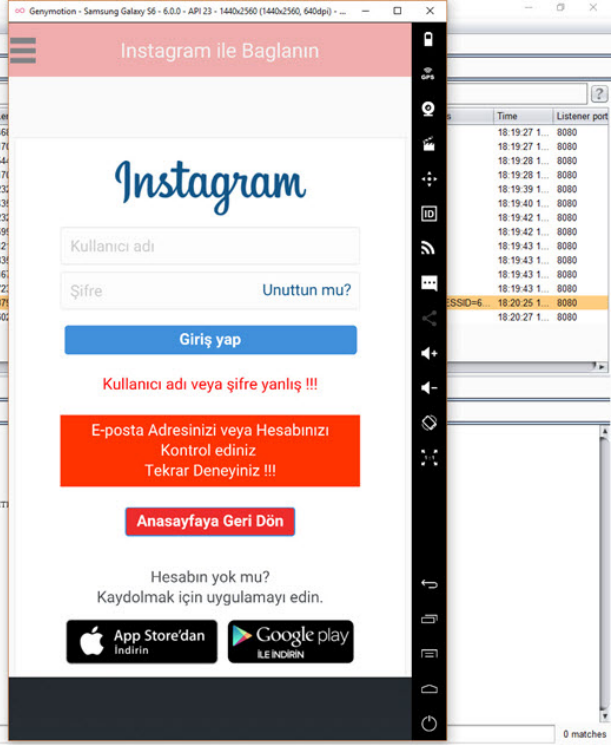
When I ran the application, I discovered that it was developed using Mobiroller, as there were requests being made to the URL <http://myapi.mobiroller.com> in the background. Upon further inspection of the outgoing requests, I was able to easily see the email addresses of the application developer.

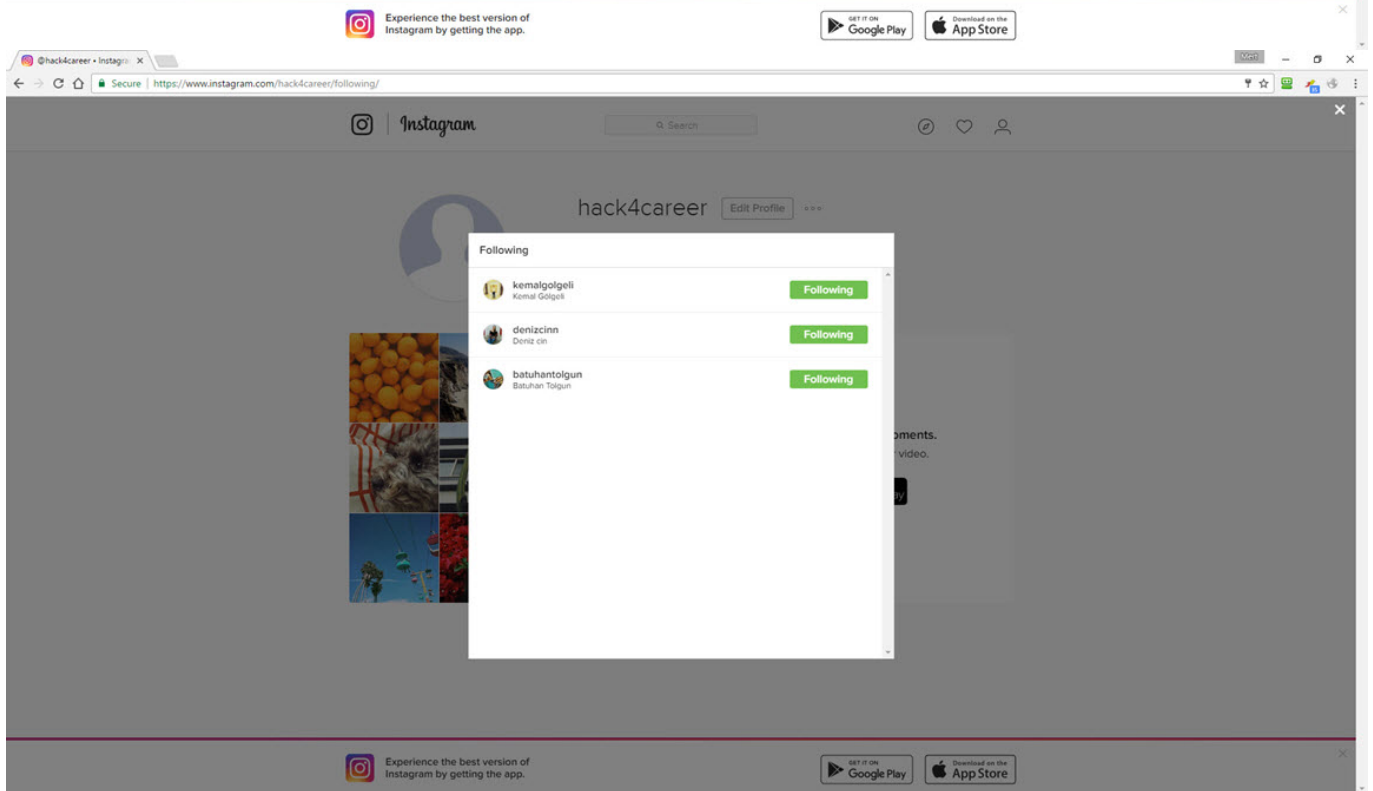
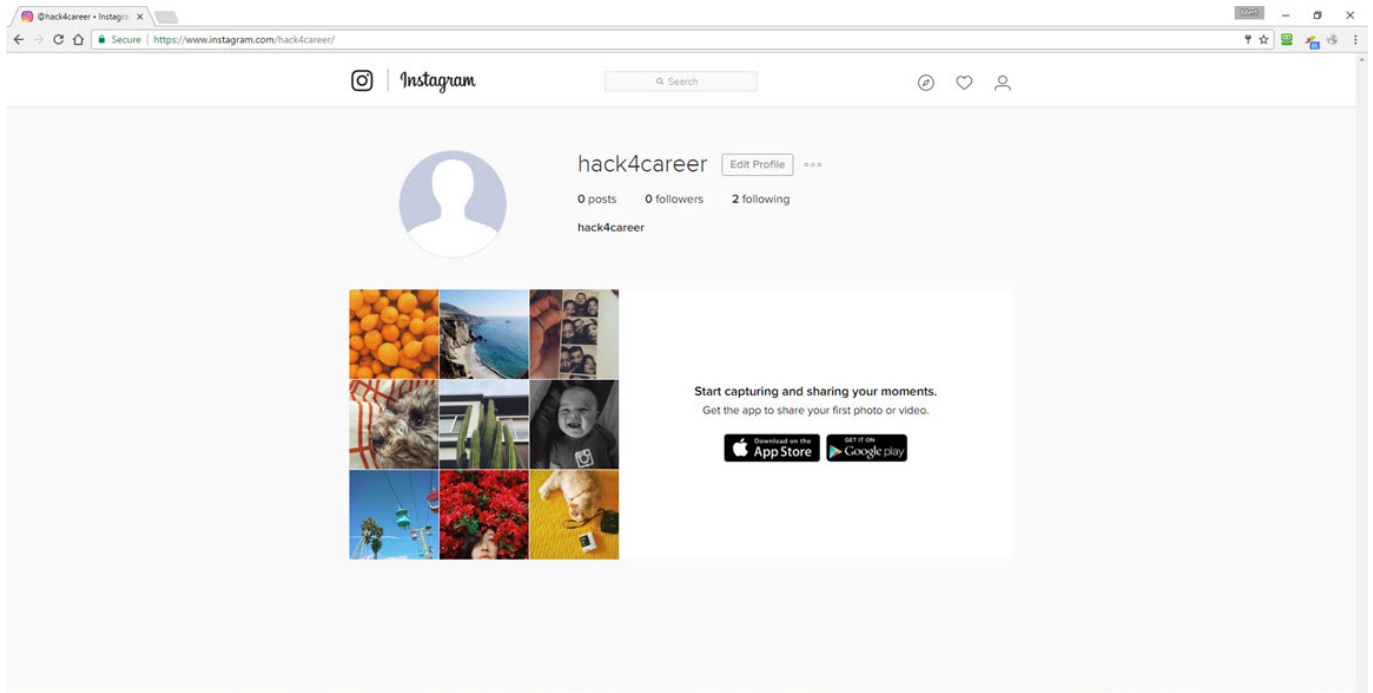


To understand the behavior of the “Takipçi Kazan” application, I first entered my incorrect Instagram password. From the error message “Username or password is incorrect!!!” it was clear that the application was capturing and instantly using the entered username and password on Instagram. After entering 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.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t.	Extension	Title
15	http://myapi.mobrollor.com	GET	/JSON/GetJSON?accountScreenID=aveNavigation_msf0600718_52353_0@gmail.com			200	468			
16	http://myapi.mobrollor.com	GET	/JSON/GetJSON?accountScreenID=msf0600718_52353_0@gmail.com			200	171			
17	http://myapi.mobrollor.com	GET	/JSON/GetJSON?accountScreenID=aveIntroMessage_msf0600718_52353_0@gmail.com			200	54			
18	http://myapi.mobrollor.com	GET	/JSON/GetJSON?accountScreenID=msf0600718_52353_0@gmail.com			200	171			
19	http://myapi.mobrollor.com	POST	/AveAnalytics/SessionStart			200	23			
20	http://myapi.mobrollor.com	GET	/JSON/GetJSON?accountScreenID=514015			200	438			
21	http://myapi.mobrollor.com	POST	/AveAnalytics/ScreenDisplay			200	23			
22	http://www.insfollow.com	GET	/sistemgirisi			200	598			
23	http://instagramatic-a.ak...	GET	/bluebar/a7a7e25/scripts/webfont.js			200	12			
24	http://ajax.googleapis.com	GET	/ajax/libs/jquery/2.0.0/jquery.min.js			200	838			
25	http://instagramatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js			200	16			
26	http://instagramatic-a.ak...	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	/sistemgirisi?error=hata			200	60			

#	Host	Method	URL	Params	Edited	Status	Length	MIME t.	Extension	Title
32	http://www.insfollow.com	POST	/login.php			302	36			
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/andless-skin.css			200	135472	CSS	css	
39	http://www.insfollow.com	GET	/css/sly.css			200	106509	CSS	css	
40	http://www.insfollow.com	GET	/css/sly-responsive.css			200	5818	CSS	css	
41	http://bc.vc	GET	/js/bvc_in.js			200	1846	script	js	
42	http://code.ionicframework...	GET	/ionicons/2.0.0/ionicons.min.css			200	51844	CSS	css	
43	http://www.insfollow.com	GET	/style/andless-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	





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 Inbox x

ihbar@usom.gov.tr 10:23 AM (6 hours ago) ☆ ↩
to me

Images are not displayed. [Display images below](#) - Always display images from ihbar@usom.gov.tr

Turkish > English [Translate message](#) [Turn off for Turkish](#) x

Sayın İlgili,
Konuyla ilgili #14343# ID'li ihbarınız tarafımıza ulaştığı olup konuyla ilgili çalışmalar başlatılmıştır.
Bilgilerinize,

Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Tel: [0312 536 53 05](tel:03125365305)
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.